$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$$

نظرية الأعداد وتطبيقاتها

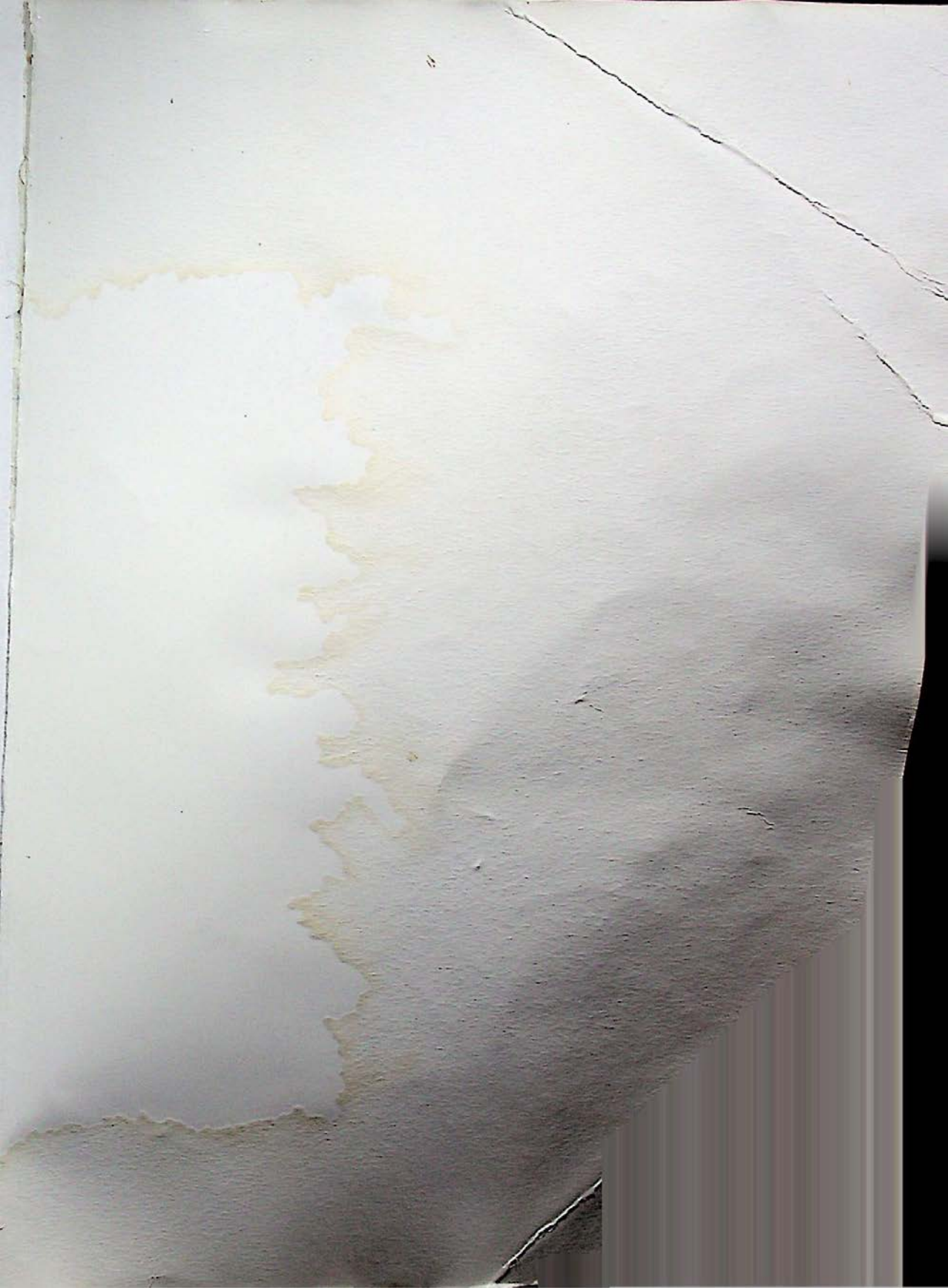
تأليف

الدكتور/معروف عبدالرحمن سمحان الدكتور/ فوزي أحمد الذكير

قسم الرياضيات - كلية العلوم

جامعة الملك سعود

الناشر دار الخريجي للنشر والتوزيع



نظريـــة الأعداد وتطبيقاتها

تأليـــف

الدكتور/ معروف عبد الرحمن سمحان الدكتور/ فوزي أحمد الذكير

قسم الرياضيات – كلية العلوم

جامعة الملك سعود

ⓒ دار الخريجي للنشر والتوزيع، ١٤٣١هـ
فهرسة مكتبة الملك فهد الوطنية أثناء النشر

سمحان، معروف عبدالرحمن
نظرية الأعداد وتطبيقاتها. / ؛معروف عبدالرحمن سمحان ؛
فوزي أحمد الذكير. - الرياض، ١٤٣١هـ
... ص ؛ ... سم
ردمك: ٨-١٨٤-٤٥-٩٩٦٠-٩٧٨

١- نظرية الأعداد ٢- الأرقام أ. فوزي أحمد (مؤلف مشارك) ب. العنوان

ديوي ٥١٣,٥ ١٤٣١/١٤٤٠

رقم الإيداع: ١٤٤٠/١٤٣١
ردمك: ٨-١٨٤-٤٥-٩٩٦٠-٩٧٨

تحذير
حقوق الطبع محفوظة للناشر، ولايجوز تصوير أو نشر أو اقتباس أي جزء من هذا الكتاب إلا بموافقة كتابيه من الناشر، وكل من يخالف ذلك يتعرض للمساءلة القانونية من جانب الناشر.

الناشر
دارالخريجي للنشروالتوزيع
AL-KHERAIJI
الرياض - العليا - طريق مكة المكرمة - المملكة العربية السعودية
تلفون: ٤٦٤٦٢٥٨ - ٤٦٤٤٣٨٤ - فاكس: ٤٦٤٩٩٢٨ ص. ب ١٧٧٣٢ - الرياض ١١٤٩٤
البريد الإلكتروني: alkheraijibooks@saudi.net.sa
قسم الجملة:
الديرة - شارع العطايف تليفون: ٢٨٦٨٨٧٤
جدة: شارع الأمير ماجد - تلفون: ٦٧٦٠٠٦٨ - ٦٧٠١٥٥٥ - ٦٧٠١٨٨٨
فاكس: ٦٧٦٠٠٥١ - ص. ب: ٥٠٦١٣ - جدة ٢١٥٣٣
البريد الإلكتروني: alkheraijibooks@saudi.net.sa

FNK

بسم الله الرحمن الرحيم

تم تأليف هذا الكتاب بدعم من مركز بحوث
كلية العلوم – جامعة الملك سعود
برقم (Math/2008/06/B)

مقدمة

إن اهتمام الإنسان بدراسة الأعداد يرجع إلى أقدم العصور وتشهد الآثار التي عُثرعليها على ما قام به البابليون وقدماء المصريين والهنود والصينيون في هذا المضمار. كما ساهم الإغريق في إثراء هذا العلم منذ إنشاء مدرسة فيثاغورس قبل ٢٥٠٠ عام. ومن أكبر إنجازاتهم ما قدّمه إقليدس الذي عاش في القرن الرابع قبل الميلاد، إذ كان أول من برهن على وجود عدد غير منته من الأعداد الأولية كما قدم طريقة حسابية لإيجاد القاسم المشترك الأعظم لعددين بالإضافة إلى نتائج أخرى ذكرها في كتبه الثلاثة عشر في الرياضيات (العناصر) . وبعد الإغريق جاء دور العرب والمسلمين في تطوير المعرفة الإنسانية بالأعداد، ويبدو هذا جلياً من خلال بعض المصطلحات التي ما زالت تستخدم إلى يومنا هذا، فكلمة (Algorithm) والتي تعني طريقة الحساب هي تحريف لكلمة خوارزم أو بالأحرى الخوارزمي وهو العالم الرياضي المعروف أبو عبدالله محمد بن موسى الخوارزمي (Alkwarezmi) الذي عاش في القرن الثالث الهجري. ولقد كان كتابه (الجبر والمقابلة) من أفضل كتب الرياضيات المؤلفة في ذلك العصر.

إن النظام العشري للأعداد الذي نستخدمه في عصرنا الحاضر هو نظام طوّره العرب والمسلمون بعد أن ابتدعه الهنود ولا يزال الغربيون يشيرون إلى رموز الأرقام العشرية 1, 2, 3, 4,. ... 8, 9 بالأرقام العربية (Arabic numerals) . ومن

العلماء العرب الذين أثروا المعرفة الإنسانية في مجال الأعداد العالم ثابت بن قرة الحراني الذي عاش في القرن الثالث الهجري من خلال دراسته للأعداد التامة وحصوله على صيغة لإيجاد أزواج من الأعداد المتحابة. ونذكر من العلماء أيضاً العالم الكرخي (الكرجي) صاحب كتاب "البديع في الحساب" وغياث الدين الكاشي الذي ألف كتاب "مفتاح الحساب" وشرح فيه طريقة التمثيل العشري، كما قرب قيمة ٢ ط (ضعف النسبة الثابتة) إلى ١٦ رقماً عشرياً. كذلك العالم نصير الدين الطوسي مؤلف كتاب "جوامع الحساب" بالإضافة إلى العديد من العلماء الذين نقلوا وترجموا عن الاغريق ثم أضافوا نتاجهم التي يمكن أن نلمس آثارها إلى وقتنا الحاضر.

إن قدم علم الأعداد لا يعني أنه علم جامد لا يواكب العصر، بل إن التقنيات الحديثة وخاصة الحاسوب أبرزت أهمية هذا العلم وتفاعلت معه. فالتقدم الهائل في علم الحاسوب (computer science) يبرز أهمية تعلم خواص الأعداد ودراستها. ومن ناحية أخرى ساهمت الحاسبات السريعة (super computers) في تقدم نظرية الأعداد من خلال التعرف على بعض خواصها وصياغة بعض الأحداس (conjecutures). وتعد نظرية التعمية (cryptology) من أبرز المواضيع التي أظهرت أهمية نظرية الأعداد في التقنية الحديثة فلطالما اعتبرت نظرية الأعداد من المواضيع الأكثر تجرداً والأكثر بعداً عن تطبيقات الحياة ولكن ظهور أنظمة التعمية الحديثة في السبعينيات من القرن العشرين أثبتت لنا أنه مهما طال الزمن أو قصر فإن الرياضيات التي توصف بالمجردة لا بد وأن تجد طريقاً عملياً للاستفادة منها وتطبيقها.

هذا الكتاب هو نسخة معدلّة كلياً على كتابنا "مقدمة في نظرية الأعـــداد" الذي كان الهدف الأساسي من كتابته هو تقديم مبادئ نظرية الأعداد بأسلوب لا يتطلب الكثير من المعرفة الرياضية المسبقة وذلك لكي نتمكن من تدريس نظريـــة الأعداد لطلاب السنة الثانية في قسم الرياضيات من مرحلة البكالوريوس. وأثنـــاء تدريسنا للكتاب المذكور تلقينا العديد من الملاحظات التي أوليناه عناية فائقة. ومن أهم هذه الملاحظات هو عدم إدراج بعض المواضيع المهمـــة في الكتـــاب وعـــدم التعرض إلى تطبيقات نظرية الأعداد مما شجعنا على الشروع في تأليف هذا الكتاب الذي يحتوي على مادة الكتاب السابق الذكر مع بعض التعديل عليهـــا وإضـــافة مواضيع جديدة هي الكسور المتواصلة، الجذور البدائيـــة، الرواســـب التربيعيـــة، وخصصنا فصلاً كاملاً (الفصل التاسع) لنظرية التعمية كتطبيق مهم على نظريـــة الأعداد. أما الفصل العاشر فإنه يحتوي على تطبيقات أخرى متفرقة لنظرية الأعداد.

نأمل أن نكون قد وفقنا في تقديم ومعالجة المادة العلمية لهذا الكتاب، كمـــا نرجو من القراء، أساتذة وطلاب أن يوافونا بملاحظاتهم التي لا غـــنى لنـــا عنـــها لتحسين مادة الكتاب في طباعته اللاحقة.

وفي الختام نقدم شكرنا وتقديرنا لزملائنا الذين قاموا بقراءة النسخة البدائية وأثرونا بملاحظاتهم وانتقاداتهم في معالجة المادة العلمية ونخص منهم الدكتور/ علي السحيباني ، الدكتور/ أحمد شراري، الدكتور/ محمد الزهيري، الدكتور/ صـــالح السنوسي وللأستاذ/ سمير كلوب الذي قام بتدريس حصص التمارين وزودنا بحلول العديد من تمارين الكتاب.

ولا يفوتنا أن نقدم الشكر الجزيل لمركز البحوث في كلية العلوم – جامعة الملك سعود على الدعم برقم (Math/2008/06/B) الذي قدمه للمؤلفين مما سهل عليهما انجاز هذا الكتاب.

والله من وراء القصد وهو الهادي إلى سواء السبيل.

المؤلفان

الرياض

١٤٣٠هـ (٢٠٠٩م)

المحتويات

الموضوع	رقم الصفحة
مقدمة	
الفصل الأول: الأعداد الصحيحة	
(١,١)مسلمات الأعداد الصحيحة	١
(١,٢)مبرهنة ذات الحدين	١٩
(١,٣)قابلية القسمة	٢٣
(١,٣,١) القاسم المشترك الأعظم	٢٧
(١,٣,٢) المضاعف المشترك الأصغر	٤٠
(١,٣,٣) تمارين محلولة	٤٢
(١,٤) المعادلات الديوفنتية الخطية	٤٩
(١,٤,١) تمارين محلولة	٥٦
(١,٥) تمثيل الأعداد الصحيحة	٦٥
(١,٥,١) تمارين محلولة	٦٨
نبذة عن حياة إقليدس الاسكندراني	٧٠
نبذة عن حياة الخوارزمي	٧١
نبذة عن حياة ديوفنتاس	٧٢
الفصل الثاني: الأعداد الأولية	
(٢,١) المبرهنة الأساسية في الحساب	٧٤
(٢,١,١) تمارين محلولة	٨٠
(٢,٢) توزيع الأعداد الأولية	٨٧

الموضوع	رقم الصفحة
(٢,٢,١) تمارين محلولة	٩٥
(٢,٣) أعداد فيرما وأعداد ميرسين	٩٨
(٢,٤) اختبار الأوليات والتحليل	١٠٦
(٢,٤,١) طريقة فيرما للتحليل	١١٤
(٢,٤,٢) طريقة أويلر للتحليل	١١٨
(٢,٤,٣) تمارين محلولة	١١٩
نبذة عن حياة آتلي سيلبرج	١٢٢
نبذة عن حياة جولدباخ	١٢٤
الفصل الثالث: التطابقات	
(٣,١) الخواص الأساسية للتطابقات	١٢٥
(٣,١,١) أنظمة الرواسب	١٣٧
(٣,١,٢) تمارين محلولة	١٤٣
(٣,٢) التطابقات الخطية	١٤٩
(٣,٢,١) التطابقات الخطية بمتغيرين	١٥٧
(٣,٢,٢) تمارين محلولة	١٦١
(٣,٣) أنظمة التطابقات الخطية بمتغير واحد	١٦٤
(٣,٣,١) تمارين محلولة	١٧٥
(٣,٤) أنظمة التطابقات الخطية في أكثر من متغير	١٨١
(٣,٥) بعض التطابقات الخاصة	١٨٩
(٣,٥,١) رتبة العدد	١٩٨
(٣,٥,٢) أشباه الأوليات	٢٠١
(٣,٥,٣) أعداد كارمايكل	٢٠٤
(٣,٥,٤) تمارين محلولة	٢٠٦

الموضوع	رقم الصفحة
(٣,٦) تطابقات كثيرات الحدود	٢١٧
(٣,٦,١) تمارين محلولة	٢٢٩
نبذة عن حياة جاوس	٢٣٥
نبذة عن حياة أويلر	٢٣٧
الفصل الرابع: معادلات ديوفنتية خاصة	
(٤,١) ثلاثيات فيثاغورس	٢٣٩
(٤,١,١) تمارين محلولة	٢٤٨
(٤,٢) مجموع المربعات	٢٥٢
(٤,٢,١) مجموع مربعين	٢٥٢
(٤,٢,٢) مجموع ثلاث مربعات	٢٦٢
(٤,٢,٣) مجموع أربع مربعات	٢٦٣
(٤,٢,٤) تمارين محلولة	٢٧١
(٤,٣) المعادلة الديوفنتية $x^4+y^4=z^4$	٢٧٦
(٤,٣,١) تمارين محلولة	٢٨٤
نبذة عن حياة فيرما	٢٨٩
نبذة عن حياة وايلز	٢٩١
الفصل الخامس: الدوال العددية	
(٥,١) الدوال الضربية	٢٩٣
(٥,١,١) تمارين محلولة	٣٠٢
(٥,٢) الأعداد التامة	٣٠٨
(٥,٢,١) تمارين محلولة	٣١٢
(٥,٣) صيغة موبياس للتعاكس	٣١٧
(٥,٣,١) تمارين محلولة	٣٢١

الموضوع	رقم الصفحة
(٥,٤) دالة أويلر	٣٢٥
(٥,٤,١) حل المعادلة $\varphi(x)=m$	٣٣٠
(٥,٤,٢) تمارين محلولة	٣٣٢
(٥,٥) ضرب دريشليه	٣٣٩
نبذة عن حياة ميرسين	٣٤٥
نبذة عن حياة ثابت بن قرة	٣٤٦
الفصل السادس: الكسور المتواصلة	
(٦,١) الكسور المتواصلة المنتهية	٣٤٩
(٦,١,١) تمارين محلولة	٣٥٨
(٦,٢) الكسور المتواصلة غير المنتهية	٣٦٢
(٦,٢,١) التقريب الكسري للأعداد غير الكسرية	٣٦٨
(٦,٢,٢) تمارين محلولة	٣٧٤
(٦,٣) الكسور المتواصلة الدورية	٣٨٠
(٦,٣,١) الكسور المتواصلة الدورية تماماً	٣٨٩
(٦,٣,٢) الكسر المتواصل للعدد $\sqrt{d}$	٣٩١
(٦,٣,٣) استخدام الكسور المتواصلة في التحليل	٣٩٥
(٦,٣,٤) تمارين محلولة	٣٩٨
(٦,٤) معادلة بيل	٤٠٢
(٦,٤,١) المعادلة $x^2-dy^2=-1$	٤٠٩
(٦,٤,٢) المعادلة $x^2-dy^2=N$	٤١٣
(٦,٤,٣) تمارين محلولة	٤١٦
نبذة عن حياة باسكارا	٤٢٤
نبذة عن حياة بيل	٤٢٦

الموضوع	رقم الصفحة
الفصل السابع: الجذور البدائية	
(٧,١) الجذور البدائية	٤٢٧
(٧,١,١) الجذور البدائية قياس 2^k	٤٣٢
(٧,١,٢) الجذور البدائية قياس p^k	٤٣٣
(٧,١,٣) الجذور البدائية قياس $2p^k$	٤٤٢
(٧,١,٤) الجذور البدائية قياس n	٤٤٣
(٧,١,٥) تمارين محلولة	٤٤٥
(٧,٢) اللوغاريتمات المنفصلة	٤٥٠
(٧,٢,١) تمارين محلولة	٤٥٦
(٧,٣) القوى الشاملة	٤٥٩
(٧,٣,١) تمارين محلولة	٤٦٢
نبذة عن حياة لاجرانج	٤٦٥
الفصل الثامن: الرواسب التربيعية	
(٨,١) التطابقات التربيعية	٤٦٧
(٨,١,١) تمارين محلولة	٤٧٢
(٨,٢) رمز ليجندر	٤٧٤
(٨,٢,١) تمارين محلولة	٤٨٠
(٨,٣) قانون التعاكس التربيعي	٤٨٢
(٨,٣,١) تمارين محلولة	٤٩٢
(٨,٤) الجذور التربيعية قياس عدد أولي	٤٩٩
(٨,٥) الجذور التربيعية قياس عدد مؤلف	٥٠٣
(٨,٥,١) تمارين محلولة	٥٠٨
(٨,٦) رمز جاكوبي	٥١٠

الموضوع	رقم الصفحة
(٨,٦,١) تمارين محلولة	٥١٩
نبذة عن حياة ليجندر	٥٢٣
نبذة عن حياة جاكوبي	٥٢٥
الفصل التاسع: علم التعمية	
(٩,١) أنظمة التعمية التقليدية	٥٢٧
(٩,١,١) نظام الإزاحة	٥٣١
(٩,١,٢) نظام التعويض	٥٣٣
(٩,١,٣) النظام التآلفي	٥٣٤
(٩,١,٤) نظام فيجنير	٥٣٥
(٩,١,٥) نظام هيل	٥٣٩
(٩,٢) تحليل التعمية	٥٤٣
(٩,٢,١) تحليل نظام الازاحة	٥٤٩
(٩,٢,٢) تحليل نظام التعويض	٥٥١
(٩,٢,٣) تحليل النظام التآلفي	٥٥٥
(٩,٢,٤) تحليل نظام فيجنير	٥٥٨
(٩,٢,٥) تحليل نظام هيل	٥٥٩
(٩,٣) أنظمة التعمية الحديثة	٥٦٧
(٩,٣,١) نظام القوة	٥٦٩
(٩,٣,٢) نظام RSA للتعمية	٥٧١
(٩,٣,٣) أمن نظام RSA	٥٧٨
(٩,٣,٤) نظام رابن للتعمية	٥٨١
(٩,٣,٥) خطة ديفي وهيلمان لتبادل المفاتيح	٥٨٥
نبذة عن حياة رون رايفست	٥٩٠

الموضوع	رقم الصفحة
الفصل العاشر : تطبيقات	
(١٠,١) المربعات السحرية	٥٩٣
(١٠,٢) الأعداد العشوائية	٦٠٨
(١٠,٣) جدل كوابل الهاتف	٦١٣
(١٠,٤) تطبيقات على صيغة موبياس للتعاكس	٦١٨
الجداول	٦٢٣
إجابات وإرشادات لتمارين مختارة	٦٤١
المراجع	٦٨٩
دليل الأسماء	٧٠٣
دليل الرموز	٧٠٩
كشاف وثبت المصطلحات	٧١٥

الفصل الأول

الأعداد الصحيحة
INTEGERS

(١,١) مسلمات الأعداد الصحيحة
Axioms of Integers

تبدأ الطريقة المتبعة في بناء الأعداد الصحيحة بتعريف الأعداد الطبيعية بوساطة مجموعة من المسلمات تدعى مسلمات بيانو (*Peano axioms*) ثم استخدام هذه المسلمات لبناء الأعداد الصحيحة وبرهان خواصها الأساسية. إلا أننا في هذا الكتاب ولتوفير الوقت سنفترض ابتداءاً وجود مجموعة الأعداد الصحيحة وأنها تحقق بعض المسلمات الأساسية ثم ننطلق بعدها لدراسة خواص هذه الأعداد اعتماداً على هذه المسلمات. القارئ المهتم بمعرفة كيفية إنشاء الأعداد الصحيحة من الأعداد الطبيعية مدعو للرجوع إلى [3].

بناءً على ذلك فإننا سنفترض وجود مجموعة من الأعداد تسمى مجموعة الأعداد الصحيحة ونرمز لها بالرمز $\mathbb{Z}=\{...,-3,-2,-1,0,1,2,3,...\}$ معرفاً عليها علاقة المساواة وعمليتي الجمع والضرب وتحقق المسلمات التالية لكل $a,b,c,d\in\mathbb{Z}$:

(١) $a+(b+c)=(a+b)+c$.

(٢) $a+b=b+a$.

(٣) يوجد عنصر وحيد $0 \in \mathbb{Z}$ يحقق: $a+0=a$.

(٤) لكل $a \in \mathbb{Z}$ يوجد عنصر وحيد $-a \in \mathbb{Z}$ يحقق: $a+(-a)=0$.

(٥) $a(bc)=(ab)c$.

(٦) $ab=ba$.

(٧) $a(b+c)=ab+ac$.

(٨) يوجد عنصر وحيد $1 \in \mathbb{Z}$ يحقق : $a.1=a$.

(٩) إذا كان $a=b$ و $c=d$ فإن $a+c=b+d$ وإن $ac=bd$.

(١٠) إذا كان $ac=bc$ وكان $c \neq 0$ فإن $a=b$.

ملحوظات

(١) يسمى النظام الرياضي الذي يحقق الخواص (١) إلى (٨) ، حلقة إبدالية بمحايد (انظر [3]) .

(٢) يسمى كل من العنصرين 0 و 1 المحايد الجمعي والمحايد الضربي على التوالي وهما وحيدان (انظر التمارين).

(٣) يسمى العنصر $-a$ بنظير a الجمعي وهو وحيد (انظر التمارين).

(٤) تسمى الخاصية (١٠) بقانون الاختصار.

نستخدم الآن مسلمات الأعداد الصحيحة لبرهان بعض الخواص الأساسية للأعداد الصحيحة.

مبرهنة (١,١)

ليكن $a,b,c \in \mathbb{Z}$. عندئذ:

(أ) إذا كان $a+b=a+c$ فإن $b=c$

(ب) $a.0=0$

(ج) $-(-a)=a$

(د) $(-a)b=a(-b)=-(ab)$

(هـ) $(-a)(-b)=ab$

(و) $-(a+b)=(-a)+(-b)$

برهان

(أ) لنفرض أن $a+b=a+c$. عندئذ:

$$\begin{aligned} a+b=a+c &\Rightarrow (-a)+(a+b)=(-a)+(a+c)\\ &\Rightarrow ((-a)+a)+b=((-a)+a)+c\\ &\Rightarrow 0+b=0+c\\ &\Rightarrow b=c \end{aligned}$$

(ب) لاحظ أن $a.0=a(0+0)=a.0+a.0$. ولكن $a.0=0+a.0$. ولذا باستخدام الفقرة (أ) نجد أن $a.0=0$.

(ج) لاحظ أن $0=a+(-a)$. ولذا من وحدانية النظير الجمعي نجد أن $-(-a)=a$.

(د) لاحظ أن $(ab)+(a(-b))=a(b+(-b))=a.0=0$. ومن وحدانية النظير الجمعي نجد أن $a(-b)=-(ab)$. وبالمثل $(-a)b=-(ab)$.

(هـ) يترك للقارئ.

(و)
$$\begin{aligned} ((-a)+(-b))+(a+b) &= (((-a)+(-b))+a)+b\\ &= ((-a)+((-b)+a))+b\\ &= ((-a)+(a+(-b)))+b\\ &= ((-a)+a)+((-b)+b)\\ &= 0+0=0 \end{aligned}$$

◆ ولذا باستخدام وحدانية النظير الجمعي نجد أن $(-a)+(-b)=-(a+b)$

نعرف الآن عملية الطرح على $\mathbb{Z}$.

تعريف (١,١)

إذا كان $a,b\in\mathbb{Z}$ فإننا نعرف $a-b=a+(-b)$.

لقد ذكرنا في بداية هذا الفصل أنه من الممكن إنشاء مجموعة الأعداد الصحيحة من مجموعة جزئية منها وهي الأعداد الطبيعية ويرمز لها عادة بالرمز $\mathbb{N}$

أو $\mathbb{Z}^+$ وهي المجموعة : $\mathbb{N}=\{1, 2, 3, ...\}$. سنفترض أن المسلمة التالية محققة للمجموعة $\mathbb{N}$.

مسلمة التثليث [*Trichotomy axiom*]

لكل $a\in\mathbb{Z}$ ، إما أن $a\in\mathbb{N}$ أو أن $a=0$ أو أن $-a\in\mathbb{N}$.

تبين لنا مسلمة التثليث أنه بإمكاننا تجزئة مجموعة الأعداد الصحيحة إلى ثلاث مجموعات منفصلة هي مجموعة الأعداد الصحيحة الموجبة ومجموعة الأعداد الصحيحة السالبة ومجموعة تحتوي على عنصر واحد فقط هو الصفر. ولذا فإننا نقول إن $a\in\mathbb{Z}$ عدد سالب إذا وفقط إذا كان $-a\in\mathbb{Z}^+$. نعرف الآن علاقة الترتيب $\leq$ على $\mathbb{Z}$.

تعريف (١,٢)

إذا كان $a,b\in\mathbb{Z}$ فإننا نقول إن a أصغر من أو يساوي b ونكتب $a\leq b$ إذا وفقط إذا كان $b-a\in\mathbb{Z}^+\cup\{0\}$. كما نقول إن a أصغر من b ونكتب $a<b$ إذا كان $b-a\in\mathbb{Z}^+$.

تتمتع علاقة الترتيب على $\mathbb{Z}$ بالخواص الأساسية التالية :

مبرهنة (١,٢)

(أ) العلاقة $\leq$ علاقة ترتيب كلي على $\mathbb{Z}$ ، أي أنها انعكاسية، متعدية، تخالفية، ولكل $a,b\in\mathbb{Z}$ إما أن $a\leq b$ أو أن $b\leq a$.

(ب) إذا كان $a<b$ وكان $c<d$ فإن $a+c<b+d$.

(ج) إذا كان $c<d$ وكان $a\in\mathbb{Z}^+$ فإن $ac<ad$.

(د) إذا كان $a\geq b\geq 0$ وكان $c\geq d\geq 0$ فإن $ac\geq bd$.

برهان

سنبرهن الفقرات (ب) و (ج) و (د) ونترك الفقرة (أ) كتمرين للقارئ.

(ب) إذا كان $a<b$ و $c<d$ فإن $b-a\in\mathbb{Z}^+$ وأن $d-c\in\mathbb{Z}^+$. ولذا فإن $(b+d)-(a+c)=(b-a)+(d-c)\in\mathbb{Z}^+$. ومنه فإن $a+c<b+d$.

(ج) بما أن $c<d$ فإن $d-c\in\mathbb{Z}^+$. وبما أن $a\in\mathbb{Z}^+$ فإن:
$a(d-c)=ad-ac\in\mathbb{Z}^+$. ولذا فإن $ac<ad$.

(د) بما أن $a\geq b\geq 0$ فإن $ac\geq bc$. وبما أن $c\geq d\geq 0$ فإن $bc\geq bd$.
وباستخدام الفقرة (أ) نجد أن $ac\geq bd$ ◆

نقدم الآن مسلمة الاستقراء الرياضي على مجموعة الأعداد الصحيحة غير السالبة حيث تعد هذه المسلمة من أهم طرائق البرهان المستخدمة لإثبات صواب تقارير مجالها مجموعة الأعداد الصحيحة غير السالبة أو مجموعة جزئية منها.

المبدأ الأول للاستقراء الرياضي [*First principle of mathematical induction*]

لتكن $P(n)$ جملة مفتوحة مجالها مجموعة الأعداد الصحيحة غير السالبة.
لنفرض أن :

(أ) $P(0)$ تقرير صائب.

(ب) لكل $k\geq 0$ كلما كان $P(k)$ تقريراً صائباً يكون $P(k+1)$ تقريراً صائباً.

عندئذ، $P(n)$ تقرير صائب لكل $n\geq 0$.

ملحوظات

(١) تسمى الخطوة (أ)، الخطوة الأساسية للاستقراء والخطوة (ب) تدعى خطوة الاستقراء . وأما المقدمة $P(k)$ في خطوة الاستقراء فإنها تدعى فرضية الاستقراء. والعدد n يسمى متغير الاستقراء.

(٢) في حالات كثيرة يستخدم الاستقراء الرياضي لإثبات صواب التقرير $P(n)$ لكل $n\geq n_0$ حيث $n_0\geq 0$. في هذه الحالة يكفي أن نثبت:

(أ) $P(n_0)$ تقرير صائب.

(ب) إذا كان $P(k)$ تقريراً صائباً فإن $P(k+1)$ تقرير صائب حيث $k \geq n_0$. لاحظ أن هذا ما هو إلا المبدأ الأول للاستقراء الرياضي على الجملة المفتوحة $Q(n) = P(n+n_0)$ لأن $Q(0) = P(n_0)$ وأن $k \geq n_0$ إذا وفقط إذا كان $k - n_0 \geq 0$.

(٣) لاحظ أنه لإثبات صواب التقرير $P(n)$ لكل $n \geq n_0$ باستخدام الاستقراء الرياضي فإن الخطوة الأساسية تضمن لنا صواب التقرير $P(n_0)$. وباستخدام خطوة الاستقراء عندما $k = n_0$ فإننا نحصل على صواب التقرير $P(n_0+1)$. الآن نطبق خطوة الاستقراء مرة أخرى عندما يكون $k = n_0 + 1$ لنحصل على صواب التقرير $P(n_0+2)$ وهكذا. أي أن خطوة الاستقراء تضمن لنا الوصول إلى الخطوة التالية مباشرة لخطوة سبق وأن وصلنا إليها وأما الخطوة الأساسية فتضمن لنا صواب الخطوة الأولى التي تعد نقطة البداية.

(٤) في العديد من البراهين نستخدم رمزي الجمع $\sum$ والضرب $\prod$ ليعنيا:

$$\sum_{i=k}^{n} f(i) = f(k) + f(k+1) + \ldots + f(n)$$

$$\prod_{i=k}^{n} f(i) = f(k) f(k+1) \ \ldots \ f(n)$$

نقدم الآن بعض الأمثلة على الاستقراء الرياضي.

مثال (١,١)

أثبت أن $\sum_{i=1}^{n} i^3 = \frac{1}{4} n^2 (n+1)^2$ لكل $n \geq 1$.

الحل

لنفرض أن $P(n)$ هي الجملة المفتوحة: $\sum_{i=1}^{n} i^3 = \frac{1}{4} n^2 (n+1)^2$.

(أ) بما أن $\sum_{i=1}^{1} i^3 = 1^3 = 1$ وأن $\frac{1}{4}\times 1^2 \times 2^2 = 1$ فإن $P(1)$ تقرير صائب.

(ب) لنفرض الآن أن $P(k)$ تقرير صائب حيث $k \geq 1$. أي أن: $\sum_{i=1}^{k} i^3 = \frac{1}{4}k^2(k+1)^2$. الآن:

$$\begin{aligned}\sum_{i=1}^{k+1} i^3 &= \sum_{i=1}^{k} i^3 + (k+1)^3 \\ &= \frac{1}{4}k^2(k+1)^2 + (k+1)^3 \qquad \text{(فرضية الاستقراء)} \\ &= \frac{1}{4}(k+1)^2(k^2+4k+4) \\ &= \frac{1}{4}(k+1)^2(k+2)^2\end{aligned}$$

ولذا فإن $P(k+1)$ تقرير صائب ونستنتج أن $P(n)$ تقرير صائب لكل $n \geq 1$ □

مثال(١,٢)

أثبت أن $3^n > 2^n + n$ لكل $n \geq 2$.

الحل

لنفرض أن $P(n)$ هي الجملة المفتوحة: $3^n > 2^n + n$.

(أ) بما أن $2^2 + 2 = 6$ وأن $3^2 = 9$ فإن $3^2 > 2^2 + 2$ ويكون $P(2)$ تقرير صائب.

(ب) نفرض أن $k \geq 2$ وأن $P(k)$ تقرير صائب. أي أن $3^k > 2^k + k$. الآن:

$$\begin{aligned}3^{k+1} &= 3\times 3^k \quad > 3(2^k + k) \qquad \text{(فرضية الاستقراء)} \\ &= 3\times 2^k + 3k \quad > 2\times 2^k + k + 1 \qquad (k \geq 2 \text{ لأن}) \\ &= 2^{k+1} + k + 1\end{aligned}$$

إذن، $P(k+1)$ تقرير صائب ونخلص إلى أن $P(n)$ تقرير صائب لكل $n \geq 2$ □

مثال (١,٣)

أثبت أن $\prod_{i=2}^{n}(1-1/i^2)=\frac{n+1}{2n}$ لكل $n\geq 2$.

الحل

لنفرض أن $P(n)$ هي: $\prod_{i=2}^{n}(1-1/i^2)=\frac{n+1}{2n}$.

(أ) بما أن $\prod_{i=2}^{2}(1-1/i^2)=\frac{3}{4}$ وأن $\frac{2+1}{2\times 2}=\frac{3}{4}$ فإن $P(2)$ تقرير صائب.

(ب) لنفرض أن $P(k)$ تقرير صائب حيث $k\geq 2$. أي $\prod_{i=2}^{k}(1-1/i^2)=\frac{k+1}{2k}$.

الآن:

$$\prod_{i=2}^{k+1}(1-1/i^2)=\prod_{i=2}^{k}(1-1/i^2)\times(1-1/(k+1)^2)$$

$$=\frac{k+1}{2k}\times(1-1/(k+1)^2) \qquad \text{(فرضية الاستقراء)}$$

$$=\frac{k+1}{2k}\times\frac{(k+1)^2-1}{(k+1)^2}$$

$$=\frac{(k+1)(k^2+2k+1-1)}{2k(k+1)^2}$$

$$=\frac{k(k+1)(k+2)}{2k(k+1)^2}$$

$$=\frac{k+2}{2(k+1)}$$

إذن، $P(k+1)$ تقرير صائب وينتج عن ذلك أن $P(n)$ تقرير صائب لكل $n\geq 2$ □

مثال (١,٤)

أثبت أن $n!>3^n$ لكل $n\geq 7$.

الحل

لنفرض أن $P(n)$ هي: $n!>3^n$.

(أ) لاحظ أن $7!=5040$ و $3^7=2187$. ولذا فإن $7!>3^7$ ويكون $P(7)$ تقرير صائب.

(ب) لنفرض أن $P(k)$ تقرير صائب حيث $k\geq 7$. أي أن $k!>3^k$. الآن:

$$(k+1)!=(k+1)k! \quad >(k+1)3^k \qquad \text{(فرضية الاستقراء)}$$
$$>3\times 3^k \quad =3^{k+1} \qquad (\text{لأن } k\geq 7)$$

إذن، $P(k+1)$ تقرير صائب ونخلص إلى أن $P(n)$ تقرير صائب لكل $n\geq 7$ □

التعريف الاستقرائي [*Inductive definition*]

لنفرض أننا نريد تعريف متتالية $\{a_n\}$. ولنفرض أيضاً أن $a_1, a_2, \ldots, a_t$ معلومة حيث $t\geq 1$ وأنه يمكن إيجاد a_{n+1} بدلالة a_n لكل $n\geq t$. عندئذ، باستخدام الاستقراء الرياضي على n نستطيع وبسهولة أن نبرهن أن a_n معرف لكل $n\geq 1$. مثل هذا التعريف للمتتالية $\{a_n\}$ يسمى التعريف الاستقرائي.

مثال(١,٥)

لتكن $\{a_n\}$ هي المتتالية المعرفة استقرائياً كالتالي:

(أ) $a_0=1$ (ب) $a_{n+1}=2a_n$ لكل $n\geq 0$.

استخدم الاستقراء الرياضي لإثبات أن $a_n=2^n$ لكل $n\geq 0$.

الحل

لنفرض أن $P(n)$ هي: $a_n=2^n$.

(أ) بما أن $a_0=2^0=1$ فإن $P(0)$ صائب.

(ب) لنفرض أن $P(k)$ صائب حيث $k\geq 0$. أي $a_k=2^k$. الآن:

$$a_{k+1}=2a_k \quad =2\times 2^k \qquad \text{(فرضية الاستقراء)}$$
$$=2^{k+1}$$

إذن، $P(k+1)$ صائب وينتج عن ذلك أن $a_n=2^n$ لكل $n\geq 0$ □

مثال (١,٦)

لتكن $\{b_n\}$ هي المتتالية المعرفة استقرائياً كالتالي:

(أ) $b_0 = 1$ (ب) $b_{n+1} = (n+1)b_n$ لكل $n \geq 0$.

أثبت باستخدام الاستقراء الرياضي أن $b_n = n!$ لكل $n \geq 0$.

الحل

لنفرض أن $P(n)$ هي الجملة المفتوحة $b_n = n!$.

(أ) بما أن $b_0 = 0! = 1$ فإن $P(0)$ تقرير صائب.

(ب) نفرض أن $P(k)$ تقرير صائب حيث $k \geq 0$. أي أن $b_k = k!$. الآن:

$$b_{k+1} = (k+1)b_k = (k+1)k! \quad \text{(فرضية الاستقراء)}$$

$$= (k+1)! \quad \text{(تعريف)}$$

إذن، $P(k+1)$ تقرير صائب ونخلص إلى أن $b_n = n!$ لكل $n \geq 0$ □

المبدأ الثاني للاستقراء الرياضي [*Second principle of mathematical induction*]

لقد لاحظنا في جميع الأمثلة المقدمة على الاستقراء الرياضي أن برهان خطوة الاستقراء اعتمد فقط على صواب الخطوة السابقة لها. في بعض الحالات يكون من الضروري الاعتماد على صواب خطوتين سابقتين فأكثر. إن هذا ممكن وتكـــون خطوات الاستقراء على النحو التالي:

(أ) $P(0)$ تقرير صائب.

(ب) إذا كانت $P(0)$ ، $P(1)$ ، ... ، $P(k)$ جميعها تقارير صائبة حيث $k \geq 0$ فإن $P(k+1)$ تقرير صائب.

يسمى هذا الاستقراء ، المبدأ الثاني للاستقراء الرياضي وهو مكافئ للمبـــدأ الأول للاستقراء الرياضي. نوضح ذلك ببعض الأمثلة.

مثال (١,٧)

تعرف متتالية فيبوناتشي *(Fibonacci sequence)* $\{f_n\}$ استقرائياً كالتالي:

(أ) $f_1 = f_2 = 1$ (ب) $f_{n+1} = f_n + f_{n-1}$ لكل $n \geq 2$.

أثبت أن $f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$ لكل $n \geq 1$.

الحل

باستخدام المبدأ الثاني للاستقراء الرياضي على n. نفرض أن $P(n)$ هي:

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

(أ) بما أن $\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)\right] = 1$ وأن $f_1 = 1$ فإن $p(1)$ تقرير صائب.

كذلك $\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right] = 1$ وأن $f_2 = 1$ فإن $p(2)$ تقرير صائب أيضاً.

(ب) نفرض الآن أن $P(1)$ ، $P(2)$ ، ... ، $P(k)$ جميعها تقارير صائبة حيث $k \geq 1$. الآن:

(تعريف) $f_{k+1} = f_k + f_{k-1}$

(فرضية الاستقراء) $= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right] + \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right]$

$$= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\left(\frac{3+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left(\frac{3-\sqrt{5}}{2}\right)\right]$$

$$= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left(\frac{1-\sqrt{5}}{2}\right)^2\right]$$

$$= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right]$$

إذن، $P(k+1)$ تقرير صائب ويكون $P(n)$ صائب لكل $n \geq 1$ □

مثال (١,٨)

تعرف متتالية لوقا (*Lucas sequence*) $\{b_n\}$ استقرائياً كالتالي:

(أ) $b_1 = 1 , b_2 = 3$ (ب) $b_{n+1} = b_n + b_{n-1}$ لكل $n \geq 2$.

أثبت أن $f_n + b_n = 2f_{n+1}$ لكل $n \geq 1$ حيث $\{f_n\}$ هي متتالية فيبوناتشي.

الحل

باستخدام المبدأ الثاني للاستقراء الرياضي على n.

نفرض أن $P(n)$ هي: $f_n + b_n = 2f_{n+1}$.

(أ) بما أن $f_1 + b_1 = 2$ وأن $2f_2 = 2$ فإن $P(1)$ تقرير صائب. كذلك، $f_2 + b_2 = 4$ و $2f_3 = 4$. ولذا فإن $p(2)$ تقرير صائب أيضاً.

(ب) لنفرض أن $P(1)$ ، $P(2)$ ، ... ، $P(k)$ تقارير صائبة حيث $k \geq 1$. الآن:

$$f_{k+1} + b_{k+1} = (f_k + f_{k-1}) + (b_k + b_{k-1}) \quad \text{(تعريف)}$$

$$= (f_k + b_k) + (f_{k-1} + b_{k-1})$$

$$= 2f_{k+1} + 2f_k \quad \text{(فرضية الاستقراء)}$$

$$= 2f_{k+2} \quad \text{(تعريف)}$$

إذن، $P(k+1)$ تقرير صائب ونخلص إلى أن $P(n)$ تقرير صائب لكل $n \geq 1$ □

ننهي هذا البند بتقديم مبدأ هام آخر يكافئ مبدأ الاستقراء الرياضي نستخدمه أحياناً كبديل عن الاستقراء الرياضي لبرهان صحة بعض تقارير الأعداد الصحيحة غير السالبة. ولكن قبل ذلك نحتاج إلى التعريف التالي:

تعريف (١,٣)

لتكن $A \subseteq \mathbb{Z}$ وليكن $a \in A$. نقول إن a عنصر أصغري (*least element*) للمجموعة A إذا كان $a \leq b$ لكل $b \in A$.

مبدأ الترتيب الحسن [*Well-ordering principle*]

إذا كانت $\phi \neq A \subseteq \mathbb{Z}$ و A محدودة من الأسفل فإن A تحتوي على عنصر أصغري.

ملحوظات

(١) العنصر الأصغري في المجموعة A (إن وجد) يجب أن يكون وحيداً. لأنه لو كان كل من a_1 و a_2 أصغرياً فإن $a_1 \leq a_2$ و $a_2 \leq a_1$. ولذا فإن $a_1 = a_2$.

(٢) لنفرض أننا بصدد إثبات صحة التقرير $(\forall n \in \mathbb{N})(P(n))$ باستخدام مبدأ الترتيب الحسن عوضاً عن مبدأ الاستقراء الرياضي. في هذه الحالة نقوم بأخذ المجموعة S من الأعداد الطبيعية بحيث يكون التقرير خاطئاً ونبرهن أن $S = \phi$. وللوصول إلى ذلك يكفي أن نبرهن أن S لا تحتوي على عنصر أصغري. أو بصورة مكافئة نطبق مبدأ الترتيب الحسن على المجموعة S (باعتبار أن $S \neq \phi$) ونبرهن إمكانية الحصول على تناقض.

مثال(١,٩)

استخدم مبدأ الترتيب الحسن لإثبات صحة التقرير:

$$(\forall n \in \mathbb{Z}^+)(2^{n+1} < 1 + (n+1)2^n)$$

الحل

نفرض أن التقرير خاطئ ونفرض أن:

$$S = \{n \in \mathbb{Z}^+ : 2^{n+1} \geq 1 + (n+1)2^n\}.$$

لاحظ أن $S \neq \phi$ (لماذا ؟) . ولذا باستخدام مبدأ الترتيب الحسن يوجد عنصر أصغري $k \in S$. ومنه فإن $k-1 \notin S$. ولذا يكون لدينا:

$$2^{k+1} \geq 1+(k+1)2^k \qquad (١)$$

$$2^k < 1+k2^{k-1} \qquad (٢)$$

بضرب المتباينة (٢) بالعدد 2 نحصل على:

$$2^{k+1} < 2+k\,2^k \qquad (٣)$$

من المتباينتين (١) و (٣) نحصل على:

$$2+k\,2^k > 1+(k+1)2^k .$$

ولذا فإن $1 > 2^k$ وهذا تناقض لأن $k \geq 1$. إذن، $S = \phi$. وبالتالي فإن التقرير صائب □

المبرهنة التالية تبين تكافؤ مبدأ الترتيب الحسن ومبدأ الاستقراء الرياضي.

مبرهنة (١,٣)

العبارات التالية متكافئة:

(أ) المبدأ الثاني للاستقراء الرياضي.

(ب) المبدأ الأول للاستقراء الرياضي.

(ج) مبدأ الترتيب الحسن.

البرهان

انظر [3] ◆

تمارين (١,١)

استخدم مبدأ الاستقراء الرياضي لإثبات صحة كل من العبارات في التمارين من (١) إلى (٢٥):

(١) $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ لكل $n \geq 1$.

(٢) $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ لكل $n \geq 1$.

(٣) $\sum_{k=1}^{n} (3k-2) = \frac{n(3n-1)}{2}$ لكل $n \geq 1$.

(٤) $\sum_{k=1}^{n} (2k-1)^2 = \frac{n(2n-1)(2n+1)}{3}$ لكل $n \geq 1$.

(٥) $\sum_{k=1}^{n} (2k+1)^3 = n(2n^3+8n^2+11n+6)$ لكل $n \geq 1$.

(٦) $\sum_{k=1}^{n} k(k+1)(k+2) = \frac{n(n+1)(n+2)(n+3)}{4}$ لكل $n \geq 1$.

(٧) $2^n > n^2 + 19$ لكل $n \geq 6$.

(٨) $\sum_{k=0}^{n} (2^k + 3^k) = 2^{n+1} + \frac{3^{n+1}}{2} - \frac{3}{2}$ لكل $n \geq 0$.

(٩) $\sum_{k=1}^{n} k\,(k!) = (n+1)! - 1$ لكل $n \geq 1$.

(١٠) $2^n < n!$ لكل $n \geq 4$.

(١١) $n^2 < n!$ لكل $n \geq 4$.

(١٢) $n^2 < 2^n$ لكل $n \geq 5$.

(١٣) $n < 2^n$ لكل $n \geq 0$.

(١٤) $n! < 2^{n^2}$ لكل $n \geq 1$.

(١٥) $\sum_{k=1}^{n} k! < (n+1)!$ لكل $n \geq 1$.

(١٦) $\sum_{k=1}^{n} \frac{1}{\sqrt{k}} > \sqrt{n}$ لكل $n \geq 2$.

(١٧) $\left(\sum_{k=1}^{n} k\right)\left(\sum_{k=1}^{n} \frac{1}{k}\right) \geq n^2$ لكل $n \geq 1$.

(١٨) $\sum_{k=1}^{n}\frac{1}{n+k}>\frac{13}{24}$ لكل $n\geq 2$.

(١٩) $\prod_{k=1}^{n}(1+a_k)\geq 1+\sum_{k=1}^{n}a_k$ حيث $a_k\in\mathbb{R}^+$ لكل $n\geq 1$.

(٢٠) $\prod_{k=1}^{n}(1-a_k)\geq 1-\sum_{k=1}^{n}a_k$ حيث $0<a_k<1$ لكل $n\geq 1$.

(٢١) إذا كان $a,r\in\mathbb{R}$ حيث $r\neq 1$ فأثبت أن $\sum_{k=0}^{n}ar^k=\frac{ar^{n+1}-a}{r-1}$ لكل $n\geq 1$.

(٢٢) $(ab)^n=a^nb^n$ حيث $a,b\in\mathbb{R}$ لكل $n\geq 1$.

(٢٣) $a^{mn}=(a^m)^n$ حيث $a\in\mathbb{R}$ لكل $m,n\geq 1$.

(٢٤) $\frac{4^n}{n+1}<\frac{(2n)!}{(n!)^2}$ لكل $n\geq 2$.

(٢٥) $(1+a)^n\geq 1+na$ حيث $a\in\mathbb{R}^+$ لكل $n\geq 0$.

في التمارين من (٢٦) إلى (٣٠) كل من المتتاليات المبينة $\{a_n\}$ معرفة استقرائياً. استخدم الاستقراء الرياضي لإثبات صواب الصيغة المطلوبة.

(٢٦) $a_0=1$ و $a_{n+1}=2(n+1)a_n$. أثبت أن $a_n=2^n n!$ لكل $n\geq 0$.

(٢٧) $a_0=1$ و $a_{n+1}=a_n+2^{n+1}$. أثبت أن $a_n=2^{n+1}-1$ لكل $n\geq 0$.

(٢٨) $a_0=1$ و $a_{n+1}=3a_n$. أثبت أن $a_n=3^n$ لكل $n\geq 0$.

(٢٩) $a_0=1$ ، $a_1=3$ و $a_{n+1}=4a_n-4a_{n-1}$. أثبت أن $a_n=2^n+n2^{n-1}$ لكل $n\geq 0$.

(٣٠) $a_0=0$ ، $a_1=4$ و $a_{n+1}=-2a_n+3a_{n-1}$. أثبت أن $a_n=1-(-3)^n$ لكل $n\geq 0$.

في التمارين من (٣١) إلى (٥٠) ، $\{f_n\}$ متتالية فيبوناتشي المعرفة على النحو التالي: $f_1=f_2=1$ و $f_{n+1}=f_n+f_{n-1}$ و $\{b_n\}$ متتالية لوقا المعرفة على النحو التالي: $b_1=1$ ، $b_2=3$ و $b_{n+1}=b_n+b_{n-1}$. استخدم الاستقراء الرياضي لإثبات صحة كل من العبارات المبينة:

(٣١) $f_n\leq f_{n+1}$ لكل $n\geq 1$.

(٣٢) $f_n + 2f_{n+1} = f_{n+3}$ لكل $n \geq 1$.

(٣٣) $f_{n+4} = 3f_{n+2} - f_n$ لكل $n \geq 1$.

(٣٤) $f_{n+6} = 4f_{n+3} + f_n$ لكل $n \geq 1$.

(٣٥) $\sum_{k=1}^{n} b_k = b_{n+2} - 3$ لكل $n \geq 1$.

(٣٦) $\sum_{k=1}^{n} f_k = f_{n+2} - 1$ لكل $n \geq 1$.

(٣٧) $\sum_{k=1}^{n} b_{2k} = b_{2n+1} - 1$ لكل $n \geq 1$.

(٣٨) $\sum_{k=1}^{n} f_{2k} = f_{2n+1} - 1$ لكل $n \geq 1$.

(٣٩) $\sum_{k=1}^{n} b_{2k-1} = b_{2n} - 2$ لكل $n \geq 1$.

(٤٠) $\sum_{k=1}^{n} f_{2k-1} = f_{2n}$ لكل $n \geq 1$.

(٤١) $\sum_{k=1}^{n} (f_k)^2 = f_n f_{n+1}$ لكل $n \geq 1$.

(٤٢) $b_n < 2^n$ لكل $n \geq 1$.

(٤٣) $f_n < 2^n$ لكل $n \geq 1$.

(٤٤) $f_{n-1} f_{n+1} - (f_n)^2 = (-1)^n$ لكل $n \geq 2$.

(٤٥) $b_{n-1} b_{n+1} - (b_n)^2 = 5(-1)^{n-1}$ لكل $n \geq 2$.

(٤٦) $1.614 < \frac{f_{n+1}}{f_n} < 1.620$ لكل $n \geq 7$.

(٤٧) $1.6169 < \frac{b_{n+1}}{b_n} < 1.621$ لكل $n \geq 7$.

(٤٨) $b_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n$ لكل $n \geq 1$.

(٤٩) $f_m f_n + f_{m+1} f_{n+1} = f_{m+n+1}$ لكل $n, m \geq 1$.

(٥٠) $f_n b_m + f_{n+1} b_{m+1} = b_{m+n+1}$ لكل $n, m \geq 1$.

(٥١) لتكن $\{a_n\}$ المتتالية المعرفة استقرائياً على النحو التالي: $a_1 = \sqrt{2}$ و $a_{n+1} = \sqrt{2 + a_n}$ لكل $n \geq 1$. أثبت أن:

(أ) $a_n < 2$ لكل $n \geq 1$ (ب) a_n عدد غير كسري لكل $n \geq 1$

(ج) $a_n < a_{n+1}$ لكل $n \geq 1$ (د) $\lim_{n\to\infty} a_n = 2$

(٥٢) إذا كانت $\{a_n\}$ متتالية معرفة كالتالي: $a_1 = a_2 = a_3 = 1$ و $a_{n+2} = a_{n+1} + a_n + a_{n-1}$ لكل $n \geq 2$. أثبت أن:

(أ) a_n عدد فردي لكل $n \geq 1$ (ب) $a_{n+1} \leq 2^n$ لكل $n \geq 0$

(ج) $a_{n+2} \geq 2a_n$ لكل $n \geq 2$ (د) $a_{n+2} \geq \left(\sqrt{2}\right)^n$ لكل $n \geq 2$

(٥٣) إذا كانت $\{a_n\}$ متتالية معرفة كالتالي: $a_1 = 1$ ، $a_2 = 5$ و $a_{n+1} = 2a_n + 3a_{n-1}$ لكل $n \geq 2$ فأثبت أن $3^n \leq a_{n+1} \leq 2 \times 3^n$ لكل $n \geq 1$.

(٥٤) لتكن $\{a_n\}$ متتالية معرفة على النحو التالي: $a_1 = 1$ و $a_{n+1} = \frac{1}{1+a_n}$ لكل $n \geq 1$. أثبت أن:

(أ) $a_n = \frac{f_n}{f_{n+1}}$ لكل $n \geq 1$ حيث $\{f_n\}$ هي متتالية فيبوناتشي.

(ب) على فرض أن للمتتالية نهاية أثبت أن $\lim_{n\to\infty} a_n = \frac{\sqrt{5}-1}{2}$.

(٥٥) إذا كانت $M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ فأثبت أن $M^n = \begin{bmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{bmatrix}$ لكل $n \geq 2$ حيث $\{f_n\}$ هي متتالية فيبوناشي.

(٥٦) استخدم مبدأ الترتيب الحسن لإثبات أنه لا يوجد $a \in \mathbb{Z}^+$ حيث $0 < a < 1$.

(٥٧) استخدم مبدأ الترتيب الحسن لإثبات أنه إذا كان $a, b \in \mathbb{Z}^+$ فإنه يوجد $n \in \mathbb{Z}^+$ حيث $na \geq b$.

(٥٨) استخدم مبدأ الترتيب الحسن لإثبات صحة العبارات المقدمة في التمارين (٧)، (١٠)، (١١) ، (١٢)، (١٣)، (١٤)، (٢٤).

(١,٢) مبرهنة ذات الحدين
Binomial Theorem

تعد مبرهنة ذات الحدين إحدى المبرهنات الأساسية المستخدمة في نظرية الأعداد إضافة إلى مواضيع أخرى في علم الرياضيات . سنفرد هذا البند القصير لإثبات هذه المبرهنة.

تعريف (١,٤)

إذا كان كل من $n,k \in \mathbb{N}\cup\{0\}$ حيث $n \geq k$ فإننا نعرف معامل ذي الحدين *(binomial coefficient)* ونرمز له بالرمز $\binom{n}{k}$ على النحو التالي:

$$\binom{n}{k}=\frac{n!}{k!(n-k)!}=\frac{(n-k+1)\ldots n(n-1)}{k!}$$

حيث $n!$ يعني مضروب العدد n ويعرف على النحو التالي:

$0!=1$ و $n!=n(n-1)\ldots 3\times 2\times 1$ لكل $n \geq 1$.

مثال (١,١٠)

احسب $\binom{10}{3}$.

الحل

$$\binom{10}{3}=\frac{10!}{3!\,7!}=\frac{10\times 9\times 8\times 7!}{3\times 2\times 1\times 7!}=120 \quad \square$$

ملحوظة

إذا كان $k>n$ فإننا نعتبر $\binom{n}{k}=0$.

مبرهنة (١,٤)

إذا كان $n,k\in\mathbb{N}$ حيث $k\le n$ فإن:

(أ) $\binom{n}{0}=\binom{n}{n}=1$

(ب) $\binom{n}{k}=\binom{n}{n-k}$

(ج) $\binom{n+1}{k}=\binom{n}{k}+\binom{n}{k-1}$

البرهان

(أ) $\binom{n}{0}=\frac{n!}{0!n!}=\frac{n!}{n!}=1$.

كذلك، $\binom{n}{n}=\frac{n!}{n!\,0!}=\frac{n!}{n!}=1$.

(ب) $\binom{n}{k}=\frac{n!}{k!(n-k)!}=\frac{n!}{(n-k)!(n-(n-k))!}=\binom{n}{n-k}$.

(ج) $$\binom{n}{k}+\binom{n}{k-1}=\frac{n!}{k!\,(n-k)!}+\frac{n!}{(k-1)!\,(n-k+1)!}$$

$$=\frac{n!(n-k+1)+n!k}{k!(n-k+1)!}$$

$$=\frac{n!(n-k+1+k)}{k!(n-k+1)!}$$

$$=\frac{n!(n+1)}{k!(n-k+1)!}$$

$$=\frac{(n+1)!}{k!(n-k+1)!}$$

ولذا فإن $\binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k}$ ◆

مبرهنة (١,٥) [مبرهنة ذات الحدين]

إذا كان $x,y\in\mathbb{R}$ وكان $n\in\mathbb{Z}^+$ فإن $(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$.

البرهان

باستخدام الاستقراء الرياضي على n. لنفرض أن العبارة $p(n)$ هي:

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$$

الخطوة الأساسية

بما أن $(x+y)^1=\binom{1}{0}x^1y^0+\binom{1}{1}x^0y^1=x+y$

فإن العبارة $P(1)$ صحيحة.

خطوة الاستقراء

لنفرض أن العبارة $P(n)$ صحيحة ، أي أن:

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$$

نعلم أن:

$$(x+y)^{n+1}=(x+y)^n(x+y)=(\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k)(x+y)$$

كذلك:

$$\sum_{k=0}^{n}\binom{n}{k}x^{n+1-k}y^k=x^{n+1}+\sum_{k=1}^{n}\binom{n}{k}x^{n+1-k}y^k$$

وأن:

$$\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1}=\sum_{k=0}^{n-1}\binom{n}{k}x^{n-k}y^{k+1}+y^{n+1}$$

$$=\sum_{k=1}^{n}\binom{n}{k-1}x^{n+1-k}y^k+y^{n+1}$$

إذن، $(x+y)^{n+1}=x^{n+1}+\sum_{k=1}^{n}\left[\binom{n}{k}+\binom{n}{k-1}\right]x^{n+1-k}y^k+y^{n+1}$.

ولكن: $\binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k}$. لذا نحصل على:

$$(x+y)^{n+1}=x^{n+1}+\sum_{k=1}^{n}\binom{n+1}{k}x^{n+1-k}y^k+y^{n+1}=\sum_{k=0}^{n+1}\binom{n+1}{k}x^{n+1-k}y^k$$

أي أن العبارة $P(n+1)$ صحيحة وهذا ينهي البرهان ◆

تمارين (١,٢)

(١) إذا كان $n\in\mathbb{N}$ فأثبت أن $2^n=\sum_{k=0}^{n}\binom{n}{k}$.

(٢) جد معامل $x^{99}y^{101}$ في مفكوك $(2x+3y)^{200}$.

(٣) أثبت أن $\binom{m+n}{n}=\binom{m+n}{m}=\frac{(m+n)!}{m!\,n!}$.

(٤) لتكن $\{c_n\}$ المتتالية المعرفة استقرائياً على النحو التالي:

$c_1=1$ و $c_n=\sum_{k=1}^{n-1}c_kc_{n-k}$ لكل $n\geq 2$. أثبت أن:

$c_{n+1}=\frac{1}{n+1}\binom{2n}{n}$ لكل $n\geq 0$.

(٥) أثبت أن $\binom{2n}{n}=\sum_{k=0}^{n}\binom{n}{k}^2$ لكل $n\geq 0$.

(٦) إذا كان $n\in\mathbb{Z}^+$ فأثبت أن $\sum_{k=0}^{n}(-1)^k\binom{n}{k}=0$.

(٧) إذا كان $0\leq k\leq r\leq n$ فأثبت أن $\binom{n}{r}\binom{r}{k}=\binom{n}{k}\binom{n-k}{r-k}$.

(٨) أثبت أن $n2^{n-1}=\sum_{k=1}^{n}k\binom{n}{k}$.

(٩) أثبت أن $3^n - 1 = \sum_{k=1}^{n} 2^k \binom{n}{k}$.

(١,٣) قابلية القسمة
Divisibility

لا شك أن القارئ قد استخدم في مراحل دراسته الأولى المفاهيم والخواص الأساسية للأعداد الصحيحة مثل مفهوم قسمة عددين صحيحين ومن ثم خوارزمية القسمة ومفهوم القاسم المشترك الأعظم، إلا أنه لم يعالج هذه المفاهيم معالجة منهجية دقيقة. ونعتقد أنه حان الوقت لهذه المعالجة. هناك أكثر من سبب لمعالجة مفاهيم رياضية متفق على صحتها معالجة دقيقة، إحدى هذه الأسباب هو أنه لا يمكن التسليم بصحة مفهوم رياضي إلا إذا وضع عليه الختم الرسمي ألا وهو البرهان الرياضي. وسبب آخر جوهري هو إمكانية تبني طرائق براهين بعض النتائج عن الأعداد الصحيحة لإثبات نتائج مماثلة في أنظمة رياضية أخرى أكثر شمولية.

تعريف (١,٥)

إذا كان $a,b \in \mathbb{Z}$ وكان $a \neq 0$ فإننا نقول إن a يقسم b (*divide*) إذا وجد عدد صحيح c يحقق $b = ac$.

ملحوظات

(١) إذا كان a يقسم b فإننا نكتب $a \mid b$. وإذا كان a لا يقسم b فإننا نكتب $a \nmid b$.

(٢) إذا كان a يقسم b فإننا نقول أيضاً إن a عامل (*factor*) من عوامل b أو نقول إن b مضاعف (*multiple*) للعدد a أو نقول إن b يقبل القسمة على a.

(٣) لاحظ أن أي عدد صحيح a يقسم 0 لأن $0=0\times a$، وأن العدد 1 يقسم أي عدد صحيح a لأن $a=1\times a$، وأن أي عدد صحيح a يقسم نفسه.

مثال (١,١١)

$18\mid 3$ ، $20\mid -5$ ، $24\mid 6$ ولكن $14\nmid 3$ ، $22\nmid -5$ ، $25\nmid 6$ □

المبرهنة التالية تزودنا بالخواص الأساسية لعلاقة القسمة على الأعداد الصحيحة.

مبرهنة (١,٦)

لتكن $a,b,c,d,m\in\mathbb{Z}$ عندئذ:

(أ) إذا كان $a\mid b$ و $b\mid c$ فإن $a\mid c$.

(ب) إذا كان $a\mid b$ و $c\mid d$ فإن $ac\mid bd$.

(ج) ليكن $m\neq 0$. عندئذ، $a\mid b$ إذا وفقط إذا كان $ma\mid mb$.

(د) إذا كان $d\mid a$ وكان $a\neq 0$ فإن $|d|\leq|a|$.

(هـ) $a\mid b$ و $b\mid a$ إذا وفقط إذا كان $a=\pm b$.

البرهان

(أ) بما أن $a\mid b$ فإن $b=ax$ وإن $b\mid c$ و $c=by$ حيث $x,y\in\mathbb{Z}$. ولذا فإن $c=by=a(xy)$. ومنه فإن $a\mid c$.

(ب) بما أن $a\mid b$ فإن $b=ax$ وإن $c\mid d$ و $d=cy$ حيث $x,y\in\mathbb{Z}$. ولذا فإن $bd=(ax)(cy)=ac(xy)$. ونستنتج أن $ac\mid bd$.

(ج) بما أن $a\mid b$ و $m\mid m$ وباستخدام الفقرة (ب) نخلص إلى أن $ma\mid mb$. وبالعكس، إذا كان $ma\mid mb$ فإن $mb=max$ حيث $x\in\mathbb{Z}$. وبما أن $m\neq 0$ فإن $b=ax$. وبالتالي فإن $a\mid b$.

(د) إذا كان $d\mid a$ فإن $a=dx$ حيث $x\in\mathbb{Z}$. ولذا فإن $|a|=|dx|=|d|\,|x|\geq|d|$ لأن $|x|\geq 1$.

(هـ) لنفرض أولاً أن $a \mid b$ وأن $b \mid a$. عندئذ، $b = ax$ و $a = by$ حيث $x, y \in \mathbb{Z}$. ولذا فإن $a = axy$. إذا كان $a \neq 0$ فإن $xy = 1$. ولذا فإن $x = y = \pm 1$. أي أن $a = \pm b$. أما إذا كان $a = 0$ فإن $b = 0$.

برهان العكس واضح ◆

مبرهنة (١,٧)

إذا كان a يقسم كلاً من $b_1, b_2, \ldots, b_k$ فإن a يقسم $b_1x_1 + b_2x_2 + \ldots + b_kx_k$ لكل $x_1, x_2, \ldots, x_k \in \mathbb{Z}$.

البرهان

بما أن $a \mid b_i$ فإن $b_i = ay_i$ لكل i حيث $y_i \in \mathbb{Z}$. ولذا فإن:

$$b_1x_1 + b_2x_2 + \ldots + b_kx_k = a(x_1y_1 + x_2y_2 + \ldots + x_ky_k).$$

وبالتالي فإن a يقسم $b_1x_1 + b_2x_2 + \ldots + b_kx_k$ ◆

إن إحدى أهم الخواص الأساسية للأعداد الصحيحة هي ما يعرف بخوارزمية القسمة *(division algorithm)* التي تقدمها لنا المبرهنة التالية:

مبرهنة (١,٨) [خوارزمية القسمة]

إذا كان $a, b \in \mathbb{Z}$ حيث $a > 0$ فهناك عددان وحيدان $q, r \in \mathbb{Z}$ حيث:

$$b = qa + r \quad ، \quad 0 \leq r < a.$$

البرهان

لبرهان وجود العددين q و r نفرض أن $S = \{x \geq 0 : x = b - ta, t \in \mathbb{Z}\}$.

لاحظ أولاً أن $b - ta \geq 0$ إذا وفقط إذا كان $t \leq b/a$. ولذا فإنه يوجد $t \in \mathbb{Z}$ حيث $b - ta \geq 0$. إذن، $S \neq \phi$. وباستخدام مبدأ الترتيب الحسن تحتوي S على

عنصر أصغري ولـيكن r. إذن، يوجد $q\in\mathbb{Z}$ حيث $r=b-qa$. أي أن $b=qa+r$ و $r\geq 0$. إذا كان $r\geq a$ فإن $r-a\geq 0$ وإن : $r-a=b-qa-a=b-(q+1)a\in S$. وبما أن $r-a<r$ فإن هذا يناقض اختيار r . إذن، نخلص إلى أن:

$$b=qa+r\ ،\ 0\leq r<a.$$

لبرهان الوحدانية، نفرض أن $b=qa+r=q_1a+r_1$ حيث $0\leq r<a$ و $0\leq r_1<a$. عندئذ، $r-r_1=(q_1-q)a$. إذا كان $q_1\neq q$ فإن $|q_1-q|\geq 1$. فيكون $|r-r_1|\geq|a|=a$ وهذا مستحيل لأن $|r-r_1|<a$. وبالتالي فإن $q=q_1$ ومن ثم $r=r_1$ ◆

ملحوظة

إذا كان $a<0$ فإن $-a>0$، ولذا فإننا نستطيع إيجاد q_1 و r حيث $b=q_1(-a)+r$، $0\leq r<-a$. ولذا فإنه بوضع $q=-q_1$ نجد أن $b=qa+r$. وبالتالي فإننا نحصل على النتيجة التالية:

نتيجة (١,٩)

إذا كان $a,b\in\mathbb{Z}$ حيث $a\neq 0$ فهناك عددان وحيدان $q,r\in\mathbb{Z}$ يحققان

$$b=qa+r\ ،\ 0\leq r<|a|$$ ◆

ملحوظة

يسمى العدد q في المبرهنة (١,٨) خارج قسمة b (*quotient*) على a، كما يسمى العدد r باقي (*remainder*) القسمة.

مثال(١,١٢)

إذا كان n مربعاً كاملاً (أي $n=a^2$) فأثبت أن باقي قسمة n على 4 هو 0 أو 1 .

الحل

باستخدام خوارزمية القسمة نجد أن $a=2q+r$ حيث $r=0,1$. ولذا فإن:

$$n=a^2=4q^2+4qr+r^2=4(q^2+qr)+r^2$$

وبما أن $r=0,1$ فإن $r^2=0,1$. وبالتالي فإن $n=a^2=4k$ أو $n=a^2=4k+1$ □

(١,٣,١) القاسم المشترك الأعظم *(Greatest Common Divisor)*

بعد تعرضنا لخوارزمية القسمة نتناول الآن أحد المفاهيم الأساسية وهو مفهوم القاسم المشترك الأعظم.

تعريف (١,٦)

ليكن $a,b\in\mathbb{Z}$ ليس كلاهما صفراً. نقول إن $d\in\mathbb{Z}^+$ هو قاسم مشترك أعظم للعددين a و b ونكتب $d=(a,b)$ إذا وفقط إذا كان:

(أ) $d\mid a$ و $d\mid b$.

(ب) إذا كان $c\mid a$ و $c\mid b$ فإن $c\le d$.

مثال (١,١٣)

الجدول التالي يبين لنا القاسم المشترك الأعظم لبعض الأزواج من الأعداد الصحيحة

a	b	$d=(a,b)$
4	5	1
9	15	3
8	32	8
15	35	5
20	30	10

□

لعل المسألتين الواجب مناقشتهما في هذا المقام هما مسألة وجود القاسم المشترك الأعظم ومسألة وحدانيته. سنقدم مبرهنتين تثبت كل منهما وجود القاسم المشترك الأعظم، إحدى هاتين المبرهنتين تسمى خوارزمية اقليدس وتصف لنا (إضافة إلى إثبات وجوده) طريقة محددة لإيجاده. أما المبرهنة الثانية فتسمى معادلة بيزو وتبين لنا أننا نستطيع كتابته كتركيب خطي للعددين. أما بالنسبة لمسألة وحدانيته فأمرها بسيط ونوضحه في المبرهنة التالية:

مبرهنة (١,١٠)

إذا كان $d_1=(a,b)$ و $d_2=(a,b)$ فإن $d_1=d_2$.

البرهان

بما أن $(d_1 \mid a \ ، \ d_1 \mid b)$ وأن d_2 قاسم مشترك أعظم فإن $d_1 \le d_2$.

وبالمثل $d_2 \le d_1$، إذن، $d_1=d_2$ ◆

قبل تقديم البرهان الأول لوجود القاسم المشترك الأعظم نحتاج إلى التمهيدية التالية:

تمهيدية (١,١١)

(أ) إذا كان $b=qa+r$ فإن $(a,b)=(a,r)$.

(ب) $(a,b)=(-a,b)=(a,-b)=(-a,-b)$.

(ج) $(a,0)=a$ عندما $a>0$.

البرهان

سنبرهن الفقرة (أ) ونترك برهان الفقرتين (ب) و (ج) للقارئ.

لنفرض أن $d=(a,b)$. بما أن $d \mid a$ و $d \mid b$ فإن $d \mid (b-qa)$. وعليه فإن $d \mid r$. إذن، $d \le (a,r)$. لنفرض الآن أن $c \mid a$ و $c \mid r$. ولذا فإن

$c \mid (qa+r)$. ويكون $c \mid b$. ولذا فإن c قاسم مشترك للعددين a و b. وعليه فإن $(a,r)=r \le d$. وبالتالي فإن $d=(a,r)$ ◆

في المبرهنة التالية نستطيع لإيجاد القاسم المشترك الأعظم للعددين a و b افتراض أنهما موجبان وذلك استعانة بالتمهيدية (١,١١) .

مبرهنة (١,١٢) [خوارزمية إقليدس - *Euclidean algorithm*]

لنفرض أن $a=r_0$ و $b=r_1$ عددان صحيحان حيث $a \ge b > 0$. إذا طبقنا خوارزمية القسمة بالتتابع لنحصل على :

$r_j = q_{j+1}\, r_{j+1} + r_{j+2}$ ، $0 < r_{j+2} < r_{j+1}$ لكل $j = 0,1,2,\dots,n-2$

وكان $r_{n+1}=0$ فإن $(a,b)=r_n$.

البرهان

باستخدام خوارزمية القسمة نحصل على:

$$r_0 = q_1 r_1 + r_2 \quad ، \quad 0 \le r_2 < r_1$$

$$r_1 = q_2 r_2 + r_3 \quad ، \quad 0 \le r_3 < r_2$$

$$\vdots$$

$$r_{j-2} = q_{j-1}\, r_{j-1} + r_j \quad ، \quad 0 \le r_j < r_{j-1}$$

$$\vdots$$

$$r_{n-3} = q_{n-2}\, r_{n-2} + r_{n-1} \quad ، \quad 0 \le r_{n-1} < r_{n-2}$$

$$r_{n-2} = q_{n-1}\, r_{n-1} + r_n \quad ، \quad 0 \le r_n < r_{n-1}$$

$$r_{n-1} = q_n r_n + r_{n+1} \quad ، \quad r_{n+1} = 0$$

بما أن $a = r_0 > r_1 > r_2 > \dots \ge 0$ فإنه لا بد من وجود n بحيث يكون $r_{n+1}=0$. الآن باستخدام التمهيدية(١,١١) نجد أن:

◆ $(a,b)=(r_0,r_1)=(r_1,r_2)=\dots=(r_{n-1},r_n)=(r_n,0)=r_n$

ملحوظات

(١) إضافة إلى إثبات وجود القاسم المشترك الأعظم فإن خوارزمية إقليدس تقدم لنا طريقة محددة لإيجاده.

(٢) لا بد من التوقف قليلاً لتقديم معنى للخوارزمية:

عند استخدامنا الحاسب الآلي لحل مسألة ما فإنه يقوم بتنفيذ خطوات دقيقة معدة مسبقاً تسمى خوارزمية. سنكتفي هنا بالقول إن الخوارزمية هي مجموعة من الخطوات المنتهية موضوعة بدقة متناهية يقوم حاسب آلي (أو شخص) بتنفيذها لحل مسألة ما. هناك تعريفات رياضية دقيقة قدمها كل من تشيرش *(Church)*، تورينغ *(Turing)*، بوست *(Post)* وآخرين غيرهم في منتصف القرن العشرين وتبين أنها جميعاً متكافئة وتكافئ التعريفات الأخرى التي ظهرت لاحقاً. لن نتطرق هنا لأي من هذه التعريفات ونكتفي بالوصف الذي قدمناه للخوارزمية لأنه يفي بالغرض.

مثال (١,١٤)

استخدم خوارزمية إقليدس لإيجاد القاسم المشترك الأعظم للعددين 1769 و 2378.

الحل

$$2378 = 1\times 1769 + 609$$
$$1769 = 2\times 609 + 551$$
$$609 = 1\times 551 + 58$$
$$551 = 9\times 58 + 29$$
$$58 = 2\times 29 + 0$$

وبالتالي فإن $(2378, 1769) = 29$ □

مثال (١,١٥)

استخدم خوارزمية إقليدس لإيجاد القاسم المشترك الأعظم للعددين 271 و 337.

الحل

$$337 = 1\times 271 + 66$$
$$271 = 4\times 66 + 7$$
$$66 = 9\times 7 + 3$$
$$7 = 2\times 3 + 1$$
$$3 = 3\times 1 + 0$$

ولذا فإن $(337, 271) = 1$ □

يقترح علينا المثال (١,١٥) التعريف التالي:

تعريف (١,٧)

نقول إن العددين a و b أوليان نسبياً (*relatively prime*) إذا كان $(a,b) = 1$.

نقدم الآن المبرهنة الثانية التي تضمن لنا وجود القاسم المشترك الأعظم لعددين.

مبرهنة (١,١٣) [معادلة بيزو – *Bezout's equation*]

افرض أن $a,b \in \mathbb{Z}$ ليس كلاهما صفراً. عندئذ، يوجد $x_0, y_0 \in \mathbb{Z}$ بحيث $(a,b) = ax_0 + by_0$. أي يمكن كتابة (a,b) كتركيب خطي (*linear combination*) للعددين a و b.

البرهان

لتكن $S = \{ax + by \in \mathbb{Z}^+ : x, y \in \mathbb{Z}\}$. بما أن a و b ليس كلاهما صفراً، نفرض أن $a \neq 0$. إذا كان $a > 0$ فإن $a = a\times 1 + b\times 0 \in S$. وإذا كان

$a<0$ فإن $-a=a(-1)+b\times 0\in S$. إذن، $S\neq\phi$. باستخدام مبدأ الترتيب الحسن يوجد عنصر أصغري $d\in S$. أي يوجد $x_0,y_0\in\mathbb{Z}$ حيث

$$d=ax_0+by_0.$$

ولإكمال البرهان نثبت أن $d=(a,b)$.

نفرض أن $d\nmid a$. باستخدام خوارزمية القسمة يوجد $q,r\in\mathbb{Z}$ حيث:

$$a=qd+r\ ،\ 0<r<d.$$

الآن لاحظ أن : $r=a-qd=a-q(ax_0+by_0)=a(1-qx_0)+b(-qy_0)\in S$.

وهذا تناقض لأن $r<d$. إذن، $d\mid a$. وبالمثل نرى أن $d\mid b$.

وأخيراً، نفرض أن $c\mid a$ و $c\mid b$. عندئذ $c\mid(ax_0+by_0)$. أي $c\mid d$.

فنستخلص أن $c\le d$. وبالتالي فإن $d=(a,b)$ ◆

ملحوظات

(١) من برهان المبرهنة (١,١٣) نجد أنه إذا كان $d=(a,b)$ وكان $c\mid a$ و $c\mid b$ فإن $c\mid d$.

(٢) ليس بالضرورة أن يكون العددان x_0,y_0 وحيدين، فمثلاً، خذ $(15,24)=3$ ولاحظ أن:

$$3=15(-3)+24(2)=15(-27)+24(17).$$

في الحقيقة إذا كان $d=ax_0+by_0$ فإن:

$$d=a(x_0+k\frac{b}{d})+b(y_0-k\frac{a}{d})$$ لكل $k\in\mathbb{Z}$.

(٣) لإيجاد x_0,y_0 نستخدم خوارزمية إقليدس بخطوات إرجاعية بعد إيجاد القاسم المشترك الأعظم، كما هو موضح في المثال التالي:

مثال(١,١٦)

جد $x_0, y_0 \in \mathbb{Z}$ حيث $(2378,1769) = 2378x_0 + 1769y_0$.

الحل

باستخدام خطوات حل المثال (١,١٤) ارتجاعياً نحصل على:

$$\begin{aligned} 29 &= 551 - 9\times 58 \\ &= 551 - 9(609 - 1\times 551) \\ &= 10\times 551 - 9\times 609 \\ &= 10(1769 - 2\times 609) - 9\times 609 \\ &= 10\times 1769 - 29(2378 - 1\times 1769) \\ &= 2378(-29) + 1769(39) \end{aligned}$$

ولذا فإن $x_0 = -29$ و $y_0 = 39$ □

إن الطريقة المقدمة في المثال (١,١٦) لوضع القاسم المشترك (a,b) كتركيب خطي للعددين a و b طريقة ليست عملية وطويلة جداً، لأنها تستلزم تنفيذ خطوات خوارزمية إقليدس، ثم حفظها واستخدامها بطريقة إرتجاعية. هناك طريقة أفضل من ذلك نقدمها الآن حيث تستخدم خوارزمية إقليدس مرة واحدة فقط.

مبرهنة (١,١٤) [خوارزمية إقليدس الموسعة *Extended Euclidean algorithm*]

ليكن $a,b \in \mathbb{Z}^+$ حيث $a \geq b$ ولتكن كل من $s_0, s_1, \ldots, s_n$ و $t_0, t_1, \ldots, t_n$ متتاليتان معرفتان استقرائياً على النحو التالي:

$s_0 = 1$ ، $s_1 = 0$ و $s_j = s_{j-2} - q_{j-1}s_{j-1}$ لكل $j \geq 2$.

$t_0 = 0$ ، $t_1 = 1$ و $t_j = t_{j-2} - q_{j-1}t_{j-1}$ لكل $j \geq 2$.

حيث الأعداد q_j هي خوارج القسمة التي نحصل عليها عند تطبيق خوارزمية إقليدس لإيجاد (a,b). عندئذ:

$$(a,b) = as_n + bt_n$$

البرهان

نستخدم المبدأ الثاني للاستقراء الرياضي على j لإثبات أن $r_j = as_j + bt_j$ لكل $0 \le j \le n$.

عند $j=0$ لدينا : $r_0 = a = a1 + b0 = as_0 + bt_0$.

عند $j=1$ لدينا : $r_1 = b = a0 + b1 = as_1 + bt_1$.

ولذا فإن العبارة صحيحة عند $j = 0,1$.

لنفرض الآن أن العبارة صحيحة لكل $0 \le j \le k-1$. باستخدام الخطوة k من خوارزمية إقليدس نجد أن : $r_k = r_{k-2} - q_{k-1}\ r_{k-1}$. وباستخدام فرضية الاستقراء نجد أن:

$$\begin{aligned} r_k &= (as_{k-2} + bt_{k-2}) - q_{k-1}(as_{k-1} + bt_{k-1}) \\ &= a(s_{k-2} - q_{k-1}\ s_{k-1}) + b(t_{k-2} - q_{k-1}\ t_{k-1}) \\ &= as_k + bt_k \end{aligned}$$

ولذا فإن العبارة صحيحة عند k.

أخيراً: بما أن $(a,b) = r_n$ و $r_n = as_n + bt_n$ فإن $(a,b) = as_n + bt_n$ ◆

مثال (١,١٧)

إذا كان $a = 75$ و $b = 45$ فإننا نجد باستخدام خوارزمية إقليدس أن:

$$75 = 1 \times 45 + 30$$
$$45 = 1 \times 30 + 15$$
$$30 = 2 \times 15 + 0$$

ولذا فإن $(75,45) = 15$ وأن: $q_1 = 1, q_2 = 1$.

الآن، نستخدم الجدول التالي لإيجاد قيم s_j و t_j :

مثال(١,١٦)

جد $x_0, y_0 \in \mathbb{Z}$ حيث $(2378,1769) = 2378x_0 + 1769y_0$.

الحل

باستخدام خطوات حل المثال (١,١٤) ارتجاعياً نحصل على:

$$\begin{aligned} 29 &= 551 - 9\times 58 \\ &= 551 - 9(609 - 1\times 551) \\ &= 10\times 551 - 9\times 609 \\ &= 10(1769 - 2\times 609) - 9\times 609 \\ &= 10\times 1769 - 29(2378 - 1\times 1769) \\ &= 2378(-29) + 1769(39) \end{aligned}$$

ولذا فإن $x_0 = -29$ و $y_0 = 39$ □

إن الطريقة المقدمة في المثال (١,١٦) لوضع القاسم المشترك (a,b) كتركيب خطي للعددين a و b طريقة ليست عملية وطويلة جداً، لأنها تستلزم تنفيذ خطوات خوارزمية إقليدس، ثم حفظها واستخدامها بطريقة إرتجاعية. هناك طريقة أفضل من ذلك نقدمها الآن حيث تستخدم خوارزمية إقليدس مرة واحدة فقط.

مبرهنة (١,١٤) [خوارزمية إقليدس الموسعة *Extended Euclidean algorithm*]

ليكن $a,b \in \mathbb{Z}^+$ حيث $a \geq b$ ولتكن كل من $s_0, s_1, \ldots, s_n$ و $t_0, t_1, \ldots, t_n$ متتاليتان معرفتان استقرائياً على النحو التالي:

$s_0 = 1$ ، $s_1 = 0$ و $s_j = s_{j-2} - q_{j-1}s_{j-1}$ لكل $j \geq 2$.

$t_0 = 0$ ، $t_1 = 1$ و $t_j = t_{j-2} - q_{j-1}t_{j-1}$ لكل $j \geq 2$.

حيث الأعداد q_j هي خوارج القسمة التي نحصل عليها عند تطبيق خوارزمية إقليدس لإيجاد (a,b). عندئذ:

$$(a,b) = as_n + bt_n$$

نظرية

البرهان

نستخدم المبدأ الثاني للاستقراء الرياض

لكل $0 \le j \le n$.

عند $j=0$ لدينا : $a = a1+b0 = as_0 + bt_0$

عند $j=1$ لدينا : $b = a0+b1 = as_1 + bt_1$

ولذا فإن العبارة صحيحة عند $j=0,1$.

لنفرض الآن أن العبارة صحيحة لكل

من خوارزمية إقليدس نجد أن : $r_{k-1} - q_{k-1}$

نجد أن:

$$) - q_{k-1}(as_{k-1} + bt_{k-1})$$

$$s_{k-1}) + b(t_{k-2} - q_{k-1}\, t_{k-1})$$

ولذا فإن العبارة صحيحة عند k.

أخيراً: بما أن $(a,b) = r_n$ و $r_n = as_n + bt_n$

مثال (١,١٧)

إذا كان $a=75$ و $b=45$ ف

ولذا فإن $(75,45) = 15$

الآن، نستخدم الجدول الت

j	q_j	$s_j = s_{j-2} - q_{j-1}s_{j-1}$	$t_j = t_{j-2} - q_{j-1}\,t_{j-1}$
0		1	0
1	1	0	1
2	1	$s_2 = 1-1\times 0 = 1$	$t_2 = 0-1\times 1 = -1$
3		$s_3 = 0-1\times 1 = -1$	$t_3 = 1-1\times(-1) = 2$

وبالتالي فإن: $15 = 75(-1) + 45(2)$ □

فيما تبقى من هذا البند نقدم بعض الخواص الأساسية للقاسم المشترك الأعظم ونعمم التعريف على أكثر من عددين ونناقش المفهوم الرديف للقاسم المشترك الأعظم ألا وهو المضاعف المشترك الأصغر.

مبرهنة (١,١٥)

ليكن $a,b \in \mathbb{Z}$ ليس كلاهما صفراً . عندئذ:

$(a,b)=1$ إذا وفقط إذا كان $1 = ax+by$ حيث $x,y \in \mathbb{Z}$.

البرهان

نفرض أن $1 = ax+by$ حيث $x,y \in \mathbb{Z}$. إذا كان $(a,b)=d$ فإن $d \mid a$ و $d \mid b$. وعليه فإن $d \mid (ax+by)$ أي $d \mid 1$. وبالتالي فإن $d=1$.

أما العكس فنحصل عليها مباشرة من المبرهنة (١,١٣) ◆

نتيجة (١,١٦)

إذا كان $(a,b)=d$ فإن $(a/d, b/d)=1$.

البرهان

بما أن $(a,b)=d$ فإن $d = ax+by$ حيث $a,b \in \mathbb{Z}$. وبقسمة طرفي المعادلة على d نحصل على المساواة $1 = \frac{a}{d}x + \frac{b}{d}y$. باستخدام المبرهنة (١,١٥)، نجد أن $(a/d, b/d)=1$ ◆

نتيجة (١,١٧)

ليكن $(a,b)=1$. عندئذ:

(أ) إذا كان $a\mid c$ و $b\mid c$ فإن $ab\mid c$.

(ب) إذا كان $a\mid bc$ فإن $a\mid c$.

البرهان

(أ) بما أن $a\mid c$ و $b\mid c$ فإن $c=ar=bs$ حيث $r,s\in\mathbb{Z}$. وبما أن $(a,b)=1$ فإن $1=ax+by$ حيث $x,y\in\mathbb{Z}$. الآن :

$$c=c(ax+by)=acx+bcy=a(bs)x+b(ar)y=ab(sx+ry)$$

ومنه نجد أن $ab\mid c$.

(ب) بما أن $1=ax+by$ حيث $x,y\in\mathbb{Z}$ فإن $c=acx+bcy$. ولكن $a\mid ac$ و $a\mid bc$. ولذا فإن $a\mid(acx+bcy)$. وبالتالي فإن $a\mid c$ ◆

ملحوظة

تسمى الفقرة (ب) من النتيجة (١,١٧)، تمهيدية إقليدس *(Euclidean lemma)*. ونلفت نظر القارئ إلى أن الشرط $(a,b)=1$ ضروري للفقرتين، على سبيل المثال، $8\mid 48$ و $12\mid 48$ ولكن $48\nmid 8\times 12=96$. كذلك $12\mid 8\times 9$ ولكن $12\nmid 8$ و $12\nmid 9$.

نقدم الآن تعميماً للقاسم المشترك الأعظم لأكثر من عددين.

تعريف (١,٨)

لتكن $a_1,a_2,\ldots,a_n\in\mathbb{Z}$ ليست جميعها أصفاراً. نقول إن $d>0$ القاسم المشترك الأعظم للأعداد $a_1,a_2,\ldots,a_n$ ونكتب $d=(a_1,a_2,\ldots,a_n)$ إذا وفقط إذا كان :

(أ) $d\mid a_i$ لكل $i=1,2,\ldots,n$.

(ب) إذا كان $c\mid a_i$ لكل $i=1,2,\ldots,n$ فإن $c\le d$.

مبرهنة (١,١٨)

لتكن $a_1,a_2,\dots,a_n \in \mathbb{Z}$ ليست جميعها أصفاراً . عندئذ:

(أ) $(a_1,a_2,\dots,a_n)=(a_1,a_2,\dots,a_{n-2},(a_{n-1},a_n))$.

(ب) توجد أعداد $x_1,x_2,\dots,x_n \in \mathbb{Z}$ حيث $(a_1,a_2,\dots,a_n)=a_1x_1+a_2x_2+\dots+a_nx_n$.

البرهان

(أ) لنفـــــرض أن $A=\{a_1,a_2,\dots,a_n\}$ وأن $B=\{a_1,a_2,\dots,a_{n-2},(a_{n-1},a_n)\}$. سنبرهن أن للمجموعتين A و B نفس القواسم المشتركة. إذا كان b قاسماً مشتركاً لمجموعة أعداد A فإن $b \mid a_{n-2}, b \mid a_2, \dots, b \mid a_1, b$. ولكون $b \mid a_{n-1}$ و $b \mid a_n$ فإن $b \mid (a_{n-1},a_n)$. وبالتالي فإن b قاسم لمجموعة أعداد B. ومن ناحية أخـــرى، إذا كان $c \mid (a_{n-1},a_n), c \mid a_{n-2}, \dots, c \mid a_1$ فإن $c \mid a_{n-1}$ و $c \mid a_n$. ولذا فإن c قاسم لمجموعة أعداد A. الآن ، بما أن مجموعة القواسم المشتركة للمجموعتين متساوية ومنتهية فبأخذ العنصر الأكبر لهذه القواسم نحصل على المطلوب.

(ب) بالاستقراء الرياضي على n. العبارة صحيحة عند $n=2$ وذلك باستخدام المبرهنة (١,١٣). نفرض أن العبارة صحيحة عند $n-1$. باســـتخدام المبرهنـــة (١,١٣) مرة أخـــرى، توجـــد $x_0,y_0 \in \mathbb{Z}$ حيـــث $(a_{n-1},a_n)=a_{n-1}x_0+a_ny_0$. وباستخدام فرضية الاستقراء والفقرة (أ) نستطيع إيجـــاد $y_1,\dots,y_{n-1} \in \mathbb{Z}$ بحيـــث يكون:

$$\begin{aligned}(a_1,a_2,\dots,a_n)&=(a_1,a_2,\dots,a_{n-2},(a_{n-1},a_n))\\&=a_1y_1+a_2y_2+\dots+a_{n-2}y_{n-2}+(a_{n-1},a_n)y_{n-1}\\&=a_1y_1+a_2y_2+\dots+a_{n-2}y_{n-2}+(a_{n-1}x_0+a_ny_0)y_{n-1}\end{aligned}$$

وبوضع $x_1=y_1,\dots,x_{n-2}=y_{n-2},x_{n-1}=x_0y_{n-1},x_n=y_0y_{n-1}$ نخلص إلى أن:

◆ $(a_1,a_2,\dots,a_n)=a_1x_1+a_2x_2+\dots+a_nx_n$

مثال(١,١٨)

احسب $(2378,1769,88)$ ثم جد $x_0,y_0,z_0 \in \mathbb{Z}$ بحيث يكون:

$$(2378,1769,88) = 2378x_0 + 1769y_0 + 88z_0$$

الحل

نفرض أن $d = (2378,1769)$. لقد وجدنا في المثال (١,١٤) أن $d = 29$، ووجدنا في المثال (١,١٦) أن $29 = (2378,1769) = 2378(-29) + 1769(39)$.

الآن، $(2378,1769,88) = (29,88)$. وباستخدام خوارزمية إقليدس نحصل على:

$$88 = 3\times 29 + 1$$
$$29 = 29\times 1 + 0$$

فنرى أن $1 = (29,88)$ وأن $1 = 88\times 1 + 29(-3)$. إذن:

$$1 = (2378,1769,88)$$
$$1 = 88\times 1 + 29(-3)$$
$$1 = 88\times 1 + [2378(-29) + 1769(39)](-3)$$
$$1 = 88\times 1 + 2378(87) + 1769(-117) \quad \square$$

تعريف (١,٩)

لتكن $a_1,a_2,\ldots,a_n \in \mathbb{Z}$ ليست جميعها أصفاراً. نقول إنها أولية جمعاً (*mutually prime*) إذا كان $(a_1,a_2,\ldots,a_n) = 1$. كما نقول إنها أولية نسبياً زوجاً زوجاً (*relatively prime in pairs*) إذا كان $(a_i,a_j) = 1$ لكل $i \neq j$.

من الواضح أن الأعداد الأولية نسبياً زوجاً زوجاً يجب أن تكون أولية جمعاً ولكن العكس غير صحيح كما هو مبين في المثال التالي:

مثال (١,١٩)

لقد رأينا في المثال (١,١٨) أن الأعداد 88 ، 1769 ، 2378 أولية جمعاً. ووجدنا في المثال (١,١٤) أن $(1769,2378)=29$. ولذا فإنها ليست أولية نسبياً زوجاً زوجاً □

نقدم الآن تعميماً لخوارزمية إقليدس لحساب القاسم المشترك الأعظم للأعداد $a_1,a_2,\dots,a_n$. سنفرض أن الأعداد غير سالبة دون أن يؤثر ذلك على عمومية الخوارزمية:

(١) نختار أصغر عدد صحيح موجب من بين الأعداد وليكن a_1 (قد يوجد أكثر من عدد بهذا الوصف نختار أحدها).

(٢) نستخدم خوارزمية القسمة لقسمة كل من $a_2,\dots,a_n$ على a_1 لنحصل على:

$$a_2=q_2a_1+r_2^{(1)} \quad ، \quad 0\le r_2^{(1)}<a_1$$
$$a_3=q_3a_1+r_3^{(1)} \quad ، \quad 0\le r_3^{(1)}<a_1$$
$$\vdots$$
$$a_n=q_na_1+r_n^{(1)} \quad ، \quad 0\le r_n^{(1)}<a_1$$

وبوضع $a_1=r_1^{(1)}$ نجد أن: $(a_1,a_2,\dots,a_n)=(r_1^{(1)},r_2^{(1)},\dots,r_n^{(1)})$.

وبتكرار الخطوتين (١) و (٢) بالنسبة للأعداد $r_1^{(1)},\dots,r_n^{(1)}$ والاستمرار مع ملاحظة أن الأعداد في كل خطوة هي أصغر من الأعداد في الخطوة السابقة لها. إذن، لا بد وأن نصل في نهاية المطاف إلى:

$$(r_1^{(k-1)},r_2^{(k-1)},\dots,r_n^{(k-1)})=(r_1^{(k)},0,0,\dots,0)=r_1^{(k)}$$

ومن ذلك نخلص إلى أن $(a_1,a_2,\dots,a_n)=r_1^{(k)}$.

مثال (١,٢٠)

استخدم الخوارزمية المقدمة أعلاه لحساب $(88,1769,2378)$.

الحل

$$1769 = 20\times 88 + 9$$
$$2378 = 27\times 88 + 2$$

ولذا فإن: $(88,1769,2378) = (88,9,2) = (2,9,88)$. الآن:

$$9 = 4\times 2 + 1$$
$$88 = 44\times 2 + 0$$

ولذا فإن: $(2,9,88) = (2,1,0) = (0,1,2)$. الآن:

$$2 = 2\times 1 + 0$$

ولذا فإن: $(0,1,2) = (1,0,0) = 1$. وهذا هو القاسم المشترك الأعظم للأعداد □

(١,٣,٢) المضاعف المشترك الأصغر (*Least Common Multiple*)

نقدم الآن المفهوم الأخير في هذا البند وهو المضاعف المشترك الأصغر.

تعريف (١,١٠)

لتكن $a,b\in\mathbb{Z}$ ليس أي منهما صفراً. نقول إن $m>0$ هو المضاعف المشترك الأصغر للعددين a و b ونكتب $m=[a,b]$ إذا وفقط إذا كان:

(أ) $a\mid m$ و $b\mid m$

(ب) إذا كان $a\mid c$ و $b\mid c$ حيث $c>0$ فإن $m\le c$.

ملحوظة

بما أن مجموعة المضاعفات الموجبة للعددين a و b مجموعة جزئية غير خالية من $\mathbb{Z}^+$ فإن مبدأ الترتيب الحسن يضمن لنا وجود عدد أصغري وحيد في هذه المجموعة وهذا العدد هو المضاعف المشترك الأصغر للعددين. والمبرهنة التالية

تزودنا بخوارزمية لإيجاد المضاعف المشترك الأصغر لعددين باستخدام القاسم المشترك الأعظم.

بما أنه من الواضح أن $(a,b)=(|a|,|b|)$ وأن $[a,b]=[|a|,|b|]$ فإننا سنفترض في المبرهنة التالية أن $a,b\in\mathbb{Z}^+$ دون التأثير على عموميتها.

مبرهنة (١,١٩)

إذا كان $a,b\in\mathbb{Z}^+$ وكان $d=(a,b)$ و $m=[a,b]$ فإن $md=ab$.

البرهان

لنفرض أن $a=dr$ و $b=ds$. عندئذ $m=\frac{ab}{d}=\frac{drds}{d}=drs$.

سنبرهن الآن أن m هو المضاعف المشترك الأصغر للعددين a و b. لاحظ أن: $m=drs=(ds)r=br$ و $m=drs=as$. ولذا فإن $b\mid m$ و $a\mid m$.

لنفرض الآن أن $a\mid c$ و $b\mid c$ حيث $c>0$. بما أن $d=(a,b)$ فإنه يوجد $x,y\in\mathbb{Z}^+$ حيث $d=ax+by$. الآن:

$$\frac{c}{m}=\frac{cd}{ab}=\frac{c(ax+by)}{ab}=(c/b)x+(c/b)y\in\mathbb{Z}$$

ولذا فإن $m\mid c$. فيكون $m\le c$. ونخلص إلى أن $m=[a,b]$ ◆

ملحوظات

(١) لاحظ أننا أثبتنا في المبرهنة (١,١٩) أنه إذا كان $m=[a,b]$ و c مضاعف آخر للعددين a و b فإن $m\mid c$.

(٢) في الحالة التي يكون فيها $(a,b)=1$ نجد أن $[a,b]=ab$.

مثال (١,٢١)

لقد وجدنا في المثال (١,١٦) أن $(75,45)=15$. ولذا فإن:

$$[75,45]=\frac{75\times 45}{15}=225 \quad \square$$

وكما هو الحال للقاسم المشترك الأعظم فإننا نستطيع تعميم مفهوم المضاعف المشترك الأصغر لأكثر من عددين على النحو التالي:

تعريف (١,١١)

لتكن $a_1,a_2,\dots,a_n\in\mathbb{Z}$ ليست جميعها أصفاراً. نقول إن $m=[a_1,a_2,\dots,a_n]>0$ هو المضاعف المشترك الأصغر إذا وفقط إذا كان:

(أ) $a_i \mid m$ لكل $i=1,2,\dots,n$.

(ب) إذا كان $c>0$ وكان $a_i \mid c$ لكل $i=1,2,\dots,n$ فإن $m\le c$.

تحذير

لإيجاد المضاعف المشترك الأصغر لأكثر من عددين لا نستطيع تطبيق المبرهنة (١,١٩) مباشرة لأنها ليست صحيحة لأكثر من عددين، على سبيل المثال ،

$(6,10,15)=1$ و $[6,10,15]=30$

ولكن $[6,10,15](6,10,15)=30\neq 900=6\times 10\times 15$.

ولكننا نستطيع بالاستقراء الرياضي إثبات أن:

$$[a_1,a_2,\dots,a_n]=[a_1,a_2,\dots,[a_{n-1},a_n]].$$

(١,٣,٣) تمارين محلولة (*Solved Exercises*)

تمرين (١)

إذا كان $(a,b)=(a,c)=1$ فأثبت أن $(a,bc)=1$.

الحل

يوجد $x,y,r,s \in \mathbb{Z}$ بحيث يكون $1=ar+cs$ و $1=ax+by$. ولذا فإن:

$$\begin{aligned}1&=(ax+by)(ar+cs)\\&=a^2xr+acxs+abyr+bcsy\\&=a(axr+cxs+byr)+bc(sy)\end{aligned}$$

وبالتالي فإن $(a,bc)=1$ △

تمرين (٢)

جد عدد الأعداد الصحيحة n حيث $500<n<2000$ التي تقبل القسمة على كل من 3 و 7.

الحل

عدد الأعداد الصحيحة الموجبة التي أصغر من أو تساوي 500 وتقبل القسمة على 21 هو $\left[\frac{500}{21}\right]=23$ حيث $[x]$ تعني أكبر عدد صحيح أصغر من أو يساوي x. بالمثل عدد الأعداد الصحيحة الموجبة التي أصغر من أو تساوي 2000 وتقبل القسمة 21 هو $\left[\frac{2000}{21}\right]=95$. ولذا فإن عدد الأعداد المحصورة بين 500 و 2000 والتي تقبل القسمة على 21 (أي على كل من 3 و 7) يساوي $95-23=72$ △

تمرين (٣)

ليكن $M=x(x+1)(x+2)(x+3)$. أثبت أن $M+1$ مربع كامل. واستنتج أنه إذا كان M مربعاً كاملاً فإن $M=0$.

الحل

$$M+1=x(x+1)(x+2)(x+3)+1$$

$$= x(x+3)[x^2+3x+2]+1$$
$$= x(x+3)(x(x+3)+2)+1$$
$$= x^2(x+3)^2+2x(x+3)+1$$
$$= (x(x+3)+1)^2 = k^2$$

ولذا فإن $M+1$ مربعاً كاملاً.

لنفرض الآن $M=s^2$ حيث $s\in\mathbb{Z}$. عندئذ: $1=k^2-s^2=(k-s)(k+s)$. ولذا فإن $k-s=k+s=1$ أو $k-s=k+s=-1$. ومنه فإن $k=1$ أو $k=-1$. ولذا فإن $M+1=k^2=1$. وبالتالي فإن $M=0$ △

تمرين (٤)

إذا كان $a\mid c$ و $b\mid c$ فأثبت أن $[a,b]\mid c$.

الحل

لنفرض أن $c=ax$ و $c=by$ حيث $x,y\in\mathbb{Z}$. بما أن $[a,b]=\frac{ab}{d}$ حيث $d=(a,b)$ وأن $d=ar+bs$ حيث $r,s\in\mathbb{Z}$ فإن:

$$\frac{c}{[a,b]}=\frac{cd}{ab}=\frac{car+cbs}{ab}=(c/b)r+(c/a)s=yr+xs\in\mathbb{Z}$$

ولذا فإن $[a,b]\mid c$ △

تمرين (٥)

(أ) أثبت أن $f_{m+n}=f_{m-1}f_n+f_m f_{n+1}$ لكل $n\geq 1$ و $m\geq 2$ حيث $\{f_n\}$ هي متتالية فيبوناتشي.

(ب) إذا كانت $m\mid n$ فأثبت أن $f_m\mid f_n$.

الحل

(أ) بالاستقراء الرياضي على n. بما أن:

$f_{m+1}=f_{m-1}+f_m=f_{m-1}f_1+f_m f_2$ فإن العبارة صحيحة عندما $n=1$.

لنفرض أن العبارة صحيحة لكل $k \le j \le 1$. باستخدام الاستقراء لدينا:

$$f_{m+k} = f_{m-1}f_k + f_m f_{k+1}$$
$$f_{m+k-1} = f_{m-1}f_{k-1} + f_m f_k$$

وبجمع هاتين المعادلتين نحصل على:

$$f_{m+k} + f_{m+k-1} = f_{m-1}(f_k + f_{k-1}) + f_m(f_{k+1} + f_k)$$

ولذا فإن $f_{m+k+1} = f_{m-1}f_{k+1} + f_m f_{k+2}$. وبالتالي فإن العبارة صحيحة عندما $n = k+1$.

(ب) بما أن $m \mid n$ فإن $n = mk$ حيث $k \in \mathbb{Z}^+$. نستخدم الاستقراء الرياضي على k.

إذا كان $k = 1$ فإن $n = m$. ومن ثم فإن $f_n = f_m$ وتكون العبارة صحيحة.

لنفرض أن $f_m \mid f_{mk}$. باستخدام الفقرة (أ) لدينا:

$$f_{m(k+1)} = f_{mk+m} = f_{mk-1}f_m + f_{mk}f_{m+1}$$

وبما أن $f_m \mid f_{mk}$ فإن $f_{mk} = f_m a$. ولذا فإن $f_{m(k+1)} = f_m(f_{mk-1} + af_{m+1})$.

أي أن $f_m \mid f_{m(k+1)}$ وتصبح العبارة صحيحة عند $k+1$ △

تمرين (٦)

(أ) أثبت أن $(a,b) = (a,b-a)$.

(ب) إذا كان $(a,c) = 1$ فأثبت أن $(a,bc) = (a,b)$.

الحل

(أ) لنفرض أن $(a,b) = d$. حينئذ، $d \mid a$ و $d \mid b$. وعليه فإن $d \mid (b-a)$.

وإذا كان $c \mid a$ و $c \mid (b-a)$ فإن $c \mid b$. لذا فإن $c \mid d$. إذن، $d = (a,b-a)$.

(ب) لنفرض أن $(a,bc) = d$. عندئذ، $d \mid a$ و $d \mid bc$. وبما أن $(a,c) = 1$ فمن الواضح أن $(d,c) = 1$. ولذا فإن $d \mid b$. كذلك إذا كان $e \mid a$ و $e \mid b$ فمن الواضح أن $e \mid a$ و $e \mid bc$. وعليه فإن $e \mid d$. إذن، $d = (a,b)$ △

تمرين (٧)

إذا كان $m,n\in\mathbb{Z}^+$ فأثبت أن $(2^m-1,2^n-1)=2^{(m,n)}-1$.

الحل

نفرض أن $m\le n$ ونستخدم الاستقراء الرياضي على n. بما أن $(2^m-1,2^1-1)=(2^m-1,1)=1=2^{(m,1)}-1$ فإن العبارة صحيحة عندما $n=1$.

لنفرض أن العبارة صحيحة لكل $k<n$. الآن، باستخدام التمرين (٦) نجد أن:

$$(2^m-1,2^n-1)=(2^m-1,2^n-2^m)=(2^m-1,(2^{n-m}-1)2^m)$$
$$=(2^m-1,2^{n-m}-1)=2^{(m,n-m)}-1=2^{(m,n)}-1$$

ونخلص إلى صحة العبارة عند n △

تمارين (١,٣)

في كل من التمارين من (١) إلى (٥) احسب (a,b).

(١) $a=512$ ، $b=320$.

(٢) $a=963$ ، $b=657$.

(٣) $a=252$ ، $b=198$.

(٤) $a=1636$ ، $b=1128$.

(٥) $a=10672$ ، $b=4147$.

(٦) اكتب القاسم المشترك الأعظم لكل زوج من الأعداد في التمارين من (١) إلى (٥) كتركيب خطي للعددين a و b.

(٧) جد $(105, 140, 350)$ ثم اكتبه كتركيب خطي للأعداد.

(٨) جد $(570, 810, 495, 125)$ ثم اكتبه كتركيب خطي للأعداد.

(٩) جد $(116, 248, 148, 152)$ ثم اكتبه كترتيب خطي للأعداد.

(١٠) جد $(1131, 594, 2907, 1517)$ ثم اكتبه كتركيب خطي للأعداد.

(١١) جد $x,y,z\in\mathbb{Z}$ بحيث يكون $11x+19y+3z=1$.

(١٢) جد $x,y,z,w\in\mathbb{Z}$ بحيث يكون $30x+60y+165z+120w=15$.

(١٣) هل تستطيع إيجاد عددين $a,b\in\mathbb{Z}$ بحيث يكون $a+b=500$ و $(a,b)=7$؟

(١٤) إذا كان $a,b,c,d\in\mathbb{Z}^+$ حيث $b\neq d$ و $(a,b)=(c,d)=1$ فأثبت أن

$$\frac{a}{b}+\frac{c}{d}\notin\mathbb{Z}.$$

(١٥) أثبت أن $(a,a+1)=1$ لكل $a\in\mathbb{Z}$.

(١٦) أثبت أن $(n!+1,(n+1)!+1)=1$.

(١٧) أثبت أن $(n,n-2)=1$ حيث n عدد صحيح فردي.

(١٨) أثبت أن $(6k+5,7k+6)=1$ لكل $k\in\mathbb{Z}^+$.

(١٩) أثبت أن 2 يقسم n^2+n لكل $n\in\mathbb{Z}^+$.

(٢٠) أثبت أن 2 يقسم n^2-n لكل $n\in\mathbb{Z}^+$.

(٢١) أثبت أن 6 يقسم n^3-n لكل $n\in\mathbb{Z}^+$.

(٢٢) أثبت أن 5 يقسم n^5-n لكل $n\in\mathbb{Z}^+$.

(٢٣) أثبت أن 7 يقسم $2^{3n}-1$ لكل $n\in\mathbb{Z}^+$.

(٢٤) أثبت أن 8 يقسم $3^{2n}+7$ لكل $n\in\mathbb{Z}^+$.

(٢٥) أثبت أن 64 يقسم $7^{2n}+16n-1$ لكل $n\in\mathbb{Z}^+$.

(٢٦) أثبت أن 24 يقسم $2\times7^n+3\times5^n-5$ لكل $n\in\mathbb{Z}^+$.

(٢٧) أثبت أن 14 يقسم $3^{4n+2}+5^{2n+1}$ لكل $n\in\mathbb{Z}^+$.

(٢٨) أثبت أن مرتبة الآحاد للعدد 16^n هي 6 لكل $n\in\mathbb{Z}^+$.

(٢٩) أثبت أن 133 يقسم $(11)^{n+2}+(12)^{2n+1}$ لكل $n\in\mathbb{Z}^+$.

(٣٠) أثبت أن 9 يقسم $n^3+(n+1)^3+(n+2)^3$ لكل $n\in\mathbb{Z}^+$.

(٣١) إذا كان العدد $n>1$ يحتوي على العدد 1 في جميع مراتبه العشرية فأثبت أن n لا يمكن أن يكون مربعاً كاملاً.

(٣٢) أثبت وجود عدد غير منته من الأعداد التي تكون مربعاً كاملاً ومكعباً في الوقت نفسه.

(٣٣) إذا كان $(a,b)=1$ فأثبت أن $(a+b,a-b)=2$ أو أن $(a+b,a-b)=1$.

(٣٤) إذا كان $(a,b)=1$ وكان $c \mid (a+b)$ فأثبت أن $(a,b)=(a,c)=1$.

(٣٥) إذا كان $(b,c)=1$ وكان $a \mid b$ فأثبت أن $(a,c)=1$.

(٣٦) إذا كان $(n,5)=1$ فأثبت أن 125 يقسم $n^{100}-1$ لكل $n \geq 1$.

(٣٧) إذا كان $(n,10)=1$ فأثبت أن 1000 يقسم $n^{100}-1$ لكل $n \geq 1$.

(٣٨) أثبت أن $a-b$ يقسم a^n-b^n لكل $n \geq 1$.

(٣٩) أثبت أن $a+b$ يقسم a^n+b^n لكل عدد صحيح فردي n.

(٤٠) أثبت أن $a+b$ يقسم a^n-b^n لكل عدد صحيح زوجي n.

(٤١) أثبت 100 يقسم $11^{10}-1$.

(٤٢) إذا كان $a \mid b$ و $c \mid d$ فهل من الضروري أن يكون $(a+c) \mid (b+d)$؟

(٤٣) إذا كان $b \mid c$ فأثبت أن $(a+c,b)=(a,b)$.

(٤٤) جد عدد الأعداد الصحيحة الموجبة التي لا تزيد عن 1000 وتقبل القسمة على 25.

(٤٥) جد عدد الأعداد الصحيحة الموجبة التي لا تزيد عن 1000 وتقبل القسمة على 3 أو 5.

(٤٦) جد عدد الأعداد الصحيحة الموجبة التي لا تزيد عن 1000 ولا تقبل القسمة على 3 أو 5.

(٤٧) جد عدد الأعداد الصحيحة الموجبة التي لا تزيد عن 1000 وتقبل القسمة على 3 ولكن لا تقبل القسمة على 4.

(٤٨) (أ) أثبت أن حاصل ضرب عددين على الصورة $4k+1$ هو أيضاً على الصورة $4k+1$.

(ب) أثبت أن حاصل ضرب عددين على الصورة $4k+3$ يجب أن يكون على الصورة $4k+1$.

في التمارين من (٤٩) إلى (٥٤) ، $\{f_n\}$ هي متتالية فيبوناتشي .

(٤٩) أثبت أن f_n زوجي إذا وفقط إذا كان $3 \mid n$.

(٥٠) أثبت أن $3 \mid f_n$ إذا وفقط إذا كان $4 \mid n$.

(٥١) أثبت أن $4 \mid f_n$ إذا وفقط إذا كان $6 \mid n$.

(٥٢) (أ) أثبت أن $f_n = 5f_{n-1} + 3f_{n-5}$ لكل $n \geq 6$.

(ب) إستخدم الفقرة (أ) لإثبات أن $5 \mid f_n$ إذا كان $5 \mid n$.

(٥٣) إذا كان $m = qn + r$ فأثبت أن $(f_m, f_n) = (f_r, f_n)$.

(٥٤) إذا كان $d = (m,n)$ فأثبت أن $(f_m, f_n) = f_d$.

(٥٥) إذا كان $(a_i, b) = 1$ لكل $i = 1, \ldots, n$ فأثبت أن $(a_1 a_2 \ldots a_n, b) = 1$.

(٥٦) إذا كان $m,n \in \mathbb{Z}^+$ وكان $a > 1$ فأثبت أن $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

(٥٧) أثبت أن :

$$[a, a+2] = \begin{cases} a(a+2)/2, & a \text{ زوجي} \\ a(a+2), & a \text{ فردي} \end{cases}$$

(١,٤) المعادلات الديوفنتية الخطية
Linear Diophantine Equations

توصلنا في أثناء دراستنا لوجود القاسم المشترك لعددين a و b إلى إمكانية كتابته كتركيب خطي للعددين a و b. أي $(a,b) = ax + by$ حيث $x,y \in \mathbb{Z}$. والسؤال الذي يطرح نفسه هنا هو: إذا كان $a,b,c \in \mathbb{Z}$ فهل نستطيع إيجاد $x,y \in \mathbb{Z}$ حيث $ax + by = c$؟ تسمى مثل هذه المعادلة، معادلة ديوفنتية خطية في متغيرين.

سنقدم هنا شرطاً كافياً ولازماً لوجود حل لهذه المعادلة وفي حالة وجود حل نقدم صيغة لوصف جميع الحلول. في ختام البند نناقش مسألة إيجاد حلول معادلة ديوفنتية في أكثر من متغيرين.

مبرهنة (١,٢٠)

يوجد حل للمعادلة الديوفنتية الخطية $ax+by=c$ إذا وفقط إذا كان $d=(a,b)$ يقسم c. وإضافة إلى ذلك ، إذا كان x_0,y_0 حلاً للمعادلة فإن الحل العام يكون على الصورة:

$$x=x_0+k\,(b/d)\ ,\ y=y_0-k\,(a/d)$$ حيث $k\in\mathbb{Z}$.

البرهان

لنفرض أولاً أن $d\mid c$. عندئذ، توجد $n,m,r\in\mathbb{Z}$ حيث $c=dr$ و $d=am+bn$. وبضرب المعادلة الأخيرة في العدد r نجد أن:

$$a(mr)+b(nr)=dr=c.$$

وبالتالي فإن $x=mr$ و $y=nr$ حل للمعادلة. ولبرهان العكس، نفرض أن x_0,y_0 حل للمعادلة. أي: $ax_0+by_0=c$. وبما أن $d\mid a$ و $d\mid b$ فمن الواضح أن $d\mid c$. ولإيجاد الحل العام نفرض أن x_0,y_0 حل للمعادلة. ونبرهن أن أي حل آخر للمعادلة يجب أن يكون على الصورة المطلوبة. ولذا نفرض أن x_1,y_1 حل آخر. عندئذ: $ax_1+by_1=c=ax_0+by_0$. ونرى أن:

$$a(x_1-x_0)=-b(y_1-y_0). \qquad (١)$$

وبما أن $d=(a,b)$ فهناك $r,s\in\mathbb{Z}$ حيث $a=dr$ و $b=ds$ و $(r,s)=1$. بالتعويض في المعادلة (١) وقسمة طرفي الناتج على d نحصل على:

$$r(x_1-x_0)=-s(y_1-y_0) \qquad (٢)$$

ولذا فإن $s\mid r(x_1-x_0)$. وبهذا يكون $s\mid(x_1-x_0)$ لأن $(r,s)=1$. أي أن $x_1-x_0=ks$ حيث $k\in\mathbb{Z}$. وبالتعويض في المعادلة (٢) نحصل على $y_1-y_0=-kr$ وبالتالي فإن:

$$x_1=x_0+ks=x_0+k\,(b/d)$$

◆ $y_1=y_0-kr=y_0-k\,(a/d)$ حيث $k\in\mathbb{Z}$

ملحوظة

لإيجاد أحد حلول (إن وجد) المعادلة الديوفنتية الخطية، نستخدم خوارزمية إقليدس أو المبرهنة (١,١٤) لوضع القاسم المشترك كتركيب خطي للعددين ومن ثم نضرب بعدد مناسب. ولإيجاد جميع الحلول نعوض في الصيغة المقدمة في المبرهنة (١,٢٠). نوضح ذلك في المثال التالي:

مثال (١,٢٢)

جد جميع حلول المعادلة الديوفنتية : $1485x+1745y=15$.

الحل

باستخدام خوارزمية إقليدس نجد أن:

$$1745=1\times1485+260$$
$$1485=5\times260+185$$
$$260=1\times185+75$$
$$185=2\times75+35$$
$$75=2\times35+5$$
$$35=7\times5+0$$

ولذا فإن $(1745,1485)=5$. وبما أن 5 يقسم 15. فللمعادلة حل. لإيجاد أحد الحلول نضع القاسم المشترك الأعظم كتركيب خطي للعددين 1745، 1485 فنجد:

$$\begin{aligned}5&=75-2\times35\\&=75-2(185-2\times75)\\&=-2\times185+5\times75\\&=-2\times185+5(260-1\times185)\\&=5\times260-7\times185\end{aligned}$$

$$=5\times260-7(1485-5\times260)$$
$$=-7\times1485+40\times260$$
$$=-7\times1485+40(1745-1\times1485)$$
$$5=-47\times1485+40\times1745$$

وبضرب المعادلة الأخيرة بالعدد 3 نجد أن :

$$1485(-141)+1745(120)=15$$

ولذا فإن $x_0=-141$ و $y_0=120$ حل للمعادلة. أما الحل العام فهو:

$$x=-141+\frac{1745}{5}k=-141+349k$$
$$y=120-\frac{1485}{5}k=120-297k$$

حيث $k\in\mathbb{Z}$ □

ملحوظة

في كثير من المسائل التطبيقية التي تستخدم المعادلات الديوفنتية ينصب اهتمامنا على إيجاد قيم صحيحة موجبة للمجاهيل.

مثال (١,٢٣)

جد جميع الحلول الموجبة للمعادلة الديوفنتية : $18x+5y=48$.

الحل

سنستخدم في هذا المثال خوارزمية إقليدس الموسعة لوضع القاسم المشترك كتركيب خطي للعددين 5 و 18. الآن باستخدام خوارزمية القسمة نجد أن:

$$18=3\times5+3$$
$$5=1\times3+2$$
$$3=1\times2+1$$
$$2=2\times1+0$$

ولذا فإن $q_1=3, q_2=1, q_3=1$. الآن ، نستخدم الجدول التالي لإيجاد قيم s_j و t_j المبينة في خوارزمية إقليدس الموسعة:

j	q_j	$s_j=s_{j-2}-q_{j-1}s_{j-1}$	$t_j=k_{j-2}-q_{j-1}t_{j-1}$
0		1	0
1	3	0	1
2	1	$s_2=1-3\times 0=1$	$t_2=0-3\times 1=-3$
3	1	$s_3=0-1\times 1=-1$	$t_3=1-1\times(-3)=4$
4		$s_4=1-1\times(-1)=2$	$t_4=-3-1\times 4=-7$

ولذا فإن: $18(2)+5(-7)=1$. وبضرب المعادلة بالعدد 48 نجد أن:
$18(96)+5(-336)=48$. فيكون الحل العام للمعادلة هو:

$$x=96+5k$$
$$y=-336-18k$$

حيث $k\in\mathbb{Z}$.

ولإيجاد الحلول الموجبة نضع $x>0$ و $y>0$ فنجد أن:

$$-19.2=\frac{-96}{5}<k<\frac{-336}{18}=-18.6$$

ولذا فإن $k=-19$. وبالتالي فإن:

$x=96+5(-19)=1$ و $y=-336-18(-19)=6$.

ونخلص إلى أن الحل الموجب الوحيد هو $x=1$ و $y=6$ □

نتنقل الآن لمعالجة المعادلات الديوفنتية الخطية في أكثر من متغيرين. والمبرهنة التالية تقدم لنا شرطاً كافياً ولازماً لوجود حل لهذه المعادلة.

مبرهنة (١,٢١)

يوجد حل للمعادلة الديوفنتية $a_1x_1+a_2x_2+\ldots+a_nx_n=c$ حيث $n\geq 2$

إذا فقط إذا كان $(a_1,a_2,\dots,a_n)=d$ يقسم c.

البرهان

إذا كان $d\mid c$ فإن $c=dr$ حيث $r\in\mathbb{Z}$. باستخدام المبرهنة (١,١٨) توجد $y_1,y_2,\dots,y_n\in\mathbb{Z}$ حيث $d=a_1y_1+a_2y_2+\dots+a_ny_n$. وبضرب المعادلة بالعدد r نحصل على $c=dr=a_1(ry_1)+\dots+a_n(ry_n)$. ونرى أن $ry_1,\dots,ry_n$ حل للمعادلة. لبرهان العكس، نفرض أن $y_1,\dots,y_n$ حل للمعادلة. عندئذ $a_1y_1+\dots+a_ny_n=c$. وبما أن $d\mid a_i$ لكل i فإن $d\mid c$ ◆

يمكن معالجة مسألة إيجاد الحل العام للمعادلة الديوفنتية في أكثر من متغيرين باتباع طريقة تعتمد على اختزال المعادلة إلى واحدة تحتوي على متغيرين فقط وإيجاد الحل لهذه المعادلة ثم استخدامه لحل المعادلة الأصلية (أنظر التمرين المحلول (٥) في نهاية البند). ولكننا سنتبع طريقة أخرى استخدمها الرياضي أويلر (*Euler*) ولذلك تعرف بإسمه، وهي طريقة عملية وسهلة الاستخدام تعتمد على أن مجموعة الأعداد الصحيحة مغلقة بالنسبة لعمليتي الجمع والطرح، كما أن هذه الطريقة يمكن استخدامها لحل معادلات في متغيرين. والخوارزمية التالية تصف لنا هذه الطريقة:

لتكن $a_1x_1+a_2x_2+\dots+a_nx_n=c$ معادلة ديوفنتية حيث $d=(a_1,a_2,\dots,a_n)$ يقسم c. بقسمة طرفي المعادلة على d نحصل على معادلة مكافئة يكون القاسم المشترك الأعظم لمعاملاتها يساوي 1. ولذا فإننا سنفترض أن $d=1$ دون التأثير على عمومية الخوارزمية. لإيجاد الحل العام ننفذ الخطوات التالية:

(١) نكتب $a_1x_1=c-a_2x_2-\dots-a_nx_n$، حيث $|a_1|\le|a_2|\le\dots\le|a_n|$.

(٢) نقسم طرفي المعادلة في الخطوة (١) على a_1 لنحصل على

$$x_1=\frac{c}{a_1}-\frac{a_2}{a_1}x_2-\dots-\frac{a_n}{a_1}x_n$$

(٣) نستخدم خوارزمية القسمة لنجد:

$$c=q_1a_1+r_1\ ,\ a_2=q_2a_1+r_2\ ,\ \dots\ ,\ a_n=q_na_1+r_n$$

ولذا فإننا نستطيع أن نكتب:

$$x_1 = (q_1 - q_2x_2 - \dots - q_nx_n) + (\frac{r_1}{a_1} - \frac{r_2}{a_1}x_2 - \dots - \frac{r_n}{a_1}x_n)$$

(٤) نضع $t_1 = \frac{r_1}{a_1} - \frac{r_2}{a_1}x_2 - \dots - \frac{r_n}{a_1}x_n$

لاحظ أنه لكي يكون للمعادلة حل ينبغي أن يكون $t_1 \in \mathbb{Z}$.

(٥) نعيد كتابة الخطوة (٤) كالتالي:

$$t_1a_1 = r_1 - r_2x_2 - \dots - r_nx_n$$

(٦) نكرر الخطوات (١) إلى (٥) على المعادلة التي وجدناها في الخطوة (٥) لنصل في النهاية إلى معادلة، معامل أحد متغيراتها يساوي 1 ثم نحصل على الحل العام بالتعويض العكسي.

ملحوظة

تؤدي طريقة أويلر دائماً إلى الحصول على معادلة، معامل أحد متغيراتها يساوي 1 وذلك لأن خطوات الحل تتبع الخوارزمية الموصوفة بعد المثال (١,١٩) لإيجاد القاسم المشترك الأعظم للأعداد $a_1, a_2, \dots, a_n$ والذي يظهر كمعامل لأحد المتغيرات في المعادلة الواردة في آخر خطوة من خطوات الحل.

مثال (١,٢٤)

جد الحل العام للمعادلة الديوفنتية $9x - 18y + 48z = 3$.

الحل

لاحظ أن $d = (9,18,48) = 3$ يقسم 3. ولذا فإنه يوجد حل للمعادلة. وبقسمة طرفي المعادلة على 3 نحصل على المعادلة المكافئة $3x - 6y + 16z = 1$.

الآن، ننفذ الخطوات التالية:

(١) $3x = 6y - 16z + 1$.

(٢) $x = 2y - 5z + \frac{1}{3} - \frac{1}{3}z$.

(٣) نضع $t_1 = \frac{1}{3} - \frac{1}{3}z$.

(٤) $3t_1 = 1 - z$.

(٥) $z = 1 - 3t_1$.

نتوقف الآن لأن معامل z يساوي 1.

بوضع $y = t_2$ والتعويض العكسي نحصل على الحل العام:

$$x = 2t_2 - 5(1 - 3t_1) + t_1 = -5 + 16t_1 + 2t_2$$

$$y = t_2$$

$$z = 1 - 3t_1$$

حيث $t_1, t_2 \in \mathbb{Z}$ □

(١,٤,١) تمارين محلولة *(Solved Exercises)*

تمرين (١)

تظهر هذه المسألة على صيغة لغز بصورة أو أخرى في أدبيات معظم الشعوب: افرض أنك أعطيت مائة ريال وطلب منك أن تشتري بها مائة من الأغراض المكونة من أقلام ومساطر وأوراق. إذا كان ثمن القلم الواحد 5 ريالات، وثمن المسطرة الواحدة ريالين وثمن كل عشرة ورقات ريالاً واحداً. فكم تستطيع تشتري من كل نوع؟

الحل

لنفرض أن x ، y ، z هو عدد الأقلام والمساطر والأوراق على التوالي.

عندئذ يكون لدينا المعادلتين:

$$5x+2y+\frac{z}{10}=100$$
$$x+y+z=100$$

لاحظ أولاً أن $10 \mid z$. ولذا فإن $z=10w$ حيث $w\in\mathbb{Z}$. ولذا يكون لدينا المعادلتين:

$$5x+2y+w=100$$
$$x+y+10w=100$$

وبضرب المعادلة الثانية بالعدد 2 وطرحها من المعادلة الأولى نحصل على:

$$3x-19w=-100$$

وبحل هذه المعادلة نجد أن الحل العام لها هو :

$$x=-27+19k \text{ ، } w=1+3k \text{ حيث } k\in\mathbb{Z}$$

وعليه فإن $z=10w=10+30k$ وأن $y=100-x-z=117-49k$

إذن الحل العام هو :

$$x=-27+19k$$
$$y=117-49k$$
$$z=10+30k$$

ولإيجاد الحلول الموجبة نضع $x>0$ ، $y>0$ ، $z>0$ فنجد أن $k>1\frac{8}{19}$ ، $k>-\frac{1}{3}$ ، $k<2\frac{19}{49}$. ولذا فإن $k=2$. وبالتالي فإن الحل الموجب الوحيد هو:

$$x=11 \text{ ، } y=19 \text{ ، } z=70 \quad \triangle$$

تمرين (٢)

باسكارا *(Bhaskara)* ، عالم هندي عاش في القرن الثاني عشر الميلادي صاحب الكتاب المشهور "الجميلة" *(Lilavati)* وهو عبارة عن مجموعة من الألغاز على شكل شعر كان يقرأها لإبنته المكتئبة للترويح عنها. وهذه احدى المسائل التي وردت في الكتاب:

إن كان ثمن خمسة حمامات هو ثلاثة دراهم، ثمن سبعة غرانيق هو خمسة دراهم، ثمن تسعة إوزات هو سبعة دراهم، وثمن ثلاثة طواويس هو تسعة دراهم. إليك مائة درهم، اشتري بها مائة من هذه الطيور لإرضاء الأميرة. ما عدد كل نوع من الطيور؟

الحل

إذا فرضنا أن x ، y ، z ، w هو عدد الحمام، الغرانيق، الإوزات ، الطواويس على التوالي فإن:

$$x+y+z+w=100$$

$$\frac{3}{5}x+\frac{5}{7}y+\frac{7}{9}z+3w=100$$

بضرب المعادلة الأولى بالعدد 3 وطرح المعادلة الثانية من الناتج نحصل على:

$$\frac{3}{5}x+\frac{4}{7}y+\frac{5}{9}z=50.$$

أي: $$189x+180y+175z=15750$$

لاحظ أن $(189,180,175)=1$. باستخدام طريقة أويلر فإننا نحصل على الحل العام:

$$x=5t_1$$

$$y=35t_2-14t_1$$

$$z=9t_1-36t_2+90$$

$$w=t_2+10$$

وبما أننا نود أن تكون x ، y ، z ، w موجبة فإننا نجد أن $t_1 > 0$ وأن $0 < t_2 < \frac{20}{3}$. ولذا فإن قيم t_2 هي: 1, 2, 3, 4, 5, 6.

عند $t_2 = 1$ نجد أن: $x = 5t_1$ ، $y = 35 - 14t_1$ ، $z = 9t_1 - 36t_2 + 45$ ، $w = 11$.

وبما أن $y > 0$ فإن $t_1 < \frac{35}{14}$. ولذا فإن: $t_1 = 1,2$.

وبالمثل عند $t_2 = 2$ نجد أن: $t_1 = 1, 2, 3, 4$.

عند $t_2 = 3$ نجد أن: $t_1 = 3, 4, 5, 6, 7$.

عند $t_2 = 4$ نجد أن: $t_1 = 7, 8, 9$.

عند $t_2 = 5$ نجد أن: $t_1 = 11, 12$.

عند $t_2 = 6$: لا توجد قيم لـ t_1.

ولذا فإننا نخلص إلى وجود 16 حل للمسألة يبينها الجدول التالي:

t_2	t_1	x	y	x	w
1	1	5	21	63	11
1	2	10	7	72	11
2	1	5	56	27	12
2	2	10	42	36	12
2	3	15	28	45	12
2	4	20	14	54	12
3	3	15	63	9	13
3	4	20	49	18	13
3	5	25	35	27	13
3	6	30	21	36	13
3	7	35	7	45	13
4	7	35	42	9	14
4	8	40	28	18	14
4	9	45	14	27	14
5	11	55	21	9	15
5	12	60	7	18	15

△

تمرين (٣)

جد جميع حلول المعادلة الديوفنتية $(8x+7y)(6x+15y)=129$.

الحل

لنفرض أن $6x+15y=a$ و $8x+7y=b$ عندئذ، $39y=4a-3b$. وبما أن: $ab=129=3\times 43$ وأن $a\mid 3$ و $a\mid 129$ فـإن $a=\pm 129$ أو أن $a=\pm 3$.

ومنه فإن $b=\pm 1$ أو أن $b=\pm 43$.

إذا كان $a=\pm 129$ و $b=\pm 1$ فإن $39y=4a-3b$ ليس لها حل. ولـذا فـإن $a=\pm 3$ و $b=\pm 43$.

إذا كان $a=3$ و $b=43$ فإن $y=-3$. ومنه فإن $x=8$.

وإذا كان $a=-3$ و $b=-43$ فإن $y=3$. ومنه فإن $x=-8$.

وإذا كان $a=\pm 3$ و $b=\mp 43$ فليس هناك حل.

إذن، الحلان الوحيدان هما $(x=8$ و $y=-3)$ ، $(x=-8$ و $y=3)$ △

تمرين (٤)

جد جميع الحلول الصحيحة للمعادلة الديوفنتية $\frac{1}{x}+\frac{1}{y}=\frac{1}{14}$.

الحل

لاحظ أن المعادلة تكافئ $xy=14x+14y$. أي أن :

$xy-14x-14y+196=196$. أو أن $(x-14)(y-14)=196$. على هذا فإن $(x-14)\mid 196$ و $(y-14)\mid 196$. فنستنتج أن:

$$(x-14,y-14)\in\{((\pm 1,\pm 196),(\pm 2,\pm 98),(\pm 4,\pm 49),(\pm 7,\pm 28),$$
$$(\pm 14,\pm 14),(\pm 28,\pm 7),(\pm 49,\pm 4),(\pm 98,\pm 2),(\pm 196,\pm 1)\}$$

ونخلص إلى أن جميع الحلول هي:

$\{(15,210),(16,112),(18,63),(21,42),(28,28),(42,21),(63,18),$
$(112,16),(210,15),(13,-182),(12,-84),(10,-35),(7,-14),(-14,7),$
$(-35,10),(-84,12),(-182,13)\}$ △

تمرين (٥)

لتكن $a_1x_1+a_2x_2+\ \dots\ +a_nx_n=c$ (١)

معادلة ديوفنتية خطية حيث $n\geq 3$ ، $a_i\neq 0$ لكل i. وليكن $d=(a_{n-1},a_n)$ ، $\beta=a_n/d$ ، $\delta=-a_{n-1}/d$. وليكن α و γ حلاً للمعادلة الديوفنتية $\alpha\delta-\beta\gamma=1$ وليكن :

$$x_{n-1}=\alpha y+\beta z$$
$$x_n=\gamma y+\delta z$$

(أ) أثبت أن :

$a_1x_1+a_2x_2+\ \dots\ +a_{n-2}x_{n-2}+(a_{n-1}\alpha+a_n\gamma)y=c$ (٢)

(ب) أثبت أن المعادلة (١) قابلة للحل إذا وفقط إذا كانت المعادلة (٢) قابلة للحل.

الحل

(أ) لاحظ أن :

$$a_1x_1+a_2x_2+\dots+a_{n-2}x_{n-2}+a_{n-1}x_{n-1}+a_nx_n=c$$
$$\Rightarrow a_1x_1+a_2x_2+\dots+a_{n-2}x_{n-2}+a_{n-1}(\alpha y+\beta z)+a_n(\gamma y+\delta z)=c$$
$$\Rightarrow a_1x_1+a_2x_2+\dots+a_{n-2}x_{n-2}+a_{n-1}(\alpha y+\frac{an}{d}z)+a_n(\gamma y-\frac{a_{n-1}}{d}z)=c$$
$$\Rightarrow a_1x_1+a_2x_2+\ \dots\ +a_{n-2}x_{n-2}+(a_{n-1}\alpha+a_n\gamma)y=c$$

(ب) لاحظ أولاً أن:

$$a_{n-1}\alpha+a_n\gamma=-d\alpha\delta+d\beta\gamma=-d(\alpha\delta-\beta\gamma)=-d$$

وبما أن $(a_1,a_2,\ \dots\ ,a_n)=(a_1,a_2,\ \dots\ ,a_{n-2},d)$ فإننا نخلص إلى أن المعادلة (١) قابلة للحل إذا وفقط إذا كانت المعادلة (٢) قابلة للحل △

تمرين (٦)

استخدم التمرين (٥) لحل المعادلة الديوفنتية:

$$9x_1 - 18x_2 + 48x_3 = 3$$

الحل

لاحظ أولاً أن:

$$d = (18,48) = 6 \ ، \ \beta = \frac{48}{6} = 8 \ ، \ \delta = \frac{-(-18)}{6} = 3$$

وبحل المعادلة الديفونتية $3\alpha - 8\gamma = 1$ نجد أن أحد الحلول هـو: $\alpha = 3$ ، $\gamma = 1$. وعليه فإن :

$$x_2 = \alpha y + \beta z = 3y + 8z$$
$$x_3 = \gamma y + \delta z = y + 3z$$

ومنه فإن:

$$9x_1 - 18x_2 + 48x_3 = 3 \Rightarrow 9x_1 - 6y = 3$$

وبحل المعادلة الديوفنتية $9x_1 - 6y = 3$ نجد أن:

$$x_1 = 1 - 2t_1$$
$$y = 1 - 3t_1$$

وبوضع $z = t_2$ نستنتج أن الحل العام للمعادلة الديوفنتية $9x_1 - 18x_2 + 48x_3 = 3$ هو:

$$x_1 = 1 - 2t_1$$
$$x_2 = 3y + 8z = 3 - 9t_1 + 8t_2$$
$$x_3 = y + 3z = 1 - 3t_1 + 3t_2$$

△

تمارين (١,٤)

في التمارين من (١) إلى (١٠) بين ما إذا كان للمعادلة الديوفنتية المعطاة حل وإذا كان للمعادلة حل فجد جميع الحلول.

(١) $2x+5y=11$
(٢) $56x+72y=40$
(٣) $60x+18y=97$
(٤) $172x+20y=1000$
(٥) $48x-438y=156$
(٦) $15x+7y=210$
(٧) $91x+221y=1053$
(٨) $165x+418y=121$
(٩) $803x+154y=33$
(١٠) $57x-99y=77$

في التمارين من (١١) إلى (٢٠) جد جميع الحلول الصحيحة الموجبة للمعادلة الديوفنتية المعطاة.

(١١) $62x+11y=788$
(١٢) $32x+55y=771$
(١٣) $2x+3y=25$
(١٤) $31x+21y=1770$
(١٥) $17x-15y=5$
(١٦) $11x+7y=200$
(١٧) $10x-7y=-17$
(١٨) $30x+17y=300$
(١٩) $123x+360y=99$
(٢٠) $158x-57y=7$

في التمرينين (٢١) و (٢٢) جد جميع الحلول للمعادلة الديوفنتية.

(٢١) $15x+12y+30z=24$
(٢٢) $7x+3y-20z=23$

(٢٣) جد جميع الحلول الموجبة للمعادلة الديوفنتية:

$$7x+5y+15z+12w=149$$

(٢٤) جد جميع الحلول الصحيحة للنظام:

$$3x-6y+16z=1$$
$$2x+5y-6z=2$$

(٢٥) جد جميع الحلول الصحيحة الموجبة للنظام:

$$7x+3y+19z=2530$$
$$8x+6y+33z=2753$$

(٢٦) جد جميع الحلول الصحيحة الموجبة للنظام :

$$2x+3y+5z=201$$

$$3x+5y+7z=315$$

(٢٧) إذا كانت وجبة رجل في مطعم تكلف 48 ريالاً ووجبة إمرأة تكلف 36 ريالاً ووجبة طفل تكلف 4 ريالات. إذا علمت أن 41 شخصاً تناولوا وجبة في المطعم وكانت الفاتورة 480 ريالاً فجد عدد كل من الرجال والنساء والأطفال.

(٢٨) جد أصغر عدد صحيح موجب M بحيث يكون باقي قسمته على 11 هو 3، باقي قسمته على 19 هو 5 وباقي قسمته على 29 هو 10.

(٢٩) اشترى أحدهم مائة من الأبقار والخرفان والماعز والأرانب ودفع 10000 ريال ثمناً لها. إذا كان سعر البقرة يساوي 1000 ريال وسعر الخروف يساوي 500 ريال وسعر الماعز يساوي 200 ريال وسعر الأرنب يساوي 50 ريال. فكم عدد كل منها؟

(٣٠) تتكون عمارة سكنية من نوعين من الشقق، شقق ممتازة، الأجرة الشهرية لكل منها هو 1230 ريالاً، وشقق عادية، الأجرة الشهرية لكل منها هو 870 ريالاً. فإذا كانت جميع الشقق مؤجرة وكان الدخل الشهري الكلي للعمارة هو 87330 ريالاً، فكم عدد شقق العمارة من كل نوع؟

(٣١) استخدم طريقة التمرين المحلول (٥) لإيجاد جميع حلول كل من المعادلات الديوفنتية التالية:

(أ) $15x_1+10x_2+6x_3=61$ (ب) $5x_1-2x_2-4x_3=10$

(ج) $x_1+2x_2+3x_3=13$ (د) $-7x_1-2x_2+3x_3+2x_4=16$

(١,٥) تمثيل الأعداد الصحيحة
Representations of Integers

لقد استخدم الإنسان في تاريخه الطويل أنظمة عددية مختلفة لعل أفضلها هو النظام العشري *(decimal system)* فهو نظام يساعد على إجراء كثير من العمليات الحسابية بسهولة وكان له فضل كبير في تطور الرياضيات. يستخدم النظام العشري الرموز 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 . التي تسمى بأرقام النظام *(digits)*. وإذا عرَّفنا الأساس *(base)* في أي نظام عددي بأنه عدد الأرقام أو الرموز المختلفة المستخدمة فيه، فإن أساس نظامنا العشري حينئذ هو عشرة.

النظام العشري ليس بالنظام العددي الوحيد ولكننا تعودنا على استخدامه (ربما لأن لدينا عشرة أصابع)، فلقد سبق للبابليين أن استخدموا نظاماً أساسه 60، كذلك استخدم المايانيون (شعوب عاشت في أمريكا الوسطى والمكسيك) نظاماً أساسه 20. والحاسبات الآلية الآن تستخدم النظام الثنائي *(binary system)*.

المبرهنة التالية تطبيق على خوارزمية القسمة وهي تثبت لنا أن أي عدد صحيح أكبر من الواحد يصلح أن يكون أساساً لنظام عددي.

مبرهنة (١,٢٢)

إذا كان k عدداً صحيحاً أكبر من الواحد فإننا نستطيع كتابة أي عدد صحيح موجب N بطريقة وحيدة على الصورة:

$$N = a_m k^m + a_{m-1} k^{m-1} + \ldots + a_2 k^2 + a_1 k + a_0$$

حيث $0 \le a_i \le k-1$ لكل $i = 0,1, \ldots, m$. $a_m \neq 0$

البرهان

باستخدام خوارزمية القسمة نستطيع إيجاد عددين صحيحين q_1 و a_0 يحققان العلاقة: $N = q_1 k + a_0$ ، $0 \le a_0 < k$.

إذا كان $q_1 \geq k$ ، فإننا نستخدم خوارزمية القسمة مرة أخرى لنحصل على عددين صحيحين q_2 و a_1 يحققان العلاقة:

$$q_1 = q_2 k + a_1 \quad ، \quad 0 \leq a_1 < k .$$

وبالتعويض عن قيمة q_1 في المعادلة الأولى نحصل على المساواة:

$$N = (q_2 k + a_1)k + a_0 = q_2 k^2 + a_1 k + a_0$$

وبالطريقة نفسها فإننا سوف نحصل في المرحلة m على عددين q_m و a_{m-1} بحيث يكون:

$$q_{m-1} = q_m k + a_{m-1} \quad ، \quad 0 \leq a_{m-1} < k$$

وبما أن $q_1 > q_2 > \ldots > 0$ متتالية تناقصية سنصل إلى مرحلة يكون فيها $q_m < k$. عندئذ نتوقف ونجعل $a_m = q_m$ وبذلك نحصل على المساواة:

$$N = a_m k^m + a_{m-1} k^{m-1} + \ldots + a_2 k^2 + a_1 k + a_0$$

ولبرهان الوحدانية ، نفرض أن:

$$N = a_m k^m + a_{m-1} k^{m-1} + \ldots + a_1 k + a_0 = b_n k^n + b_{n-1} k^{n-1} + \ldots + b_1 k + b_0$$

تمثيلان مختلفان، ولنفرض أن $m \geq n$. بإضافة معاملات صفرية إن احتاج الأمر نستطيع أن نفرض أن $m = n$. من المعادلة أعلاه نحصل على:

$$(a_m - b_m)k^m + (a_{m-1} - b_{m-1})k^{m-1} + \ldots + (a_1 - b_1)k + (a_0 - b_0) = 0 \quad (١)$$

وبما أن التمثيلين مختلفان فإنه يوجد على الأقل i حيث $a_i - b_i \neq 0$. وعلى افتراض أن $a_i - b_i$ هو أول معامل غير صفري في المعادلة (١) فإننا نجد بحذف الحدود ذات المعاملات الصفرية ونقل الحد $(a_i - b_i)k^i$ إلى الطرف الأيمن في العلاقة (١):

$$(a_m - b_m)k^m + (a_{m-1} - b_{m-1})k^{m-1} + \ldots + (a_{i+1} - b_{i+1})k^{i+1} = -(a_i - b_i)k^i$$

وبالقسمة على k^i وأخذ k عامل مشترك من الطرف الأيسر نحصل على:

$$k[(a_m - b_m)k^{m-i-1} + \ldots + (a_{i+1} - b_{i+1})] = -(a_i - b_i) \quad (٢)$$

ومنه فإن $k \mid |a_i - b_i|$. ولذا فإن $|a_i - b_i| \geq k$. ولكن $0 \leq b_i \leq k-1$ و $0 \leq a_i \leq k-1$. أي أن $|a_i - b_i| \leq k$ وهذا تناقض. وبالتالي فإننا نخلص إلى أن التمثيلين متساويان ◆

ملحوظة

لغرض التمييز بين التمثيل بأساسات مختلفة فإننا نكتب $(a_m a_{m-1} \ldots a_1 a_0)_k$ لتعني $a_m k^m + a_{m-1} k^{m-1} + \ldots + a_1 k + a_0$.

مثال(١,٢٥)

اكتب العدد 37 للأساس $k = 2$.

الحل

$$37 = 2 \times 18 + 1 \ , \quad q_1 = 18 > k$$
$$18 = 2 \times 9 + 0 \ , \quad q_2 = 9 > k$$
$$9 = 2 \times 4 + 1 \ , \quad q_3 = 4 > k$$
$$4 = 2 \times 2 + 0 \ , \quad q_4 = 2 \geq k$$
$$2 = 2 \times 1 + 0 \ , \quad q_5 = 1 < k$$

نضع $q_5 = a_5$ فنحصل على التمثيل:

$$37 = 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = (100101)_2 \quad \square$$

مثال (١,٢٦)

اكتب العدد 61469 للأساس $k = 16$.

الحل

$$61469 = 16 \times 3841 + 13 \ , \quad q_1 = 3841 > k$$
$$3841 = 16 \times 240 + 1 \ , \quad q_2 = 240 > k$$
$$240 = 16 \times 15 + 0 \ , \quad q_3 = 15 < k$$

نضع $q_3 = a_3$ فنحصل على التمثيل :

$$61469 = 15 \times 16^3 + 0 \times 16^2 + 1 \times 16^1 + 13 \times 16^0$$
$$= F \times 16^3 + 0 \times 16^2 + 1 \times 16^1 + D \times 16^0$$
$$= (F01D)_{16}$$

حيث إنه في النظام الستة عشري (*hexadecimal system*) تدل الحروف A, B, C, D, E, F على الأعداد $10, 11, 12, 13, 14, 15$ على الترتيب □

مثال (١,٢٧)

حول العدد $(BC35A8F)_{16}$ إلى عدد عشري.

الحل

$$(BC35A8F)_{16} = 11\times16^6 + 12\times16^5 + 3\times16^4 + 5\times16^3 + 10\times16^2 + 8\times16^1 + 15$$
$$= (197352079)_{10} \quad \square$$

(١,٥,١) تمارين محلولة (*Solved Exercises*)

تمرين (١)

(أ) حول العدد الثنائي $(1100011110101)_2$ إلى عدد ستة عشري.

(ب) حول العدد الستة عشري $(ABCDEF)_{16}$ إلى عدد ثنائي.

الحل

يمكن كتابة كل عدد ستة عشري كعدد ثنائي مكون من أربعة أرقام كما هو مبين في الجدول التالي:

العدد الستة عشري	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
الثنائي	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

(أ) لتحويل العدد الثنائي إلى عدد ستة عشري نقوم بتقسيم العدد إلى أعداد مكونة من أربعة أرقام من اليمين إلى اليسار (وإضافة الرقم 0 إلى يسار العدد إذا لزم الأمر). ولذا يكون لدينا : 0101 1111 1000 0001. الآن، نستخدم التقابل بين الأعداد الثنائية والستة عشرية المبينة في الجدول أعلاه لنحصل على:

$$(1100011110101)_2 = (18F5)_{16}$$

(ب) باستخدام الجدول نجد أن:

$$(ABCEF)_{16} = (1010\ 1011\ 1100\ 1101\ 1110\ 1111)_2 \quad \triangle$$

تمرين (٢)

إذا كان $n = (a_m a_{m-1} \dots a_1 a_0)_k$ فما هو تمثيل العدد $k^r n$ للأساس k.

الحل

بما أن $n = a_m k^m + a_{m-1} k^{m-1} + \dots + a_1 k + a_0$. فإن:

$$k^r n = a_m k^{m+r} + a_{m-1} k^{m+r-1} + \dots a_1 k^{r+1} + a_0 k^r$$
$$+0 \times k^{r-1} + 0 \times k^{k-2} + \dots\ 0 \times k + 0$$

وبالتالي فإن: $k^r n = (a_m a_{m-1} \dots a_1 a_0\ 00 \dots 0)_k$

حيث عدد الأصفار في البداية يساوي r $\triangle$

تمارين (١,٥)

(١) حول العدد العشري 1864 إلى عدد ثنائي.

(٢) حول العدد الستة عشري $A35B0F$ إلى عدد عشري.

(٣) حول العدد الستة عشري $2FB3$ إلى عدد ثنائي.

(٤) حول العدد الثنائي 11110111101001 إلى عدد ستة عشري.

(٥) حول العدد العشري 57 إلى عدد ثنائي.

(٦) حول العدد العشري 61469 إلى عدد ستة عشري.

(٧) حول العدد العشري 2417 إلى عدد خماسي.

(٨) حول العدد السباعي 4062 إلى عدد خماسي.

(٩) حول العدد الستة عشري $A3C$ إلى عدد عشري.

(١٠) حول العدد الستة عشري $9A0B$ إلى عدد ثنائي.

نبذة عن حياة إقليدس الاسكندراني
Biography of Euclid of Alexandria



ولد: سنة ٣٦٥ قبل الميلاد.

توفي: سنة ٢٧٥ قبل الميلاد في الاسكندرية.

يعد إقليدس الاسكندراني أشهر رياضي العصور القديمة. لم يصلنا الشيء الكثير عن حياته الخاصة عدا أنه عاش في الاسكندرية وعمل مدرساً في الأكاديمية العلمية في الاسكندرية. وعلى الرغم من أنه وضع العديد من المؤلفات في الفلك، الضوء، الموسيقى، والميكانيكا، إلا أن اسمه ارتبط كمؤسس للهندسة الإقليدية حيث وضع أسسها في كتابه المشهور العناصر *(elements)* المكون من ثلاثة عشر مجلداً، خصص المجلدات الست الأولى لدراسة الهندسة الإقليدية، وخصص المجلدات السابع، الثامن والتاسع لنظرية الأعداد، وأما المجلد العاشر فلقد درس فيه نظرية الأعداد غير الكسرية وأفرد الثلاث مجلدات الأخيرة لدراسة الهندسة في الفضاء ثلاثي البعد.

يعد كتاب العناصر أحد المصادر الأساسية (إن لم يكن المصدر الأساسي الوحيد) للرياضيين عبر العصور حيث أعيدت طباعته أكثر من ألف مرة منذ ظهور الطبعة الأولى في العام ١٤٨٢م.

نبذة عن حياة الخوارزمي
Biography of Al-Khwarizmi



ولد: سنة ٧٨٠م في مدينة بغداد.

توفي: سنة ٨٥٠م في مدينة بغداد.

هو أبو جعفر محمد بن موسى الخوارزمي كان رئيساً لبيت الحكمة أيام الخليفة العباسي المأمون، كتب العديد من المؤلفات في مواضيع مختلفة منها حساب الخوارزمي في الأرقام العربية والهندية حيث اشتقت كلمة (خوارزمية) *(Algorithm)* من عنوان هذا الكتاب، كتاب السندباد في علم الفلك، كتاب في علم الجغرافيا. ولكن شهرته ترجع إلى كتابه المشهور، علم الجبر والمقابلة الذي كان أول كتاب يعالج الجبر كعلم مستقل عن الحساب، حيث قدم في هذا الكتاب حل لمعادلتي الدرجة الأولى والثانية في مجهول واحد وقسم معادلة الدرجة الثانية إلى ستة أقسام يسهل فهمها. ولقد كتب جاندز *(Gandz)*: يعد كتاب الخوارزمي الجبر والمقابلة حجر الزاوية الأساس لجميع العلوم. ولذا فإنه يستحق لقب أبي الجبر أكثر من ديوفنتاس لأن الخوارزمي كان أول من عالج المسائل الجبرية بصورتها الحالية. وأما ديوفنتاس فكان اهتمامه منصباً على دراسة نظرية الأعداد.

نبذة عن حياة ديوفنتاس



عاش العالم اليوناني ديوفنتاس *(Diophantus)* في القرن الثالث قبل الميلاد (بعض المؤرخين يعتقدون أنه مصري تتلمذ على أيدي العلماء اليونانيين في مدينة الاسكندرية). وترجع شهرته إلى كتابه علم الحساب *(Arithmetica)* الذي يمكن وصفه بأنه أقدم كتاب قام بمعالجة المسائل الجبرية ولذلك يلقبه بعض المؤرخين بأبي الجبر ولكننا نعتقد أن العالم المسلم محمد بن موسى الخوارزمي أحق بهذا اللقب لأنه أول من عالج المسائل الجبرية، أما ديوفنتاس فكان مهتماً بصورة رئيسية بنظرية الأعداد.

ويرجع المؤرخين فضل حل المعادلات الديوفنتية بطريقة عامة إلى ديوفنتاس، إلا أنه في الحقيقة لم يعط حلاً عاماً لها وكان يكتفي في معظم الأحيان بإيجاد حل واحد للمعادلة، فضلاً عن أنه لم يستخدم الأعداد الصحيحة السالبة وكان يعالج المسائل باستخدام طرائق خاصة جداً يصعب على القارئ أن يتبناها لحل معادلات مشابهة.

الفصل الثاني

الأعداد الأولية
PRIME NUMBERS

يوجد للعدد 1 قاسم موجب واحد فقط. وأي عدد صحيح $n>1$ يوجد له على الأقل قاسمين موجبين هما 1 و n. العدد الأولي هو العدد الصحيح الأكبر من العدد 1 الذي له قاسمان موجبان فقط هما 1 والعدد نفسه.

تكمن أهمية الأعداد الأولية باعتبارها حجر الأساس في بناء الأعداد الصحيحة حيث المبرهنة الأساسية في الحساب تضمن لنا كتابة أي عدد صحيح أكبر من1 كحاصل ضرب قوى أعداد أولية وبطريقة وحيدة. ولذا فإنه يمكن الإجابة على العديد من مسائل نظرية الأعداد بدراسة الأعداد الأولية.

ولأهمية الأعداد الأولية فإننا نفرد هذا الفصل لدراستها حيث نقوم في البند الأول بإثبات المبرهنة الأساسية في الحساب وندرس توزيع الأعداد الأولية في البند الثاني ونقدم أعداد فيرما وميرسين في البند الثالث ونوظف هذه المفاهيم لاختبار ما إذا كان العدد الصحيح أولياً وإمكانية تحليله في البند الرابع.

(٢,١) المبرهنة الأساسية في الحساب
The Fundamental Theorem of Arithmetic

تعريف (٢,١)

نقول إن العـــدد الصحيح p عدد أولي *(prime number)* إذا كان $p>1$ وله قاسمان موجبان فقط هما 1 و p. ونسمي العدد الصحيح $n>1$ غـــير الأولي عدداً مؤلفاً *(composite number)*. أي أن العدد المؤلف هو العدد الصحيح n الذي يمكن كتابته على الصورة $n=ab$ حيث $1<a,b<n$.

يزودنا الجدول (١) في نهاية الكتاب بجميع الأعداد الأولية التي تقـــل عـــن 10000. لاحظ أننا لم نعتبر العدد1 عدداً أولياً وسنوضح السبب لاحقاً . كما أن العدد الأولي الزوجي الوحيد هو العدد 2 وباقي الأعداد الأولية هي أعداد فردية.

مبرهنة (٢,١)

ليكن p عدداً أولياً ولتكن $a,b,a_1,a_2,...,a_n\in\mathbb{Z}$. عندئذ:

(أ) إما أن $p\mid a$ أو أن $(a,p)=1$.

(ب) إذا كان $p\mid ab$ فإن $p\mid a$ أو إن $p\mid b$.

(ج) إذا كان $p\mid a_1a_2\ldots a_n$ فهناك i ، $1\le i\le n$ حيث $p\mid a_i$.

البرهان

(أ) بما أن $(a,p)\mid p$ فإن $(a,p)=1$ أو إن $(a,p)=p$. ولذا فإن $(a,p)=1$ أو إن $p\mid a$.

(ب) إذا كان $p\mid ab$ و $p\nmid a$ فإن $(a,p)=1$. ولذا باستخدام تمهيدية إقليدس نجد أن $p\mid b$.

(ج) باستخدام الاستقراء الرياضي على n. من الواضح أن العبارة صحيحة عندما $n=1$. لنفرض أن العبارة صحيحة عند $n-1$. ولنفرض أن $a=a_1a_2\ldots a_{n-1}$.

بما أن $p \mid aa_n$ فإننا نجد باستخدام الفقرة (ب) أن $p \mid a_n$ أو $p \mid a$.
وباستخدام الاستقراء الرياضي نجد أن $p \mid a_n$ أو أن $p \mid a_i$ حيث $1 \le i \le n-1$. ولذا فإن $p \mid a_i$ حيث $1 \le i \le n$ ◆

مبرهنة (٢,٢) [المبرهنة الأساسية في الحساب]

يمكن كتابة أي عدد صحيح $n > 1$ بشكل وحيد (باستثناء الترتيب) على الصورة :

$$n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s} \qquad (١)$$

حيث $p_1, p_2, \dots, p_s$ أعداد أولية مختلفة و $a_1, \dots, a_s \in \mathbb{Z}^+$.

البرهان

سنبرهن أولاً باستخدام الاستقراء الرياضي على إمكانية كتابة n على الصورة (١). من الواضح أن العبارة صحيحة عند $n = 2$. لنفرض الآن أن العبارة صحيحة لكل $2 \le k < n$.

إذا كان n عدداً أولياً فإن العبارة واضحة. لنفرض إذن أن $n = ab$ حيث $1 < a, b < n$. باستخدام فرضية الاستقراء نجد أن :

$$a = r_1^{a_1} r_2^{a_2} \dots r_t^{a_t}$$
$$b = q_1^{b_1} q_2^{b_2} \dots q_k^{b_k}$$

حيث $q_k, \dots, q_1, q_2$ أعداد أولية مختلفة، $r_1, r_2, \dots, r_t$ أعداد أولية مختلفة وحيث $a_1, a_2, \dots, a_t, b_1, b_2, \dots, b_k \in \mathbb{Z}^+$. ولذا فإن $n = ab = r_1^{a_1} r_2^{a_2} \dots r_t^{a_t} q_1^{b_1} q_2^{b_2} \dots q_k^{b_k}$.
وإذا كان $r_i = q_j$ فإننا نستبدل $r_i^{a_i} q_j^{b_j}$ بالعدد $r_i^{a_i + b_j}$. وبالتالي نحصل على الصيغة (١).
ولإثبات وحدانية التحليل نستخدم الاستقراء الرياضي على n. من الواضح أن العبارة صحيحة عند $n = 1$. لنفرض أن العبارة صحيحة لكل $2 \le k < n$.
ولنفرض أن:

$$n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s} = q_1^{b_1} q_2^{b_2} \dots q_t^{b_t} \qquad (٢)$$

إذا كان n أولياً فإن $s = t = 1$ وإن $a_1 = 1 = b_1$. ولذا فإن التحليل وحيد في هذه الحالة. أما إذا كان n مؤلفاً فإن $p_1 \mid n$. ولذا فإن :

$$\frac{n}{p_1} = p_1^{a_1-1} p_2^{a_2} \dots p_s^{a_s}$$

وبما أن $p_1 \mid q_1^{b_1} q_2^{b_2} \dots q_t^{b_t}$ فإن $p_1 \mid q_i^{b_i}$ حيث $1 \le i \le t$. وبإعادة الترتيب نستطيع أن نفرض أن $p_1 \mid q_1^{b_1}$. ولذا فإن $p_1 \mid q_1$. أي أن $p_1 = q_1$. ومنه فإن:

$$\frac{n}{p_1} = p_1^{a_1-1} p_2^{a_2} \dots p_s^{a_s} = p_1^{b_1-1} q_2^{b_2} \dots q_t^{b_t} \qquad (٣)$$

لاحظ أن $a_1 - 1 = 0$ إذا وفقط إذا كان $b_1 - 1 = 0$. لأنه لو كان $a_1 - 1 = 0$ وكان $b_1 - 1 > 0$ فإن $\frac{n}{p_1} = p_2^{a_2} \dots p_s^{a_s}$ يؤدي إلى أن $p_1 \nmid \frac{n}{p_1}$ وأن $\frac{n}{p_1} = p_1^{b_1-1} q_2^{b_2} \dots q_t^{b_t}$ يؤدي إلى أن $p_1 \mid \frac{n}{p_1}$ وهذا مستحيل. وبالمثل نستبعد الحالة $b_1 - 1 = 0$ ، $a_1 - 1 > 0$. الآن باستخدام الاستقراء الرياضي نجد من (٣) أن $s = t$ وأن $p_i = q_i$ وأن $a_1 - 1 = b_1 - 1$ وأن $a_i = b_i$. أي أن التحليل وحيد ◆

ملحوظات

(١) ترجع أهمية المبرهنة الأساسية في الحساب إلى وحدانية تحليل العدد إلى قوى عوامله الأولية، وهناك مجموعات كثيرة من الأعداد تفتقد هذه الخاصة المهمة. على سبيل المثال، إذا كانت E مجموعة الأعداد الزوجية واتفقنا أن نقول إن العدد الزوجي، عدداً أولياً إذا لم نستطع كتابته كحاصل ضرب عددين زوجين فإن كلاً من 2، 6، 10 ، 30 عدد أولي وإن :

$$60 = 2 \times 30 = 6 \times 10 .$$

(٢) تزودنا المبرهنة الأساسية في الحساب بطريقة أخرى لحساب القاسم المشترك الأعظم والمضاعف المشترك الأصغر ، فإذا كان :

$$a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$
$$b = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$$

حيث $a_i, b_i \ge 0$ فمن الواضح أن:

$$(a,b)=p_1^{m_1}p_2^{m_2}\dots p_k^{m_k}$$
$$[a,b]=p_1^{M_1}p_2^{M_2}\dots p_k^{M_k}$$

حيث $m_i=\min\{a_i,b_i\}$ و $M_i=\max\{a_i,b_i\}$ لكل $1\le i\le k$. على سبيل المثال إذا كان:

$$a=132=2^2\times3\times5^0\times11$$
$$b=400=2^4\times3^0\times5^2\times11^0$$

فإن:

$$(a,b)=2^2\times3^0\times5^0\times11^0=4$$
$$[a,b]=2^4\times3\times5^2\times11=13200$$

(٣) سنتبنى الترميز التالي لفائدته في بعض الأحيان. إذا كان p عدداً أولياً سنكتب $p^a \| n$ ليعني أن $p^a \mid n$ ولكن $p^{a+1} \nmid n$. على سبيل المثال $2^3 \| 200$ و $5^2 \| 200$.

نقدم الآن بعض نتائج المبرهنة الأساسية في الحساب ذوات الاستخدام المتكرر في هذا الكتاب.

مبرهنة (٢,٣)

إذا كان $a,b\in\mathbb{Z}^+$ حيث $(a,b)=1$ وكان $ab=c^n$ فإنه يوجد $d,e\in\mathbb{Z}^+$ حيث $a=d^n$ و $b=e^n$.

البرهان

إذا كان $a=1$ فإن العبارة صحيحة بأخذ $d=1$ و $e=c$. وإذا كان $b=1$ فإن العبارة صحيحة بأخذ $e=1$ و $d=c$. لنفرض إذن أن $a>1$ و $b>1$. باستخدام المبرهنة الأساسية في الحساب نجد أن :

$$a=p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$$
$$b=p_{r+1}^{a_{r+1}}p_{r+2}^{a_{r+2}}\dots p_{r+s}^{a_{r+s}}$$

بما أن $(a,b)=1$ فإن جميع الأعداد الأولية $p_1, p_2, \ldots, p_{r+s}$ مختلفة. الآن، ليكن $c=q_1^{b_1}q_2^{b_2}\ldots q_k^{b_k}$ هو تحليل c إلى قوى عوامله الأولية. بما أن $ab=c^n$ فإننا نجد:

$$p_1^{a_1}p_2^{a_2}\ldots p_{r+s}^{a_{r+s}}=q_1^{nb_1}q_2^{nb_2}\ldots q_k^{nb_k}$$

ومن وحدانية التحليل نجد أن $r+s=k$ وأن $p_i=q_i$ وأن $a_i=nb_i$ لكل $1\le i\le r+s$. الآن بوضع $d=p_1^{b_1}p_2^{b_2}\ldots p_r^{b_r}$ و $e=p_{r+1}^{b_{r+1}}p_{r+2}^{b_{r+2}}\ldots p_{r+s}^{b_{r+s}}$ نحصل على $a=d^n$ و $b=e^n$ ◆

مبرهنة (٢,٤)

إذا كان $m,n\in\mathbb{Z}^+$ حيث $(m,n)=1$ وكان $d\mid mn$ فإنه يوجد عددان وحيدان $d_1,d_2\in\mathbb{Z}^+$ حيث $d_1\mid m$ ، $d_2\mid n$ ، $d=d_1d_2$ ، $(d_1,d_2)=1$.

البرهان

بتحليل كل من m و n إلى قوى عوامله الأولية نجد أن:

$m=p_1^{m_1}p_2^{m_2}\ldots p_s^{m_s}$ و $n=q_1^{n_1}q_2^{n_2}\ldots q_t^{n_t}$.

وبما أن $(m,n)=1$ فإن جميع الأعداد p_i و q_i مختلفة ولذا فإن:

$$mn=p_1^{m_1}p_2^{m_2}\ldots p_s^{m_s}q_1^{n_1}q_2^{n_2}\ldots q_t^{n_t}$$

هو تحليل mn إلى قوى عوامله الأولية. وبما أن $d\mid mn$ فإن:

$$d=p_1^{a_1}p_2^{a_2}\ldots p_s^{a_s}q_1^{b_1}q_2^{b_2}\ldots q_t^{b_t}$$

حيث $0\le a_i\le m_i$ لكل $1\le i\le s$ و $0\le b_j\le n_j$ لكل $1\le j\le t$. وبالتالي إذا وضعنا $d_1=p_1^{a_1}p_2^{a_2}\ldots p_s^{a_s}$ و $d_2=q_1^{b_1}q_2^{b_2}\ldots q_t^{b_t}$ فإننا نخلص إلى أن $d=d_1d_2$ و $(d_1,d_2)=1$.

ولإثبات الوحدانية نفرض أن $d=d_1d_2=e_1e_2$ حيث $(d_1,d_2)=(e_1,e_2)=1$، $d_1\mid m$ ، $e_1\mid m$ ، $d_2\mid n$ ، $e_2\mid n$. لاحظ أن $(d_1,e_2)=1$. فلو كان $(d_1,e_2)=r$ لتوصلنا إلى أن $r\mid d_1$ و $r\mid e_2$. الأمر الذي يعني أن $r\mid m$ و

$r \mid n$. فيكون $(m,n)>1$. وهذا مستحيل. وبالمثل $(d_2,e_1)=1$. وبما أن $e_1 \mid d_1d_2$ فإننا نجد أن $e_1 \mid d_1$. وبالمثل، نرى أن $d_1 \mid e_1$. إذن، $e_1=d_1$. ومن ثم فإن $e_2=d_2$ ◆

مبرهنة (٢,٥)

إذا كانت $f(x)=x^n+c_{n-1}x^{n-1}+\ldots+c_1x+c_0$ كثيرة حدود واحدية حيث $c_i \in \mathbb{Z}$ وإذا كان α جذراً لكثيرة الحدود $f(x)$ فإن أن α عدداً صحيح أو عدد غير كسري (غير نسبي).

البرهان

لنفرض أن α عدد كسري. أي أن $\alpha=\frac{a}{b}$ حيث $a,b \in \mathbb{Z}$ ، $b \neq 0$ ، $(a,b)=1$. سنبرهن أن $\alpha \in \mathbb{Z}$. الآن $f(\alpha)=0$ يؤدي إلى :

$$\left(\frac{a}{b}\right)^n+c_{n-1}\left(\frac{a}{b}\right)^{n-1}+\ldots+c_1\left(\frac{a}{b}\right)+c_0=0 .$$

وعليه $a^n=b(-c_{n-1}a^{n-1}-\ldots-c_1ab^{n-2}-c_0b^{n-1})$. فنرى أن $b \mid a^n$.

وبما أن $(a,b)=1$ فإن $b \mid a$ وبالتالي فإن $\alpha=\frac{a}{b} \in \mathbb{Z}$ ◆

مثال (٢,١)

إذا كان $a,n \in \mathbb{Z}^+$ وكان $\sqrt[n]{a}$ عدداً كسرياً فإن $\sqrt[n]{a} \in \mathbb{Z}$.

الحل

بما أن $\sqrt[n]{a}$ جذر للمعادلة $x^n-a=0$ فإنه باستخدام المبرهنة (٢,٥) نجد أن $\sqrt[n]{a} \in \mathbb{Z}$ □

مثال (٢,٢)

$\sqrt{2}$ عدد غير كسري.

الحل

بما أن $1<\sqrt{2}<2$ فإن $\sqrt{2}$ عدد غير صحيح. وبما أنه جذر للمعادلة $x^2-2=0$ فإنه يجب أن يكون عدد غير كسري □

مثال (٢,٣)

$\sqrt[3]{10}$ عدد غير كسري.

الحل

بما أن $2<\sqrt[3]{10}<3$ فإن $\sqrt[3]{10}$ عدد غير صحيح. وبما أنه جذر للمعادلة $x^3-10=0$ فإنه عدد غير كسري □

مثال(٢,٤)

$\log_{10}2$ عدد غير كسري.

الحل

إذا كان $\log_{10}2$ عدداً كسرياً فإن $\log_{10}2=\frac{a}{b}$ حيث $a,b\in\mathbb{Z}$ و $b\neq 0$. ولذا فإن $10^a=2^b$. أي أن $2^a\times 5^a=2^b$. وباستخدام وحدانية التحليل نجد أن $a=b$ و $a=0$. أي أن $b=0$ وهذا مستحيل □

(٢,١,١) تمارين محلولة (*Solved Exercises*)

تمرين(١)

نقول إن كثيرة الحدود $f(x)$ التي معاملاتها أعداداً صحيحة غير قابلة للتحليل *(irreducible)* إذا كانت المساواة $f(x)=g(x)h(x)$ تقتضي أن واحدة من $g(x)$ و $h(x)$ على الأقل كثيرة حدود ثابتة.

لتكن $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$ كثيرة حدود معاملاتها أعداد صحيحة حيث $a_n\neq 0$. وليكن p عدداً أولياً حيث:

(أ) $p\mid a_i$ لكل $0\le i\le n-1$ (ب) $p\nmid a_n$ (ج) $p^2\nmid a_0$.

أثبت أن $f(x)$ غير قابلة للتحليل.

الحل

لنفرض أن $f(x)$ قابلة للتحليل. $f(x)=g(x)h(x)$ حيث $g(x)=b_sx^s+...+b_1x+b_0$ و $h(x)=c_tx^t+...+c_1x+c_0$ و $s,t\ge 1$. بما أن $p\mid(a_0=b_0c_0)$ وأن $p^2\nmid a_0$ فإن $p\mid b_0$ أو $p\mid c_0$ وليس كلاهما معاً. ولذا نفرض أن $p\mid b_0$ وأن $p\nmid c_0$.

وبما أن $p\nmid a_n$ فإن $p\nmid b_sc_t$. ولذا فإن $p\nmid b_s$. وعليه فإنه يوجد $i\le s$ حيث p يقسم كل من $b_0,b_1,...,b_{i-1}$ ولكن $p\nmid b_i$. الآن :

$$a_i=b_0c_i+b_1c_{i-1}+...+b_{i-1}c_1+b_ic_0$$

حيث $p\mid a_i$ و $p\mid(b_0c_i+b_1c_{i-1}+...+b_{i-1}c_1)$. ولذا فإن $p\mid b_ic_0$. ومنه فإن $p\mid b_i$ أو $p\mid c_0$ وهذا مستحيل. إذن، $f(x)$ غير قابلة للتحليل △

تمرين (٢)

(أ) أثبت أن $(a^n,b^n)=(a,b)^n$ لكل $n\ge 1$.

(ب) أثبت أن $a^n\mid b^n$ إذا وفقط إذا كان $a\mid b$.

الحل

(أ) لنفرض أن: $a=p_1^{a_1}p_2^{a_2}...p_k^{a_k}$ وأن : $b=p_1^{b_1}p_2^{b_2}...p_k^{b_k}$ حيث $a_i,b_i\ge 0$.

حينئذ : $(a,b)=p_1^{m_1}p_2^{m_2}...p_k^{m_k}$ وإن: $(a^n,b^n)=p_1^{t_1}p_2^{t_2}...p_k^{t_k}$

حيث $m_i=\min\{a_i,b_i\}$ و $t_i=\min\{na_i,nb_i\}=nm_i$. ولذا فإن :

$$(a^n,b^n)=(p_1^{m_1}p_2^{m_2}...p_k^{m_k})^n=(a,b)^n$$

(ب) لنفرض أن $a^n \mid b^n$. عندئذ $(a,b)^n=(a^n,b^n)=a^n$. ولذا فإن $(a,b)=a$ ومن ثم فإن $a \mid b$. وبالعكس، إذا كان $a \mid b$ فإن $(a,b)=a$. ومنه فإن $(a,b)^n=a^n$. حينئذ $(a^n,b^n)=a^n$. ونستخلص أن $a^n \mid b^n$ △

تمرين (٣)

(أ) إذا كان $n,b \in \mathbb{Z}^+$ فأثبت أن عدد مضاعفات b الواقعة بين 1 و n هو $[n/b]$ حيث $[x]$ أكبر عدد لا يزيد عن x.

(ب) إذا كان p عدداً أولياً وكان $p^e \parallel n!$ فأثبت أن $e=[n/p]+[n/p^2]+[n/p^3]+\ldots$.

(ج) جد e حيث $15^e \parallel 60!$.

الحل

(أ) لنفرض أن عدد مضاعفات العدد b الواقعة بين 1 و n يساوي k. عندئذ، مضاعفات العدد b هي $b,2b,\ldots,kb$ حيث $kb \le n < (k+1)b$. ولذا فإن $k \le \frac{n}{b} < k+1$. وبالتالي فإن $k=[n/b]$.

(ب) المطلوب هنا هو إيجاد عدد القواسم p التي تحدث في $n!$. الآن باستخدام الفقرة (أ) نجد أن عدد مضاعفات p بين 1 و n هو $[n/p]$. ولكن بعض هذه المضاعفات هو مضاعف للعدد p^2. ولذا فإنه يساهم بقاسم جديد للعدد p. على وجه الخصوص عدد مضاعفات p^2 بين 1 و n هو $[n/p^2]$. وهلم جرا. ولذا فإن: $e=[n/p]+[n/p^2]+[n/p^3]+\ldots$.
لاحظ أنه لا بد من وجود k حيث $n/p^k<1$. ولذا فإن $[n/p^k]=0$.

(ج) بما أن $15=3\times5$ فإنه لكي نجد e حيث $15^e \parallel 60!$ يكفي أن نجد e حيث $5^e \parallel 60!$. وباستخدام الفقرة (ب) نجد أن $e=[60/5]+[60/25]=12+2=14$ △

تمرين (٤)

جد جميع الحلول للمعادلة $m^n = n^m$ حيث $m,n \in \mathbb{Z}$.

الحل

لنفرض أن: $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ وأن $n = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$

هو تحليل كل من m و n حيث $a_i,b_i \geq 0$. بما أن $m^n = n^m$ فإن $na_i = mb_i$ لكل $1 \leq i \leq k$.

لنفرض أن $n > m$. عندئذ $a_i < b_i$ لكل i، لذا فإن $m \mid n$. أي أن $n = mc$ حيث $c > 1$. هذا يعني أن $m^{mc} = (mc)^m$. أي أن $m^c = mc$. ولذا فإن $m^{c-1} = c$.

إذا كان $c = 2$ و $m = 2$ فإن $m = 2$ و $n = 4$ حل.

إذا كان $c = 2$ و $m > 2$ فإن $m^{c-1} = m > 2 = c$. ولذا فإنه لا يوجد حلول في هذه الحالة.

إذا كان $c > 2$ و $m > 2$ فإن $m^{c-1} > 2^{c-1} > c$. ومن ثم لا يوجد حلول ايضاً.

وبالمثل، إذا كان $m < n$ فالحل هو $m = 4$ و $n = 2$.

إذن، جميع الحلول هي: $(n = 4$ و $m = 2)$ ، $(n = 2$ و $m = 4)$ △

تمارين (١، ٢)

(١) إذا كان $(a,p^2) = p$ فأثبت أن $(a^2,p^2) = p^2$ حيث p عدد أولي و $a \in \mathbb{Z}^+$.

(٢) إذا كان $(a,p^2) = (b,p^2) = p$ فأثبت أن $(ab,p^4) = p^2$ حيث p عدد أولي و $a,b \in \mathbb{Z}^+$.

(٣) إذا كان $(a,p^2)=p$ و $(b,p^2)=p^2$ حيث p عدد أولي و $a,b\in\mathbb{Z}^+$ فهل تصح المساواة $(ab,p^4)=p^3$؟

(٤) إذا كان $(a,p^2)=p$ حيث p عدداً أولياً و $a\in\mathbb{Z}^+$ فهل من الصحيح أن $(a+p,p^2)=p$؟

(٥) جد جميع الأعداد الأولية p بحيث يكون p^2+2 أولياً أيضاً.

(٦) إذا كان $p>1$ وكان p يقسم $(p-1)!+1$ فأثبت أن p عدد أولي.

(٧) إذا كان $a^3\mid b^2$ فأثبت أن $a\mid b$.

(٨) إذا كان $a^2\mid b^3$ فهل من الصحيح أن $a\mid b$؟

(٩) (أ) جد جميع الأعداد الأولية p بحيث يكون $17p+1$ مربعاً كاملاً.

(ب) جد جميع الأعداد الأولية p بحيث يكون $3p+1$ مربعاً كاملاً.

(١٠) إذا كان كل من p و $p+2$ عدداً أولياً حيث $p>3$ فأثبت أن 12 يقسم $2p+2$.

(١١) إذا كان $n>1$ فأثبت أن n^3+1 عدد مؤلف.

(١٢) إذا كان n^3-1 عدداً أولياً فأثبت أن $n=2$.

(١٣) أثبت خطأ الحدس التالي: إذا كان $n\in\mathbb{Z}^+$ فإن $n=p+a^2$ حيث $p=1$ أو p عدد أولي و $a\geq 0$.

(١٤) أثبت أن a^4+4 عدد مؤلف لكل $a>1$.

(١٥) أثبت أن 8^n+1 عدد مؤلف لكل $n\geq 1$.

(١٦) أثبت امكانية كتابة أي عدد $n>11$ كحاصل جمع عددين مؤلفين.

(١٧) إذا كان $p\geq q\geq 5$ حيث كل من p و q عدد أولي فأثبت أن $24\mid(p^2-q^2)$.

(١٨) إذا كان $p>5$ عدداً أولياً فأثبت أن $10\mid(p^2-1)$ أو أن $10\mid(p^2+1)$.

(١٩) إذا كان p عدداً أولياً وكان $1\leq k<p$ فأثبت أن $p\mid\binom{p}{k}$.

(٢٠) إذا كان $p^m \| a$ وكان $p^n \| b$ فأثبت أن $p^{m+n} \| ab$.

(٢١) إذا كان $p^m \| a$ وكان $p^n \| (a,b)$ فأثبت أن $a+b$ عدد أولي.

(٢٢) إذا كان $p^m \| a$ و $p^n \| b$ حيث $m<n$ فأثبت أن $p^m \| (a+b)$.

(٢٣) إذا كان $p^m \| (a,b)$ فهل من الضرورة أن يكون $p^{2m} \| ab$؟

(٢٤) إذا كان 2^n-1 عدداً أولياً فأثبت أن n عدد أولي. هل العكس صحيح؟

(٢٥) إذا كان أحد العددين 2^n-1 و 2^n+1 حيث $n>2$ أولياً فأثبت أن العدد الآخر عدد مؤلف.

(٢٦) إذا كان كل من p و $8p-1$ عدداً أولياً فأثبت أن $8p+1$ عدد مؤلف.

(٢٧) إذا كان كل من p و $8p^2+1$ عدداً أولياً فأثبت أن $8p^2-1$ عدد أولي.

(٢٨) إذا كان $n=p_1^{k_1}p_2^{k_2}\dots p_t^{k_t}$ فأثبت أن n مربع كامل إذا وفقط إذا كان k_i زوجياً لكل $1\le i\le t$.

(٢٩) إذا كان كل من ab ، ac ، bc مكعباً فأثبت أن كلاً من a، b ، c مكعب.

(٣٠) أثبت أن آخر مرتبة غير صفرية في العدد $n!$ حيث $n\ge 2$ يجب أن تكون عدد زوجي.

(٣١) جد عدد الأصفار الذي ينتهي بها العدد $169!$.

(٣٢) جد عدد الأصفار الذي ينتهي بها العدد $500!/200!$.

(٣٣) أثبت أن $1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{n}$ لا يمكن أن يكون عدداً صحيحاً لكل $n>1$.

(٣٤) أثبت أن $1+\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\dots+\frac{1}{n!}+\dots$ عدد غير كسري.

(٣٥) إذا كانت $S=\{3k+1 : k\in\mathbb{N}\}$. نقول إن $a\,|\,b$ إذا وجد $c\in S$ حيث $b=ac$. ونقول إن $p\in S$ عدد أولي إذا كانت قواسم p هي 1 و p فقط. أثبت أن S لا تتمتع بخاصية التحليل الوحيد.

(٣٦) أثبت أن $\sqrt{2}+\sqrt{3}$ عدد غير كسري.

(٣٧) أثبت أن كل من $\sqrt[3]{5}$ و $\sqrt[10]{17}$ عدد غير كسري.

(٣٨) إذا كان $a+b=798$ وكان $[a,b]=10780$ فجد a و b.

(٣٩) أثبت أن:

(أ) $[a,(a,b)]=a$ (ب) $(a,[a,b])=a$

(٤٠) أثبت أن:

(أ) $(a,[b,c])=[(a,b),(a,c)]$ (ب) $[a,(b,c)]=([a,b],[a,c])$

(٤١) إذا كان $a,b,c\in\mathbb{Z}^+$ فأثبت أن:

(أ) $\max\{a,b,c\}=a+b+c-\min\{a,b\}-\min\{a,c\}-\min\{b,c\}$
$+\min\{a,b,c\}$

(ب) $[a,b,c]=\dfrac{abc(a,b,c)}{(a,b)(a,c)(b,c)}$

(٤٢) أثبت أن $(a,b,c)[ab,ac,bc]=abc$.

(٤٣) أثبت أن $[a,b,c](ab,ac,bc)=abc$.

(٤٤) إذا كان $a\mid bc$ فأثبت أن $a\mid(a,b)c$.

(٤٥) إذا كان $a\mid bc$ فأثبت أن $a\mid(a,c)(a,b)$.

(٤٦) نقول إن العدد الصحيح n خال من المربعات إذا لم نستطع إيجاد عدد صحيح $m>1$ حيث $m^2\mid n$. أثبت أن:

(أ) $n>1$ خال من المربعات إذا وفقط إذا أمكن كتابة n كحاصل ضرب عدد منته من الأعداد الأولية المختلفة.

(ب) إذا كان $n>1$ فإن $n=ab^2$ حيث a خال من المربعات.

(٤٧) أثبت أن $f(x)=x^3-4x+2$ غير قابلة للتحليل.

(٤٨) أثبت أن $\Phi_p(x)=x^{p-1}+x^{p-2}+\ldots+x+1$ غير قابلة للتحليل حيث p عدد أولي.

(٢,٢) توزيع الأعداد الأولية
Distribution of Primes

للرياضي المشهور إدموند لاندو *(Edmund Landau)* الذي عاش في الفترة ١٨٧٧م – ١٩٣٨م مقولة تنص على "يجب أن تحتل دراسة توزيع الأعداد الأولية أهم فصل من فصول العلوم الرياضية".

سنبدأ دراستنا لكيفية توزيع الأعداد الأولية بتقديم قائمة الأعداد الأولية التي لا تزيد عن100 وهي:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,
43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

عدد الأعداد الأولية في هذه القائمة هو 25 وإذا كان للأعداد الأولية نمط معين في توزيعها فمن الواضح أن القائمة أعلاه تفشل فشلاً ذريعاً في تبيان هذا النمط. على سبيل المثال لا يوجد أي عدد أولي بين 24 و 28 ولا بين 90 و 96 . من ناحية أخرى تحتوي القائمة على توائم أولية *(twin primes)* p و $p+2$ ، مثل (3 و 5) ، (5 و 7)، (71 و 73). ولو تأملنا قائمة الأعداد الأولية بين100 و 200 وهي:

101, 103, 107, 109, 113, 127, 131, 137, 139,149, 151, 157,
163, 167, 173, 179, 181, 191, 193, 197, 199

لرأينا أن عددها هذه المرة هو 21. ولكن لا تزال لدينا الاشكالية نفسها وتتمثل في وجود فجوات بين الأعداد الأولية ووجود توائم أولية. الأسئلة التي تطرح نفسها هنا هي:

(١) هل مجموعة الأعداد الأولية غير منتهية؟

(٢) هل توجد فجوات كبيرة بين الأعداد الأولية؟

(٣) هل يوجد عدد غير منته من التوائم الأولية؟

لقد أجاب إقليدس في المجلد التاسع من كتابه العناصر عن السؤال الأول حيث برهن أكثر المبرهنات جذباً للإنتباه وأكثرها قدماً وهي أن عدد الأعداد

الأولية غير منته. نقدم هنا برهان إقليدس وسنتعرض لبراهين أخرى لهذه الحقيقة في هذا الكتاب.

مبرهنة (٢,٦)

يوجد عدد غير منته من الأعداد الأولية.

البرهان

نستخدم البرهان بالتناقض. ولذا نفرض أن $p_1 < p_2 < \ldots < p_k$ هي جميع الأعداد الأولية. ولنفرض أن $m = p_1 p_2 \ldots p_k + 1$. بما أن $m > 1$ فإنه يوجد قاسم أولي p للعدد m. ولذا فإنه يوجد $1 \le i \le k$ حيث $p = p_i$. ومنه فإن p يقسم $p_1 p_2 \ldots p_k$. وبالتالي فإن $p \mid 1$ وهذا مستحيل. إذن، نخلص إلى أن عدد الأعداد الأولية غير منته ◆

الإجابة عن السؤال الثاني سهلة أيضاً فسنثبت الآن وجود فجوات كبيرة بين الأعداد الأولية.

مبرهنة (٢,٧)

إذا كان $n \in \mathbb{Z}^+$ فإنه يوجد على الأقل n من الأعداد الصحيحة المؤلفة المتتالية.

البرهان

جميع الأعداد الصحيحة: $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$ أعداد مؤلفة لأن k يقسم $(n+1)!$ لكل $2 \le k \le n+1$. ولذا فإن k يقسم $(k+1)!+k$ لكل $2 \le k \le n+1$ ◆

أما بالنسبة للسؤال الثالث فهو من الأسئلة التي لم تتم الإجابة عنها حتى الآن. وبالتقدم السريع في صناعة الحاسبات الآلية استطاع علماء الرياضيات اكتشاف توائم أولية كبيرة جداً، فمثلاً اكتشف الرياضيان آتكن ودينر *(Atkin and Dubner)* في العام ١٩٨٥م التوأم $107570463 \times 10^{2250} \pm 1$. ولكنه

من الطريف أن البحث عن الثلاثيات الأولية، أي الأعداد الأولية من الشاكلة p، $p+2$ ، $p+4$ قد حسم كما تبين لنا المبرهنة التالية.

مبرهنة (٢,٨)

الثلاثيات الأولية الوحيدة هي $3, 5, 7$.

البرهان

لنفرض أن $p, p+2, p+4$ ثلاثي من الأوليات.

إذا كان $p=3k$ فإن $p=3$. ومنه فإن $p+2=5$ و $p+4=7$. ولذا فإن $3, 5, 7$ ثلاثي أولي.

إذا كان $p=3k+1$ فإن $p+2=3(k+1)$ ليس أولياً.

وأخيراً إذا كان $p=3k+2$ فإن $p+4=3(k+2)$ ليس أولياً. ونخلص إلى أن الثلاثي الأولي الوحيد هو $3, 5, 7$ ◆

من الممكن استغلال فكرة برهان المبرهنة (٢,٦) لإثبات وجود عدد غير منته من الأعداد الأولية التي تحظى بخاصة مشتركة. تبرر المبرهنة التالية نشاطاً من هذا النوع.

مبرهنة (٢,٩)

(أ) إذا كانت $m_1, m_2, \ldots, m_k$ أعداداً صحيحة كل منها على الصورة $4s+1$ فإن العدد $m_1 m_2 \ldots m_k$ على الصورة $4s+1$.

(ب) يوجد عدد غير منته من الأعداد الأولية التي على الصورة $4s+3$.

البرهان

(أ) بالاستقراء الرياضي على k. من الواضح أن العبارة صحيحة عند $k=1$. لنفرض أن العبارة صحيحة عند $k-1$. أي أن $m_1 m_2 \ldots m_{k-1} = 4s+1$. ولنفرض أن $m_k = 4t+1$. ولذا فإن:

$$m_1 m_2 \ldots m_{k-1}\, m_k = (4s+1)(4t+1) = 4(4st+s+t)+1$$

وبالتالي فإن العبارة صحيحة عند k.

(ب) لنفرض أن $p_k, \ldots, p_2, p_1$ هي جميع الأعداد الأولية التي على الصورة $4s+3$. وليكن $m = 4p_1p_2 \ldots p_k - 1$. ومن الجلي أن m على الصورة $4s+3$. ليكن $p \mid m$. عندئذ: $p = 4s+1$ أو $p = 4s+3$.

إذا كان كل قاسم أولي للعدد m على الصورة $4s+1$ فإن m على الصورة $4s+1$. ولذا فإنه يوجد قاسم أولي p للعدد m على الصورة $4s+3$. ومنه فإنه يوجد $1 \le i \le k$ حيث $p = p_i$. إذن، p يقسم $4p_1p_2 \ldots p_k$. ومن ثم فإن p يقسم 1 وهذا مستحيل. وبالتالي فإن عدد الأعداد الأولية التي على الصورة $4s+3$ غير منته ◆

سنبرهن لاحقاً أن عدد الأعداد الأولية التي على الصورة $4s+1$ غير منته أيضاً. وبصورة عامة فلقد برهن ديرشليه *(Dirichlet)* عام ١٨٣٧م المبرهنة التالية:

مبرهنة (٢,١٠) [مبرهنة ديرشليه]

إذا كان $(a,b) = 1$ فإنه يوجد عدد غير منته من الأعداد الأولية التي على الصورة $as+b$.

برهان المبرهنة (٢,١٠) يخرجنا على نطاق هذا الكتاب ويستطيع القارئ المهتم أن يجده في العديد من كتب نظرية الأعداد ، على سبيل المثال أنظر [10].

مع التقدم السريع في الحاسبات الآلية بدأ اهتمام بعض علماء نظرية الأعداد محاولة إيجاد أكبر عدد ممكن من الأعداد الأولية المتتالية في متتالية دريشليه وكان آخر ما توصل إليه الرياضي مانفرد توبيلك *(Manfred Toplic)* عشرة أعداد أولية متتالية في العام ١٩٩٨م وهي:

$$p,\ p+210,\ p+420,\ p+630,\ p+840,\ p+1050,$$
$$p+1260,\ p+1470,\ p+1680,\ p+1890$$

حيث $p = 100\ 99697\ 24697\ 14247\ 63778\ 66555$

$87969\ \ 84032\ 95093\ 24689\ 19004\ 18036\ 03417$

$75890\ 43417\ 03348\ 88215\ 90672\ 29719$

بعد أن برهنا على وجود فجوات كبيرة بين الأعداد الأولية يصبح من الطبيعي أن نسأل: إذا كان $x \in \mathbb{R}^+$ فما هو عدد الأعداد الأولية التي لا تزيد عن x؟ سنرمز لهذا العدد بالرمز $\pi(x)$. تعد المبرهنة التي تجيبنا على هذا السؤال من أهم مبرهنات نظرية الأعداد وتدعى مبرهنة الأعداد الأولية *(Prime number therorem)* . وإليك نصها:

مبرهنة (٢,١١) [مبرهنة الأعداد الأولية]

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1 .$$

أي أن عدد الأعداد الأولية التي لا تزيد عن x هو تقريباً $\frac{x}{\ln x}$ عندما يكون x عدداً كبيراً ما فيه الكفاية.

تنسب هذه المبرهنة إلى كل من جاوس *(Gauss)* الذي توقع صحتها عام ١٧٩٣م وليجندر *(Legendre)* الذي توقع صحتها عام ١٧٩٨م باستخدام جداول الأعداد الأولية لحساب $\pi(x)$ لكل $x < 10000$.

البراهين المختلفة المعروفة لمبرهنة الأعداد الأولية، إما أنها صعبة جداً أو أنها تعتمد على رياضيات متقدمة. وأول برهان قدم لها كان في العام ١٨٩٦م على يد الرياضي الفرنسي هادامار *(Hadamard)* والرياضي البلجيكي بواسن *(Poussin)* كل على انفراد. ولفترة قريبة كان رأي معظم الرياضيين أنه ليس بالإمكان الحصول على برهان لها دون استخدام التحليل المركب، إلى أن اكتشف الرياضي النرويجي سيلبرج *(Selberg)* عام ١٩٤٩م برهاناً يعتمد كلياً على مفاهيم نظرية الأعداد ولكنه لا يقل صعوبة عن البراهين السابقة .

لقد بات من المعروف الآن أن $\pi(x) \geq \frac{x}{\ln x}$ لكل $x \geq 17$ والجدول التالي يزودنا ببعض قيم $\pi(x)$ و $\frac{x}{\ln x}$.

x	$\pi(x)$	$x/\ln x$	$\pi(x)/\frac{x}{\ln x}$
10^3	168	144.8	1.160
10^4	1229	1085.7	1.132
10^5	9592	8685.9	1.104
10^6	78498	72382.4	1.085
10^7	664579	620420.7	1.071
10^8	5761455	5428681.0	1.061
10^9	50847534	48254942.4	1.054
10^{10}	455025512	434294481.9	1.048
10^{11}	4118054813	3948131663.7	1.043
10^{12}	37607912018	36191206825.3	1.039
10^{13}	346065536839	334072678387.1	1.036
10^{14}	32049417550802	3102103442166	1.033

إذا كان p_n العدد الأولي الذي رتبته n فإنه من الواضح أن $\pi(p_n) = n$. ولذا بأخذ $x = p_n$ واستخدام الحقيقة $\lim_{x\to\infty} \frac{\ln(x/\ln x)}{\ln x} = 1$ فإنه من الممكن إثبات أن $\lim_{n\to\infty} \frac{p_n}{n \ln n} = 1$. لذا يكون لدينا النص المكافئ التالي لمبرهنة الأعداد الأولية:

إذا كان p_n العدد الأولي الذي رتبته n فإن $\lim_{n\to\infty} \frac{p_n}{n \ln n} = 1$.

في واقع الأمر من المعلوم أن $p_n > n \ln n$ لكل n ، ومع أن $p_n - n \ln n$ قد يكون كبير جداً، إلا أنه يصبح عدداً صغيراً عندما يكون n عدد كبير جداً.

ملحوظات

(١) لاحظ أننا نستطيع أن نستنتج من مبرهنة الأعداد الأولية أن $\frac{\pi(x)}{x}<\frac{c}{\ln x}$ حيث $x>1$ و c عدد ثابت. ولذا فإن $1-\frac{\pi(x)}{x}>1-\frac{c}{\ln x}$. أي أن:

$$\lim_{x\to\infty}(1-\frac{\pi(x)}{x})=\lim_{x\to\infty}\frac{x-\pi(x)}{x}=1 .$$

ومن الممكن تفسير ذلك على النحو التالي:

بما أن $n-\pi(n)$ هو عدد الأعداد الصحيحة الموجبة المؤلفة التي لا تزيد عن n فإن $\frac{n-\pi(n)}{n}$ يمثل نسبة الأعداد المؤلفة بين أول n من الأعداد. وبما أن هذه النسبة تؤول إلى 1 عندما n يؤول إلى ∞ فإننا نستنتج من مبرهنة الأعداد الأولية أن "تقريبا جميع" الأعداد الصحيحة الموجبة مؤلفة. ولكن هل هذا يعني أن الأعداد الأولية نادرة؟ بالطبع لا، وذلك لأن الدالة $\ln x$ بطيئة التزايد، فعلى سبيل المثال، $\ln 10^{100}\approx 230$. وإذا اخترنا عشوائياً عدداً صحيحاً N قريباً من 10^{100} فإن احتمال أن يكون هذا العدد أولياً هو تقريباً $\frac{1}{230}$. وإذا استطعنا أن نختار N بحيث لا يقبل القسمة على الأعداد الأولية الصغيرة 2، 3 و 5 فإن احتمال أن يكون أولياً يصبح تقريباً $\frac{1}{61}$. ولذا باختيار مناسب فإننا نستطيع أن نجد أعداد أولية كبيرة جداً وعلى هذه الأعداد الأولية الكبيرة جداً تعتمد أنظمة التعمية الحديثة.

(٢) إذا كان $a,b\in\mathbb{R}^+$ حيث $a<b$ فنجد باستخدام مبرهنة الأعداد الأولية، عدداً أولياً على الأقل بين ax و bx وذلك عندما يكون x كبير ما فيه الكفاية. وبوضع $a=1$ و $b=1+\varepsilon$ حيث $\varepsilon>0$ فإننا نخلص إلى وجود عدد أولي على الأقل بين n و $n(1+\varepsilon)$ (عندما يكون n عدد كبير جداً).

(٣) لقد أثبت لاندو *(Landau)* أن $\pi(2n)<2\pi(n)$ عندما يكون n كبير جداً. ولذا فإننا نستطيع الاستنتاج أن عدد الأعداد الأولية بين 1 و n أكبر من عدد

الأعداد الأولية بين n و $2n$ عندما يكون n كبير جداً. وهذا يقودنا إلى مبرهنة أخرى هامة جداً تدعى مبرهنة بيرتراند *(Bertrand)*.

مبرهنة (٢,١٢) [حدس بيرتراند]

لكل عدد صحيح $n>1$ يوجد عدد أولي p يحقق $n<p<2n$.

توقع بيرتراند صحة الحدس عام ١٨٤٥م بعد أن أثبت صحته لكل $n<3\times10^6$ ولكنه لم يستطع تقديم برهان له. وبعد سبع سنوات استطاع الرياضي الروسي تشبشيف *(Chebyshev)* أن يبرهن صحته. وعلى الرغم من أن برهانه أقل صعوبة من مبرهنة الأعداد الأولية إلا أنه يخرجنا عن نطاق هذا الكتاب (انظر[10]) .

ملحوظات

(١) التعميم التالي لحدس بيرتراند صحيح أيضاً:

إذا كان $n>5$ فإنه يوجد على الأقل عددين أوليين بين n و $2n$.

(٢) قدم سيلفستر *(Sylvester)* التعميم التالي في العام ١٨٩٢م لحدس بيرتراند:

إذا كان $m>n>0$ فإنه يوجد قاسم أولي أكبر من n لأحد الأعداد $m,m+1,m+2,\ldots,m+n-1$.

لاحظ أننا نحصل على حدس بيرتراند بوضع $m=n+1$.

(٣) هل يوجد عدد أولي p حيث $n^2<p<(n+1)^2$؟ هذه المسألة لا زالت تنتظر حلاً.

ننهي هذا البند بتقديم حدس مهم آخر في نظرية الأعداد يدعى حدس جولدباخ *(Goldbach's conjecture)*. حيث كتب جولدباخ رسالة إلى أويلر في العام ١٧٤٢م مفادها أنه يعتقد أن كل عدد صحيح زوجي أكبر من 2 يمكن كتابته كمجموع عددين أوليين. ومنذ ذلك الحين والمحاولات جارية لإيجاد حل

لهذا الحدس، ولقد اعتبر الرياضي الإنجليزي المشهور هاردي *(Hardy)* الذي عاش في الفترة بين ١٨٧٧م و ١٩٤٧م هذا الحدس هو أصعب المسائل غير المحلولة في الرياضيات.

اختبار هذا الحدس يقود إلى الإعتقاد بصوابه، فقد تبين أنه صحيح لكل عدد زوجي أقل من 2×10^{10}. وقد استطاع الرياضي تشن *(Chen)* أن يبرهن في العام ١٩٧٣م على امكانية كتابة أي عدد صحيح كبير جداً على الصورة $p+m$ حيث p عدد أولي وحيث m إما أولي أو حاصل ضرب عددين أوليين.

(٢,٢,١) تمارين محلولة *(Solved Exercises)*

تمرين (١)

إذا كان p_n هو العدد الأولي صاحب الرتبة n فأثبت أن $p_n \le 2^{2^{n-1}}$ ثم استنتج أن $\pi(x) \ge [\log_2(\log_2 x)]+1$.

الحل

باستخدام الاستقراء الرياضي على n. إذا كان $n=1$ فإن $p_1=2=2^{2^0}$. ولذا فالعبارة صحيحة عند $n=1$.

لنفرض أن العبارة صحيحة لكل $n=1,2,\dots,k$. ضع $m=p_1p_2\dots p_k+1$. ولنفرض أن $p \mid m$. إذا كان $p=p_i$ حيث $1\le i\le k$ فإن $p \mid 1$ وهذا مستحيل. إذن، $p\ge p_{k+1}$. الآن:

$$p_{k+1} \le p \le p_1p_2\dots p_k+1 \le 2^{2^0}2^{2^1}\dots 2^{2^{k-1}}+1$$
$$=2^{1+2+4+\dots+2^{k-1}}+1=2^{2^k-1}+1=\frac{1}{2}\times 2^{2^k}+1\le 2^{2^k}$$

إذن، العبارة صحيحة عند $k+1$.

أخيراً، لاحظ أن $[\log_2(\log_2 x)]+1$ هو أكبر عدد صحيح n يحقق $x \le 2^{2^{n-1}}$. لكن من أعلاه يوجد على الأقل n من الأعداد الأولية $p_1, p_2, \dots, p_n \le 2^{2^{n-1}}$. وبالتالي فجميعها أقل من أو تساوي x. بهذا نخلص إلى أن $\pi(x) \ge [\log_2(\log_2 x)]+1$ △

تمرين (٢)

أثبت أنه لا يمكن إيجاد كثيرة حدود $f(x)$ غير ثابتة معاملاتها أعداد صحيحة بحيث يكون $f(x)$ عدداً أولياً لكل $x \in \mathbb{Z}^+$.

الحل

لنفرض أن $f(x)=a_k x^k + a_{k-1}x^{k-1} + \dots + a_1 x + a_0$ كثيرة حدود حيث $a_i \in \mathbb{Z}$ لكل $0 \le i \le k$، $a_k \ne 0$ وحيث $f(n)$ عدد أولي لكل $n \in \mathbb{Z}^+$. لنفرض أن $f(n)=p$ وليكن $t \in \mathbb{Z}^+$. الآن:

$$\begin{aligned} f(n+tp) &= a_k(n+tp)^k + \dots + a_1(n+tp) + a_0 \\ &= (a_k n^k + \dots + a_1 n + a_0) + pg(t) \\ &= f(n) + pg(t) \\ &= p + pg(t) \\ &= p(1+g(t)) \end{aligned}$$

حيث $g(t)$ كثيرة حدود معاملاتها أعداد صحيحة. ولذا فإن $p \mid f(n+tp)$. وبما أن $f(n+tp)$ عدد أولي فإن $f(n+tp)=p$ لكل $t \in \mathbb{Z}^+$. أي يوجد عدد غير منته من الأعداد $y \in \mathbb{Z}^+$ حيث $f(y)=p$ وهذا مستحيل لأن درجة f هي k △

تمارين (٢,٢)

(١) أثبت أنه يوجد عدد أولي $p_n > n$ لكل $n \geq 1$. ثم استنتج أن عدد الأعداد الأولية غير منته. [إرشاد : ضع $Q_n = n!+1$].

(٢) لتكن $p_1 < p_2 < \ldots < p_n$ أول n من الأعداد الأولية وليكن $1 < m < n$. ولنفرض أن $S = p_1 p_2 \ldots p_m$ وأن $R = p_{m+1}\, p_{m+2} \ldots p_n$. إذا كان p عدداً أولياً يقسم $S+R$ فأثبت أن $p \neq p_i$ لكل $1 \leq i \leq n$. ثم استنتج وجود عدد غير منته من الأعداد الأولية.

(٣) لتكن $p_1 < p_2 < \ldots < p_n$ أول n من الأعداد الأولية وليكن $N = p_1 p_2 \ldots p_n$. إذا كان p عدد أولياً يقسم $N-1$ فأثبت أن $p \neq p_i$ لكل $1 \leq i \leq n$. ثم استنتج وجود عدد غير منته من الأعداد الأولية.

(٤) أثبت وجود عدد غير منته من الأعداد الأولية التي على الصورة $3k+2$.

(٥) أثبت وجود عدد غير منته من الأعداد الأولية التي على الصورة $6k-1$.

(٦) إذا كانت $f(n) = n^2+n+41$ فأثبت أن $f(n)$ عدد أولي لكل $0 \leq n \leq 39$ ولكن $f(40)$ عدد مؤلف.

(٧) إذا كان $f(n) = n^2-n+41$ فأثبت أن $f(n)$ عدد أولي لكل $0 \leq n \leq 40$ ولكن $f(41)$ عدد مؤلف.

(٨) إذا كانت $f(n) = n^2-79n+1601$ فأثبت أن $f(n)$ عدد أولي لكل $0 \leq n \leq 79$ ولكن $f(80)$ عدد مؤلف.

(٩) إذا كان $(a,b)=1$ فأثبت وجود عدد غير منته من الأعداد المؤلفة في المتتالية الحسابية $a, a+b, a+2b, a+3b, \ldots$.

(١٠) إذا كان كل من p و $p+3$ عدداً أولياً فأثبت أن $p=2$.

(١١) استخدم مبرهنة بيرتراند لإثبات أن $p_n < 2^n$ حيث $n \geq 2$ و p_n هو العدد الأولي الذي رتبته n.

(١٢) إذا كان p_k هو العدد الأولي الذي رتبته k فاستخدم الحقيقة "يوجد على الأقل عددين أوليين بين n و $2n$ لكل $n \geq 6$" لإثبات أن $p_{k+2} \leq p_k + p_{k+1}$.

(١٣) استخدم مبرهنة بيرتراند لإثبات أن $m!$ لا يمكن أن يكون مربعاً كاملاً لكل $m \geq 2$.

(١٤) ليكن $a,b \in \mathbb{Z}^+$ حيث $(a,b)=1$. إذا وجد عدد أولي على الصورة $ak+b$ فأثبت أنه يوجد عدد غير منته من الأعداد الأولية على الصورة $ak+b$.

(١٥) استخدم حدس جولدباخ لإثبات أن أي عدد صحيح فردي $n > 7$ يمكن كتابته كمجموعة ثلاثة أعداد أولية فردية.

(١٦) أثبت أن العبارتين التاليتين متكافئتين:

(أ) حدس جولدباخ.

(ب) كل عدد صحيح $n > 5$ يمكن كتابته كمجموع ثلاثة أعداد أولية

(٢,٣) أعداد فيرما وأعداد ميرسين
Fermat and Mersenne Numbers

لقد لاحظ فيرما أن جميع الأعداد :

$2^{2^0}+1=3$ ، $2^{2^1}+1=5$ ، $2^{2^2}+1=17$ ، $2^{2^3}+1=257$ ، $2^{2^4}+1=65537$

هي أعداد أولية وتوقع أن تكون جميع الأعداد التي على الصورة $F_n = 2^{2^n}+1$ حيث $n \geq 0$ أعداد أولية حيث كتب للرياضي ميرسين "لقد وجدت أن جميع الأعداد F_n يجب أن تكون أولية ولكنني غير قادر على إثبات ذلك" وفي رسالة لاحقة أعرب عن

استيائه لأن جميع محاولاته لإثبات حدسه باءت بالفشل. بقيت المسألة حتى تمكن أويلر *(Euler)* من حلها عام ١٧٣٢م إذ وجد أن العدد $F_5 = 2^{2^5}+1 = 4294967297$ يقبل القسمة على 641. فبعد أن لاحظ أويلر أن $641 = 2^4 + 5^4 = 5\times 2^7 + 1$، استنتج التالي:

$$\begin{aligned} 2^{32} = 2^4 \times 2^{28} &= (641 - 5^4)\times 2^{28} \\ &= 641\times 2^{28} - 5^4 \times 2^{28} \\ &= 641\times 2^{28} - (5\times 2^7)^4 \\ &= 641\times 2^{28} - (641-1)^4 \\ &= 641k - 1 \end{aligned}$$

حيث $k \in \mathbb{Z}$. ولذا فإن 641 يقسم $F_5 = 2^{32}+1$.

تسمى الأعداد $F_n = 2^{2^n}+1$ حيث $n \geq 0$ أعداد فيرما. نقدم هنا بعض خصائصها الأساسية ونستخدمها لتقديم برهان آخر على وجود عدد غير منته من الأعداد الأولية.

مبرهنة (٢,١٣)

$(F_n, F_m) = 1$ لكل $m \neq n$.

البرهان

لنفرض أن $m = n+k$ حيث $k > 0$ ولنفرض أن $(F_n, F_{n+k}) = d$. ولذا فإن $d \mid F_n$ و $d \mid F_{n+k}$. الآن إذا كانت $f(x) = x^{2^k} - 1$ فإن $f(-1) = 0$. ولذا فإن $x+1$ يقسم $x^{2^k} - 1$. وبوضع $x = 2^{2^n}$ نجد أن F_n يقسم $F_{n+k} - 2$. ولذا فإن $d \mid (F_{n+k} - 2)$. أي أن $d \mid 2$. وبما أن أعداد فيرما جميعها فردية فإن $d = 1$ ◆

نتيجة (٢,١٤)

يوجد عدد غير منته من الأعداد الأولية.

البرهان

لكل $m,n\in\mathbb{Z}^+$ حيث $m\neq n$ يوجد عددان أوليان p_n و p_m يحققان $p_n\mid F_n$ و $p_m\mid F_m$. وبما أن $(F_m,F_n)=1$ فإن $p_n\neq p_m$. ولذا فإنه يوجد عدد غير منته من الأعداد الأولية ◆

لعله من المناسب أن نسأل الآن عن الأعداد الأولية التي على الصورة 2^m+1. المبرهنة التالية تبين لنا أن هذه الأعداد يجب أن تكون أعداد فيرما. أي أنه هناك $n\geq 0$ بحيث يكون $m=2^n$.

مبرهنة (٢,١٥)

إذا كان $a=2^m+1$ عدداً أولياً فهناك $n\geq 0$ $a=F_n$.

البرهان

سنبرهن المكافئ العكسي، أي إذا كان $m\neq 2^n$ لكل $n\geq 0$ فإن a مؤلف. بما أن $m\neq 2^n$ لكل $n\geq 0$ فإنه يوجد عدد فردي $k>1$ حيث $m=2^n k$. الآن ، إذا كانت $f(x)=x^k+1$ فإن $f(-1)=0$. ولذا فإن $x+1$ يقسم x^k+1. وبوضع $x=t^{2^n}$ نجد أن $t^{2^n}+1$ يقسم $t^{2^n k}+1$. أي أن $t^{2^n}+1$ يقسم t^m+1. وبوضع $t=2$ نجد أن $2^{2^n}+1$ يقسم 2^m+1. أي أن 2^m+1 عدد مؤلف ◆

هل يوجد عدد غير منته من أعداد فيرما الأولية؟ إن أعداد فيرما الأولية المعروفة لتاريخ إعداد هذا الكتاب هي فقط الأعداد التي اكتشفها فيرما وهي F_0 , F_1 , F_2 , F_3 , F_4. ولقد تم إثبات أن جميع الأعداد F_n حيث $5\leq n\leq 22$ مؤلفة وذلك بتحليل الأعداد F_n ، $5\leq n\leq 11$ تحليلاً كاملاً إلى عواملها الأولية بمساعدة حاسبات سريعة جداً. وأما الأعداد F_n حيث $12\leq n\leq 22$ فإنه تم إيجاد بعض عواملها الأولية وننتظر تحليلها كاملاً. حتى الآن فإن عدد أعداد فيرما المؤلفة المعروفة هو 84 وأكبرها F_{23471} الذي اكتشفه الرياضي كيلر (*Keller*) عام ١٩٨٤م حيث يحتوي على أكثر من 10^{7000} مرتبة

عشرية وأحد قواسمه هو $5\times 2^{23473}+1$. كما أن أصغر أعداد فيرما التي لم يتم معرفة ما إذا كانت أولية هو العدد F_{28} . حيث أعلن في تاريخ ١٩٩٩/٩/٢٢م عن إثبات أن العدد F_{24} والذي يحتوي على أكثر من خمسة ملايين مرتبة عشرية أنه مؤلفاً دون معرفة أي من قواسمه، وتوصل إلى ذلك كل من ماير (*Mayer*)، باپادابولس (*Papadopoulos*) وكراندال (*Crandall*) (وللمزيد من المعلومات أنظر حلقة النقاش حول نظرية الأعداد على:

(NMBRTHRY@LISTERV.NODAK.EDU)

ننتقل الآن إلى دراسة أعداد ميرسين.

مبرهنة (٢,١٦)

إذا كان $m>1$ وكان a^m-1 عدداً أولياً فإن $a=2$ و m عدد أولي.

البرهان

إذا كان $a>2$ فإن: $a^m-1=(a-1)(a^{m-1}+a^{m-2}+\ldots+a+1)$

عدداً مؤلفاً . ولذا فإن $a=2$. وإذا كان m عدداً مؤلفاً فإن $m=rs$ حيث $1<r,s<m$ ونرى من المساواة

$2^m-1=(2^r)^s-1=(2^r-1)\,(2^{r(s-1)}+2^{r(s-2)}+\ldots+1)$ أن 2^m-1

مؤلف وهذا تناقض. فإذن m عدد أولي ◆

لقد كان سائداً أن عكس المبرهنة (٢,١٦) صحيح أيضاً، إلى أن بين الرياضي ريجيز (*Regius*) في العام ١٥٣٦م أن العدد $2^{11}-1=2047=23\times 89$ مؤلفاً. وفي العام ١٦٠٣م أثبت الرياضي كاتالدي (*Cataldi*) أن كلاً من العددين $2^{17}-1$ و $2^{19}-1$ أولي. كذلك ادعى ميرسين في العام ١٦٤٤م أن العدد 2^n-1 أولي للقيم :

$n=2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ وأنه مؤلف لجميع قيم n الأخرى التي تقل عن 257. وانقضى قرن من الزمان قبل أن يتحقق أويلر في العام

١٧٥٠م من أن $2^{31}-1$ هو بالفعل عدد أولي، وبعد مرور قرن آخر استطاع لوقا *(Locus)* في العام ١٨٧٦م أن يثبت أن العدد $2^{127}-1$ عدد أولي، وبعد سبع سنوات وجد بيرفوتشن *(Pervouchin)* أن $2^{61}-1$ عدد أولي مثبت خطأ إدعاء ميرسين. ومع بداية القرن العشرين وجد باورز *(Powers)* أن العددين $2^{89}-1$ و $2^{107}-1$ أوليان. وأصبحت القائمة الصحيحة مع نهاية الحرب العالمية الثانية هي:

$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$ (أنظر الجدول في نهاية البند).

وعلى الرغم من الخطأ الذي وقع به ميرسين إلا أن الأعداد التي على الصورة $M_n = 2^n - 1$ حملت اسمه وتعرف بأعداد ميرسين. وإذا كانت أولية فإنها تسمى أعداد ميرسين الأولية وسيكون لها أهمية خاصة عند دراستنا للأعداد التامة. وكما هو الحال مع أعداد فيرما فإنه لا زال هناك الكثير من الأسئلة حول أعداد ميرسين تنتظر الإجابة عنها ، من هذه الأسئلة:

هل يوجد عدد غير منته من أعداد ميرسين الأولية؟

هل يوجد عدد غير منته من أعداد ميرسين المؤلفة؟

تشير الدلائل إلى صواب هاتين المسألتين ولكن أحداً لم يتوصل إلى برهان أي منهما.

الجدول التالي يبين أعداد مرسين الأولية التي تم اكتشافها إلى تاريخ اعداد هذا الكتاب.

التسلسل	p	M_p	عدد مراتب M_p	تاريخ الاكتشاف	المكتشف
1	2	3	1	5th century BC	Ancient Greek mathematicians
2	3	7	1	5th century BC	Ancient Greek mathematicians

التسلسل	p	M_p	عدد مراتب M_p	تاريخ الاكتشاف	المكتشف
3	5	31	2	3rd century BC	Ancient Greek mathematicians
4	7	127	3	3rd century BC[8]	Ancient Greek mathematicians
5	13	8191	4	1456	*anonymous*
6	17	131071	6	1588	Cataldi
7	19	524287	6	1588	Cataldi
8	31	2147483647	10	1772	Euler
9	61	2305843009213693951	19	1883	Pervushin
10	89	618970019...449562111	27	1911	Powers
11	107	162259276...010288127	33	1914	Powers
12	127	170141183...884105727	39	1876	Lucas
13	521	686479766...115057151	157	January 30, 1952	Robinson, using SWAC (computer)
14	607	531137992...031728127	183	January 30, 1952	Robinson
15	1,279	104079321...168729087	386	June 25, 1952	Robinson
16	2,203	147597991...697771007	664	October 7, 1952	Robinson
17	2,281	446087557...132836351	687	October 9, 1952	Robinson
18	3,217	259117086...909315071	969	September 8, 1957	Riesel, using BESK
19	4,253	190797007...350484991	1,281	November 3, 1961	Hurwitz, using IBM 7090
20	4,423	285542542...608580607	1,332	November 3, 1961	Hurwitz
21	9,689	478220278...225754111	2,917	May 11,	Gillies, using

التسلسل	p	M_p	عدد مراتب M_p	تاريخ الاكتشاف	المكتشف
				1963	ILLIAC II
22	9,941	346088282…789463551	2,993	May 16, 1963	Gillies
23	11,213	281411201…696392191	3,376	June 2, 1963	Gillies
24	19,937	431542479…968041471	6,002	March 4, 1971	Tuckerman, using IBM 360/91
25	21,701	448679166…511882751	6,533	October 30, 1978	Noll & Nickel, using CDC Cyber 174
26	23,209	402874115…779264511	6,987	February 9, 1979	Noll
27	44,497	854509824…011228671	13,395	April 8, 1979	Nelson & Slowinski
28	86,243	536927995…433438207	25,962	September 25, 1982	Slowinski
29	110,503	521928313…465515007	33,265	January 28, 1988	Colquitt & Welsh
30	132,049	512740276…730061311	39,751	September 19, 1983	Slowinski
31	216,091	746093103…815528447	65,050	September 1, 1985	Slowinski
32	756,839	174135906…544677887	227,832	February 19, 1992	Slowinski & Gage on Harwell Lab Cray-2
33	859,433	129498125…500142591	258,716	January 4, 1994	Slowinski & Gage
34	1,257,787	412245773…089366527	378,632	September 3, 1996	Slowinski & Gage
35	1,398,269	814717564…451315711	420,921	November 13, 1996	GIMPS / Joel Armengaud

التسلسل	p	M_p	عدد مراتب M_p	تاريخ الاكتشاف	المكتشف
36	2,976,221	623340076…729201151	895,932	August 24, 1997	GIMPS / Gordon Spence
37	3,021,377	127411683…024694271	909,526	January 27, 1998	GIMPS / Roland Clarkson
38	6,972,593	437075744…924193791	2,098,960	June 1, 1999	GIMPS / Nayan Hajratwala
39	13,466,917	924947738…256259071	4,053,946	November 14, 2001	GIMPS / Michael Cameron
40	20,996,011	125976895…855682047	6,320,430	November 17, 2003	GIMPS / Michael Shafer
41	24,036,583	299410429…733969407	7,235,733	May 15, 2004	GIMPS / Josh Findley
42	25,964,951	122164630…577077247	7,816,230	February 18, 2005	GIMPS / Martin Nowak
43	30,402,457	315416475…652943871	9,152,052	December 15, 2005	GIMPS / Curtis Cooper & Steven Boone
44	32,582,657	124575026…053967871	9,808,358	September 4, 2006	GIMPS / Curtis Cooper & Steven Boone
45	37,156,667	202254406…308220927	11,185,272	September 6, 2008	GIMPS / Hans-Michael Elvenich
46	43,112,609	316470269…697152511	12,978,189	August 23, 2008	GIMPS / Edson Smith

تمارين (٢,٣)

(١) إذا كان $a \geq 2$ وكان $a^m + 1$ عدداً أولياً فأثبت أن a عدد زوجـــي وأن m قوة للعدد 2.

(٢) أثبت أن $F_0 F_1 F_2 \ldots F_{n-1} = F_n - 2$ لكل $n \geq 1$.

(٣) (أ) أثبت أن $F_{n+1} = F_n^2 - 2F_n + 2$ لكل $n \geq 0$.

(ب) استخدم الفقرة (أ) لإثبات أنه إذا كان p عدداً أولياً حيث $p \mid F_n$ فإن $p \mid (F_{n+k} - 2)$ لكل $k \geq 1$.

(ج) استخدم الفقرة (أ) لإثبات أن $(F_n, F_{n+k}) = 1$ لكل $k \geq 1$.

(٤) لتكن $\{C_n\}$ المتتالية المعرفة استقرائياً على النحو التالي:

$C_0 = 2$ و $C_{n+1} = C_n^2 - C_n + 1$ لكل $n \geq 0$.

(أ) إذا كان p عدداً أولياً حيث $p \mid C_n$ فأثبت أن $p \mid (C_{n+k} - 1)$ لكل $k \geq 1$.

(ب) استخدم الفقرة (أ) لإثبات أن $(C_n, C_{n+k}) = 1$ لكل $k \geq 1$.

(ج) استنتج من الفقرة (ب) أن عدد الأعداد الأولية غير منته.

(٥) لقد ادعى فيرما أنه إذا كان a عدداً زوجياً فإن العدد $N = a^{2^n} + 1$ أولياً ما لم يقبل القسمة على أحد أعداد فيرما F_k . هل ادعاء فيرما صحيح؟

(٦) أثبت أن مرتبة الآحاد لعدد فيرما F_n تساوي 7 لكل $n > 1$.

(٧) أثبت أن $F_n + 4$ عدد مؤلف لكل $n \geq 1$.

(٢,٤) اختبار الأوليات والتحليل
Primality Testing and Factorization

لعل أهم مسائل نظرية الأعداد المسألتين التاليتين:

(١) إذا كان $n \in \mathbb{Z}^+$ فكيف نختبر ما إذا كان n أولياً أم لا؟

(٢) إذا كان $n \in \mathbb{Z}^+$ فكيف يمكن إيجاد عوامله الأولية؟ أي تحليله إلى قوى عوامله الأولية.

في هذا البند سنقدم فكرة بسيطة حول كيفية التعامل مع كل من هاتين المسألتين وسنرجع إليهما بين الحين والآخر في هذا الكتاب وذلك كلما قدمنا مفهوماً جديداً يساعدنا على اكتشاف طرق جديدة.

نبدأ تناول المسألة الأولى والتي تعرف عادة باسم اختبار الأوليات بتقديم المبرهنة التالية:

مبرهنة (٢,١٧)

يكون العدد الصحيح $n > 1$ مؤلفاً إذا وفقط إذا وجد له قاسم أولي p حيث $p \le \sqrt{n}$.

البرهان

لنفرض أولاً أن $n > 1$ مؤلف. ولذا فإن $n = ab$ حيث $1 < a \le b < n$. ومنه فإن $n = ab \ge a^2$. ولذا فإن $a \le \sqrt{n}$. وبما أنه يوجد قاسم أولي p للعدد a فإن $p \le a \le \sqrt{n}$ وأن p قاسم للعدد n. وبرهان العكس واضح ◆

المبرهنة (٢,١٧) تقدم لنا إحدى الطرق لاختبار أولية العدد n حيث نجرب جميع الأعداد الأولية التي لا تزيد عن $\sqrt{n}$. وننوه هنا أن هذه الطريقة مناسبة جداً إذا كان العدد n صغير نسبياً حيث تكون الأعداد الأولية التي نجربها قليلة نوعاً ما.

مثال(٢,٥)

بين ما إذا كان العدد 859 أولياً أم لا.

الحل

بما أن $\sqrt{859} < 30$ فإنه يكفي أن نختبر ما إذا كان العدد 859 يقبل القسمة على أي من الأعداد الأولية $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$. وبالتجريب نجد أن كلاً من هذا الأوليات لا يقسم 859. ولذا فإن 859 عدد أولي □

اختبارات القسمة التي تقدمها المبرهنة التالية تعيننا على اختبار الأوليات.

مبرهنة (٢,١٨)

ليكن $N = a_m 10^m + a_{m-1}10^{m-1} + \ldots + a_1 10 + a_0$ وليكن لكل $k \le m$. وليكن

$$N_k = a_{k-1}10^{k-1} + a_{k-2}10^{k-2} + \ldots + a_1 10 + a_0$$

$S = \sum_{k=0}^{m} a_k$ و $T = \sum_{k=0}^{m} (-1)^k a_k$. عندئذ:

(أ) $2^k \mid N$ إذا وفقط إذا كان $2^k \mid N_k$.

(ب) $5^k \mid N$ إذا وفقط إذا كان $5^k \mid N_k$.

(ج) $3 \mid N$ إذا وفقط إذا كان $3 \mid S$.

(د) $9 \mid N$ إذا وفقط إذا كان $9 \mid S$.

(هـ) $11 \mid N$ إذا وفقط إذا كان $11 \mid T$.

البرهان

برهان الفقرة (أ) يشابه برهان الفقرة (ب) وكذلك برهانا الفقرتين (ج) و (د) متشابهتان. لذا نكتفي بإثبات الفقرات (أ) ، (د) ، (هـ).

(أ) لاحظ أن $2^k \mid 10^n$ لكل $n \ge k$. ولذا فإن:

$$\begin{aligned} 2^k \mid N &\Leftrightarrow 2^k \mid (a_m 10^m + \ldots + a_k 10^k + a_{k-1}10^{k-1} + \ldots + a_1 10 + a_0) \\ &\Leftrightarrow 2^k \mid (a_{k-1}10^{k-1} + \ldots + a_1 10 + a_0) \\ &\Leftrightarrow 2^k \mid N_k \end{aligned}$$

(د) من مبرهنة ذات الحدين نلاحظ ابتداءاً أن

$10^i = (9+1)^i = 9r+1$ لكل $1 \le i \le m$. ولذا فإن:

$N = 9t + a_m + a_{m-1} + \ldots + a_1 + a_0 = 9t + S$. ونخلص إلى أن:

$9 \mid N \Leftrightarrow 9 \mid S$.

(هـ) من مبرهنة ذات الحدين لدينا:

$10^i = (11-1)^i = 11r + (-1)^i$ لكل $1 \le i \le m$. ولذا فإن :

$N = 11t + (-1)^m a_m + (-1)^{m-1} a_{m-1} + \ldots - a_1 + a_0 = 11t + T$

فنستنتج $11 \mid N \Leftrightarrow 11 \mid T$ ◆

مثال (٢,٦)

جدْ أعلى قوة k للعدد 2 بحيث يقبل العدد $N = 4157892348$ القسمة على 2^k.

الحل

بما أن $2^2 = 4 \mid 48$ فإن $4 \mid N$. وبما أن $2^3 \nmid 348$ فإن $2^3 \nmid N$. إذن أعلى قوة هي $k = 2$ □

مثال (٢,٧)

جدْ أعلى قوة k للعدد 5 بحيث إن العدد $N = 7963625$ يقبل القسمة على 5^k.

الحل

بما أن $5^3 \mid 625$ فإن $5^3 \mid N$. وبما أن $5^4 \nmid 3625$ فإن $5^4 \nmid N$. إذن أعلى قوة هي $k = 3$ □

مثال(٢,٨)

اختبر قابلية العدد $N=894325734$ للقسمة على كل من 9 و 11.

الحل

بما أن: $S=4+3+7+5+2+3+4+9+8=45$ يقبل القسمة على 9 فإن N يقبل القسمة على 9. وبما أن $T=4-3+7-5+2-3+4-9+8=5$ لا يقبل القسمة على 11 فإن العدد N لا يقبل القسمة على 11 □

تزودنا المبرهنة التالية باختبار قابليّة القسمة على الأعداد الأولية 7، 11 ، 13.

مبرهنة (٢,١٩)

ليكن $q(n)$ و $r(n)$ خارج القسمة والباقي اللذان نحصل عليهما عند قسمة العدد n على العدد 1000. فإذا كان $c=7$ أو $c=11$ أو $c=13$ فإن:

$c \mid n$ إذا وفقط إذا كان $c \mid (q(n)-r(n))$.

البرهان

لاحظ أن $7\times11\times13=1001$. بما أن $n=1000q(n)+r(n)$ فإن:

$$q(n)-r(n)=q(n)-n+1000q(n)=1001q(n)-n.$$

ومنه نجد أن: $c \mid n$ إذا وفقط إذا كان $c \mid (1001q(n)-n)$ ، أي إذا وفقط إذا كان $c \mid (q(n)-r(n))$ ◆

مثال(٢,٩)

اختبر قابلية قسمة العدد $n=14824017659$ على كل من 7 و 11 و 13 .

الحل

$$14824017659=1000\times14824017+659$$

وعليه فإن: $q(n)-r(n)=14824017-659=14823358$

وبقسمة العدد $n_1=14823358$ على 1000 نجد:

$$14823358 = 1000 \times 14823 + 358$$

ونحصل على : $q(n_1) - r(n_1) = 14823 - 358 = 14465$.

وبقسمة العدد $n_2 = 14465$ على 1000 مرة أخرى نجد:

$$14465 = 1000 \times 14 + 465 .$$

ونحصل على $q(n_2) - r(n_2) = 14 - 465 = -451$.

بما أن $11 \mid (-451)$ وأن $7 \nmid (-451)$ وأن $13 \nmid (-451)$ فإننا نجد $11 \mid n$ ولكن $7 \nmid n$ و $13 \nmid n$ □

نقدم الآن مبرهنة تساعدنا على اختبار ما إذا كان عدد ميرسين أولياً وأخرى لاختبار ما إذا كان عدد فيرما أولياً ولكننا نؤجل برهانهما إلى وقت لاحق.

مبرهنة (٢,٢٠)

إذا كان p عدداً أولياً وكان q قاسماً أولياً لعدد ميرسين $M_p = 2^p - 1$ فإن $q = 2kp + 1$ حيث $k \in \mathbb{Z}$.

البرهان

◆ انظر التمرين (٨) من التمارين المحلولة (٣,٥,٤)

مبرهنة (٢,٢١)

إذا كان p قاسماً أولياً لعدد فيرما $F_n = 2^{2^n} + 1$ حيث $n > 1$ فإن $p = 2^{n+2}k + 1$ حيث $k \in \mathbb{Z}$.

البرهان

◆ انظر التمرين (٧) من التمارين المحلولة (٧,١,١)

مثال (٢,١٠)

بين ما إذا كان $M_{23} = 2^{23} - 1$ أولياً أم لا.

الحل

إذا كان p قاسماً أولياً للعدد M_{23} فإن $p=46k+1$ حيث $k\in\mathbb{Z}$. أي أن $p=47,139,277,\ldots$. من السهل أن نرى أن $47\mid M_{23}$. ولذا فإن M_{23} عدد مؤلف □

مثال (٢,١١)

أثبت أن $F_5=2^{2^5}+1$ عدد مؤلف.

الحل

إذا كان p قاسماً أولياً للعدد F_5 فإن $p=2^7k+1$. أي أن $p=257,641,\ldots$. ولكن $641\mid F_5$. إذن، F_5 مؤلف □

كما أسلفنا تصلح الاختبارات التي قدمناها عندما يكون العدد n صغيراً نسبياً. أما إذا كان العدد n كبيراً فهذه الطرق غير مجدية إذ يتعين علينا اختبار عدد كبير جداً من قواسم n الأولية، على سبيل المثال إذا كان $n\approx 10^{100}$ فإننا نجد باستخدام مبرهنة الأعداد الأولية أن عدد الأعداد الأولية $p\le\sqrt{n}$ هو :

$$\pi(\sqrt{n})\approx\frac{\sqrt{n}}{\ln\sqrt{n}}=\frac{2\sqrt{n}}{\ln n}\approx 8\times 10^{47}$$

ومن الواضح حتى لو استخدمنا أسرع الحاسبات الآلية فإننا لن نستطيع اجراء الحسابات المطلوبة. ولحسن الحظ هناك طرق أفضل بكثير من ذلك، سنتعرض لها لاحقاً.

قبل الانتقال إلى المسألة الثانية من هذا البند، نقدم طريقة تعرف بمرشح آراتوستينس *(Sieve of Eratosthenes)* لتحديد الأعداد الأولية التي تقل عن عدد معطى n. لتوضيح هذه الطريقة نقوم بإيجاد الأعداد الأولية بين 1 و 100.

الخطوة الأولى هي كتابة هذه الأعداد:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100

ثم نقوم بكتابة جميع مضاعفات العدد 2 بخط أزرق لنحصل على:

1, **2**, 3, **4**, 5, **6**, 7, **8**, 9, **10**, 11, **12**, 13, **14**, 15, **16**, 17, **18**, 19, **20**, 21, **22**, 23, **24**, 25, **26**, 27, **28**, 29, **30**, 31, **32**, 33, **34**, 35, **36**, 37, **38**, 39, **40**, 41, **42**, 43, **44**, 45, **46**, 47, **48**, 49, **50**, 51, **52**, 53, **54**, 55, **56**, 57, **58**, 59, **60**, 61, **62**, 63, **64**, 65, **66**, 67, **68**, 69, **70**, 71, **72**, 73, **74**, 75, **76**, 77, **78**, 79, **80**, 81, **82**, 83, **84**, 85, **86**, 87, **88**, 89, **90**, 91, **92**, 93, **94**, 95, **96**, 97, **98**, 99, **100**

الآن نقوم بكتابة جميع مضاعفات العدد الأولي 3 بخط أزرق لنحصل على:

1, 2, 3, **4**, 5, **6**, 7, **8**, **9**, **10**, 11, **12**, 13, **14**, **15**, **16**, 17, **18**, 19, **20**, **21**, **22**, 23, **24**, 25, **26**, **27**, **28**, 29, **30**, 31, **32**, **33**, **34**, 35, **36**, 37, **38**, **39**, **40**, 41, **42**, 43, **44**, **45**, **46**, 47, **48**, 49, **50**, **51**, **52**, 53, **54**, 55, **56**, **57**, **58**, 59, **60**, 61, **62**, **63**, **64**, 65, **66**, 67, **68**, **69**, **70**, 71, **72**, 73, **74**, **75**, **76**, 77, **78**, 79, **80**, **81**, **82**, 83, **84**, 85, **86**, **87**, **88**, 89, **90**, 91, **92**, **93**, **94**, 95, **96**, 97, **98**, **99**, **100**

نقوم الآن بكتابة جميع مضاعفات العدد 5 والعدد 7 بخط أزرق لنحصل في النهاية على:

1, 2, 3, **4**, 5, **6**, 7, **8**, **9**, **10**, 11, **12**, 13, **14**, **15**, **16**, 17, **18**, 19, **20**, **21**, **22**, 23, **24**, **25**, **26**, **27**, **28**, 29, **30**, 31, **32**, **33**, **34**, **35**, **36**, 37, **38**, **39**, **40**, 41, **42**, 43, **44**, **45**, **46**, 47, **48**, **49**, **50**, **51**, **52**, 53, **54**, **55**, **56**, **57**, **58**, 59, **60**, 61, **62**, **63**, **64**, **65**, **66**, 67, **68**, **69**, **70**, 71, **72**, 73, **74**, **75**, **76**, **77**, **78**, 79, **80**, **81**, **82**, 83, **84**, **85**, **86**, **87**, **88**, 89, **90**, **91**, **92**, **93**, **94**, **95**, **96**, 97, **98**, **99**, **100**

بما أن $\sqrt{100} = 10$ وأن 7 أكبر عدد أولي أصغر من $\sqrt{100}$ فإننا نتوقف هنا وتكون جميع الأعداد التي لم يتم كتابتها بخط أزرق وأكبر من 1 هي الأعداد الأولية المطلوبة.

لا تعتبر مرشحة أراتوستينس طريقة عملية لاختبار أولية العدد n ولكن أهميتها تكمن في استخدامها كمؤشر على اختبار سرعة الحاسب الآلي المستخدم.

ننتقل الآن إلى المسألة الثانية في هذا البند وهي مسألة تحليل العدد إلى عوامله الأولية.

من الواضح أن هذه المسألة أكثر صعوبة من مسألة اختبار الأوليات. لأنها لا يمكن أن تكون أسهل، فمتى ما حصلنا على تحليل للعدد إلى قوى عوامله الأولية فسنعرف مباشرة ما إذا كان العدد أولياً أم لا.

لكل $n>1$ ، تتم مسألة تحليل n إلى قوى عوامله الأولية (على الأقل من الناحية النظرية) على النحو التالي: نختبر قابلية قسمة العدد على الأعداد الأولية $p=2,3,5,...$ إلى أن نجد قاسماً أولياً p. عندئذٍ نستبدل العدد n بالعدد $\frac{n}{p}$ ونعيد الكرة إلى أن نحصل على جميع عوامل p الأولية. ومن ثم نستطيع تحليله.

إن هذه طريقة ممتازة إذا كان العدد n صغيراً نسبياً ولكنها ليست عملية إذا كان n كبيراً لأنه كما هو الحال في اختبار أولية العدد نحتاج إلى تجريب عدد كبير من الأوليات. في الحقيقة هناك طرائق أخرى أفضل من ذلك لتحليل العدد سنتطرق إليها لاحقاً في هذا الكتاب ولكننا نود الإشارة هنا إلى أن أفضل الخوارزميات الموجودة وأسرع الحاسبات لا تستطيع أن تحلل عدد مكون من بضع مئات من المراتب بوقت مقبول. نقدم هنا طريقتان للتحليل هما طريقتي فيرما وأويلر.

(٢,٤,١) طريقة فيرما للتحليل *(Fermat Factorization Method)*

تُعنى هذه الطريقة بتحليل الأعداد الفردية فقط ويمكن الاستفادة منها بكتابة العدد m على الصورة $m=2^k n$ حيث n عدد فردي.

مبرهنة (٢,٢٢)

إذا كان $n \in \mathbb{Z}^+$ عدداً فردياً فإنه يمكن كتابة n كحاصل ضرب عددين إذا وفقط إذا أمكن كتابته كفرق بين مربعين.

البرهان

إذا كان $n = ab$ حيث $1 < a,b < n$ فمن الواضح أن:

$$n = ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 .$$

(لاحظ أن كل من a و b فردي لأن n فردي).

وبالعكس، إذا كان $n = x^2 - y^2$ فإن $n = (x-y)(x+y)$ ◆

لاستخدام المبرهنة (٢,٢٢) لتحليل العدد الفردي n ، نكتب $x^2 = n + y^2$. وبما أن $x^2 \geq n$ فإن $x \geq \sqrt{n}$. ولذا فإننا يجب أن نبحث عن مربع كامل بين حدود المتتالية: $x^2 - n, (x+1)^2 - n, (x+2)^2 - n, \ldots$.

وهذا البحث بالتأكيد يجب أن ينتهي لأن تحليل العدد $n = n \times 1$ يؤدي إلى

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 .$$

مثال (٢,١٢)

استخدم طريقة فيرما لتحليل العدد 119143.

الحل

بما أن $346 < \sqrt{119143}$ فإننا نبحث عن مربع كامل في المتتالية:

$$(346)^2 - 119143 = 573 \neq y^2$$
$$(347)^2 - 119143 = 1266 \neq y^2$$
$$(348)^2 - 119143 = 1961 \neq y^2$$
$$(349)^2 - 119143 = 2658 \neq y^2$$

$$(350)^2 - 119143 = 3347 \neq y^2$$
$$(351)^2 - 119143 = 4058 \neq y^2$$
$$(352)^2 - 119143 = 4761 = (69)^2$$

ولذا فإن: $119143 = (352-69)(352+69) = 283 \times 421$

كلا العددين 421 و 283 أولي □

مثال(٢,١٣)

استخدم طريقة فيرما لتحليل العدد $n = 2027651281$ (هذا هو العدد الذي استخدمه فيرما).

الحل

بما أن $45030 < \sqrt{n}$ فإننا نبحث عن مربع كامل في المتتالية:

$$(45030)^2 - n = 49619 \neq y^2$$
$$(45031)^2 - n = 139680 \neq y^2$$
$$(45032)^2 - n = 229743 \neq y^2$$
$$(45033)^2 - n = 319808 \neq y^2$$
$$(45034)^2 - n = 409875 \neq y^2$$
$$(45036)^2 - n = 499944 \neq y^2$$
$$(45036)^2 - n = 490015 \neq y^2$$
$$(45037)^2 - n = 680088 \neq y^2$$
$$(45038)^2 - n = 770163 \neq y^2$$
$$(45039)^2 - n = 860240 \neq y^2$$
$$(45040)^2 - n = 950319 \neq y^2$$
$$(45041)^2 - n = 1040400 = (1020)^2$$

ولذا فإن: $n = (45041-1020)(45041+1020) = 44021 \times 46061$.

ومن الممكن التأكد من أن كلا العددين 44021 و 46061 أولي □

ملحوظات

(١) من المعلوم أنه إذا كان $n=ab$ حيث $a-b$ صغير نسبياً فإن طريقة فيرما لتحليل n تصبح فعالة حيث نستطيع إيجاد العاملين a و b بسرعة، على سبيل المثال، إذا كان $n=23350947609$ فإن $\sqrt{n}<152843$ ونجد في المحاولة الثالثة أن $(152845)^2-n=(804)^2$. ولذا $n=152041\times153649$.

(٢) إذا كان الفرق $a-b$ كبيراً في تحليل العدد $n=ab$ فإن طريقة فيرما للتحليل تصبح عديمة الفعالية في هذه الحالة لأننا نحتاج إلى محاولات عديدة قبل الحصول على مربع كامل. لتحسين طريقة فيرما نقدم الطريقة المعممة التالية والتي غالباً ما تكون أفضل من طريقة فيرما، حيث نقوم باختيار عدد صغير k ثم نضع

$$t=\left[\sqrt{kn}\right]+1,\left[\sqrt{kn}\right]+2,\ldots$$

إلى أن نحصل على t بحيث يكون $t^2-kn=s^2$، وسنبين في الفصل السادس كيفية استخدام الكسور المتواصلة لإيجاد العدد k. وعليه فإن $(t+s)(t-s)=kn$. وبالتالي فإنه يوجد قاسم مشترك غير تافه بين العددين $t+s$ و n والذي يمكن الحصول عليه بإيجاد القاسم المشترك الأعظم $(t+s,n)$. نوضح ذلك بالمثال التالي:

مثال (٢,١٤)

استخدم طريقة فيرما المعممة حيث $k=3$ لتحليل العدد $n=135991$.

الحل

بما أن $\sqrt{3n}<639$ فإننا نبحث عن مربع كامل في المتتالية:

$$(639)^2-3n=348$$
$$(640)^2-3n=1627$$
$$(641)^2-3n=2908$$
$$(642)^2-3n=4191$$

$$(643)^2 - 3n = 5476 = (74)^2$$

الآن نقوم باستخدام خوارزمية إقليدس فنجد أن:

$$(643+74,135991) = (717,135991) = 239$$

وبالتالي فإن $135991 = 239 \times 569$ □

(٢,٤,٢) طريقة أويلر للتحليل *(Euler Factorization Method)*

لقد كتب أويلر في العام ١٦٤١م إلى فيرما رسالة اقترح فيها المسألة التالية: استخدم $221 = 10^2 + 11^2 = 5^2 + 14^2$ لتحليل العدد 221 إلى عواملـه الأوليـة. ولقد استخدم ميرسين فكرة كتابة العدد الفردي كمجموع مـربعين بطـريقتين مختلفتين لتحليل العدد ولكن أول من قدم برهاناً لذلك هو أويلر ولذا فإن الطريقة تنسب إليه .

ليكن $N = a^2 + b^2 = c^2 + d^2$ حيث N عدد فردي. ولذا فإننا نستطيع افتراض أن كلاً من a و c فردياً وكلاً من b و d زوجي. الآن :

$$a^2 - c^2 = d^2 - b^2 .$$

أي أن:

$$(a-c)(a+c) = (d-b)(d+b) \qquad (١)$$

لنفرض الآن أن $(a-c,d-b) = k$. ولـذا فإنـه يوجـد $u,w \in \mathbb{Z}$ حيـث $a-c = ku$ ، $d-b = kw$ ، $(u,w) = 1$. لاحظ أيضا أن k زوجي لأن كلاً من $a-c$ و $d-b$ زوجي. بالتعويض في (١) والاختصار نحصل على:

$$u(a+c) = w(d+b) \qquad (٢)$$

ومنه فإن $w \mid u(a+c)$. وبما أن $(u,w) = 1$ فإننا نجـد أن $w \mid (a+c)$. أي أن $a+c = wr$. وبالتعويض في (٢) نحصل على: $d+b = ur$. الآن:

$$[(k/2)^2+(r/2)^2)\,(w^2+u^2)=\frac{1}{4}[(kw)^2+(ku)^2+(rw)^2+(ru)^2]$$

$$=\frac{1}{4}[(d-b)^2+(a-c)^2+(a+c)^2+(d+b)^2]$$

$$=\frac{1}{4}[2a^2+2b^2+2c^2+2d^2]$$

$$=\frac{1}{4}[2N+2N]=N$$

وبهذا نكون قد وجدنا تحليلاً للعدد N.

مثال (٢,١٥)

بما أن $221=11^2+10^2=5^2+14^2$ فإن: $a=11\,،\ b=10\,،\ c=5\,،\ d=14$،
$k=2\,،\ u=3\,،\ w=2\,،\ r=8\,،\ a-c=6\,،\ a+c=16\,،\ d-b=4\,،\ d+b=24$.

ومن ثم فإن: $221=(1^2+4^2)\,(2^2+3^2)=17\times13$ □

(٢,٤,٣) تمارين محلولة (Solved Exercises)

تمرين (١)

إذا كان $0\le m<121$ وكان $210k+m$ عدداً أولياً فأثبت أن m عدد أولي.

الحل

لنفرض أن m عدد مؤلف. عندئذ يوجد قاسم أولي p للعدد m حيث $p\le\sqrt{m}<11$. هذا يعني أن p واحداً من الأعداد $2, 3, 5, 7$. ولكن $210=2\times3\times5\times7$. إذن، $p\mid(210k+m)$ وهذا مستحيل. وبالتالي فإن m أولي △

تمرين (٢)

إذا كان p أصغر قاسم أولي للعدد n وكان $p > \sqrt[3]{n}$ فأثبت أن $n = pq$ حيث q عدد أولي.

الحل

إذا كان $q = ab$ فإنه من الواضح أن $a,b > \sqrt[3]{n}$. حينئذ

$$n = pq = pab > \sqrt[3]{n}\sqrt[3]{n}\sqrt[3]{n} = n .$$

وهذا مستحيل. إذن q عدد أولي $\triangle$

تمارين (٢,٤)

(١) (أ) استخدم طريقة فيرما لتحليل كل من الأعداد التالية:

11021 ، 14317 ، 853751 ، 9954023 ، 2414068.

(ب) استخدم طريقة فيرما المعممة حيث $k = 3$ لتحليل كل من الأعداد التالية:

45313 ، 61577 ، 361667

(٢) استخدم طريقة أويلر لتحليل كل من الأعداد التالية:

$$2501 = 50^2 + 1^2 = 49^2 + 10^2$$

$$1000009 = 1000^2 + 3^2 = 972^2 + 235^2$$

(٣) عين أعلى قوة k تجعل 2^k يقسم كلاً من الأعداد التالية:

(أ) 201984 (ب) 1423408 (ج) 89375744

(د) 3468926 (هـ) 2414068 (و) 10763732

(٤) عين أعلى قوة k تجعل 5^k يقسم كلاً من الأعداد التالية:

(أ) 18375 (ب) 161250 (ج) 21343775

(٥) بين أياً من الأعداد التالية يقبل القسمة على 3:

(أ) 46884 (ب) 1451307 (ج) 21726612 (د) 27000243

(٦) بين أياً من الأعداد المقدمة في التمرين (٥) يقبل القسمة على 9

(٧) بين أياً من الأعداد التالية يقبل القسمة على أي من الأعداد 7، 11 ، 13:

(أ) 6743109 (ب) 10763732 (ج) 1086320015

(٨) أثبت أن العدد $2^{3n+2}+234235236237238239$ يقبل القسمة على 7 لكل $n \geq 0$.

(٩) إذا علمت أن $37 \mid (10^3-1)$ فصمم اختباراً لقابلية القسمة على 37.

(١٠) استخدم تمرين (٩) لاختبار قسمة الأعداد التالية للقسمة على 37:

(أ) 2688238145 (ب) 101800771617212

(١١) استخدم المبرهنة (٢,٢٠) لإثبات أولية أعداد ميرسين التالية: M_{19}، M_{31}، M_{89}.

(١٢) استخدم المبرهنة (٢,٢١) لإثبات أن كل من أعداد فيرما التالية مؤلف: F_7، F_9.

(١٣) استخدم مرشح أراتوستينس لإيجاد جميع الأعداد الأولية بين 100 و 1000.

(١٤) استخدم المتطابقة $4x^4+1=(2x^2+2x+1)(2x^2-2x+1)$ لتحليل العدد $2^{18}+1$.

نبذة عن حياة آتلي سيلبرج
Biography of Atle Selberg



ولد : ١٩١٧/٦/١٤ م في النرويج

بدأت اهتمامات سيلبرج في الرياضيات مبكرة جداً، حيث بدأ قراءة أبحاث الرياضي رامانجان *(Ramanujan)* عندما كان طالباً في المرحلة الثانوية وتأثر بها وبشخصية رامانجان نفسه تأثراً شديداً بالإضافة إلى الأثر الذي تركته في نفسه إحدى محاضرات الرياضي هيك *(Hecke)* التي ألقاها في مؤتمر الرياضيات العالمي الذي عقد في أوسلو في العام ١٩٣٦م.

حصل سيلبرج على درجة الدكتوراه في الرياضيات من جامعة أوسلو عام ١٩٤٣ م وعمل باحثاً في الجامعة نفسها إلى أن تزوج وهاجر إلى الولايات المتحدة الأمريكية في العام ١٩٤٧م حيث قضى السنة الأولى في معهد الدراسات العليا في جامعة برنستون، وترك المعهد ليحصل على وظيفة أستاذ مشارك في جامعة سيركيوز و لم يستمر في الوظيفة إلا عاماً واحداً عاد بعدها إلى جامعة برنستون وترقى إلى رتبة أستاذ في العام ١٩٥١م.

حصل سيلبرج على جائزة فيلدز *(Fields)* في الرياضيات أثناء إنعقادالمؤتمر العالمي في الرياضيات في جامعة هارفارد عن أبحاثه التي عمم فيها طريقة المرشحة التي اكتشفها برون *(Brun)* بالإضافة إلى أبحاثه المتعلقة بأصفار دالة زيتا لريمان *(Reimann)*. ولكن أكثر أبحاثه شهرة هو البرهان الذي قدمه لمبرهنة الأعداد

الأولية معتمداً على مفاهيم نظرية الأعداد فقط دون الاستعانة بالتحليل المركب خلافاً للبراهين السابقة المقدمة لهذه المبرهنة.

وبالإضافة إلى جائزة فيلدز فقد حصل سيلبرج على تقدير المؤسسات الرياضية في العالم حيث تم إنتخابه في مجلس إدارة الأكاديمية العلمية النرويجية والأكاديمية الملكية الدينماركية للعلوم والأكاديمية الأمريكية للعلوم والآداب، كما جمعت أبحاثه ونشرت في مجلدين عامي ١٩٨٩ و ١٩٩١م.

نبذة عن حياة جولدباخ

Biography of Goldbach



ولد : ١٨/٣/١٦٩٠م في روسيا.

توفي: ٢٠/١١/١٧٦٤م في روسيا.

عين جولدباخ أستاذاً للرياضيات في مدينة سانت بطرس في العام ١٧٢٥م ثم انتقل في العام ١٧٢٨م إلى موسكو ليشرف على تعليم القيصر بطرس الثاني. قابل العديد من الرياضيين أثناء تجواله المتعدد في أوروبا أمثال الأخوين برنولي، ديموفار ، هيرمان.

إن معظم اكتشافات جولدباغ في نظرية الأعداد كانت على صورة مراسلات بينه وبين أويلر. وترجع شهرته إلى الحدس المعروف باسمه الذي يدَّعي فيه أنه من الممكن كتابة أي عدد زوجي أكبر من 2 كمجموع عددين أوليين في إحدى رسائله إلى أويلر. هذا الحدس يعتبره الكثير من الرياضيين من أهم المسائل في نظرية الأعداد التي تنتظر الإجابة عليها، حيث اعتبرها الرياضي هاردي من أصعب المسائل غير المحلولة في الرياضيات.

و لم يقتصر اهتمام جولدباخ على نظرية الأعداد فله إسهامات مهمة في المتسلسلات اللانهائية، نظرية المنحنيات ونظرية المعادلات.

الفصل الثالث

التطابقـــات
CONGRUENCES

(٣,١) الخواص الأساسية للتطابقات
Basic Properties of Congruences

درسنا في الفصل الأول أحد المفاهيم الأساسية في نظرية الأعداد ألا وهـــو مفهوم قابلية القسمة وفي هذا الفصل نواصل هذه الدراسة من خـــلال مفهـــوم أساسي آخر في نظرية الأعداد وهو التطابقات. يعتبر جاوس أول من قدم تعريفـــاً رياضياً للتطابق في كتابه المشهور الحساب النظامي *(Disquisitione Arithmetica)* وهو الكتاب الذي قال عنه كانتور "إذا صح قول جاوس بأن الرياضيات هي ملكة العلوم وأن نظرية الأعداد تاج على رأس هذه الملكة فإن كتاب جاوس هو أعظـــم وثائق نظرية الأعداد".

مفهوم التطابق في الواقع هو تطوير لمفهوم قابلية القسمة إذ باستخدامنا لـــه نستطيع التوصل للبراهين بصورة أسهل، وبوساطته نستطيع ابتكار مسائل علميـــة أكثر جِدّة.

تعريف (٣,١)

ليكن $a,b\in\mathbb{Z}$ و $n\in\mathbb{Z}^+$. نقول إن a يطابق b قياس n $(a \text{ congruent to } b \text{ modulo } n)$ ونرمز لذلك بالرمز $a\equiv b(\text{mod } n)$، إذا كان $n \mid (a-b)$. وأما إذا كان $n \nmid (a-b)$ فإننا نقول إن a لا يطابق b قياس n ونكتب $a\not\equiv b(\text{mod } n)$. على سبيل المثال، $32\equiv 5(\text{mod } 9)$ ، $3\equiv -15(\text{mod } 9)$ ولكن $22\not\equiv 5(\text{mod } 9)$.

قبل الاسترسال في دراسة الخواص الأساسية للتطابقات نقدم المثال التالي الذي يبين لنا إحدى فوائد استخدام التطابقات في العمليات الحسابية.

مثال (٣,١)

(أ) إذا كان n مربعاً كاملاً فأثبت أن $n\equiv 0(\text{mod } 4)$ أو أن $n\equiv 1(\text{mod } 4)$.

(ب) أثبت أن العدد 22051946 ليس مربعاً كاملاً.

الحل

(أ) لنفرض أن $n=a^2$ حيث $a\in\mathbb{Z}$. باستخدام خوارزمية القسمة نعلم أن $a=4q+r$ حيث $r=0,1,2,3$. ولذا فإن:

$$n=a^2=(4q+r)^2=16q^2+8qr+r^2$$

إذا كان $r=0$ فإن $n=16q^2=4(4q^2)+0$.

إذا كان $r=1$ فإن $n=16q^2+8q+1=4(4q^2+2q)+1$.

إذا كان $r=2$ فإن $n=16q^2+16q+4=4(4q^2+4q+1)+0$.

وإذا كان $r=3$ فإن $n=16q^2+24q+9=4(4q^2+6q+2)+1$.

وبالتالي فإننا نخلص إلى أن $n\equiv 0(\text{mod } 4)$ أو أن $n\equiv 1(\text{mod } 4)$.

(ب) لاحظ أن $22051946=4\times 5512986+2$. ولذا فإن $22051946\equiv 2(\text{mod } 4)$. ومن الفقرة (أ) نجد أنه لا يمكن أن يكون مربعاً كاملاً □

المبرهنة التالية تقدم تعريفين مكافئين لتعريف التطابق قياس n .

مبرهنة (٣,١)

إذا كان $n \in \mathbb{Z}^+$ وكان $a,b \in \mathbb{Z}$ فإن العبارات التالية متكافئة:

(أ) $a \equiv b \pmod{n}$.

(ب) $a = b + kn$ حيث $k \in \mathbb{Z}$.

(ج) باقي قسمة a على n يساوي باقي قسمة b على n .

البرهان

(أ) $\Leftarrow$ (ب): بما أن $a \equiv b \pmod{n}$ فإن $n \mid (a-b)$. ولـــذا فـــإن $nk = a-b$ حيث $k \in \mathbb{Z}$. وبالتالي فإن $a = b + kn$.

(ب) $\Leftarrow$ (ج) : باستخدام خوارزمية القسمة نجد أن:

$$0 \le r < n \ ، \ a = qn + r$$

$$0 \le r_1 < n \ ، \ b = q_1 n + r_1$$

الآن ، بما أن $a-b = kn$ فإن $n \mid (a-b)$. ولذا $n \mid (a-b)-(q-q_1)n$. أي أن $n \mid (r-r_1)$. ولكن $-n < r-r_1 < n$. ومنه فإن $r-r_1 = 0$. وبالتالي فإن $r = r_1$.

(ج) $\Leftarrow$ (أ): لنفرض أن $r = r_1$. عندئذ $r-r_1 = 0$ فيكـــون $a-b = (q-q_1)n$.

ومن ذلك نرى $n \mid (a-b)$. وبالتالي فإن $a \equiv b \pmod{n}$ ◆

تبين المبرهنة التالية أن علاقة التطابق قياس n هي علاقة تكافؤ على $\mathbb{Z}$.

مبرهنة (٣,٢)

إذا كان $a,b,c \in \mathbb{Z}$ وكان $n \in \mathbb{Z}^+$ فإن:

(١) $a \equiv a \pmod{n}$.

(٢) إذا كان $a \equiv b \pmod{n}$ فإن $b \equiv a \pmod{n}$.

(٣) إذا كان $a \equiv b \pmod{n}$ وكان $b \equiv c \pmod{n}$ فإن $a \equiv c \pmod{n}$.

البرهان

(١) بما أن $n \mid (a-a)=0$ فإن $a \equiv a \pmod{n}$.

(٢) بما أن $a \equiv b \pmod{n}$، فهناك $k \in \mathbb{Z}$ بحيث: $a-b=kn$، ومن هذا نرى أن $b-a=(-k)n$. أي أن $b \equiv a \pmod{n}$.

(٣) بما أن $a \equiv b \pmod{n}$ وأن $b \equiv c \pmod{n}$ فهناك عددان صحيحان k و j بحيث إن $kn=a-b$ وإن $jn=b-c$. وبناءً على ذلك نجد أن:

$$a-c=(a-b)+(b-c)=kn+jn=(k+j)n \quad .$$

ونحصل على $n \mid (a-c)$. أي أن: $a \equiv c \pmod{n}$ ◆

المبرهنة التالية تبين لنا إمكانية جمع وطرح وضرب التطابقات.

مبرهنة (٣,٣)

إذا كانت a، b، c، d أعداداً صحيحة وكان n عدداً صحيحاً موجباً يحقق: $a \equiv b \pmod{n}$ و $c \equiv d \pmod{n}$ فإن

(١) $a+c \equiv b+d \pmod{n}$.

(٢) $a-c \equiv b-d \pmod{n}$.

(٣) $ac \equiv bd \pmod{n}$.

البرهان

بما أن $a \equiv b \pmod{n}$ وأن $c \equiv d \pmod{n}$ فهناك عددان صحيحان k، j بحيث إن $kn=a-b$ وإن $jn=c-d$.

(١) بما أن: $(a+c)-(b+d)=(a-b)+(c-d)=kn+jn=(k+j)n$. فإننا نجد $a+c \equiv b+d \pmod{n}$.

(٢) لاحظ أن: $(a-c)-(b-d)=(a-b)-(c-d)=kn-jn=(k-j)n$. وبالتالي فإن $a-c \equiv b-d \pmod{n}$.

(٣) بما أن: $ac-bd=ac-bc+bc-bd=c(a-b)+b(c-d)=(ck+bj)n$

فإن: $ac \equiv bd \pmod{n}$ ◆

نتيجة (٣,٤)

إذا كان $n \in \mathbb{Z}^+$ وكان $a_i \equiv b_i \pmod{n}$ لكل i حيث $1 \le i \le k$ فإن:

(١) $a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k \pmod{n}$.

(٢) $a_1 a_2 \ldots a_k \equiv b_1 b_2 \ldots b_k \pmod{n}$.

البرهان

يتم برهان الفقرتين باستخدام الاستقراء الرياضي على العدد k وسنبرهن الفقرة الأولى ونترك برهان الفقرة الثانية كتمرين للقارئ.

الخطوة الأساسيّة

العبارة صحيحة عندما $k = 2$ استناداً إلى المبرهنة (٣,٣).

خطوة الاستقراء

لنفرض أن $a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k \pmod{n}$. بما أن $a_1 + a_2 + \ldots + a_{k+1} = (a_1 + a_2 + \ldots + a_k) + a_{k+1}$ فباستخدام فرضية الاستقراء نجد أن: $(a_1 + a_2 + \ldots + a_k) + a_{k+1} \equiv (b_1 + b_2 + \ldots + b_k) + b_{k+1} \pmod{n}$.

ونستنتج أن: $a_1 + a_2 + \ldots + a_k + a_{k+1} \equiv b_1 + b_2 + \ldots + b_k + b_{k+1} \pmod{n}$ ◆

نتيجة (٣,٥)

إذا كان $a \equiv b \pmod{n}$ فإن $a^k \equiv b^k \pmod{n}$ لكل $k \ge 1$.

البرهان

نحصل على المطلوب باستخدام الفقرة الثانية من نتيجة (٣,٤) وبوضع $a = a_i$ و $b = b_i$ لكل i ، $1 \le i \le k$ ◆

ملحوظة

من برهان المبرهنة (٣,٣) نجد أنه إذا كان $a \equiv b \pmod{n}$ فإن $ac \equiv bc \pmod{n}$ لكل $c \in \mathbb{Z}$، ومن البديهي أن نسأل ما إذا كان العكس صحيحاً أم لا. والإجابة هي بالنفي كما يوضح المثال التالي:

مثال (٣,٢)

لاحظ أن $7 \times 2 \equiv 4 \times 2 = 2 \pmod{6}$ ولكن $7 \not\equiv 4 \pmod{6}$ □

مبرهنة(٣,٦)

إذا كانت a، b ، c أعداداً صحيحة وكان n عدداً صحيحاً موجباً فإن:

$ac \equiv bc \pmod{n}$ إذا وفقط إذا كان $a \equiv b \pmod{n/d}$ حيث $d = (c,n)$.

البرهان

نفرض أولا أن $ac \equiv bc \pmod{n}$. عندئذ، يوجد عدد صحيح k يحقق $c(a-b) = ac - bc = kn$. وبقسمة طرفي المعادلة على d نحصل على المعادلة: $(c/d)(a-b) = k(n/d)$. وبما أن $1 = (c/d\ ,\ n/d)$، فنجد استناداً إلى تمهيدية إقليدس أن $(n/d) \mid (a-b)$. أي أن $a \equiv b \pmod{n/d}$.

برهان العكس مباشر ونتركه للقارئ ◆

ملحوظة

من المبرهنة (٣,٦) نستنتج الحالتين التاليتين اللتين سيكون لهما استخدامات كثيرة:

(١) إذا كانت a ، b ، c أعداداً صحيحة وكان n عدداً صحيحاً موجباً بحيث إن $ac \equiv bc \pmod{n}$ وإن $(c\ ,\ n) = 1$ فإن $a \equiv b \pmod{n}$.

(٢) إذا كان $ac \equiv bc \pmod{p}$ حيث p عدد أولي لا يقسم c فإن $a \equiv b \pmod{p}$.

سنجد في المبرهنة التالية عوناً كبيراً لنا في إجراء بعض الحسابات على التطابق.

مبرهنة (٣,٧)

إذا كان $a \equiv b \pmod{n}$ وكان $m \mid n$ فإن $a \equiv b \pmod{m}$.

البرهان

بما أن $a \equiv b \pmod{n}$ فإن $n \mid (a-b)$. وبما أن $m \mid n$ فإن $m \mid (a-b)$

وبالتالي فإن $a \equiv b \pmod{m}$ ◆

نقدم الآن مفهوم النظير الضربي قياس العدد n.

تعريف (٣,٢)

ليكن a عدداً صحيحاً. نسمى العدد b نظيراً ضربياً (Multiplicative inverse) للعدد a قياس n إذا كان $ab \equiv 1 \pmod{n}$.

ملحوظة

مفهوم النظير الضربي للعدد الصحيح قياس n هو المفهوم المرادف لمقلوب العدد. وفي واقع الأمر سننظر إلى التطابق $ab \equiv 1 \pmod{n}$ على أنه المرادف للمعادلة $a \times \frac{1}{a} = 1$. ونلاحظ ابتداءً أنه ليس بالضرورة أن يحظى كل عدد صحيح نظير ضربي قياس n، كما يوضح المثال التالي:

مثال(٣,٣)

لاحظ أن $2 \times 0 \equiv 0 \pmod{4}$ ، $2 \times 1 \equiv 2 \pmod{4}$ ، $2 \times 2 \equiv 0 \pmod{4}$ ،

$2 \times 3 \equiv 2 \pmod{4}$. إذن، العدد 2 ليس له نظير ضربي قياس 4 □

المبرهنة التالية تقدم لنا الشرط اللازم والكافي لوجود نظير ضربي قياس n.

مبرهنة (٣,٨)

يوجد للعدد الصحيح a نظير ضربي قياس n إذا وفقط إذا كان $(a,n)=1$.

البرهان

لنفرض أولاً أن $(a\ ,\ n)=1$. عندئذ، يوجد عددان صحيحان x، y بحيث إن $ax+ny=1$، ومنه نجد أن $ax\equiv 1(\mathrm{mod}\ n)$. وبالتالي فإن x هو النظير الضربي للعدد a.

وللبرهان على العكس نفرض أن b نظير ضربي للعدد a قياس n. بناء على ذلك فإن $ab\equiv 1(\mathrm{mod}\ n)$، ومنه $n\mid(ab-1)$. أي أن $ab-kn=1$ حيث $k\in\mathbb{Z}$، وبالتالي فإن $(a,n)=1$ ◆

ملحوظات

(١) لاحظ أنه إذا كان $n\in\mathbb{Z}^+$ وكان كل من b و c نظيراً ضربياً للعدد a قياس n فإن $ab\equiv 1(\mathrm{mod}\,n)$ وإن $ac\equiv 1(\mathrm{mod}\,n)$. ومن ثم فإن $ab\equiv ac(\mathrm{mod}\,n)$. وبما أن $(a,n)=1$ فإننا نجد استناداً إلى المبرهنة (٣,٦) أن $b\equiv c(\mathrm{mod}\,n)$. وبالتالي فإن النظير الضربي للعدد a قياس n وحيد (متى وجد)، وسنرمز له من الآن فصاعداً بالرمز a^{-1}.

(٢) تقدم لنا المبرهنة (٣,٨) مع خوارزمية إقليدس طريقة لإيجاد النظير الضربي للعدد a قياس n (في حالة وجوده) وهذا ما يوضحه المثال التالي:

مثال(٣,٤)

استخدم خوارزمية إقليدس لإيجاد النظير الضربي للعدد 17 قياس 25.

الحل

$$25=1\times 17+8$$
$$17=2\times 8+1$$
$$8=8\times 1+0$$

إذن، $(25,17)=1$ وحسب مبرهنة (٣,٨) فإن 17^{-1} قياس 25 موجود. ولإيجاد 17^{-1} نضع 1 كتركيب خطي للعددين 17 و 25 فنجد: $1=17\times 3+25(-2)$، أي أن $17\times 3\equiv 1 \pmod{25}$. وبالتالي فإن 3 هو النظير الضربي للعدد 17 قياس 25 □

سيكون للمبرهنة التالية تطبيقات عديدة.

مبرهنة (٣,٩)

ليكن a و b عددين صحيحين ولتكن $n_1, n_2, \dots, n_k$ أعداداً صحيحة موجبة. إذا كان $a\equiv b \pmod{n_i}$ لكل $1\le i\le k$، فإن $a\equiv b \pmod{n}$ حيث $n=[n_1, n_2, \dots, n_k]$.

البرهان

بما أن $a\equiv b \pmod{n_i}$ فإن $n_i \mid (a-b)$ لكل i ، $1\le i\le k$. الآن، باستخدام خوارزمية القسمة يوجد $q, r\in\mathbb{Z}$ حيث

$$(a-b)=nq+r \quad ، \quad 0\le r<n$$

لنفرض لغرض التناقض أن $r\neq 0$. بما أن $n_i \mid n$ و $n_i \mid (a-b)$ لكل $1\le i\le k$ فإن $n_i \mid r$ لكل $1\le i\le k$. أي أن r مضاعف مشترك للأعداد n_i، وهذا يناقض كون n أصغر مضاعف مشترك للأعداد n_i. إذن، $r=0$. وبالتالي فإن $n \mid (a-b)$. أي أن $a\equiv b \pmod{n}$ ◆

من المبرهنة (٣,٩) نستنتج النتيجة المهمة التالية:

نتيجة (٣,١٠)

إذا كان $a\equiv b \pmod{n_i}$ لكل $i=1, 2, \dots, k$ وكانت n_i أعداداً موجبة أولية نسبياً زوجاً زوجاً فإن $a\equiv b \pmod{n_1 n_2 \dots n_k}$.

البرهان

بما أن $(n_i,n_j)=1$ لكل $i\neq j$ فإن $[n_1,n_2,\ \dots\ ,n_k]=n_1\ n_2\ \dots\ n_k$.

ونحصل على المطلوب بتطبيق المبرهنة (٣,٩) ◆

نتيجة (٣,١١)

إذا كان $n=p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}$ هو تحليل n إلى قوى عوامله الأوّلية وكان $a\equiv b\pmod{p_i^{r_i}}$ لكل $1\le i\le k$ فإن $a\equiv b(\bmod n)$.

البرهان

ضع $n_i=p_i^{r_i}$ واستخدم النتيجة (٣,١٠) ◆

تبين الأمثلة التالية عظم الفائدة التي تقدمها لنا علاقة التطابق في اجراء بعض الحسابات.

لقد بينا في الفصل الأول أن العدد 641 يقسم العدد F_5. سنقدّم برهاناً آخر لهذه الحقيقة بالاستعانة بعلاقة التطابق.

مثال (٣,٥)

أثبت أن $F_5=2^{32}+1\equiv 0(\bmod 641)$.

الحل

بالتربيع المتتالي نحصل على:

$$2^4\equiv 16(\bmod\ 641)$$
$$2^8\equiv 256(\bmod\ 641)$$
$$2^{16}\equiv 154(\bmod\ 641)$$
$$2^{32}\equiv 640(\bmod\ 641)$$

إذن، $F_5=2^{32}+1\equiv 0(\bmod\ 641)$ □

مثال (٣,٦)

جد أصغر عدد صحيح موجب k يحقق $31 \mid (33(26)^2 - k)$.

الحل

المطلوب هو إيجاد أصغر عدد صحيح موجب k يحقق $33(26)^2 \equiv k \pmod{31}$.

لاحظ أولاً أن $33 \equiv 2 \pmod{31}$ وأن $26 \equiv -5 \pmod{31}$. من ذلك نرى أن

$$(33)(26)^2 \equiv 2(-5)^2 \pmod{31} \equiv 50 \pmod{31} \equiv 19 \pmod{31}$$

إذن، $k = 19$ □

في العديد من تطبيقات نظرية الأعداد نحتاج إلى حساب تطابقات أعدادها كبيرة جداً، على سبيل المثال، إذا أردنا حساب $2199^{2269} \pmod{2633}$ بحساب العدد 2199^{2269} فيجب علينا التعامل مع عدد طوله العشري $7584 = [2269 \log 2199] + 1$. وهذا بلا شك عدد كبير جداً. كبديل عن ذلك نستخدم الخوارزمية التالية وتدعى خوارزمية التربيع والضرب (*square and multiply*) التي توفر علينا الكثير من الجهد. يجري وصف هذه الخوارزمية على النحو المبين أدناه.

خوارزمية التربيع والضرب [*Square And Multiply Algorithm*]

لحساب $b^N \pmod{m}$ حيث $b, m, N \in \mathbb{N}^+$ نقوم بتنفيذ الخطوات التالية:

(١) حول العدد N إلى النظام الثنائي $N = (a_{k-1}a_{k-2} \ldots a_1a_0)_2$.

(٢) احسب $b^{2^i} \pmod{m}$ لكل $0 \le i \le k-1$ وذلك بالتربيع المتتالي.

(٣) نقوم الآن بضرب الأعداد b^{2^i} قياس m لكل $a_i = 1$ لنحصل على المطلوب.

المثال التالي يوضح لنا خطوات الخوارزمية:

مثال (٣,٧)

احسب $2199^{2269} \pmod{2633}$.

الحل

بتحويل العدد 2269 إلى النظام الثنائي نجد أن:

$$2269 = (a_{11}\,a_{10}\,a_9\,a_8\,a_7\,a_6\,a_5\,a_4\,a_3\,a_2\,a_1\,a_0) = (100011011101)_2$$

الآن:

$$2199 \equiv 2199 (\text{mod } 2633)$$
$$2199^2 \equiv 1413 (\text{mod } 2633)$$
$$2199^4 \equiv 755 (\text{mod } 2633)$$
$$2199^8 \equiv 1297 (\text{mod } 2633)$$
$$2199^{16} \equiv 2355 (\text{mod } 2633)$$
$$2199^{32} \equiv 927 (\text{mod } 2633)$$
$$2199^{64} \equiv 971 (\text{mod } 2633)$$
$$2199^{128} \equiv 227 (\text{mod } 2633)$$
$$2199^{256} \equiv 1502 (\text{mod } 2633)$$
$$2199^{512} \equiv 2156 (\text{mod } 2633)$$
$$2199^{1024} \equiv 1091 (\text{mod } 2633)$$
$$2199^{2048} \equiv 165 (\text{mod } 2633)$$

ولذا فإن:

$$2199^{2269} = 2199^1 \times 2199^4 \times 2199^8 \times 2199^{16} \times 2199^{64} \times 2199^{128} \times 2199^{2048}$$
$$\equiv 2199 \times 755 \times 1297 \times 2355 \times 971 \times 227 \times 165 (\text{mod } 2633)$$
$$\equiv 1455 \times 155 \times 1878 \times 165 (\text{mod } 2633)$$
$$\equiv 1720 \times 1809 (\text{mod } 2633)$$
$$\equiv 1907 (\text{mod } 2633)$$

إذن، $2199^{2269} \equiv 1907 (\text{mod } 2633)$ □

(٣,١,١) أنظمة الرواسب (Residue Systems)

لقد بينا في المبرهنة (٣,٢) أن علاقة التطابق قياس n هي علاقـــة تكـــافؤ على $\mathbb{Z}$، ولذا فإنها تجزئ $\mathbb{Z}$ إلى فصول التكافؤ التالية:

$$[a]=\{b\in\mathbb{Z}: a\equiv b(\bmod n)\}$$
$$=\{\dots,a-2n,a-n,a,a+n,a+2n,\dots\}$$

حيث $a\in\mathbb{Z}$. ولكن باستخدام خوارزمية القسمة نجد أن:

$$a=qn+r \quad \text{حيث} \quad r=0,1,2,\dots,n-1$$

ولذا فإن $a\equiv r(\bmod n)$ ، ومن ثم فإن $[a]=[r]$. وبالتالي فإننا نخلـــص إلى أن عدد فصول التكافؤ المختلفة قياس n هو بالضبط n وهي:

$$[0]=\{\dots,-2n,-n,0,2n,\dots\}$$
$$[1]=\{\dots,1-2n,1-n,1,1+n,1+2n,\dots\}$$
$$\vdots$$
$$[n-1]=\{\dots,-n-1,-1,n-1,2n-1,3n-1,3n-1,\dots\}$$

لكل $n\geq 1$. سنرمز لمجموعة فصول التكافؤ قياس n بالرمز $\mathbb{Z}_n$.

ملحوظة

من الممكن تعريف عمليتي الجمع والضرب على $\mathbb{Z}_n$ على النحو التالي:

$$[a]\oplus[b]=[a+b]$$
$$[a]\odot[b]=[ab]$$

ومن السهل الآن البرهان على أن $(\mathbb{Z}_n,\oplus,\odot)$ حلقة إبدالية بمحايد انظر[3].

الآن، ممـــا ســـبق نجـــد أنـــه لكـــل $a\in\mathbb{Z}$ يوجـــد عـــدد وحيـــد $r\in S=\{0,1,2,\dots,n-1\}$ يحقق $a\equiv r(\bmod n)$. تسمى المجموعـــة S نظـــام رواسب تام (*complete residue system*) قياس العدد n. لاحـــظ ابتـــداءاً أن المجموعة S ليست الوحيدة التي تتمتع بهذه الخاصية ، في الحقيقة أي مجموعة مـــن

الأعداد، عدد عناصرها n بحيث تنتمي هذه العناصر إلى فصول تكافؤ مختلفة تحقق هذه الخاصية. إن ذلك يقترح علينا التعريف التالي:

تعريف (٣,٣)

نقول إن المجموعة $S=\{a_1,a_2,\dots,a_n\}$ نظام رواسب تام قياس n إذا كان كل من a_i ممثلاً لفصل تكافؤ واحد فقط من فصول تكافؤ $\mathbb{Z}_n$.

ملحوظات

(١) لاحظ أنه لكل $a\in\mathbb{Z}$ يوجد عدد وحيد $a_i\in S$ يحقق $a\equiv a_i \pmod n$.

(٢) يسمى نظام الرواسب التام $\{0,1,2,\dots,n-1\}$ ، نظام الرواسب التام القياسي (أو المعياري) قياس n. *(Standard complete residue system mod n)* ونأخذه كمعيار لإثبات أن مجموعة مكونة من n من الأعداد تمثل نظام رواسب تام قياس n ، إذ يكفي أن نثبت أن كل عدد منها يطابق عدداً وحيداً من بين الأعداد $0,1,\dots,n-1$.

مثال (٣,٨)

أثبت أن المجموعة $S=\{0,\pm1,\pm2\}$ نظام رواسب تام قياس 5.

الحل

لاحظ أن: $0\equiv 0 \pmod 5$ ، $-1\equiv 4 \pmod 5$ ، $-2\equiv 3 \pmod 5$،
$1\equiv 1 \pmod 5$ و $2\equiv 2 \pmod 5$. إذن، S نظام رواسب تام قياس 5 □

تزودنا المبرهنة التالية بتعريف مكافيء لنظام الرواسب التام قياس n.

مبرهنة (٣,١٢)

لتكن $S=\{a_1,a_2,\ldots,a_n\}$ مجموعة تحتوي على n من الأعداد الصحيحة. عندئذ S نظام رواسب تام قياس n إذا وفقط إذا كـــان $a_i \not\equiv a_j \pmod n$ لكـــل $1\le i,j\le n$ ، $i\ne j$.

البرهان

لنفرض أولاً أن S نظام رواسب تام قياس n . عندئـــذ، لكـــل $i\ne j$ نجـــد أن $[a_i]\ne[a_j]$. وعليه فإن $a_i \not\equiv a_j \pmod n$. لكل $i\ne j$.

لبرهان العكس، نفرض أن $a_i \not\equiv a_j \pmod n$ لكل $i\ne j$ ، ونفـــرض لغـــرض التناقض أنه يوجد $a\in\mathbb{Z}$ بحيث يكون $a_i,a_j\in[a]$. عندئذ، $a_i\equiv a \pmod n$ و $a_j\equiv a \pmod n$. وحينها نحصل على $a_i\equiv a_j \pmod n$ وهو أمر مـــستحيل. إذن، كل $a_i\in S$ ينتمي إلى فصل تكافؤ وحيد من فصول $\mathbb{Z}_n$. وبالتالي فإن S نظام رواسب تام قياس n ◆

نتيجة (٣,١٣)

أي n من الأعداد الصحيحة المتتالية تمثل نظام رواسب تام قياس n.

البرهان

لتكن $b,b+1,b+2,\ldots,b+n-1$ أعداداً صحيحة متتاليـــة عـــددها n. ولنفـــرض أن $b+j\equiv b+k \pmod n$ ، $0\le k\ne j\le n-1$. ومنـــه نجـــد أن $j\equiv k \pmod n$ وهذا تناقض لأن $0,1,2,\ldots,n-1$ نظام رواسب تام ◆

النتيجة التالية تبين كيفية الحصول على أنظمة رواسب تامة جديدة من نظام رواسب معطى.

نتيجة (٣,١٤)

إذا كان $r_1, r_2, \ldots, r_n$ نظام رواسب تام قياس n وكان $(a,n)=1$ فإن $ar_1+b, ar_2+b, \ldots, ar_n+b$ نظام رواسب تام قياس n لكل $b \in \mathbb{Z}$.

البرهان

باستخدام مبرهنة (٣,١٢) يكفي أن نبرهن على أن:

$$ar_i+b \not\equiv ar_j+b \pmod{n} \quad \text{لكل } 1 \le i \ne j \le n$$

لنفرض لغرض التناقض أن: $ar_i+b \equiv ar_j+b \pmod{n}$.

عندئذ $ar_i \equiv ar_j \pmod{n}$. وبما أن $(a,n)=1$ فإن $r_i \equiv r_j \pmod{n}$ وهذا مستحيل إلا إذا كان $i=j$ ◆

تعريف (٣,١٤)

ليكن $S=\{r_1, r_2, \ldots, r_n\}$ نظام رواسب تام قياس n. نقول إن المجموعة الجزئية $T=\{a \in S : (a,n)=1\}$ نظام رواسب مختزل (*reduced residue system*) قياس n.

مثال (٣,٩)

إذا كان $n=12$، وأخذنا $S=\{0,1,2,\ldots,11\}$ كنظام رواسب تام قياس 12 فإن $T=\{1,5,7,11\}$ تكوّن نظام رواسب مختزل قياس 12. وإذا أخذنا المجموعة $S_1=\{0, \pm1, \pm2, \pm3, \pm4, \pm5, 6\}$ كنظام رواسب تام قياس 12 فعندئذ تكون المجموعة $T_1=\{\pm1, \pm5\}$ نظام رواسب مختزل قياس 12 □

نلاحظ من مثال (٣,٩) أن النظامين المختزلين قياس 12 يحتويان على نفس العدد من العناصر، وهذا ليس من قبيل الصدفة فالملاحظة صحيحة لأي عدد n وهو ما ستقدمه المبرهنة التالية التي سنمهد لها بما يلي.

تمهيدية (٣,١٥)

ليكن $T=\{a_1,a_2,\ldots,a_k\}$ نظام رواسب مختزل قياس n. إذا كان $a\in\mathbb{Z}$ حيث $(a,n)=1$ فيوجد عدد وحيد a_i ، $1\le i\le k$ يحقق $a\equiv a_i \pmod n$.

البرهان

ليكن S نظام رواسب تام قياس n يحتوي T. من تعريف S نستطيع الحصول على عدد وحيد $b\in S$ بحيث يكون $a\equiv b \pmod n$. وبما أن $(a,n)=1$ فإن $(b,n)=1$ ، ولذا فإن $b\in T$. ولبرهان الوحدانية، نفرض أن $a_i,a_j\in T$ حيث $a_i\neq a_j$ وحيث $a\equiv a_i \pmod n$ ، $a\equiv a_j \pmod n$. عندئذ، $a_i\equiv a_j \pmod n$. وبما أن $a_i,a_j\in S$ فإننا نحصل على تناقض ◆

مبرهنة (٣,١٦)

لجميع أنظمة الرواسب المختزلة قياس n نفس العدد من العناصر.

البرهان

لنفرض أن $n\in\mathbb{Z}^+$ وأن $T=\{a_1,a_2,\ldots,a_t\}$ و $S=\{b_1,b_2,\ldots,b_s\}$ نظاما رواسب مختزلان قياس العدد n. لكل $b_j\in S$ يوجد استناداً إلى التمهيدية (٣,١٥) عدداً وحيداً $a_i\in T$ يحقق $a_i\equiv b_j \pmod n$. الآن، نعرف التطبيق $f:S\to T$ كالتالي: $f(b_j)=a_i$ حيث a_i هو العدد الوحيد الذي ينتمي إلى T ويحقق $a_i\equiv b_j \pmod n$. من الواضح أن f شامل. ولبرهان أن f أحادي، نفرض أن $b_i,b_j\in S$ بحيث يكون $f(b_i)=f(b_j)=a_r$. عندئذ، $b_j\equiv a_r \pmod n$ و $b_i\equiv a_r \pmod n$. وعليه فإن $b_i\equiv b_j \pmod n$ وهذا مستحيل إلا إذا كان $b_i=b_j$ ، ومن ثم فإن f أحادي. وبالتالي فإن عدد عناصر S يساوي عدد عناصر T ◆

تبرر المبرهنة(٣,١٦) تعريف دالة عددية مهمة نسجل تعريفها الآن ونعد بدراستها أكثر في الفصل الخامس.

تعريف (٣,٥)

ليكن $n \in \mathbb{Z}^+$. نُعرِّف دالّة أويلر (*Euler's function*) على أنها عدد العناصر التي يحتويها أي نظام رواسب مختزل قياس n ونرمز لها بالرمز $\varphi(n)$.

ملحوظات

(١) من تعريف نظام الرواسب المختزل قياس n والمأخوذ من النظام التام $\{1,2,\dots,n\}$ نجد أن عناصره هي الأعداد الأوّلية نسبياً مع n والتي لا تزيد عن n ، ومن ثم فإنه يكون واضحاً لدينا أن $\varphi(n)$ هو عدد الأعداد الأوّلية نسبياً مع n والتي لا تزيد عن n.

(٢) إذا كانت $U_n = \{[a] \in \mathbb{Z}_n : (a,n) = 1\}$ فإن ممثلات فصول تكافؤ U_n نظام رواسب مختزل قياس n وأن $|U_n| = \varphi(n)$.

(٣) من السهل أن نرى أن $(U_n, \odot)$ زمرة إبدالية.

(٤) لاحظ أن $\varphi(n) \le n-1$ لكل $n \in \mathbb{Z}^+$. وإذا كان n عدداً أولياً فإن جميع الأعداد a ، $1 \le a < n$ أولية نسبياً مع n. وعليه فإن $\varphi(n) = n-1$.

مثال (٣,١٠)

$\varphi(9) = 6$ لأن الأعداد الأوليّة نسبياً مع 9 والتي لا تزيد عن 9 هي: 1, 2, 4, 5, 7, 8. أما $\varphi(12) = 4$ لأن الأعداد الأولية نسبياً مع 12 والتي لا تزيد عن 12 هي: 1, 5, 7, 11 □

ننهي هذا البند بمبرهنة تظهر الحاجة لها في البند (٣,٥) حيث اثبات مبرهنة أويلر.

مبرهنة (٣,١٧)

لنفرض أن $S = \{a_1, a_2, \dots, a_n\}$ نظام رواسب تام قياس n ولنفرض أن المجموعة الجزئية $T = \{r_1, r_2, \dots, r_{\varphi(n)}\} \subseteq S$ هي نظام رواسب مختزل قياس n. إذا كان $a \in \mathbb{Z}^+$ حيث $(a,n) = 1$ فإن $T' = \{ar_1, ar_2, \dots, ar_{\varphi(n)}\}$ نظام رواسب مختزل قياس n.

البرهان

من النتيجة (٣,١٤) نجد أن $S'=(aa_1,aa_2,\dots,aa_n\}$ نظام رواسب تـــام قياس n. وبما أن $T'\subseteq S'$ فإنه يكفي إثبات أن $(ar_i,n)=1$ لكل i، $1\le i\le\varphi(n)$. إذا كان $(ar_i,n)>1$ فإنه يوجد عدد أوّلي p بحيث إن $p\mid ar_i$ و $p\mid n$. وبهـــذا نـــرى أن $p\mid a$ أو $p\mid r_i$) و $p\mid n$. وبهـــذا يكـــون ($p\mid a$ و $p\mid n$) أو ($p\mid r_i$ و $p\mid n$). إذن، $(n,a)>1$ أو $(n,r_i)>1$ وهـــذا مـــستحيل إذ أن $(r_i,n)=(a,n)=1$ ◆

(٣,١,٢) تمارين محلولة *(Solved Excercises)*

تمرين (١)

إذا كان k عدداً فردياً فأثبت أن 229 يقسم العدد $13^{2k}+17^{2k}$.

الحل

بما أن k عدد فردي فإن:

$$13^{2k}+17^{2k}=169^k+289^k\equiv(-60)^k+60^k\equiv0(\text{mod }229).$$

وبالتالي فإن 229 يقسم $13^{2k}+17^{2k}$ △

تمرين (٢)

إذا كانـــت $p_1,p_2,\dots,p_n$ أعـــداداً أوليـــة فرديـــة فأثبـــت أن $N=(p_1p_2\dots p_n)^2+1$ لا يمكن أن يكون مكعباً.

الحل

بما أن p_i عـــدد أولي فـــردي فـــإن $p_i\equiv\pm1(\text{mod }4)$. وبهـــذا يكـــون $N\equiv2(\text{mod }4)$. ومنه فإن $N\equiv2\equiv0(\text{mod }2)$. أي أن $2\mid\mid N$. وبالتـــالي لا يمكن أن يكون N معكباً △

تمرين (٣)

(أ) إذا كان $N=8k+7$ فأثبت استحالة كتابة N كمجموع ثلاث مربعات.

(ب) إذا كان $N=4^m(8k+7)$ حيث $m\in\mathbb{Z}^+$ عدم امكانية كتابة N كمجموع ثلاث مربعات.

الحل

(أ) لاحظ أولاً أن $S=\{0,\pm1,\pm2,\pm3,4\}$ نظام رواسب تام قياس 8. ولذا فكل $x\in\mathbb{Z}$ يطابق عدداً وحيداً من أعداد S قياس 8. ومن ثم فإن $x^2\equiv 0,1,4 \pmod 8$. ومجموع أي ثلاث أعداد منها لا يمكن أن يطابق 7 قياس 8. وبهذا لا يمكن أن يكون N مجموعاً لثلاث مربعات.

(ب) لنفرض أن $N=4^m(8k+7)=x^2+y^2+z^2$. بما أن $N\equiv 0(\mathrm{mod}\ 4)$ وأن أي مربع يطابق 0 أو 1 قياس 4 فإن $x^2\equiv y^2\equiv z^2\equiv 0(\mathrm{mod}\ 4)$. ولذا فكل من x ، y ، z عدد زوجي. أي أن $z=2t$ ، $y=2s$ ، $x=2r$. نستنتج أن $N/4=r^2+s^2+t^2$.

بالاستمرار على هذا المنوال نخلص إلى إمكانية كتابة $8k+7$ كمجموع ثلاث مربعات مما يناقض الفقرة (أ) △

تمرين (٤)

إذا كان p عدداً أولياً وكان $0\le n<p$ فأثبت أن $N=\binom{n+p}{p}\equiv 1(\mathrm{mod}\ p)$.

الحل

$$n!N=n!\frac{(n+p)!}{p!n!}=(n+p)(n+p-1)\dots(p+1)$$

$$\equiv n(n-1)\ \ldots\ 1 \equiv n!(\text{mod } p)$$

وبما أن $n < p$ فإن $n! \not\equiv 0(\text{mod } p)$. ولذا فإن $N \equiv 1(\text{mod } p)$ △

تمرين (٥)

إذا كـــان 792 يقسم العدد العشري $13xy45z$ فجد كل من المراتب x ، y ، z .

الحل

لاحـــظ أولاً أن $792 = 8 \times 9 \times 11$. بمـــا أن 8 يقـــسم $13xy45z$ فـــإن 8 يقسم $45z$. ولذا فإن $z = 6$. وبما أن 9 يقسم $13xy456$ و 11 يقـــسم $13xy456$ فإن $x + y \equiv 8(\text{mod } 9)$ وأن $x - y \equiv 8(\text{mod } 11)$ (استناداً إلى المبرهنة (١,١٨)) وبهذا يكون $x + y = 8$ و $x - y = 8$. وبحل المعادلتين نجد أن $x = 8$ و $y = 0$ △

تمرين (٦)

أثبت عدم وجود جذور صحيحة لكثيرة الحدود $f(x) = x^5 - x^2 + x - 3$.

الحل

لاحظ أولاً أن $\{0, \pm 1, 2\}$ نظام رواسب تام قياس 4 وأن:

$$f(0) = -3,\ f(1) = -2,\ f(-1) = -6,\ f(2) = 27$$

ولذا فإن $f(x) \not\equiv 0(\text{mod } 4)$. ونرى أن $f(x) \neq 0$ لكل $x \in \mathbb{Z}$ (لاحظ أنه إذا كان $f(x) = 0$ فإن $f(x) \equiv 0(\text{mod } n)$ لكل $n \geq 1$) △

تمرين (٧)

إذا كان $x, y, z \in \mathbb{Z}$ حلاً للمعادلة $x^3 + y^3 = z^3$ فأثبت أن $3 \mid x$ أو $3 \mid y$ أو $3 \mid z$.

الحل

إذا كان $x, y, z \in \mathbb{Z}$ حـــلاً للمعادلـــة $x^3 + y^3 = z^3$ فمـــن الواضـــح أن $x^3 + y^3 \equiv z^3(\text{mod } 9)$. ولذا فإن $x^3 + y^3 \equiv z^3(\text{mod } 3)$. لكن $t^3 \equiv t(\text{mod } 3)$

لكل $t \in \mathbb{Z}$. وعليه فـإن $x+y \equiv z \pmod 3$. إذن، $z = x+y+3a$ حيـث $a \in \mathbb{Z}$. من هذا نخلص إلى أن:

$$x^3+y^3 \equiv (x+y+3a)^3$$
$$= x^3+y^3+3x^2y+3y^2x+9x^2a+9y^2a+27a^2x+27a^2y+27a^3+18xya$$
$$\equiv x^3+y^3+3x^2y+3y^2x \pmod 9$$

فيصبح واضحاً أن: $3x^2y+2y^2x = 3xy(x+y) \equiv 0 \pmod 9$. أي أن:
$xy(x+y) \equiv 0 \pmod 3$. وبالتالي فإن $xyz \equiv 0 \pmod 3$. إذن، $3 \mid xyz$. ولـذا إما أن $3 \mid x$ أو أن $3 \mid y$ أو أن $3 \mid z$ △

تمارين (١, ٣)

(١) جد باقي قسمة 3^{57} على 26.
(٢) جد باقي قسمة 2^{43} على 31.
(٣) جد باقي قسمة 41^{65} على 7.
(٤) جد باقي قسمة 2^{48} على 97.
(٥) جد باقي قسمة 6^{48} على 13.
(٦) جد باقي قسمة 4^{30} على 23.
(٧) أثبت أن $2^{37} \equiv 1 \pmod{223}$.
(٨) أثبت أن $3^{500} \equiv 9 \pmod{13}$.
(٩) أثبت أن $12! \equiv 12 \pmod{13}$.
(١٠) أثبت أن $5^{500} \equiv 13 \pmod{17}$.
(١١) أثبت أن $43^{37} \equiv 10 \pmod{11}$.
(١٢) أثبت أن $5^{23} \equiv 46 \pmod{47}$.
(١٣) أثبت أن $7 \times 3^{20} \equiv -7 \pmod{41}$.
(١٤) أثبت أن $2^{644} \equiv 1 \pmod{645}$.
(١٥) أثبت أن $2^{44} \equiv 1 \pmod{89}$.

في التمارين من (١٦) إلى (٢٦) استخدم الاستقراء الرياضي لإثبات كـل مـن علاقات التطابق المعطاة لكل $n \in \mathbb{Z}^+$.

(١٦) $16^n \equiv 6 \pmod{10}$.
(١٧) $6^n - 5n \equiv 1 \pmod{25}$.

(١٨) $2^{3n} \equiv 1 \pmod 7$.

(١٩) $3^{6n-3} \equiv -1 \pmod 7$.

(٢٠) $5^{3n} \equiv 1 \pmod{31}$.

(٢١) $2^{2n} \equiv 3n+1 \pmod 9$.

(٢٢) $(-4)^n \equiv 1-5n \pmod{25}$.

(٢٣) $5^n \equiv 8n^2-4n+1 \pmod{64}$.

(٢٤) $2^{2^n}+5 \equiv 0 \pmod 3$.

(٢٥) $5^n \equiv 1+4n \pmod{16}$.

(٢٦) $3^{2^n} \equiv 1 \pmod{2^{n+2}}$.

(٢٧) إذا كان $a \equiv b \pmod k$ وكان $k \mid n$ فهل صحيح أن $a \equiv b \pmod n$؟

(٢٨) إذا كان k عدداً فردياً فأثبت أن 241 يقسم العدد $11^{2k}+19^{2k}$.

(٢٩) إذا كان p عدداً أولياً حيث $p \geq 5$ فأثبت أن p^2+2 عدد مؤلف.

(٣٠) أثبت أن $(n-1)^3+n^3+(n+1)^3 \equiv 0 \pmod 9$ لكل $n \in \mathbb{Z}^+$.

(٣١) أثبت أن $n^3+11n+1$ لا يقبل القسمة على أي من الأعداد الأوليـــة 2، 3، 5 أو 7 لكل $n \in \mathbb{N}^+$.

(٣٢) إذا كان 36 يقسم $x739y$ فجد قيم كل من x و y.

(٣٣) إذا كان 72 يقسم $72x20y2$ فجد قيم كل من x و y.

(٣٤) إذا كان $a \equiv b \pmod m$ فأثبت أن $(a,m)=(b,m)$. هل العكس صحيح؟

(٣٥) إذا كان p عدداً أولياً فأثبت أن $\binom{2p}{p} \equiv 2 \pmod p$.

(٣٦) أثبت أن $a^4 \equiv 0,1,5,6 \pmod{10}$ لكل $a \in \mathbb{Z}^+$.

(٣٧) أثبت أن $a^2 \equiv 1 \pmod 8$ لكل عدد فردي a.

(٣٨) أثبت أن $a^3 \equiv a \pmod 3$ لكل $a \in \mathbb{Z}$.

(٣٩) إذا كان $a^2 \equiv b^2 \pmod n$ فهل صحيح أن $a \equiv b \pmod n$؟

(٤٠) إذا كان $a^k \equiv b^k \pmod n$ وكـــان $k \equiv j \pmod n$ فهـــل صـــحيح أن $a^j \equiv b^j \pmod n$؟

(٤١) إذا كان $ab \equiv cd \pmod n$ وكان $b \equiv d \pmod n$ حيث $(b,n)=1$ فأثبت أن $a \equiv c \pmod n$.

(٤٢) إذا كان $a \equiv b \pmod{n}$ و $a \equiv c \pmod{m}$ وكان $d = (m,n)$ فأثبت أن $b \equiv c \pmod{d}$

(٤٣) إذا كان $a^2 \equiv b^2 \pmod{p}$ وكان p عدداً أولياً فأثبت أن $a \equiv \pm b \pmod{p}$.

(٤٤) إذا كان $a^k \equiv b^k \pmod{m}$ وكان $a^{k+1} \equiv b^{k+1} \pmod{m}$ حيث $(a,m) = 1$ فأثبت أن $a \equiv b \pmod{m}$. هل تبقى النتيجة صحيحة إذا كان $(a , m) > 1$؟

(٤٥) إذا كان p عدداً أولياً وكان $x^2 \equiv x \pmod{p}$ فأثبت أن $x \equiv 0 \pmod{p}$ أو أن $x \equiv 1 \pmod{p}$.

(٤٦) أثبت أن كثيرة الحدود $f(x) = x^3 + x^2 + 3$ ليس لها جذور صحيحة.

(٤٧) جد نظام رواسب تام قياس 7 ويحقق:

(أ) جميع عناصره أعداداً فردية (ب) جميع عناصره أعداداً زوجية

(ج) جميع عناصره أعداداً أولية

(٤٨) هل يوجد نظام رواسب تام قياس 7 بحيث تكون جميع عناصره مربعات كاملة؟

(٤٩) أثبت أن $\{0, 1, 3, 3^2, \ldots, 3^{15}\}$ نظام رواسب تام قياس 17.

(٥٠) جد نظام رواسب مختزل قياس 2^m حيث $m \in \mathbb{Z}^+$.

(٥١) إذا كان $m > 2$ فهل $\{1^2, 2^2, \ldots, m^2\}$ نظام رواسب تام قياس m؟

(٥٢) إذا كان $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$ نظام رواسب مختزل قياس n وكان $a \in \mathbb{Z}$ فهل أن $\{a_1 + a, \ldots, a_{\varphi(n)} + a\}$ نظام رواسب مختزل قياس n؟

(٥٣) إذا كان كل من $\{r_1, r_2, \ldots, r_n\}$ و $\{s_1, s_2, \ldots, s_m\}$ نظام رواسب تام قياس n و m على التوالي حيث $(m , n) = 1$ فأثبت أن $\{ns_i + mr_j : 1 \le i \le m, 1 \le j \le n\}$ نظام رواسب تام قياس mn.

(٥٤) إذا كان كل من $\{a_1,a_2,\dots,a_p\}$ و $\{b_1,b_2,\dots,b_p\}$ نظام رواسب تام قياس العدد الأولي p فهل من الضروري أن يكون $\{a_1b_1,a_2b_2,\dots,a_pb_p\}$ نظام رواسب تام قياس p ؟

(٥٥) إذا كان n عدداً فردياً وكان $\{a_1,a_2,\dots,a_n\}$ نظام رواسب تـــام قيـــاس n فأثبت أن $\sum_{i=1}^{n} a_i \equiv 0 \pmod n$.

(٥٦) جد النظير الضربي للعدد 160 قياس العدد 841 .

(٥٧) إذا كان $a \equiv b \pmod m$ و $c \equiv d \pmod m$ وكان $(c,m)=(d,m)=1$ فأثبت أن $ac^{-1} \equiv bd^{-1} \pmod m$.

(٥٨) استخدم خوارزمية التربيع والضرب لحساب $1907^{29} \pmod{2633}$.

(٥٩) استخدم خوارزمية التربيع والضرب لحساب $5^{596} \pmod{1234}$.

(٣,٢) التطابقات الخطية

Linear Congruences

بعد أن قمنا بتعريف التطابق ودرسنا خواصه الأساسية ننـــصرف الآن إلى دراسة بعض المعادلات التطابقية. سنقصر اهتمامنا في هذا البند علـــى معـــادلات التطابقات الخطية في متغير واحد ومتغيرين ونرجئ دراسة أنـــواع أخـــرى مـــن المعادلات إلى وقت لاحق من هذا الكتاب.

ليكن لدينا التطابق الخطي $ax \equiv b \pmod n$. لاحظ أن x حل للتطابق إذا وفقط إذا كان $ax-kn=b$ حيث $k \in \mathbb{Z}$. فنرى أن مسألة حل التطابق الخطـــي تكافئ مسألة حل المعادلة الديوفنتية في متغيرين. كذلك من الواضح أنه إذا كان x_1 حلاً للتطابق الخطي $ax \equiv b \pmod n$ وكـــان $x_1 \equiv x_2 \pmod n$ فـــإن x_2 حـــل للتطابق الخطي أيضاً. ولذا سنبحث عن الحلول غير المتطابقة قياس n . أي الحلول

التي تنتمي إلى فصول تكافؤ مختلفة من $\mathbb{Z}_n$. والمبرهنة التالية تجد لنا جميع هذه الحلول.

مبرهنة (٣,١٨)

إذا كان $(a,n)=d$، فللتطابق الخطي $ax\equiv b(\bmod n)$ حل إذا وفقط إذا كان $d\mid b$. وإذا كان $d\mid b$ وكان x_0 حلاً للتطابق فإن جميع الحلول غير المتطابقة قياس n هي: $x=x_0+kn/d$ حيث $0\le k\le d-1$.

البرهان

لقد لاحظنا أن التطابق $ax\equiv b(\bmod n)$ يكافئ المعادلة الديوفنتيّة الخطيّة $ax-ny=b$. وباستخدام مبرهنة (١,٢٠) نجد أن للمعادلة الأخيرة حلاً إذا وفقط إذا كان $d\mid b$. وبالتالي فإن للمعادلة $ax\equiv b(\bmod n)$ حلاً إذا وفقط إذا كان $d\mid b$. وباستخدام مبرهنة (١,٢٠) مرة أخرى نجد أنه إذا كان y_0، x_0 حلاً للمعادلة الديوفنتية $ax-ny=b$ فإن جميع الحلول تكتب على الصورة:

$$x=x_0+\frac{n}{d}k\ ,\ y=y_0+\frac{a}{d}k \quad \text{حيث } k\in\mathbb{Z}.$$

لنأخذ من بين جميع الأعداد الصحيحة التي تحقق المعادلة الأولى الأعداد التي تكون قيم k عندها $0,1,2,\dots,d-1$ وهذه القيم هي:

$$x_0, x_0+\frac{n}{d}, x_0+\frac{2n}{d}, \dots, x_0+\frac{(d-1)n}{d}$$

سنبرهن الآن على أن جميع هذه الحلول غير متطابقة قياس n وأن أي حل آخر يجب أن يطابق أحد هذه الحلول قياس n.

ولهذا الغرض نفرض أن $x_0+\frac{n}{d}k_1\equiv x_0+\frac{n}{d}k_2(\bmod n)$ حيث إن $0\le k_1<k_2\le d-1$. عندئذ نجد أن $\frac{n}{d}k_1\equiv\frac{n}{d}k_2(\bmod n)$. وبما أن

$(n/d,n)=\frac{n}{d}$ فإن : $k_1 \equiv k_2 \pmod d$. أي أن: $d \mid (k_2-k_1)$ وهذا مستحيل لأن $0<k_2-k_1<d$.

لنفرض الآن أن $x_0+\frac{n}{d}k$ حل للتطابق. باستخدام خوارزمية القسمة نستطيع كتابة k على الصورة: $k=qd+r$ و $0 \le r \le d-1$. وعليه فإن:

$$x_0+\frac{n}{d}k = x_0+\frac{n}{d}(qd+r) = x_0+nq+\frac{n}{d}r \equiv x_0+\frac{n}{d}r \pmod n$$

وبهذا يتم البرهان ◆

لإيجاد حلول التطابق الخطي $ax \equiv b \pmod n$ نجد أولاً $d=(a,n)$. إذا كان $d \nmid n$ فإنه استناداً إلى المبرهنة (٣,١٨) لا يوجد حل للتطابق. أما إذا كان $d \mid n$ فإنه يوجد d من الحلول غير المتطابقة قياس n . إذا استطعنا إيجاد أحد الحلول x_0 فاستناداً إلى المبرهنة (٣,١٨) نستطيع إيجاد جميع الحلول الأخرى. ولذا فإننا نركز اهتمامنا على إيجاد حل x_0 للتطابق.

توجد العديد من الطرائق التي يمكن اتباعها لإيجاد حل x_0 ، نقدم بعضاً منها ثم نوضحها ببعض الأمثلة.

الطريقة الأولى:

إذا كان القياس n صغيراً فإننا نقوم بتجريب عناصر نظام رواسب تام قياس n حتى نحصل على حل x_0 .

مثال(٣,١١)

عين جميع الحلول غير المتطابقة قياس 15 للتطابق $27x \equiv 3 \pmod{15}$.

الحل

بما أن $(27,15)=3$ يقسم 3 فإنه توجد ثلاثة حلول غير متطابقة قياس 15.
ولإيجاد أحد هذه الحلول نقوم بتجريب عناصر نظام الرواسب التام $\{0,1,2,\ldots,14\}$ لنجد أن $x_0=4$ يحقق التطابق. ولذا فإن جميع الحلول غير المتطابقة قياس 15 هي: $x=4+5k$ حيث $k=0,1,2$. أي أن: $x=4$ ، $x=9$ ، $x=14$ □

الطريقة الثانية:

نكتب المعادلة الخطية المكافئة للتطابق الخطي ثم نستخدم خوارزمية إقليدس لإيجاد أحد الحلول x_0.

مثال (٣,١٢)

استخدم خوارزمية إقليدس لإيجاد أحد حلول التطابق $27x\equiv 3 \pmod{15}$.

الحل

$$27=1\times 15+12$$
$$15=1\times 12+3$$
$$12=4\times 3+0$$

ولذا فإن $(27,15)=3$. نضع الآن القاسم المشترك الأعظم 3 كتركيب خطي للعدد 15 و 27 فنجد أن:

$$\begin{aligned}3&=15-1\times 12\\&=15-1(27-1\times 15)\\&=2\times 15+(-1)\times 27\end{aligned}$$

ومنه فإن $27\times(-1)\equiv 3 \pmod{15}$. أي أن $x_0=-1\equiv 14 \pmod{15}$ هو أحد حلول التطابق. وعليه تكون جميع الحلول غير المتطابقة قياس 15 هي:
$14+5k$ حيث $k=0,1,2$. أي 14,19,24. وهذه بدورها تكافئ 14,4,9 قياس 15 □

الطريقة الثالثة:

تستخدم هذه الطريقة عادة إذا كان القياس n كبيراً نسبياً والاستراتيجية المتبعة في هذه الطريقة هو محاولة جعل القيمة المطلقة لمعامل x تساوي 1. أي $a=\pm 1$ ونخلص إلى أن $x_0=\pm b$ هو أحد الحلول.

يعتمد تبرير خطوات هذه الطريقة على الحقيقتين التاليتين حيث نقدم برهاناً لهما في التمارين المحلولة في نهاية هذا البند:

(أ) ليكن d يقسم كل من a ، b ، n وليكن $a_1=\frac{a}{d}$ ، $b_1=\frac{b}{d}$ ، $n_1=\frac{n}{d}$. عندئذ يكون التطابق $ax\equiv b(\mathrm{mod}\,n)$ قابلاً للحل إذا وفقط إذا كان التطابق $a_1x\equiv b_1(\mathrm{mod}\,n_1)$ قابلاً للحل.

(ب) ليكن $(a,n)=1$ وليكن d يقسم كل من a و b وليكن $a_1=\frac{a}{d}$ و $b_1=\frac{b}{d}$. عندئذ:

$ax\equiv b(\mathrm{mod}\,n)$ إذا وفقط إذا كان $a_1x\equiv b_1(\mathrm{mod}\,n)$.

نبين الآن كيفية استخدام ذلك في حل التطابق الخطي:

(١) بما أن $d=(a,n)$ يقسم كل من a، n، b فإننا نحصل من التطابق $ax\equiv b(\mathrm{mod}\,n)$ على التطابق : $a_1x\equiv b_1(\mathrm{mod}\,n_1)$ (١)

حيث $a_1=\frac{a}{d}$ ، $b_1=\frac{b}{d}$ ، $n_1=\frac{n}{d}$.

(٢) نجد الآن $d_1=(a_1,b_1)$ ثم نحصل على التطابق :

$$a_2x\equiv b_2(\mathrm{mod}\,n_1) \qquad (٢)$$

حيث $a_2=\frac{a_1}{d_1}$ و $b_2=\frac{b_1}{d_1}$ لأن $(a_2,b_2)=(a_2,n_1)=1$. الآن، إذا كان $a_2=\pm 1$ نتوقف ونحصل على الحل المطلوب $x_0=\pm b_2$. أما إذا كان $a_2\neq\pm 1$ فإننا ننفذ الخطوة (٣).

(٣) لدينا في هذه الخطوة خياران:

(أ) بملاحظة أن $b_2 \equiv b_2 \pm n_1 \equiv b_2 \pm 2n_1 \equiv \ldots \bmod(n_1)$ فإنه يكون بإمكاننا استبدال b_2 بعدد $b_3 = b_2 + kn_1$ يطابق b_2 قياس n_1 بحيث يكون $(a_2, b_3) > 1$ ثم ننفذ الخطوة (٢) على التطابق:

$a_2 x \equiv b_3 (\bmod\ n_1)$ للحصول على عدد جديد أصغر من $|a_2|$. أو

(ب) نقوم بضرب التطابق (٢) بعدد مناسب c لنحصل على:

$$ca_2 x \equiv cb_2 (\bmod\ n_1) \qquad (٣)$$

إذا اخترنا العدد c بحيث تكون القيمة المطلقة لأصغر باقي a_3 للعدد ca_2 يحقق $|a_3| < |a_2|$ فإننا نحصل على التطابق: $a_3 x \equiv b_3 (\bmod\ n_1)$ (٤)

حيث $b_3 = cb_2$.

وأخيراً، بتطبيق خيارات الخطوة (٣) نحصل في النهاية على تطابق تكون فيه القيمة المطلقة لمعامل x تساوي 1 ومن ثم نجد الحل x_0.

مثال(٣,١٣)

استخدم الطريقة الثالثة المقدمة أعلاه لإيجاد أحد حلول التطابق $27x \equiv 3 (\bmod\ 15)$.

الحل

(١) بما أن $(27,15) = 3$ فإننا نحصل على التطابق المكافئ

$$9x \equiv 1 (\bmod\ 5) \qquad (١)$$

وبما أن $(9,1) = 1$ فإننا لسنا بحاجة للخطوة (٢).

(٢) بضرب التطابق (١) بالعدد 4 نحصل على التطابق المكافئ:

$36x \equiv 4 (\bmod\ 5)$. أي $x \equiv 4 (\bmod\ 5)$. ومن ثم فإن $x_0 = 4$ حل للتطابق.

أو من الممكن استبدال التطابق (١) بالتطابق المكافئ :

$$9x \equiv 1 + 35 \equiv 36 (\bmod\ 5) \qquad (٢)$$

بما أن $(9,36) = 9$ فإننا نحصل من التطابق (٢) على التطابق المكافئ:

$x \equiv 4 \pmod 5$. ومن ثم نجد أن $x_0 = 4$ حل للتطابق □

مثال (٣,١٤)

عين جميع حلول التطابق $18x \equiv 42 \pmod{50}$.

الحل

بما أن $(18,50) = 2$ فإنه يوجد حلان للتطابق. وبقسمة طرفي التطابق على العدد 2 نحصل على التطابق المكافيء: $9x \equiv 21 \pmod{25}$. بضرب طرفي التطابق الآخير بالعدد 14 نحصل على: $126x \equiv 294 \pmod{25}$. أي أن $x \equiv 19 \pmod{25}$. ولذا فإن $x_0 = 19$ حل للتطابق. وأما الحل الآخر فهو $19 + 25 = 44$ □

مثال (٣,١٥)

عين جميع حلول التطابق $108x \equiv 171 \pmod{529}$.

الحل

بما أن $(108,529) = 1$ فإنه يوجد حل وحيد للتطابق. الآن:

$108x \equiv 171 + 529 \equiv 700 \pmod{529}$ وبما أن $(108,700) = 4$ فإننا نحصل على التطابق المكافئ: $27x \equiv 175 \pmod{529}$. وهذا التطابق يكافئ

$27x \equiv 175 + 2 \times 529 \equiv 1233 \pmod{529}$. وبما أن $(27,1233) = 9$ فإننا نحصل على التطابق المكافئ: $3x \equiv 137 \pmod{529}$. وبضرب التطابق الأخير بالعدد 176 نحصل على التطابق $528x \equiv 24112 \pmod{529}$. أي على التطابق $-x \equiv 307 \pmod{529}$. وبالتالي نخلص إلى أن $x = -307 \equiv 222 \pmod{529}$ هو الحل الوحيد للتطابق □

مثال (٣,١٦)

جد حل التطابق $729x \equiv 1 \pmod{8180}$.

الحل

بما أن $(729,8180) = 1$ فإن للتطابق حل وحيد. الآن، التطابق المعطى يكافئ التطابق: $729x \equiv 1+8180 \equiv 8181 \pmod{8180}$. بملاحظة أن $(729,8181) = 81$ نحصل على التطابق المكافئ $9x \equiv 101 \pmod{8180}$. الآن: $9x \equiv 101+2\times 8180 \equiv 16461 \pmod{8180}$. وبما أن $(9,16461) = 9$ فإننا نحصل على التطابق: $x \equiv 1829 \pmod{8180}$ □

مثال (٣,١٧)

استخدم التطابق لحل المعادلة الديوفنتية $87x - 105y = 57$.

الحل

المعادلة الديوفنتية تكافئ التطابق $87x \equiv 57 \pmod{105}$. وبما أن $(87,105) = 3$ وأن $3 \mid 57$ فإنه يوجد ثلاثة حلول للتطابق. لايجاد أحد هذه الحلول نقسم التطابق على 3 لنحصل على $29x \equiv 19 \pmod{35}$. بضرب طرفي التطابق بالعدد 6 نحصل على: $174x \equiv 114 \pmod{35}$. ومنه فإن $-x \equiv 9 \pmod{35}$. أي أن :

$x = -9 \equiv 26 \pmod{35}$. ومنه فإن $x = 26+35k$ وبالتعويض في المعادلة الديوفنتية نجد أن: $105y = 87x - 57 = 87(26+35k) - 57 = 2205 + 3045k$. ومنه فإن:

$y = 21+29k$. وبالتالي فإن جميع حلول المعادلة الديوفنتية هي:

$x = 26+35k$ ، $y = 21+29k$ حيث $k \in \mathbb{Z}$ □

(٣,٢,١)التطابقات الخطية بمتغيرين

(Linear Congruences in Two Variables)

بعد أن قدمنا التطابقات الخطية بمتغير واحد وبينا كيفية إيجاد جميع حلولهـــا غير المتطابقة، فإننا نقوم الآن بدراسة التطابقات الخطية بمتغيرين. أي التطابقـــات التي على الصورة $ax+by \equiv c \pmod{n}$.

إذا كان x_1 و y_1 عددين صحيحين يحققان التطـــابق فنقـــول إن (x_1,y_1) حـــل للتطابق. لاحظ أنه إذا كان (x_1,y_1) حل للتطابق فإن (x_1+rn,y_1+sn) حل أيضاً لكل $r,s \in \mathbb{Z}$ وإن :

$$x_1+rn \equiv x_1 \pmod{n}$$
$$y_1+sn \equiv y_1 \pmod{n}$$

ولهذا نقول إن جميع هذه الحلول متطابقة قياس n. والحلول التي تكون فيها قيم x أو قيم y تنتمي إلى فصول تكافؤ مختلفة قياس n فإنها تسمى حلول غير متطابقـــة قياس n.

تزودنا المبرهنة التالية بالشرط اللازم والكـــافي لوجـــود حـــل للتطـــابق $ax+by \equiv c \pmod{n}$.

مبرهنة (٣,١٩)

يوجد حل للتطابق $ax+by \equiv c \pmod{n}$ إذا وفقط إذا كان $d \mid c$ حيث $d=(a,b,n)$.

البرهان

لاحظ أن للتطابق $ax+by \equiv c \pmod{n}$ حل إذا وفقط إذا كان للمعادلة الديوفنتية $ax+by-nz=c$ حل حيث $z \in \mathbb{Z}$. ولذا فإننا نحصل على المطلوب بتطبيق المبرهنة (١,٢١) ◆

مثال (٣,١٨)

جد جميع حلول التطابق $2x+3y\equiv 1 \pmod 7$ غير المتطابقة.

الحل

لاحظ أن:

$$2x+3y\equiv 1 \pmod 7 \Leftrightarrow 2x\equiv 1-3y \pmod 7$$
$$\Leftrightarrow 2x\equiv -6+4y \pmod 7$$
$$\Leftrightarrow x\equiv -3+2y \pmod 7$$

ولذا فلكل قيمة y تنتمي إلى نظام الرواسب التام $\{0, \pm 1, \pm 2, \pm 3\}$ قياس 7 نستطيع إيجاد قيمة واحدة فقط x قياس 7. وبالتالي فإن جميع الحلول غير المتطابقة قياس 7 هي: $(-3,0)$, $(-1,1)$ ، $(2,-1)$, $(1,2)$, $(0,-2)$, $(3,3)$ ، $(-2,-3)$ □

المبرهنة التالية تزودنا بعدد الحلول غير المتطابقة قياس n في الحالة الخاصة التي يكون فيها $(a,n)=1$ أو $(b,n)=1$.

مبرهنة (٣,٢٠)

إذا كان $(a,n)=1$ أو $(b,n)=1$ فإن عدد الحلول غير المتطابقة للتطابق $ax+by\equiv c \pmod n$ يساوي n.

البرهان

لنفرض أن $(a,n)=1$. التطابق يكافئ التطابق : $ax\equiv c-by \pmod n$ (١)

وبما أن $(a,n)=1$ فإنه يوجد حل وحيد x للتطابق (١) لكل y في نظام الرواسب التام $\{0,1,2,\ldots,n-1\}$. وبالتالي فعدد الحلول غير المتطابقة قياس n يساوي n.

والبرهان مشابه إذا كان $(b,n)=1$ ◆

عدد الحلول غير المتطابقة في الحالة العامة تزودنا به المبرهنة التالية:

مبرهنة (٣,٢١)

إذا كان $d=(a,b,n)$ يقسم c فهناك dn من الحلول غير المتطابقة قياس n للتطابق $ax+by\equiv c(\bmod n)$.

البرهان

لنفـــــرض أن $a=da_1$ ، $b=db_1$ ، $c=dc_1$ ، $n=dn_1$ حيـــــث $(a_1,b_1,n_1)=1$. حينئذ ، $a_1x+b_1y\equiv c_1(\bmod n_1)$ (١)

لنفرض أن $d_1=(a_1,n_1)$. عندئذ يوجد حل للتطابق (١) إذا وفقط إذا وجد حـــل للتطابق $b_1y\equiv c_1(\bmod d_1)$ (٢)

وبما أن $(a_1,b_1,n_1)=1$ وأن $(a_1,n_1)=d_1$ فإن $(b_1,d_1)=1$. ولذا فإن للتطـــابق (٢) حل وحيد y_0 قياس d_1 . الآن جميع حلول التطابق (٢) هي:

$$y_0,y_0+d_1,y_0+2d_1,\ldots,y_0+\left(\frac{n_1}{d_1}-1\right)d_1$$

وعددها $\frac{n_1}{d_1}$ وهي متطابقة قياس d_1 ولكنها غير متطابقة قياس n_1. ولكل قيمة y لهذه الحلول يوجد d_1 من قيم x للتطابق (١). ولذا فإن عدد حلول التطـــابق (١) غير المتطابقة قياس n_1 هو $d_1\times\frac{n_1}{d_1}=n_1$.

لنفرض الآن أن (x_1,y_1) حل للتطابق (١). عندئذ القيم:

$$x_1,x_1+n_1,x_1+2n_1,\ldots,x_1+(d-1)n_1$$

وعددها d متطابقة قياس n_1 وغير متطابقة قياس n. وكذلك القيم :

$$y_1,y_1+n_1,y_1+2n_1,\ldots,y_1+(d-1)n_1$$

متطابقة قياس n_1 وغير متطابقة قياس n.

ولذا فلكل حل للتطابق (١) نستطيع إيجاد d^2 من الحلول غير المتطابقة للتطابق $ax+by\equiv c(\bmod n)$. ولذا فإن عدد الحلول غير المتطابقة قياس n هو $d^2n_1=dn$ ◆

مثال (٣,١٩)

جد جميع حلول $8x+6y\equiv 10(\bmod 16)$ غير المتطابقة.

الحل

بما أن $(8,6,10)=2$ يقسم 10 فإنه يوجد $2\times 16=32$ حل غير متطابق قياس 16 . الآن التطابق $8x+6y\equiv 10(\bmod 16)$ يؤدي إلى التطابق $4x+3y\equiv 5(\bmod 8)$.

وبما أن $(4,8)=4$ فإن $3y\equiv 5(\bmod 4)$. ومنه فإن $y\equiv 3(\bmod 4)$. ولذا فإن كل من القيمتين $y\equiv 3(\bmod 4)$ و $y\equiv 7(\bmod 4)$ تعطينا أربع قيم x غير متطابقة قياس 8 بحيث يكون $4x+3y\equiv 5(\bmod 8)$.

عند $y\equiv 3(\bmod 4)$ نجد أن: $4x+3\times 3\equiv 5(\bmod 8)$. فيكون $x\equiv 1(\bmod 2)$. ونستخلص أن

$x\equiv 1(\bmod 8)$ ، $x\equiv 3(\bmod 8)$ ، $x\equiv 5(\bmod 8)$ ، $x\equiv 7(\bmod 8)$

وعند $y\equiv 7(\bmod 4)$ نجد أن: $4x+3\times 7\equiv 5(\bmod 8)$.

فيكون $x\equiv 0(\bmod 2)$. ولذا فإننا نجد أن:

$x\equiv 0(\bmod 8)$، $x\equiv 2(\bmod 8)$، $x\equiv 4(\bmod 8)$، $x\equiv 6(\bmod 8)$. إذن الحلول غير المتطابقة للتطابق $4x+3y\equiv 5(\bmod 8)$ هي

$(1,3)$، $(3,3)$ ، $(5,3)$ ، $(7,3)$، $(0,7)$ ، $(2,7)$، $(4,7)$ ، $(6,7)$

ولكل حل (x,y) من هذه الحلول توجد أربعة حلول للتطابق $8x+6y\equiv 10(\bmod 16)$ هي:

(x,y) ، $(x+8,y)$، $(x,y+8)$، $(x+8,y+8)$

وبذا نرى أن جميع حلول التطابق هي:

(1,3) , (9, 3), (1, 11), (9, 11), (3,3), (11, 3), (3, 11), (11, 11), (5,3), (13, 3), (5, 11), (13, 11), (7, 3), (15, 3), (7, 11), (15, 11), (0, 7), (8, 7), (0, 15), (8, 15), (2, 7), (10, 7), (2, 15), (10, 15), (4, 7), (12, 7), (4, 15), (12, 15), (6, 7), (14, 7), (6, 15), (14, 15)

□

(٣,٢,٢) تمارين محلولة (*Solved Exercises*)

تمرين (١)

عين جميع الأعداد b حيث $0 \le b < 30$ لكي يكون للتطابق $12x \equiv b \pmod{30}$ حل، ثم احسب عدد الحلول غير المتطابقة.

الحل

استناداً إلى المبرهنة (٣,١٨) يوجد حل للتطابق $12x \equiv b \pmod{30}$ إذا وفقط إذا كان $(12,30) = 6$ يقسم العدد b. ولذا فإن قيم b قياس 30 التي تحقق ذلك هي: 0، 6، 12، 18، 24. ولكل من هذه القيم يوجد 6 حلول غير متطابقة قياس العدد 30 △

تمرين (٢)

(أ) إذا كان y_0 حلاً للتطابق $ny \equiv -b \pmod{a}$ فأثبت أن $\frac{ny_0 + b}{a}$ حل للتطابق $ax \equiv b \pmod{n}$.

(ب) استخدم الفقرة (أ) لحل التطابق $108x \equiv 17 \pmod{529}$.

الحل

(أ) بما أن $ny_0 \equiv -b \pmod{a}$ فإن $ny_0 + b = ka$ حيث $k \in \mathbb{Z}$. إذن، $ak \equiv b \pmod{n}$. ومنه فإن $k = \frac{ny_0 + b}{a}$ حل للتطابق $ax \equiv b \pmod{n}$.

(ب) باستخدام الفقرة (أ) نجد أولاً حل للتطـــابق $529y \equiv -171 \pmod{108}$.
وهذا التطابق بكافئ التطابق $11y \equiv 63 \pmod{108}$. وباستخدام الفقرة (أ) مرة أخرى لاختزال التطابق الأخير نجد أن $108z \equiv -63 \pmod{11}$. أي أن $-2z \equiv -8 \pmod{11}$. ومنه فإننا نجد وبسهولة أن $z_0 = 4$ حـــل للتطـــابق الأخير. ولذا فإن :

$$y_0 = \frac{nz_0 + b}{a} = \frac{108 \times 4 + 63}{11} = 45$$

$$x_0 = \frac{ny_0 + b}{a} = \frac{529 \times 45 + 171}{108} = 222$$

ونخلص إلى أن $x_0 = 222$ حل للتطابق $108x \equiv 171 \pmod{529}$. وهذا يتفق مع ما وجدناه في المثال (٣,١٥) △

تمرين (٣)

(أ) أفرض d يقسم كلاً من a ، b ، n وليكن $a_1 = \frac{a}{d}$ ، $b_1 = \frac{b}{d}$ ، $n_1 = \frac{n}{d}$.
أثبت أن: $ax \equiv b \pmod{n}$ إذا وفقط إذا كان $a_1 x \equiv b_1 \pmod{n}$.

(ب) ليكن $(a,n) = 1$ وليكن d يقسم a ويقسم b وليكن $a_1 = \frac{a}{d}$ و $b_1 = \frac{b}{d}$.
أثبت أن : $ax \equiv b \pmod{n}$ إذا وفقط إذا كان $a_1 x \equiv b_1 \pmod{n}$.

الحل

(أ) لاحظ أن:

$$ax \equiv b \pmod{n} \Leftrightarrow ax - b = kn$$

$$\Leftrightarrow \frac{a}{d}x - \frac{b}{d} = k\frac{n}{d}$$

$$\Leftrightarrow a_1 x - b_1 = kn_1$$

$$\Leftrightarrow a_1 x \equiv b_1 \pmod{n_1}$$

(ب) لنفرض أولاً أن $ax \equiv b \pmod{n}$. عندئذ:

$ax - b = kn$. ومنه فإن $\frac{a}{d}x - \frac{b}{d} = k\left(\frac{n}{d}\right)$.

ولذا فإن $d \mid kn$. وبما أن $d \mid a$ وأن $(a,n)=1$ فإن $(d,n)=1$. وعليه فـــإن $d \mid k$. وبالتالي $a_1x \equiv b_1 (\mathrm{mod}\, n)$.

لبرهان العكس، نفرض أن $a_1x \equiv b_1 (\mathrm{mod}\, n)$ عندئذ: $a_1x - b_1 = kn$.

وبضرب المعادلـــة الأخـــيرة بالعـــدد d نجـــد أن $a_1dx - b_1d = kd_1n$. أي أن $ax - b = kd_1n$. وبالتالي فإن $ax \equiv b (\mathrm{mod}\, n)$ △

تمارين (٣,٢)

في التمارين من (١) إلى (٢٦) ، جد جميع حلول التطابق الخطي المبين:

(١) $36x \equiv -78 (\mathrm{mod}\, 131)$.

(٢) $11x \equiv 28 (\mathrm{mod}\, 1943)$.

(٣) $10x \equiv 3 (\mathrm{mod}\, 12)$.

(٤) $35x \equiv 14 (\mathrm{mod}\, 182)$.

(٥) $27x \equiv 3 (\mathrm{mod}\, 15)$.

(٦) $7x \equiv 22 (\mathrm{mod}\, 31)$.

(٧) $36x \equiv 8 (\mathrm{mod}\, 102)$.

(٨) $18x \equiv 30 (\mathrm{mod}\, 42)$.

(٩) $19x \equiv 1 (\mathrm{mod}\, 140)$.

(١٠) $144x \equiv 216 (\mathrm{mod}\, 360)$.

(١١) $128x \equiv 833 (\mathrm{mod}\, 1001)$.

(١٢) $987 \equiv 610 (\mathrm{mod}\, 1597)$.

(١٣) $513x \equiv -17 (\mathrm{mod}\, 1163)$.

(١٤) $66x \equiv 121 (\mathrm{mod}\, 737)$.

(١٥) $4x \equiv 13 (\mathrm{mod}\, 47)$.

(١٦) $10x \equiv 6 (\mathrm{mod}\, 14)$.

(١٧) $12x \equiv 15 (\mathrm{mod}\, 22)$.

(١٨) $19x \equiv 42 (\mathrm{mod}\, 50)$.

(١٩) $143x \equiv 4 (\mathrm{mod}\, 315)$.

(٢٠) $519x \equiv 311 (\mathrm{mod}\, 1967)$.

(٢١) $11x \equiv 25 (\mathrm{mod}\, 60)$.

(٢٢) $64x \equiv 16 (\mathrm{mod}\, 84)$.

(٢٣) $42x \equiv 90 (\mathrm{mod}\, 156)$.

(٢٤) $64x \equiv 897 (\mathrm{mod}\, 1001)$.

(٢٥) $179x \equiv 283 (\mathrm{mod}\ 313)$. (٢٦) $251x \equiv 125 (\mathrm{mod}\ 521)$.

في التمارين من (٢٧) إلى (٣٦) جد جميع حلول كل من التطابقات المعطاة:

(٢٧) $3x - 7y \equiv 11 (\mathrm{mod}\ 13)$. (٢٨) $7x + 8y \equiv 6 (\mathrm{mod}\ 10)$.

(٢٩) $3x + 4y \equiv 7 (\mathrm{mod}\ 12)$. (٣٠) $2x + 4y \equiv 6 (\mathrm{mod}\ 8)$.

(٣١) $6x + 3y \equiv 0 (\mathrm{mod}\ 9)$. (٣٢) $10x + 5y \equiv 9 (\mathrm{mod}\ 15)$.

(٣٣) $7x + 9y \equiv 21 (\mathrm{mod}\ 14)$. (٣٤) $16x - 12y \equiv 45 (\mathrm{mod}\ 60)$.

(٣٥) $3x + y \equiv 7 (\mathrm{mod}\ 5)$. (٣٦) $6x - 2y \equiv 122 (\mathrm{mod}\ 8)$.

(٣٧) استخدم طريقة التمرين المحلول (٢) لحل التطابقات المقدمة في التمارين (١٠)، (١٤)، (٢٥)، (٢٦).

(٣,٣) أنظمة التطابقات الخطيّة بمتغير واحد
System of Linear Congruences in One Variable

لنفرض أن لدينا التطابقين التاليين:

$$6x \equiv 4 (\mathrm{mod}\ 8)$$

$$3x \equiv 2 (\mathrm{mod}\ 5)$$

تعلمنا في البند (٣,٢) كيفية حل كل من التطابقين على حدة، والسؤال المطروح الآن هل باستطاعتنا إيجاد عدد x يحقق المعادلتين معاً؟ إذا وجد مثل هذا العدد فنسميه حلاً لنظام التطابقات. بحل التطابق الأول نجد أن:

$x = 2+4k$ حيث $k = 0,1$ هي جميع الحلول غير المتطابقة قيـــاس 8 للتطـــابق الأول، أما التطابق الثاني فله حل واحد فقط قياس 5 وهو $x = 4$. ولحل النظـــام يجب أن نجد عدد x يحقق:

$$x \equiv 2 \pmod 4 \qquad (١)$$

$$x \equiv 4 \pmod 5 \qquad (٢)$$

من (١) لـــدينا $x = 2+4k_1$ حيـــث $k_1 \in \mathbb{Z}$، وبـــالتعويض في (٢) نجـــد أن: $2+4k_1 \equiv 4 \pmod 5$، أي أن: $4k_1 \equiv 2 \pmod 5$. بحل التطابق الأخـــير نـــرى أن $k_1 \equiv 3 \pmod 5$، وعليه فإن $k_1 = 3+5k_2$ حيث $k_2 \in \mathbb{Z}$. وبالتعويض عـــن قيمة k_1 في المعادلـــة $x = 2+4k_1$ نجـــد أن $x = 14+20k_2$. وبالتـــالي فـــإن $x \equiv 14 \pmod{20}$ يحقق التطابقين معاً.

في المثال أعلاه تمكنا من إيجاد حل للنظام، وسيكون من المفيد جـــداً لـــو استطعنا الحصول على طريقة لمعرفة فيما إذا كان هناك حل للنظام قبل البـــدء في محاولة الحل. ومتى تيقنا من وجود حل أن نستطيع حسابه بخوارزمية كالتي حصلنا عليها في حالة التطابق الخطي في البند السابق. هذا بالفعل ما سنقوم بدراســـته في هذا البند.

تمهيدية (٣,٢٢)

ليكن لدينا نظام التطابقات التالي:

$$\begin{aligned} a_1x &\equiv c_1 \pmod{m_1} \\ a_2x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ a_kx &\equiv c_k \pmod{m_k} \end{aligned} \qquad (١)$$

ولـــيكن $(a_i, m_i) = d_i$ ، $1 \le i \le k$، ولـــيكن x_i حـــلاً للتطـــابق $a_i x \equiv c_i \pmod{m_i}$ حيث $1 \le i \le k$. عندئذ x حل للنظام (١) إذا وفقط إذا كان x حلاً للنظام:

$$\begin{aligned} x &\equiv x_1 \pmod{m_1/d_1} \\ x &\equiv x_2 \pmod{m_2/d_2} \\ &\vdots \\ x &\equiv x_k \pmod{m_k/d_k} \end{aligned} \qquad (٢)$$

البرهان

لنفـــرض أولاً أن x حـــل للنظـــام (١). بمـــا أن x_i حـــل للتطـــابق $a_i x \equiv c_i \pmod{m_i}$ لكل i فإن $a_i x_i \equiv c_i \pmod{m_i}$ لكـــل i. ولـــذا فـــإن $a_i x \equiv a_i x_i \pmod{m_i}$. وبمـــا أن $(a_i , m_i) = d_i$ فإننـــا نجـــد أن $x \equiv x_i \pmod{m_i/d_i}$ لكل $1 \le i \le k$. وبالتالي فإن x حل للنظام.

ولبرهـــان العكـــس، نفـــرض أن x حـــل للنظـــام (٢). وعليـــه فـــإن $x \equiv x_i \pmod{m_i/d_i}$ لكـــل i. وبمـــا أن $(a_i , m_i) = d_i$ فإننـــا نجـــد أن $a_i x = a_i x_i \pmod{m_i}$ لكـــل i. ولمـــا كـــان x_i حـــلاً للتطـــابق $a_i x \equiv c_i \pmod{m_i}$ فإننا نجـــد أن $a_i x_i \equiv c_i \pmod{m_i}$ لكـــل i. وبالتـــالي فإن $a_i x \equiv c_i \pmod{m_i}$ لكل i. ونخلص إلى أن x حل للنظام (١) ◆

مثال (٣,٢٠)

لقد وجدنا أن $x \equiv 14 \pmod{20}$ حل للنظام:

$$6x \equiv 4 \pmod{8}$$
$$3x \equiv 2 \pmod{5}$$

وبما أن $(6 , 8) = 2$ و $(3, 5) = 1$ وأن $x_1 \equiv 2 \pmod{4}$ و $x_2 \equiv 4 \pmod{5}$ حل لكل من للتطابقين على الترتيب. فباستخدام تمهيدية (٣,٢٢) نجد أنـــه يجـــب أن يكون هناك حل للنظام:

$$x \equiv 2(\text{mod } 4)$$
$$x \equiv 4(\text{mod } 5)$$ □

ملحوظات

(١) باستخدام التمهيدية (٣,٢٢) يكفي أن ندرس الأنظمة الـــتي تكـــون فيهـــا معاملات المتغير x تساوي العدد 1.

(٢) من الواضح أنه إذا كان أحد التطابقات في نظام ما غير قابل للحل فإن النظام غير قابل للحل، ولكن العكس ليس صحيحاً، كما يوضح المثال التالي:

مثال(٣,٢١)

ليكن لدينا النظام:

$$6x \equiv 4(\text{mod } 8)$$
$$9x \equiv 3(\text{mod } 12) \quad (١)$$

بما أن $4 \mid 2 = (6,8)$ وأن $3 \mid 3 = (9,12)$ فإنه يوجد حـــل لكـــل تطـــابق مـــن التطابقين. ومـــن الـــسهل رؤيـــة أن $x \equiv 2(\text{mod } 4)$ حـــل للتطـــابق الأول وأن $x \equiv 3(\text{mod } 4)$ حل للتطابق الثاني.

وباستخدام تمهيدية (٣,٢٢) فإنه يكون للنظام (١) حل إذا وفقط إذا كان للنظام:

$$x \equiv 2(\text{mod } 4)$$
$$x \equiv 3(\text{mod } 4) \quad (٢)$$

حل. ولكن من الواضح أن ليس هناك حل للنظام (٢) . وعليه لا يوجـــد حـــل للنظام (١) □

المبرهنة التالية تعرف بمبرهنة الباقي الصينية *(the Chinese remainder theorem)* وهي تضمن لنا وجود حل للأنظمة التي تكون القياسات فيها أولية نسبياً.

مبرهنة (٣,٢٣) [مبرهنة الباقي الصينية]

إذا كانت الأعداد $m_1, m_2, \ldots, m_k$ أعداداً أولية نسبياً زوجاً زوجاً فهناك حل وحيد قياس العدد $M = m_1 m_2 \ldots m_k$ للنظام:

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv c_k \pmod{m_k}$$

البرهان

لإيجاد حل للنظام نفرض أن:

$M_r = \frac{M}{m_r} = m_1 m_2 \ldots m_{r-1} m_{r+1} \ldots m_k$ لكل $r = 1, 2, \ldots, k$. بما أن $(m_r, m_s) = 1$ عندما $r \neq s$ فبالاستناد إلى تمرين (٤) من تمارين (١,٣,٣) نجد أن $(M_r, m_r) = 1$. وبهذا يكون للعدد M_r نظيراً ضربياً قياس m_r وليكن M_r^{-1}، أي أن $M_r M_r^{-1} \equiv 1 \pmod{m_r}$. سنبرهن الآن أن:

$$x = c_1 M_1 M_1^{-1} + c_2 M_2 M_2^{-1} + \ldots + c_k M_k M_k^{-1}$$

حل للنظام قياس M، ولهذه الغاية علينا إثبات أن $x \equiv c_r \pmod{m_r}$ لكل r حيث $1 \leq r \leq k$. بما أن $m_r \mid M_s$ عندما $r \neq s$ فإن: $M_s \equiv 0 \pmod{m_r}$. ومنه فإن $x \equiv c_r M_r M_r^{-1} \equiv c_r \pmod{m_r}$.

لبرهان الوحدانية نفرض أن x_0 و x_1 حلان للنظام. من تعريف الحل نجد أن $x_0 \equiv x_1 \equiv c_r \pmod{m_r}$ لكل r، $1 \leq r \leq k$. ومنه نجد أن $m_r \mid (x_0 - x_1)$. ولكون الأعداد $m_1, m_2, \ldots, m_k$ أولية نسبياً زوجاً فإن $M = m_1 m_2 \ldots m_k = [m_1, m_2, \ldots, m_k]$ ومن ذلك نستنتج أن $M \mid (x_0 - x_1)$. إذن، $x_0 \equiv x_1 \pmod{M}$ ◆

مثال (٣,٢٢)

جد أصغر عدد صحيح موجب بحيث تكون بواقي قسمته على الأعداد 3، 4، 5 هي على التوالي: 1 ، 2 ، 3 .

الحل

إن العدد المطلوب x يحقق النظام:

$$x \equiv 1(\text{mod } 3)$$
$$x \equiv 2(\text{mod } 4)$$
$$x \equiv 3(\text{mod } 5)$$

لدينا $M = 3\times4\times5 = 60$ ، $M_1 = 20$ ، $M_2 = 15$ ، $M_3 = 12$. لإيجاد M_1^{-1} ، M_2^{-1} ، M_3^{-1} يجب أن نجد حلاً لكل من التطابقات:

$20M_1^{-1} \equiv 1(\text{mod } 3)$ ، $15M_2^{-1} \equiv 1(\text{mod } 4)$ و $12M_3^{-1} \equiv 1(\text{mod } 5)$.

من التطابق الأول نجد أن $M_1^{-1} = 2$ ومن الثاني $M_2^{-1} = 3$ ومن التطابق الثالث $M_3^{-1} = 3$. وبتطبيق المبرهنة نجد أن:

□ $x \equiv 1\times20\times2 + 2\times15\times3 + 3\times12\times3 = 238 \equiv 58(\text{mod } 60)$

ملحوظة

يمكن حل هذا المثال بطريقة التعويض المتتالي التي ذكرناها في مقدمة البند ويتم ذلك على النحو التالي:

من التطابق الأول يوجد k_1 يحقق $x = 1+3k_1$. بالتعويض في الثاني نحصل على $1+3k_1 \equiv 2(\text{mod } 4)$. أي أن $3k_1 \equiv 1(\text{mod } 4)$ ، وبالضرب في 3 نحصل على: $k_1 \equiv 3(\text{mod } 4)$. ومنه يوجد k_2 بحيث إن $k_1 = 3+4k_2$. ومنه نجد أن: $x = 1+3(3+4k_2) = 1+9+12k_2 = 10+12k_2$. وبالتعويض في التطابق الثالث نحصل على: $10+12k_2 \equiv 3(\text{mod } 5)$. أي أن: $2k_1 \equiv 3(\text{mod } 5)$. وبالضرب في 3 نحصل على $k_2 \equiv 9 \equiv 4(\text{mod } 5)$. إذن، يوجد k_3 بحيث إن $k_2 = 4+5k_3$. وبالتالي فإن:

$$x = 10 + 12(4 + 5k_3) = 58 + 60k_3 \equiv 58 \pmod{60}$$ □

مثال (٣,٢٣)

استخدم مبرهنة الباقي الصينية لحل التطابق: $19x \equiv 1 \pmod{140}$.

الحل

التطابق يكافئ النظام:

$$19x \equiv 1 \pmod 4$$
$$19x \equiv 1 \pmod 5$$
$$19x \equiv 1 \pmod 7$$

وهذا بدوره يكافئ النظام:

$$x \equiv 3 \pmod 4$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 3 \pmod 7$$

ومنه نجد أن: $M_1 = 35$ ، $M_2 = 28$ و $M_3 = 20$. بحل المعادلة $35M_1^{-1} \equiv 1 \pmod 4$ نجد أن: $M_2^{-1} = -1$. ومن المعادلة $28M_3^{-1} \equiv 1 \pmod 5$ نجد أن $M_2^{-1} = 2$. ومن المعادلة $20M_3^{-1} \equiv 1 \pmod 7$ نجد أن $M_3^{-1} = -1$.

ونخلص إلى أن الحل:

$$x \equiv 35 \times (-1) \times 3 + 28 \times 2 \times 4 + 20 \times (-1) \times 3 \equiv 59 \pmod{140}$$ □

بعد أن تمّ البت في حل الأنظمة ذات القياسات الأولية نسبياً زوجاً زوجاً سنركّز اهتمامنا الآن على الأنظمة بصورة عامة.

تعريف (٣,٦)

ليكن لدينا النظام التالي:

$$x \equiv c_1 (\text{mod } m_1)$$
$$x \equiv c_2 (\text{mod } m_2)$$
$$\vdots$$
$$x \equiv c_k (\text{mod } m_k)$$

وليكن أن $(m_i, m_j) = d_{ij}$ لكل $1 \le i \ne j \le k$. نقول إن النظام منسجم *(compatible system)* إذا كان $c_i \equiv c_j (\text{mod } d_{ij})$ لكل $1 \le i \ne j \le k$.

مثال (٣,٢٤)

النظام
$$x \equiv 5(\text{mod } 12)$$
$$x \equiv 7(\text{mod } 9)$$

غير منسجم لأن $(12,9) = 3$ ولكن $5 \not\equiv 7(\text{mod } 3)$. ولكن النظام:

$$x \equiv 4(\text{mod } 21)$$
$$x \equiv 18(\text{mod } 35)$$
$$x \equiv 13(\text{mod } 15)$$

منسجماً لأن:

$$(21,35) = 7 \text{ ، } 4 \equiv 18(\text{mod } 7)$$
$$(21,15) = 3 \text{ ، } 4 \equiv 13(\text{mod } 3)$$
$$(35,15) = 5 \text{ ، } 18 \equiv 13(\text{mod } 5) \quad \square$$

ملحوظة

لاحظ أن انسجام أي نظام من التطابقات يعتمد على انسجام كل زوج من التطابقات في النظام.

تزودنا المبرهنة التالية بالشرط اللازم والكافي لحل أنظمة التطابقات الخطية.

مبرهنة (٣,٢٤)

ليكن $m_1, m_2, \dots, m_k \in \mathbb{Z}^+$ وليكن $c_1, c_2, \dots, c_k \in \mathbb{Z}$. عندئذ، يوجد لنظام التطابقات

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned} \qquad (١)$$

حل وحيد قياس $m = [m_1, m_2, \dots, m_k]$ إذا وفقط إذا كان النظام (١) منسجماً.

البرهان

لنفرض أولاً أن x حل للنظام. ولذا فإن $x \equiv c_i \pmod{m_i}$ لكل $1 \le i \le k$. ومنه فإن $m_i \mid (x - c_i)$ لكل $1 \le i \le k$. وبما أن $d_{ij} \mid m_i$ و $d_{ij} \mid m_j$ فإن $d_{ij} \mid (x - c_i)$ و $d_{ij} \mid (x - c_j)$. ومنه فإن $d_{ij} \mid (c_i - c_j)$. وبالتالي فإن النظام منسجم.

ولبرهان العكس، نفرض أن $d_{ij} \mid (c_i - c_j)$ لكل $i \ne j$. ولنفرض أن:

$$\begin{aligned} m_1 &= p_{11}^{a_{11}} \; p_{12}^{a_{12}} \cdots p_{1t_1}^{a_{1t_1}} \\ m_2 &= p_{21}^{a_{21}} \; p_{22}^{a_{22}} \cdots p_{2t_2}^{a_{2t_2}} \\ &\vdots \\ m_k &= p_{k1}^{a_{k1}} \; p_{k2}^{a_{k2}} \cdots p_{kt_k}^{a_{kt_k}} \end{aligned}$$

هو تحليل الأعداد $m_1, m_2, \dots, m_k$ إلى قوى عواملها الأولية. الآن نستخدم مبرهنة الباقي الصينية كي نثبت وجود حل للنظام المنسجم:

$$\begin{aligned} x &\equiv c_1 \pmod{p_{11}^{a_{11}}} \\ x &\equiv c_1 \pmod{p_{12}^{a_{12}}} \\ &\vdots \\ x &\equiv c_1 \pmod{p_{1t_1}^{a_{1t_1}}} \\ &\vdots \end{aligned} \qquad (٢)$$

$$x \equiv c_k \pmod{p_{k1_k}^{a_{k1_k}}}$$
$$x \equiv c_k \pmod{p_{k2_k}^{a_{k2_k}}}$$
$$\vdots$$
$$x \equiv c_k \pmod{p_{kt_k}^{a_{kt_k}}}$$

بما أن الأعداد m_i ليست بالضرورة أولية نسبياً زوجاً زوجاً فمن الممكن وجـــود عددين متساويين p_{ir} و p_{js} . من دون الاخلال بالعمومية نستطيع أن نفـــرض أن $a_{js} \le a_{ir}$. الآن بمـــــا أن $p_{ir}^{a_{ir}} \mid m_i$ وأن $p_{js}^{a_{js}} \mid m_j$ وأن $d_{ij} = (m_i, m_j)$ فإن $p_{js}^{a_{js}} \mid d_{ij}$. وعليـــه يكـــون $p_{js}^{a_{js}} \mid (c_i - c_j)$. أي أن $c_i \equiv c_j \pmod{p_{js}^{a_{js}}}$. وبملاحظـــــة أن $x = c_i \pmod{p_{p_{ir}}^{a_{ir}}}$ وأن $p_{js}^{a_{js}} \mid p_{ir}^{a_{ir}}$ نحـــــصل علـــــى أن $x \equiv c_i \pmod{p_{js}^{a_{js}}}$. ومن ثم فإننا نخلـــص إلى أن $x \equiv c_j \pmod{p_{js}^{a_{js}}}$. إذن، بحذف مثل هذه التطابقات من النظام (٢) نحصل على نظام من التطابقات يكافيء النظام (٢) وقياساته أولية نسبياً زوجاً زوجاً. ومن ثم باستخدام مبرهنـــة البـــاقي الصينية نستطيع إيجاد حل وحيد لهذا النظام (ومن ثم حل وحيد للنظام (١)) قياس العدد m ونكون قد انتهينا ◆

ملحوظة

لاحظ أننا بعد إجراء الخطوات الواردة في برهان المبرهنة (٣,٢٤) نكون قد حسبنا القوى الأولية الـــتي تقـــسم المـــضاعف المـــشترك الأصـــغر للأعـــداد $m_1, m_2, \dots, m_k$ وعليه فمن الناحية الحسابية يكون حل النظام المنـــسجم علـــى النحو التالي:

نقوم بحساب $m = [m_1, m_2, \dots, m_k]$ ثم نحلله إلى قوى عواملـــه الأوليـــة وليكن $m = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$. وبذلك نحصل على نظام مكافئ للنظـــام المعطـــى بحيث تكون قياسات النظام الجديد أولية نسبياً وبالتحديد:

$$x \equiv c_1 (\text{mod } p_1^{k_1})$$
$$x \equiv c_2 (\text{mod } p_2^{k_2})$$
$$\vdots$$
$$x \equiv c_t (\text{mod } p_t^{k_t})$$

وللحصول على الحل نستخدم مبرهنة الباقي الصينية.

مثال (٣,٢٥)

حل نظام التطابقات

$$x \equiv 11 (\text{mod } 36)$$
$$x \equiv 7 \ (\text{mod } \ 40)$$
$$x = 32 (\text{mod } 75)$$

الحل

لاحظ أولاً أن $m_1 = 36, m_2 = 40, m_3 = 75$ وأن:

$d_{12} = (36 \ , \ 40) = 4, d_{13} = (36 \ , \ 75) = 3, d_{23} = (40 \ , \ 75) = 5$. وأن:

$c_1 - c_2 = 4, c_1 - c_3 = -21, c_2 - c_3 = -25$. ولذا فإن $d_{ij} \mid (c_i - c_j)$. وعليه فإن النظام منسجم ويكون له حل وحيد قياس $m = [36, 40, 75] = 1800$.

ولإيجاد هذا الحل، لاحظ أن النظام يكافئ

$$x \equiv 11 (\text{mod } 2^2)$$
$$x \equiv 11 (\text{mod } 3^2)$$
$$x \equiv 7 (\text{mod } 2^3)$$
$$x \equiv 7 (\text{mod } 5)$$
$$x \equiv 32 (\text{mod } 3)$$
$$x \equiv 32 (\text{mod } 5^2)$$

وهذا النظام يكافئ بدوره:

$$x \equiv 7(\text{mod } 2^3) \equiv 7(\text{mod } 8)$$
$$x \equiv 11(\text{mod } 3^2) \equiv 2(\text{mod } 9)$$
$$x \equiv 32(\text{mod } 5^2) \equiv 7(\text{mod } 25)$$

باستخدام مبرهنة الباقي الصينية لحل هـــذا النظـــام نجـــد أن الحـــل الوحيـــد هو $x \equiv 407(\text{mod } 1800)$ □

ملحوظة

لاحظ أنه بالإمكان حل النظام (بعد التأكد من انسجامه) بحل كـــل مـــن التطابقات على حده والتعويض المتتالي في التطابقات على النحو التالي:

باستخدام التطابق الأول نجد أن $x = 11 + 36k_1$ حيث $k_1 \in \mathbb{Z}$. وبـــالتعويض في التطابق الثاني والاختصار نجد أن $k_1 \equiv 1(\text{mod } 40)$. أي أن $k_1 = 1 + 40k_2$ حيث $k_2 \in \mathbb{Z}$. ولذا فإن $x = 11 + 36k_1 = 47 + 1440k_2$. وبـــالتعويض عـــن x في التطابق الثالث والاختصار نجد أن:

$k_2 \equiv -1 \equiv 74(\text{mod } 75)$. أي أن $k_2 = 74 + 75k_3$ حيث $k_3 \in \mathbb{Z}$.

ولذا فإن : $x = 47 + 1440(74 + 75k_3) = 106607 + 108000k_3$.

أي أن: $x \equiv 106607(\text{mod } 108000)$.

وبالتالي فإن: $x \equiv 106007(\text{mod } 1800) \equiv 407(\text{mod } 1800)$. وهذا يتفق مع ما وجدنا في المثال (٣,٢٥) □

(٣,٣,١) تمارين محلولة (*Solved Exercises*)

تمرين (١)

أثبت وجود n من الأعداد الصحيحة المتتالية كل منها يقبل القسمة علـــى مربع كامل.

الحل

لنفرض أن $p_1 < p_2 < \ldots < p_n$ هي أول n من الأعداد الأولية. باستخدام مبرهنة الباقي الصينية يوجد عدد x يحقق النظام:

$$x \equiv -1 (\text{mod } p_1^2)$$
$$x \equiv -2 (\text{mod } p_2^2)$$
$$\vdots$$
$$x \equiv -n (\text{mod } p_n^2)$$

ولذا فإن $p_1^2 \mid (x+1)\ ,\ p_2^2 \mid (x+2)\ ,\ \ldots\ ,\ p_n^2 \mid (x+n)$ △

تمرين (٢)

جد أصغر عدد صحيح موجب n بحيث يكون $\frac{n}{3}$ معكباً، $\frac{n}{5}$ قوة للعدد 5 ، $\frac{n}{7}$ قوة للعدد 7.

الحل

بما أن كل من 3، 5، 7 يقسم n فإننا نستطيع كتابة n على الصورة $n = 3^a\ 5^b\ 7^c$.

بما أن $\frac{n}{3} = 3^{a-1}\ 5^b\ 7^c$ مكعباً فنجد أن:

$$a \equiv 1 (\text{mod } 3)\ ,\ b \equiv c \equiv 0 (\text{mod } 3)$$

وبما أن $\frac{n}{5} = 3^a\ 5^{b-1}\ 7^c$ قوة للعدد 5 فنجد أن:

$$a \equiv c \equiv 0 (\text{mod } 5)\ ,\ b \equiv 1 (\text{mod } 5)$$

وبما أن $\frac{n}{7} = 3^a\ 5^b\ 7^{c-1}$ قوة للعدد 7 فنجد أن:

$$a \equiv b \equiv 0 (\text{mod } 7)\ ,\ c \equiv 1 (\text{mod } 7)$$

الآن باستخدام مبرهنة الباقي الصينية لحل كل نظام من الأنظمة:

$$a \equiv 1 (\text{mod } 3), a \equiv 0 (\text{mod } 5),\ a \equiv 0 (\text{mod } 7)$$

$$b = 0(\text{mod } 3), b \equiv 1(\text{mod } 5), b = 0(\text{mod } 7)$$

$$c \equiv 0(\text{mod } 3), c \equiv 0(\text{mod } 5), c \equiv 1(\text{mod } 7)$$

نجد أن $a = 70$ ، $b = 21$ ، $c = 15$. وبالتالي فإن $n = 3^{70}\,5^{21}\,7^{15}$ △

تمرين (٣)

نقول إن العدد الصحيح $x \neq 1$ ذاتي الـــشكل *(automorph)* إذا كانـــت المراتب n الأولى لكل من العددين x و x^2 متساوية. جد جميع الأعـــداد ذاتيـــة الشكل المكونة من أربع مراتب (يسمح للأصفار على اليسار).

الحل

بما أن مراتب x و x^2 متساوية فإن $x^2 \equiv x(\text{mod } 10^4)$.

ولذا فإن $x^2 \equiv x(\text{mod } 2^4)$ و $x^2 \equiv x(\text{mod } 5^4)$.

ومنه فإن: $x(x-1) \equiv 0(\text{mod } 2^4)$ و $x(x-1) \equiv 0(\text{mod } 5^4)$.

وبما أن $(x, x-1) = 1$ فإننا نحصل على أربع أنظمة تطابقات هي:

$$x \equiv 0(\text{mod } 2^4), x \equiv 0(\text{mod } 5^4).$$

$$x \equiv 0((\text{mod } 2^4), x \equiv 1(\text{mod } 5^4).$$

$$x \equiv 1(\text{mod } 2^4), x \equiv 0(\text{mod } 5^4)$$

$$x \equiv 1(\text{mod } 2^4), x \equiv 1(\text{mod } 5^4)$$

وباستخدام مبرهنة الباقي الصينية لحل كل من هذه الأنظمة نجد أن:

$$x \equiv 0(\text{mod } 10^4)$$

$$x \equiv 1(\text{mod } 10^4)$$

$$x \equiv 625(\text{mod } 10^4)$$

$$x \equiv 9376(\text{mod } 10^4)$$

وبالتالي فإن الأعداد المطلوبة هي 0000 ، 0001 ، 0625 ، 9376 △

تمرين (٤)

حل النظام:

$$x^2 \equiv 1 (\mathrm{mod}\ 3)$$
$$x \equiv 2 (\mathrm{mod}\ 4)$$

الحل

بالتجريب نستطيع أن نجد أن حلول التطابق $x^2 \equiv 1 (\mathrm{mod}\ 3)$ وهي $x \equiv 1 (\mathrm{mod}\ 3)$ و $x \equiv 2 (\mathrm{mod}\ 3)$. وبهذا يكون لدينا النظامين:

(١)
$$x \equiv 1 (\mathrm{mod}\ 3)$$
$$x \equiv 2 (\mathrm{mod}\ 4)$$

(٢)
$$x \equiv 2 (\mathrm{mod}\ 3)$$
$$x \equiv 2 (\mathrm{mod}\ 4)$$

وباستخدام مبرهنة الباقي الصينية نجد أن حل النظام الأول هو $x \equiv -2 (\mathrm{mod}\ 12)$ وحل النظام الثاني هو $x \equiv 2 (\mathrm{mod}\ 12)$. وبالتالي فللنظام الأصلي حلان هما $x \equiv \pm 2 (\mathrm{mod}\ 12)$ △

تمارين (٣,٣)

في التمارين من (١) إلى (٢٤) حل نظام التطابقات المعطى:

(١) $x \equiv 2 (\mathrm{mod}\ 7)$ ، $x \equiv 3 (\mathrm{mod}\ 5)$ ، $x \equiv 2 (\mathrm{mod}\ 3)$.

(٢) $x \equiv 15 (\mathrm{mod}\ 31)$ ، $x \equiv 14 (\mathrm{mod}\ 29)$ ، $x \equiv 5 (\mathrm{mod}\ 11)$.

(٣) $x \equiv 3 (\mathrm{mod}\ 5)$ ، $x \equiv 2 (\mathrm{mod}\ 4)$ ، $x \equiv 1 (\mathrm{mod}\ 3)$.

(٤) $x \equiv 9 (\mathrm{mod}\ 11)$ ، $x \equiv 4 (\mathrm{mod}\ 10)$ ، $x \equiv 2 (\mathrm{mod}\ 4)$.

(٥) $x \equiv 10 (\mathrm{mod}\ 35)$ ، $x \equiv 5 (\mathrm{mod}\ 9)$ ، $x \equiv 3 (\mathrm{mod}\ 4)$.

(٦) $x \equiv 18(\mod 22)$ ، $x \equiv 12(\mod 15)$ ، $x \equiv 5(\mod 7)$.

(٧) $x \equiv 1(\mod 7)$ ، $x \equiv 10(\mod 4)$ ، $x \equiv 7(\mod 9)$.

(٨) $11x \equiv 6(\mod 37)$ ، $3x \equiv 19(\mod 32)$ ، $5x \equiv 11(\mod 17)$.

(٩) $3x \equiv 1(\mod 5)$ ، $2x \equiv 5(\mod 7)$ ، $3x \equiv 6(\mod 12)$.

(١٠) $x \equiv 33(\mod 16)$ ، $x \equiv -4(\mod 35)$ ، $x \equiv 17(\mod 504)$.

(١١) $x \equiv 0(\mod 2)$، $x \equiv 0(\mod 3)$ ، $x \equiv 1(\mod 5)$ ، $x \equiv 6(\mod 7)$.

(١٢) $x \equiv 2(\mod 11)$ ، $x \equiv 3(\mod 12)$ ، $x \equiv 4(\mod 13)$ ،
$x \equiv 5(\mod 17)$ ، $x \equiv 6(\mod 19)$.

(١٣) $2x \equiv 1(\mod 5)$، $3x \equiv 9(\mod 6)$، $4x \equiv 1(\mod 7)$، $5x \equiv 9(\mod 11)$.

(١٤) $x \equiv 13(\mod 15)$ ، $x \equiv 18(\mod 35)$ ، $x \equiv 4(\mod 21)$.

(١٥) $x \equiv 14(\mod 15)$ ، $x \equiv 5(\mod 9)$ ، $x \equiv 8(\mod 12)$.

(١٦) $x \equiv 8(\mod 15)$ ، $x \equiv 3(\mod 10)$ ، $x \equiv 5(\mod 6)$.

(١٧) $x \equiv 10(\mod 30)$ ، $x \equiv 16(\mod 21)$ ، $x \equiv 2(\mod 14)$.

(١٨) $x \equiv 10(\mod 25)$ ، $x \equiv 8(\mod 15)$ ، $x \equiv 2(\mod 9)$.

(١٩) $x \equiv 2(\mod 6)$، $x \equiv 4(\mod 8)$، $x \equiv 2(\mod 14)$، $x \equiv 14(\mod 15)$.

(٢٠) $x \equiv 7(\mod 9)$، $x \equiv 2(\mod 10)$، $x \equiv 3(\mod 12)$، $x \equiv 6(\mod 15)$.

(٢١) $x \equiv 4(\mod 6)$، $x \equiv 13(\mod 15)$، $x \equiv 8(\mod 14)$، $x \equiv 1(\mod 7)$.

(٢٢) $x \equiv 1(\mod 6)$ ، $x \equiv 5(\mod 14)$ ، $x \equiv 4(\mod 21)$.

(٢٣) $x \equiv 13(\mod 40)$ ، $x \equiv 5(\mod 44)$ ، $x \equiv 38(\mod 275)$.

(٢٤) $x \equiv 3(\mod 4)$، $x \equiv 6(\mod 15)$، $x \equiv 7(\mod 36)$، $x \equiv 22(\mod 48)$.

في التمارين من (٢٥) إلى (٢٩) استخدم مبرهنة الباقي الصينية لإيجاد جميع حلول كل من التطابقات المعطاة:

(٢٥) $3^6 x \equiv 1(\mod 8180)$. (٢٦) $13x \equiv 71(\mod 380)$.

(٢٧) $8x \equiv 7(\mod 165)$. (٢٨) $108x \equiv 171(\mod 529)$.

(٢٩) $17x \equiv 9 \pmod{276}$.

(٣٠) جد أصغر عدد صحيح موجب $x > 2$ يحقق:

$2 \mid x$ ، $3 \mid (x+1)$ ، $4 \mid (x+2)$ ، $5 \mid (x+3)$ ، $6 \mid (x+4)$.

(٣١) جد أصغر عدد صحيح موجب x يحقق:

$2^4 \mid (x+2)$ ، $3^3 \mid (x+1)$ ، $5^2 \mid x$.

(٣٢) جد أصغر عدد صحيح موجب بحيث تكون بواقي قسمته على كل من 2، 3 ، 6 ، 12 هي 1، 2 ، 5 ، 5 على التوالي.

(٣٣) جد أصغر عدد صحيح موجب بحيث تكون بواقي قسمته على كل من 3، 4، 5، 6 هي 2 ، 3 ، 4 ، 6 على التوالي.

(٣٤) جد أصغر عدد صحيح موجب بحيث تكون بواقي قسمته على كل من 10، 13 ، 17 هي 3 ، 11 ، 15 على التوالي.

(٣٥) جد جميع الأعداد $3000 < x < 5000$ التي تكون بواقي قسمتها على 7 ، 11 ، 13 هي 1 ، 3 ، 5 على التوالي.

(٣٦) جد جميع الأعداد الصحيحة $0 < x < 140$ التي تحقق النظام:

$x \equiv 1 \pmod{4}$ ، $2x \equiv 3 \pmod{5}$ ، $4x \equiv 5 \pmod{7}$.

(٣٧) أراد ثلاثة مزارعين بيع إنتاجهم المشترك من الأرز بعد جني المحصول فذهب الأول إلى تاجر يستخدم وحدة وزن مقدارها 83 كغم. وذهب الثاني إلى تاجر آخر يستخدم وحدة وزن مقدارها 110 كغم وأما الثالث فذهب إلى تاجر يستخدم وحدة وزن مقدارها 135 كغم. وعندما باع كل منهم أكبر كمية ممكنة مما لديه من الأرز بقي مع الأول 32 كغم وبقي مع الثاني 70 كغم وأما الثالث فبقي معه 30كغم. احسب كمية الانتاج من محصول الأرز بالكليوغرامات.

(٣٨) تحتوي سلة على عدد من البيض وإذا قسم هذا العدد إلى أقسام يحتوي كل منها على 2 ، 3 ، 4 ، 5 ، 6 بيضات بقي في كل مرة 1 ، 2 ، 3 ، 4

، 5 بيضات في السلة على التوالي. أما إذا قسمنا البيض إلى 7 أقسام فإنه لا يبقى أي شيء في السلة. ما هو أصغر عدد من البيض يحقق هذه الشروط؟

(٣٩) إذا وضعنا عدداً من الكرات في صفوف يحتوي كل منها على 15 كرة يبقى لدينا 4 كرات وإذا وضعناها في صفوف يحتوي كل منها على 8 كرات فإنه يبقى لدينا 3 كرات. وأما إذا وضعناها في صفوف يحتوي كل منها على 23 كرة يبقى لدينا 10 كرات. ما هو أصغر عدد للكرات يحقق الشروط؟ وكم عدد الصفوف من كل نوع؟

(٤٠) حل نظام التطابقات: $x^2+2x+2\equiv 0 \pmod 5$ ، $7x\equiv 3 \pmod{11}$.

(٤١) حل نظام التطابقات:

$$x^2\equiv 2 \pmod 7,\ x^2\equiv 3 \pmod{11},\ x^2\equiv 4 \pmod{13}.$$

(٣,٤) أنظمة التطابقات الخطية في أكثر من متغير

Systems of Linear Congruences in More than One Variable

بعد أن قمنا في البند (٣,٣) بدراسة أنظمة التطابقات الخطية في متغير واحد فإننا نقدم أنظمة التطابقات الخطية في أكثر من متغير ونحاول إيجاد حلول هذه الأنظمة. نبدأ أولاً بمعالجة الأنظمة الخطية التي يتساوى عدد متغيراتها مع عدد المعادلات. الصورة العامة لهذه الأنظمة هي:

$$\begin{aligned} a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n &\equiv b_1 \pmod m\\ a_{21}x_1+a_{22}x_2+\ldots+a_{2n}x_n &\equiv b_2 \pmod m\\ &\vdots\\ a_{n1}x_1+a_{n2}x_2+\ldots+a_{nn}x_n &\equiv b_n \pmod m \end{aligned}$$

وكما هو الحال في الجبر الخطي فإن هذه النظام يكافئ التطابق المصفوفي $AX\equiv B \pmod m$ حيث:

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & & \vdots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}\text{ ، }X=\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}\text{ و }B=\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

ولذا يكون من المناسب استخدام لغة المصفوفات حين نعالج أنظمة التطابقات الخطية. جميع المصفوفات في هذا البند هي مصفوفات عناصرها أعداد صحيحة.

تعريف(٣,٧)

لتكن كل من $A=[a_{ij}]$ و $B=[b_{ij}]$ مصفوفة من الدرجة $n\times k$. نقول إن A تطابق B قياس m ونكتب $A\equiv B\pmod m$ إذا كان $a_{ij}\equiv b_{ij}\pmod m$ لكل $1\le i\le n$ و $1\le j\le k$.

مثال (٣,٢٦)

إذا كانت $A=\begin{bmatrix} 18 & 6 \\ -5 & -3 \end{bmatrix}$ فإن $A\equiv\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}\pmod 8$ □

مبرهنة (٣,٢٥)

إذا كانت كل من $A=[a_{ij}]$ و $B=[b_{ij}]$ مصفوفة من الدرجة $n\times k$ حيث $A\equiv B\pmod m$ وكانت $C=[c_{ij}]$ مصفوفة من الدرجة $k\times p$ وكانت $D=[d_{ij}]$ مصفوفة من الدرجة $p\times n$ فإن:

(أ) $AC\equiv BC\pmod m$ (ب) $DA\equiv DB\pmod m$.

البرهان

(أ) لاحظ أن $[AC]_{ij}=\sum_{t=1}^{n}a_{it}c_{tj}$ وأن $[BC]_{ij}=\sum_{t=1}^{n}b_{it}c_{tj}$. بما أن $a_{it}\equiv b_{it}\pmod m$ فإن $a_{it}c_{tj}\equiv b_{it}c_{tj}\pmod m$. ولذا فإن $[AC]_{ij}\equiv[BC]_{ij}\pmod m$. وبالتالي فإن $AC\equiv BC\pmod m$.

(ب) مماثل لبرهان الفقرة (أ) ◆

لحل التطابق المصفوفي $AX \equiv B \pmod m$ فإننا نحتاج إلى مفهوم معكوس المصفوفة قياس m وهذا ما نقدمه في التعريف التالي:

تعريف (٣,٨)

إذا كانت كل من A و B مصفوفة مربعة من الدرجة n فنقول إن المصفوفة B معكوس للمصفوفة A قياس m إذا كان $AB \equiv BA \equiv I_n \pmod m$.

ملحوظة

إذا كان B معكوس للمصفوفة A وكان $C \equiv B \pmod m$ فإن $CA \equiv BA \equiv I_n \pmod m$ وإن $AC \equiv AB \equiv I_n \pmod m$. ولذا فإن C معكوس للمصفوفة A أيضاً.

وبالعكس، إذا كانت كل من B_1 و B_2 معكوساً للمصفوفة A فإن $B_1 \equiv B_2 \pmod m$ وذلك لأن: $B_1A \equiv B_2A \equiv I_n \pmod m$. ولذا فإن $B_1AB_1 \equiv B_2AB_1 \pmod m$. وبما أن $AB_1 \equiv I_n \pmod m$ فإننا نخلص إلى أن $B_1 \equiv B_2 \pmod m$. من الآن فصاعداً سنرمز لمعكوس A (في حالة وجوده) بالرمز A^{-1}.

المبرهنة التالية تقدم لنا الشرط اللازم والكافي لوجود معكوس لمصفوفة مربعة A قياس m. كما تبين لنا طريقة لإيجاد هذا المعكوس.

مبرهنة (٣,٢٦)

لتكن A مصفوفة مربعة من الدرجة n . عندئذ، يوجد معكوس A^{-1} للمصفوفة A قياس m إذا وفقط إذا كان $(\det A, m) = 1$.

البرهان

لنفرض أولاً أن A^{-1} معكوس A قياس m. ولذا فإن $AA^{-1} \equiv I_n \pmod m$. ومنه فإن:

$$\det(AA^{-1}) = \det A \ \det A^{-1} \equiv \det I_n \equiv 1 \pmod m .$$

ولذا فإن $\det A^{-1}$ نظير $\det A$ قياس m . وبالتالي فإن $(\det A, m) = 1$.

لبرهان العكس، نفرض أن $(\det A, m) = 1$. سنبرهن الآن أن $A^{-1} = (\det A)^{-1} adjA$ هو معكوس A قياس m . لاحظ أولاً أن $\det A \neq 0$ لأن $(\det A, m) = 1$. الآن ، نعلم من الجبر الخطي ، (انظر [2]) :

$$(adjA)A = A(adjA) = (\det A) I_n .$$ ولذا فإن:

$$A(\det A)^{-1} adjA = A\, adjA\, (\det A)^{-1} = (\det A)(\det A)^{-1} I_n \equiv I_n \pmod m$$ وأن:

$$(\det A)^{-1}(adjA)A = (\det A)^{-1}(\det A) I_n \equiv I_n \pmod m .$$

وبالتالي فإن: $A^{-1} \equiv (\det A)^{-1} adjA \pmod m$ ◆

في الحالة الخاصة التي تكون فيها A من الدرجة 2 نحصل على النتيجة التالية:

نتيجة (٣,٢٧)

إذا كانت $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ وكان $(\det A, m) = 1$ فإن

$$A^{-1} \equiv (\det A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod m .$$

البرهان

نحصل على المطلوب باستخدام المبرهنة (٣,٢٦) وملاحظة أن

$$adjA = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$ ◆

نستطيع الآن استخدام معكوس المصفوفة لحل نظام المعادلات $AX \equiv B \pmod m$ حيث A مصفوفة مربعة.

نتيجة (٣,٢٨)

إذا كانت A مصفوفة مربعة حيث $(\det A, m) = 1$ فإنه يوجد حل وحيد للنظام $AX \equiv B \pmod m$ هو $X \equiv A^{-1} B \pmod m$.

البرهان

بما أن $AX \equiv B \pmod m$ فإن $A^{-1}(AX) \equiv A^{-1}B \pmod m$. ومنه فإن $X \equiv A^{-1}B \pmod m$ حل للنظام. وإذا كان X_1 و X_2 حلين للنظام فإن $AX_1 \equiv AX_2 \equiv B \pmod m$. ولذا فإن $A^{-1}(AX_1) \equiv A^{-1}(AX_2) \pmod m$.

أي أن $X_1 \equiv X_2 \pmod m$ ◆

مثال (٣,٢٧)

جد حل النظام:

$$11x + 8y \equiv 3 \pmod{26}$$
$$3x + 7y \equiv 4 \pmod{26}$$

الحل

النظام يكافئ التطابق المصفوفي $AX \equiv B \pmod{26}$ حيث:

$A = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$ ، $X = \begin{bmatrix} x \\ y \end{bmatrix}$ و $B = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$. الآن :

$\det A = 11 \times 7 - 8 \times 3 = 53 \equiv 1 \pmod{26}$ ، ولذا فإن

$A^{-1} \equiv \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} \pmod{26}$. ومنه فإن الحل الوحيد للنظام هو:

$$X \equiv A^{-1}B \equiv \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}\begin{bmatrix} 3 \\ 4 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 9 \end{bmatrix} \pmod{26}$$ □

مثال (٣,٢٨)

حل النظام:

$$11x + 2y + 19z \equiv 2 \pmod{26}$$
$$5x + 23y + 25z \equiv 3 \pmod{26}$$
$$20x + 7y + z \equiv 1 \pmod{26}$$

الحل

النظام يكافئ التطابق المصفوفي $AX \equiv B \pmod{26}$ حيث :

$$A = \begin{bmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{bmatrix} \text{ ، } X = \begin{bmatrix} x \\ y \\ z \end{bmatrix} \text{ ، } B = \begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix}.$$

$$\det A = 11(23-175) - 2(5-500) + 19(35-460) \equiv 5 \pmod{26}.$$

كذلك $(\det A)^{-1} = 5^{-1} \equiv 21 \pmod{26}$. الآن بحساب $adjA$ قياس 26 نجد أن:

$$C_{11} \equiv (23+7) \equiv 4 \text{ , } C_{12} \equiv -(5-6) \equiv 1 \text{ , } C_{13} \equiv (35-18) \equiv 17$$

$$C_{21} \equiv -(2+49) \equiv 1 \text{ , } C_{22} \equiv (11-42) \equiv 21 \text{ , } C_{23} \equiv -(77+12) \equiv 15$$

$$C_{32} \equiv (-2-21) \equiv 3 \text{ , } C_{32} \equiv -(-11+35) \equiv 2 \text{ , } C_{33} \equiv (-33-10) \equiv 9$$

ولذا فإن:

$$A^{-1} \equiv 21 \begin{bmatrix} 4 & 1 & 3 \\ 1 & 21 & 2 \\ 17 & 15 & 9 \end{bmatrix} \equiv \begin{bmatrix} 6 & 21 & 11 \\ 21 & 25 & 16 \\ 19 & 3 & 7 \end{bmatrix} \pmod{26}.$$

ويكون الحل الوحيد للنظام هو:

$$\square \quad X \equiv A^{-1}B \equiv \begin{bmatrix} 6 & 21 & 11 \\ 21 & 25 & 16 \\ 19 & 3 & 7 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 3 \\ 2 \end{bmatrix} \pmod{26}$$

إن مسألة معالجة أنظمة التطابقات الخطية بصورة عامة تتم بإستخدام طريقة مشابهة لطريق الحذف لجاوس في حل المعادلات الخطية ونوضحها في المثال التالي:

مثال (٣,٢٩)

جد جميع الحلول غير المتطابقة لكل من النظامين التاليين:

(أ) $3x + 2y \equiv 1 \pmod{36}$

$5x + 10y \equiv 3 \pmod{36}$

(ب) $x + y + z \equiv 1 \pmod{5}$

$2x + 4y + 3z \equiv 1 \pmod{5}$

الحل

(أ) بضرب التطابق الثاني بالعدد 29 (نظير 5 قياس 36) نجد أن النظام يكافئ:

$$3x+2y \equiv 1 \pmod{36}$$
$$x+2y \equiv 15 \pmod{36}$$

بضرب التطابق الثاني بالعدد 3 وطرح التطابق الأول من الناتج نحصل على النظـــام المكافئ:

$$4y \equiv 8 \pmod{36}$$
$$x+2y \equiv 15 \pmod{36}$$

الآن: بما أن $(4,8) = 4$ يقسم 36 فإن للتطابق الأول 4 حلـــول غـــير متطابقـــة قياس 36. وبحل التطابق نجد أن هذه الحلول هي : $y \equiv 2,11,20,29 \pmod{36}$.

نعوض كل من هذه الحلول في التطابق الثاني لنحصل على على:

. $x \equiv 11 \pmod{36}$

. $x \equiv 29 \pmod{36}$

. $x \equiv 11 \pmod{36}$

. $x \equiv 29 \pmod{36}$

وبالتالي فإن حلول النظام هي:

$(11,2)$ ، $(11,20)$ ، $(29,11)$ ، $(29,29)$.

(ب) بضرب التطابق الأول بالعدد 2– والجمع نحصل على النظام المكافئ:

$$x+y+z \equiv 1 \pmod{5}$$
$$2y+z \equiv 4 \pmod{5}$$

الآن، لكل $z \in \{0,1,2,3,4\}$ نحصل على قيمة مقابلة لـــــ y وقيمـــة أخـــرى لـــ x. وبالتالي لدينا خمسة حلول غير متطابقة قياس 5 هي:

$(4,2,0)$ ، $(1,4,1)$ ، $(3,1,2)$ ، $(0,3,3)$ ، $(2,0,4)$ □

تمارين (٣,٤)

جد جميع حلول كل من أنظمة التطابقات التالية:

(١) $3x+2y\equiv 4 \pmod{11}$ ، $x-2y\equiv 2 \pmod{11}$.

(٢) $2x+3y\equiv 1 \pmod{26}$ ، $7x+8y\equiv 2 \pmod{26}$.

(٣) $x+3y\equiv 1 \pmod{26}$ ، $7x+9y\equiv 2 \pmod{26}$.

(٤) $x+3y\equiv 1 \pmod{26}$ ، $7x+9y\equiv 1 \pmod{26}$.

(٥) $x+4y\equiv 1 \pmod{9}$ ، $5x+7y\equiv 1 \pmod{9}$.

(٦) $x+4y\equiv 1 \pmod{9}$ ، $5x+8y\equiv 1 \pmod{9}$.

(٧) $x+4y\equiv 1 \pmod{9}$ ، $5x+8y\equiv 2 \pmod{9}$.

(٨) $17x+11y\equiv 7 \pmod{29}$ ، $13x+10y\equiv 8 \pmod{29}$.

(٩) $9x+20y\equiv 0 \pmod{29}$ ، $16x+13y\equiv 0 \pmod{29}$.

(١٠) $9x+20y\equiv 1 \pmod{29}$ ، $16x+13y\equiv 2 \pmod{29}$.

(١١) $x+y\equiv 1 \pmod{7}$ ، $x+z\equiv 2 \pmod{7}$ ، $y+z\equiv 3 \pmod{7}$.

(١٢) $x+2y+3z\equiv 1 \pmod{7}$ ، $x+2y+5z\equiv 1 \pmod{7}$ ،
$x+4y+6z\equiv 1 \pmod{7}$.

(١٣) $x+y+z\equiv 1 \pmod{7}$ ، $x+y+w\equiv 1 \pmod{7}$ ،
$x+z+w\equiv 1 \pmod{7}$ ، $y+z+w\equiv 1 \pmod{7}$.

(١٤) $2x+3y-z\equiv 0 \pmod{17}$ ، $x-5y+7z\equiv 7 \pmod{17}$ ،
$3x+y+6z\equiv 2 \pmod{17}$.

(١٥) $2x+3y+z\equiv 2 \pmod{15}$ ، $4x-3z\equiv 1 \pmod{15}$ ،
$2x+4y+z\equiv 3 \pmod{15}$.

(١٦) $2x+3y+z\equiv 2 \pmod{15}$ ، $4x-3z\equiv 13 \pmod{15}$ ،
$2x+4y+z\equiv 3 \pmod{15}$.

(٣,٥) بعض التطابقات الخاصة
Special Congruences

سنثبت في هذا البند ثلاث مبرهنات لها بجانب الأهمية الرياضية أهمية تاريخية في نظرية الأعداد. الأولى منها هي مبرهنة ويلسن *(Wilson's theorem)* والثانية هي مبرهنة فيرما الصغرى *(Fermat's little theorem)* وأما الثالثة فهي مبرهنة أويلر *(Euler's theorem)* وهي تعميم لمبرهنة فيرما الصغرى. كما سنقدم بعض التطبيقات على هذه المبرهنات.

هناك العديد من الطرق المتبعة لاستنباط هذه المبرهنات ولقد اخترنا هنا البرهان الذي قدمه دريشليه *(Dirichlet)* في العام ١٨٢٨م ومن فوائده أنه يعطينا برهاناً لكل من مبرهنة ويلسن وفيرما الصغرى، كما يقدم لنا معلومات هامة عن التطابقات التي على الصورة $x^2 \equiv a \pmod{p}$ والتي سنحتاجها لاحقاً في هذا الكتاب. أما بالنسبة إلى مبرهنة أويلر فمن الممكن الحصول على برهان لها بتعديل برهان مبرهنة فيرما الصغرى غير أننا هنا سنعرض برهاناً أفضل قدمه أيفوري *(Ivory)* عام ١٨٠٤م أثناء محاولته إثبات صحة مبرهنة فيرما الصغرى وعدَّله هورنر *(Horner)* في العام ١٨٢٦م ليثبت مبرهنة أويلر.

مبرهنة (٣,٢٩)

ليكن $a \in \mathbb{Z}^+$ وليكن p عدداً أولياً فردياً لا يقسم a. إذا وجد حل b للتطابق $x^2 \equiv a \pmod{p}$ فهناك بالضبط حلان غير متطابقين قياس p.

البرهان

لاحظ أولاً أن $b \not\equiv -b \pmod{p}$ ، لأنه لو كان $b \equiv -b \pmod{p}$ لحصلنا على $2b \equiv 0 \pmod{p}$. وبما أن $(b,p)=1$ ، فنرى أن $2 \equiv 0 \pmod{p}$. أي أن $p \mid 2$ وهذا مستحيل لأن p فردي . لنفرض الآن أن c حل آخر للتطابق. آنئذ

نرى أن $c^2 \equiv b^2 \pmod{p}$. أي أن $p \mid (c-b)(c+b)$. ولذا فإن $p \mid (c-b)$ أو $p \mid (c+b)$. وبهذا يكون $c \equiv b \pmod{p}$ أو أن $c \equiv -b \pmod{p}$ ◆

مبرهنة (٣,٣٠) [دريشليه]

ليكن $1 \le a \le p-1$ حيث p عدد أولي فردي وليكن $x^2 \equiv a \pmod{p}$.

(أ) إذا وجد حل للتطابق فإن $(p-1)! \equiv -a^{\frac{(p-1)}{2}} \pmod{p}$.

(ب) في حالة عدم وجود حل للتطابق يكون $(p-1)! \equiv a^{\frac{(p-1)}{2}} \pmod{p}$.

البرهان

بما أن $(i,p)=1$ لكل $1 \le i \le p-1$ فيوجد حل وحيد $1 \le j \le p-1$ للتطابق الخطي $ix \equiv a \pmod{p}$. على ذلك فلكل $1 \le i \le p-1$ يوجد عدد وحيد $1 \le j \le p-1$ يحقق $ij \equiv a \pmod{p}$. سنقول حينئذ إن العددين i و j متقابلان.

(أ) لنفرض أنه يوجد حل للتطابق $x^2 \equiv a \pmod{p}$. عندئذ، باستخدام المبرهنة (٣,٢٩) يوجد حلان فقط للتطابق هما b و $p-b$ حيث $1 \le b \le p$. ولذا يتبقى لدينا $\frac{p-3}{2}$ زوجاً من الأعداد المتقابلة بين 1 و $p-1$. ونرى أن

$$1 \times 2 \times 3 \times \ldots \times (b-1) \times (b+1) \times \ldots \times (p-b-1) \times (p-b+1) \times \ldots \times (p-2)(p-1)$$
$$\equiv aaa \ldots a \pmod{p} \equiv a^{\frac{p-3}{2}} \pmod{p}$$

حيث a مضروب بنفسه $\frac{p-3}{2}$ مرة. ولكن

$$b(p-b) = bp - b^2 \equiv -b^2 \equiv -a \pmod{p}$$ ، إذن .

$$(p-1)! \equiv -aa^{\frac{p-3}{2}} = -a^{\frac{p-1}{2}} \pmod{p}.$$

(ب) لنفرض أنه لا يوجد حل للتطابق $x^2 \equiv a \pmod{p}$. عندئذ تكـــون جميـــع الأعداد المتقابلة بين 1 و $p-1$ مختلفة. ولذا فإننا نستطيع تكوين $\frac{p-1}{2}$ زوجاً من الأعداد المتقابلة بين1 و $p-1$، ونستنتج أن:

$$1\times 2\times 3\times \ldots \times (p-2)(p-1) \equiv aa \ldots a \pmod{p}$$

حيث a مضروب بنفسه $\frac{p-1}{2}$ مرة. وبهذا نستنتج أن $(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}$ ◆

نتيجة (٣,٣١) [مبرهنة ويلسن]

إذا كان p عدداً أولياً فإن $(p-1)! \equiv -1 \pmod{p}$.

البرهان

بما أن للتطابق $x^2 \equiv 1 \pmod{p}$ حل فإنه باستخدام المبرهنة (٣,٣٠أ) نجـــد أن: $(p-1)! \equiv -(1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ ◆

في واقع الأمر إن عكس مبرهنة ويلسن صحيح أيضاً وبرهانه سهل تزودنـــا به المبرهنة التالية:

مبرهنة (٣,٣٢)

إذا كان $(p-1)! \equiv -1 \pmod{p}$ فإن p عدد أولي.

البرهان

إذا كان p مؤلفاً فإن $p = ab$ حيث $1 < a,b < p$. وعليه فإن $a \mid (p-1)!$.

وبما أن $p \mid (p-1)! + 1$ و $a \mid p$ فإن $a \mid (p-1)! + 1$. ونرى أن $a \mid 1$ وهـــذا مستحيل. إذن، p عدد أولي ◆

ملحوظة

من الواضح أنه باستخدام مبرهنة ويلسن وعكسها نحصل على اختبار جديد لأولية العدد n . ولكن للأسف فهذا الاختبار عديم الفائدة من الناحية العملية خاصة إذا كان n عدداً كبيراً.

النتيجة التالية تعرف بمعيار أويلر *(Euler's Criterion)* ونحصل عليها من مبرهنتي دريشليه وويلسن.

مبرهنة (٣,٣٣) [معيار أويلر]

ليكن p عدداً أولياً حيث $p \nmid a$. عندئذ:

(أ) إذا كان التطابق $x^2 \equiv a \pmod p$ قابلاً للحل فإن $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

(ب) إذا كان التطابق $x^2 \equiv a \pmod p$ غير قابل للحل فإن $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

البرهان

(أ) لنفرض أن $x^2 \equiv a \pmod p$ قابل للحل. عندئذ، باستخدام مبرهنة دريشليه نجد أن $(p-1)! \equiv -a^{\frac{p-1}{2}} \pmod p$. ولكن باستخدام مبرهنة ويلسن لدينا: $(p-1)! \equiv -1 \pmod p$. وبالتالي فإن $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

(ب) مماثل للفقرة (أ) ◆

نحصل الآن على مبرهنة فيرما الصغرى مباشرة من معيار أويلر.

مبرهنة (٣,٣٤) [مبرهنة فيرما الصغرى]

إذا كان p عدداً أولياً وكان $p \nmid a$ فإن $a^{p-1} \equiv 1 \pmod p$.

البرهان

باستخدام معيار أويلر لدينا $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$. وبتربيع طرفي التطابق نحصل على $a^{p-1} \equiv 1 \pmod p$ ◆

في بعض الأحيان يُطرح نص مبرهنة فيرما الصغرى كالتالي:

نتيجة (٣,٣٥)

إذا كان p عدداً أولياً فإن $a^p \equiv a \pmod{p}$ لكل $a \in \mathbb{Z}$.

البرهان

إذا كان $(a,p)=1$ فباستخدام المبرهنة (٣,٣٤) نجد أن $a^{p-1} \equiv 1 \pmod{p}$.

ولذا فإن $a^p \equiv a \pmod{p}$. أما إذا كان $p \mid a$ فإن $a^p \equiv a \equiv 0 \pmod{p}$ ◆

إن عكس مبرهنة فيرما الصغرى ليس صحيحاً بالضرورة حيث من الممكن إيجاد عدد مؤلف n يحقق $a^{n-1} \equiv 1 \pmod{n}$ لكل عدد a أولي نسبياً مع n، والمثال التالي يزودنا بأحد هذه الأعداد .

مثال(٣,٣٠)

أثبت أن $a^{560} \equiv 1 \pmod{561}$ لكل a حيث $(a,561)=1$.

الحل

لاحظ أولاً أن $561 = 3 \times 11 \times 17$. بما أن $(a,561)=1$ فإن $a \nmid 3$ و $a \nmid 11$ و $a \nmid 17$. ولذا باستخدام مبرهنة فيرما الصغرى نجد أن $a^2 \equiv 1 \pmod{3}$، $a^{10} \equiv 1 \pmod{11}$ ، $a^{16} \equiv 1 \pmod{17}$. ونرى أن

$$a^{560} = (a^2)^{280} \equiv 1 \pmod{3}$$
$$a^{560} = (a^{10})^{56} \equiv 1 \pmod{11}$$
$$a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}$$

وبالتالي فإن $a^{560} \equiv 1 \pmod{561}$ □

إن العدد 561 المقدم في المثال (٣,٣٠) واحد من مجموعة أعداد تسمى، أعداد كارمايكل *(Carmichael numbers)* وسنقوم بدراستها بشيء من التفصيل لاحقاً في هذا البند.

نقدم الآن بعض التطبيقات على مبرهنتي فيرما وويلسن.

مبرهنة (٣,٣٦)

إذا كان p عدداً أولياً فردياً فهناك حل للتطابق $x^2 \equiv -1 \pmod{p}$ إذا وفقط إذا كان $p \equiv 1 \pmod{4}$.

البرهان

لنفرض أولاً أن $x^2 \equiv -1 \pmod{p}$ قابل للحل. عندئذ، استناداً إلى مبرهنتي دريشليه وويلسون نرى أن

$$-1 \equiv (p-1)! \equiv -1(-1)^{\frac{p-1}{2}} \pmod{p}$$

ومن ذلك يكون $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ وهذا يؤدي إلى أن $\frac{p-1}{2}$ عدد زوجي وليكن $\frac{p-1}{2} = 2k$. أي أن، $p = 4k+1$ ونستنتج أن $p \equiv 1 \pmod{4}$.

لبرهان العكس، نفرض أن $p \equiv 1 \pmod{4}$. ولنفرض لغرض التناقض أنه لا يوجد حل للتطابق $x^2 \equiv -1 \pmod{p}$. عندئذ، باستخدام المبرهنة (٣,٣٣) نجد أن $(-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$، لذا فإن $\frac{p-1}{2}$ عدد فردي. أي أن $\frac{p-1}{2} = 2k+1$ حيث $k \in \mathbb{Z}$. الأمر الذي يعني أن $p = 4k+3$ وهذا تناقض ◆

لقد سبق وأن أثبتنا (انظر مبرهنة (٢,٩)) وجود عدد غير منته من الأعداد الأولية التي على الصورة $4k+3$. سنبرهن الآن وجود عدد غير منته من الأعداد الأولية التي على الصورة $4k+1$.

مبرهنة (٣,٣٧)

يوجد عدد غير منته من الأعداد الأولية التي على الصورة $4k+1$ حيث $k \in \mathbb{Z}^+$.

البرهان

لنفرض أن p_n هي جميع الأعداد الأولية التي على الصورة $4k+1$ وليكن $M=(2p_1p_2\ldots p_n)^2+1$. بما أن $M>1$ فإنه يوجد عدد أولي p بحيث $p \mid M$. ونرى أن $M=(2p_1p_2\ldots p_n)^2+1\equiv 0 \pmod p$. بهذا يكون $(2p_1p_2\ldots p_n)^2$ حل للتطابق $x^2\equiv -1 \pmod p$. وباستخدام المبرهنة (٣,٣٦) نجد أن $p=4k+1$. أي أن $p=p_i$ حيث $1\le i\le n$. ولذا فإن $p \mid (2p_1p_2\ldots p_n)^2$. وبما أن $p \mid M$ فإن $p \mid 1$ وهذا مستحيل. إذن، عدد الأعداد الأولية التي على الصورة $4k+1$ غير منته ◆

مبرهنة (٣,٣٨)

ليكن $a\in\mathbb{Z}$ وليكن $x,y\in\mathbb{Z}^+$ حيث $d=(x,y)$.

إذا كان $a^x\equiv a^y\equiv 1 \pmod n$ فإن $a^d\equiv 1 \pmod n$.

البرهان

بما أن $d=(x,y)$ فإن $d=sx+ty$ حيث $s,t\in\mathbb{Z}$. ولذا فإن:

◆ $a^d=(a^x)^s(a^y)^t\equiv (1)^s(1)^t\equiv 1 \pmod n$

نقدم الآن بعض الأمثلة الحسابية على مبرهنتي ويلسن وفيرما.

مثال(٣,٣١)

جد أصغر عدد صحيح موجب k يحقق $3^{91}\equiv k \pmod{23}$.

الحل

بما أن $(3,23)=1$ فنجد باستخدام مبرهنة فيرما الصغرى أن $3^{22}\equiv 1 \pmod{23}$. وبهذا نرى أن $3^{91}=(3^{22})^4 3^3\equiv 3^3\equiv 27\equiv 4 \pmod{23}$ □

مثال(٣,٣٢)

حل التطابق $x^{17}+6x^{14}+2x^5+1\equiv 0 \pmod 5$.

الحل

باستخدام مبرهنة فيرما الصغرى نجد أن:

$$\begin{aligned} x^{17}+6x^{14}+2x^5+1 &= (x^5)^3x^2+6(x^5)^2x^4+2x^5+1 \\ &\equiv x^3x^2+x^2x^4+2x+1 \pmod 5 \\ &\equiv x+x^2+2x+1 \pmod 5 \\ &\equiv x^2+3x+1 \pmod 5 \end{aligned}$$

وبهذا يكفي أن نجد حلول التطابق $x^2+3x+1\equiv 0 \pmod 5$. وبتجريب عناصر نظام الرواسب التام $\{0, \pm 1, \pm 2\}$ قياس 5 نجد أن $x=1$ هو الحل الوحيد للتطابق □

مثال (٣,٣٣)

أثبت أن $3^{6n}-2^{6n}\equiv 0 \pmod{35}$ لكل $n\geq 0$.

الحل

باستخدام مبرهنة فيرما الصغرى نجد أن:

$3^{6n}=(3^6)^n\equiv 1 \pmod 7$ وأن $2^{6n}\equiv (2^6)^n\equiv 1 \pmod 7$. ولذا فإن:

$$3^{6n}-2^{6n}\equiv 0 \pmod 7 \qquad (١)$$

كذلك، $2^6\equiv (-3)^6\equiv 3^6 \pmod 5$. ولذا فإن $2^{6n}\equiv 3^{6n} \pmod 5$.

أي أن: $$3^{6n}-2^{6n}\equiv 0 \pmod 5 \qquad (٢)$$

وبالتالي نحصل من (١) و (٢) على أن $3^{6n}-2^{6n}\equiv 0 \pmod{35}$ □

نقدم فيما يلي مبرهنة أويلر وهي تعميم لمبرهنة فيرما الصغرى.

مبرهنة (٣,٣٩) [مبرهنة أويلر]

إذا كان $n \in \mathbb{Z}^+$ وكان $(a,n)=1$ فإن $a^{\varphi(n)} \equiv 1 (\text{mod } n)$ حيث $\varphi(n)$ هي دالة أويلر.

البرهان

لنفرض أن $\{r_1, r_2, ..., r_{\varphi(n)}\}$ نظام رواسب مختزل قياس n. بما أن $(a,n)=1$ فباستخدام المبرهنة (٣,١٧) نجد أن $\{ar_1, ar_2, ..., ar_{\varphi(n)}\}$ نظام رواسب مختزل قياس n. ولذا نجد لكل $1 \le i \le \varphi(n)$ عدد وحيد $1 \le j \le \varphi(n)$ يحقق $r_i \equiv ar_j (\text{mod } n)$. ونرى أن $(ar_1)(ar_2) ... (ar_{\varphi(n)}) \equiv r_1 r_2 ... r_{\varphi(n)} (\text{mod } n)$.

وبملاحظة أن $(r_1 r_2 ... r_{\varphi(n)}, n) = 1$ نخلص إلى أن $a^{\varphi(n)} \equiv 1 (\text{mod } n)$ ◆

ملحوظات

(١) إذا كان p عدداً أولياً فإن $\varphi(p) = p - 1$. ونحصل على مبرهنة فيرما الصغرى كنتيجة مباشرة لمبرهنة أويلر. أو من الممكن إثبات مبرهنة فيرما بالطريقة نفسها التي استخدمت لبرهان مبرهنة أويلر.

(٢) إذا كان $(a,n)=1$ فإن $a^{\varphi(n)} \equiv aa^{\varphi(n)-1} \equiv 1 (\text{mod } n)$. ولذا فإن $a^{\varphi(n)-1}$ هو النظير الضربي للعدد a قياس n. بهذا فالحل الوحيد للتطابق $ax \equiv b (\text{mod } n)$ هو $x \equiv a^{\varphi(n)-1} b (\text{mod } n)$.

(٣) سنقدم في الفصل الخامس صيغة سهلة لحساب $\varphi(n)$ لكل $n \in \mathbb{Z}^+$.

(٤) لاحظ أن عكس مبرهنة أويلر صحيح، فإذا كان $a^{\varphi(n)} \equiv 1 (\text{mod } n)$ فإن $a^{\varphi(n)} + nk = 1$ حيث $k \in \mathbb{Z}$. أي أن $aa^{\varphi(n)-1} + nk = 1$. ونستنتج أن $(a,n)=1$.

(٣,٥,١) رتبة العدد (*Order of an Element*)

إذا كان $(a,n)=1$ فمن مبرهنة أويلر نعلم أن $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$. ولـذا فهناك عدد صحيح k يحقق $a^k \equiv 1 (\mathrm{mod}\ n)$. لعل التعريف التالي ليس مستغرباً:

تعريف (٣,٩)

ليكن $a \in \mathbb{Z}$ و $n \in \mathbb{Z}^+$ حيث $(a,n)=1$. نقول إن رتبة العدد a قياس n (*order of a module n*) هي k ونكتب $k = ord_n(a)$ إذا كان k هو أصغر عدد صحيح موجب يحقق $a^k \equiv 1 (\mathrm{mod}\ n)$.

تزودنا المبرهنة التالية بالخصائص الأساسية لرتبة العدد الصحيح a قياس n.

مبرهنة (٣,٤٠)

ليكن $a \in \mathbb{Z}$ و $n \in \mathbb{Z}^+$ حيث $(a,n)=1$ و $k = ord(a)$.

(أ) إذا كان $a^m \equiv 1 (\mathrm{mod}\ n)$ حيث $m \in \mathbb{Z}^+$ فإن $k \mid m$.

(ب) $k \mid \varphi(n)$.

(ج) $a^r \equiv a^s (\mathrm{mod}\ n)$ إذا وفقط إذا كان $r \equiv s (\mathrm{mod}\ k)$.

(د) جميع الأعداد $a, a^2, a^3, \ldots, a^k$ غير متطابقة قياس n.

(هـ) إذا كان $m \in \mathbb{Z}^+$ فإن $ord_n(a^m) = \dfrac{k}{(k,m)}$.

(و) $ord_n(a^m) = k$ إذا وفقط إذا كان $(k,m)=1$.

البرهان

(أ) لنفرض أن $a^m \equiv 1 (\mathrm{mod}\ n)$. باستخدام خوارزمية القسمة نجد أن $m = qk + r$ ، $0 \le r < k$. ولذا فإن :

$1 \equiv a^m = (a^k)^q a^r \equiv a^r (\mathrm{mod}\ n)$. هذا يناقض تعريف رتبة a إلا إذا كان $r = 0$. وبالتالي فإن $k \mid m$.

(ب) باستخدام مبرهنة أويلر لدينا $a^{\varphi(n)} \equiv 1 (\text{mod } n)$. وباستخدام الفقرة (أ) نجد أن $k \mid \varphi(n)$.

(ج) لنفـــرض أن $a^r \equiv a^s (\text{mod } n)$ وأن $r > s$. بمـــا أن $(a,n) = 1$ فـــإن $a^{r-s} \equiv 1 (\text{mod } n)$. باســـتخدام الفقـــرة (أ) نجـــد أن $k \mid (r-s)$ ، أي أن $r \equiv s (\text{mod } k)$.

لبرهان العكس، نفرض أن $r \equiv s (\text{mod } k)$. فيكون $r \equiv s + kt$ حيث $t \in \mathbb{Z}$. وبهذا نحصل على $a^r = a^s (a^k)^t \equiv a^s (1)^t \equiv a^s (\text{mod } n)$.

(د) لنفرض أن $1 \le r < s \le k$ حيث $a^s \equiv a^r (\text{mod } n)$. عندئـــذ $s \equiv r (\text{mod } k)$ وهذا مستحيل.

(هـــ) لنفرض أن $d = (k,m)$. ولذا فإن $k = ud$ وأن $m = vd$ حيث $u,v \in \mathbb{Z}$ وأن $(u,v) = 1$. سنبرهن أن $ord_n(a^m) = \frac{k}{d}$. لاحظ أولاً $(a^m)^{k/d} = (a^k)^{m/d} = (a^k)^v \equiv (1)^v \equiv 1 (\text{mod } n)$ لأن $ord_n(a) = k$.

لنفرض الآن أن $t \in \mathbb{Z}^+$ حيث $(a^m)^t \equiv 1 (\text{mod } n)$. أي أن $a^{mt} \equiv 1 (\text{mod } n)$. ومن ثم فإن $k \mid mt$. ومنه فـــإن $ud \mid vdt$. أي أن $u \mid vt$. وبمـــا أن $(u,v) = 1$ فإن $u \mid t$. أي أن $\frac{k}{d}$ يقسم t. وبهذا يكون $ord_n(a^m) = \frac{k}{d}$.

(و) نحصل عليها مباشرة من الفقرة (هـــ) ◆

مثال (٣,٣٤)

جد $ord_{14}(a)$ لكل a حيث $(a,14) = 1$.

الحل

لاحظ أن a هو أحد عناصر نظام الرواسب المختزل $\{1, 3, 5, 9, 11, 13\}$.

لنجد أولاً $ord_{14}(5)$. بحساب قوى العدد 5 قياس 14 نجد أن:

$5^1 \equiv 5$ ، $5^2 \equiv 11$ ، $5^3 \equiv 13$ ، $5^4 \equiv 9$ ، $5^5 \equiv 3$ ، $5^6 \equiv 1$. ولـذا فـإن $ord_{14}(5) = 6$. وبصورة مماثلة يمكن حساب رتب باقي العناصر. والجدول التـالي يبين هذه الرتب:

a	1	3	5	9	11	13
$ord_{14}(a)$	1	6	6	3	3	2

□

مبرهنة (٣,٤١)

ليكن $(a,n) = (b,n) = 1$ وليكن $h = ord_n(a)$ و $k = ord_n(b)$. عندئذ:

(أ) إذا كان $(h,k) = 1$ فإن $ord_n(ab) = hk$.

(ب) إذا كان $(h,k) > 1$ فإنه يوجد عدد صحيح c حيث $ord_n(c) = [h,k]$.

البرهان

(أ) بما أن $(ab)^{hk} = a^{hk}b^{hk} = 1 \times 1 \equiv 1 \pmod{n}$ فإن $ord_n(ab) \mid hk$. لنفـرض أن $r = ord_n(ab)$. عندئذ:

$b^{rh} \equiv (1)^{rh} b^{rh} \equiv (a^h)^{rh} b^{rh} = (ab)^{rh} = [(ab)^r]^h \equiv 1 \pmod{n}$. ولـذا فـإن $k \mid rh$. وبما أن $(h,k) = 1$ فإن $k \mid r$. وبالمثل يمكن إثبات أن $h \mid r$. وبهـذا نرى أن $hk \mid r$. وبالتالي فإن $r = ord_n(ab) = hk$.

(ب) لنفـرض أن $(h,k) > 1$ وأن $M = [h,k]$. إذا كـان $h = p_1^{h_1} p_2^{h_2} \ldots p_t^{h_t}$ وكـان $k = p_1^{k_1} p_2^{k_2} \ldots p_t^{k_t}$ فـإن $M = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$ حيـث $\alpha_i = \max\{h_i, k_i\}$ لكل $1 \le i \le t$. لنفرض الآن أن h_1 هـو حاصـل ضـرب الأعداد $p_i^{\alpha_i}$ حيث $h_i \ge k_i$ وأن k_1 هو حاصل ضـرب الأعـداد $p_i^{\alpha_i}$ حيـث $k_i > h_i$. من الواضح أن $h_1 \mid h$ و $k_1 \mid k$ وأن $(h_1, k_1) = 1$ وأن $M = h_1 k_1$. الآن بتوظيف المبرهنة (٣,٤٠) نجد أن $ord_n(a^{h/h_1}) = h_1$ وأن $ord_n(a^{k/k_1}) = k_1$. وإذا كـان $c = a^{n/n_1} b^{k/k_1}$ فباسـتخدام الفقـرة (أ) نتوصـل إلى أن $ord_n(c) = ord_n(a^{h/h_1}) ord_n(b^{k/k_1}) = h_1 k_1 = M$ ◆

(٣,٥,٢) أشباه الأوليات (Pseudoprimes)

لقد بينا في مبرهنة فيرما الصغرى على أنه إذا كان p عدداً أولياً فإن $a^p \equiv a(\text{mod } p)$ لكل $a \in \mathbb{Z}$. لو كان عكس مبرهنة فيرما الصغرى صحيحاً لحصلنا على اختبار سهل لأولية العدد وذلك لسهولة حساب $a^p (\text{mod } p)$ ، ولكن للأسف فإن عكس مبرهنة فيرما الصغرى ليس صحيحاً ، فلقد بينا في المثال (٣,٣٠) وجود أعداد مؤلفة n وأعداد a بحيث يكون $a^n \equiv a(\text{mod } n)$ وهذا يقترح علينا التعريف التالي:

تعريف (٣,١٠)

ليكن $a \in \mathbb{Z}^+$ وليكن $n \in \mathbb{Z}^+$ عدداً مؤلفاً. نقول إن n شبه أولي (*pseudoprime*) للأساس a إذا كان $a^n \equiv a(\text{mod } n)$.

ملحوظة

لاحظ أنه إذا كان $(a,n)=1$ فإن التطابق $a^n \equiv a(\text{mod } n)$ يكافيء التطابق $a^{n-1} \equiv 1(\text{mod } n)$.

مثال (٣,٣٥)

أثبت أن العدد $341 = 11 \times 31$ شبه أولي للأساس 2 ولكنه ليس شبه أولي للأساس 3.

الحل

باستخدام مبرهنة فيرما الصغرى لدينا :

$2^{10} \equiv 1(\text{mod } 11)$ و $2^{30} \equiv 1(\text{mod } 31)$.

عندئذ، $2^{340} = (2^{10})^{34} \equiv 1(\text{mod } 11)$ و

$2^{340} = (2^{30})^{11} 2^{10} \equiv 1 \times (2^5)^2 \equiv 1 \times 1 \equiv 1(\text{mod } 31)$.

وعليه فإن $2^{340} \equiv 1 \pmod{341}$. أي أن $2^{341} \equiv 2 \pmod{341}$. وبهذا يكون 241 شبه أولي للأساس 2. أما بالنسبة للأساس 3 فلاحظ أن:

$341 \equiv 11 \pmod{30}$. ولذا باستخدام التمرين المحلول (٦) من هذا البند نجد أن $3^{341} \equiv 3^{11} \pmod{31}$. لكن

$3^{11} = (3^5)^2 3 \equiv (-5)^2 3 \equiv 13 \not\equiv 3 \pmod{31}$. وبهذا نرى أن $3^{341} \not\equiv 3 \pmod{31}$.

ويكون $3^{341} \not\equiv 3 \pmod{341}$. ونخلص إلى أن 341 ليس شبه أولي للأساس 3 □

مثال (٣,٣٦)

أثبت أن العدد $n = 161038 = 2 \times 73 \times 1103$ شبه أولي للأساس 2.

الحل

من الواضح أن $2^n \equiv 0 \equiv 2 \pmod{2}$. وبما أن $n = 161088 \equiv 46 \pmod{72}$ فنجد باستخدام التمرين المحلول (٦) من هذا البند أن $2^n \equiv 2^{46} \pmod{73}$. لكن:

$2^{46} \equiv (2^6)^7 2^4 \equiv (-9)^7 2^4 \equiv (8)^3 (-9)(16) \equiv -71 \equiv 2 \pmod{73}$.

ولذا فإن $2^n \equiv 2 \pmod{73}$. كذلك، $n = 161038 \equiv 146 \pmod{1102}$ ونرى أن $2^n \equiv 2^{146} \pmod{1103}$. بملاحظة أن

$2^{30} = (2^{10})^3 \equiv (-79)^3 \equiv 2 \pmod{1103}$، نرى أن $2^{29} \equiv 1 \pmod{1103}$. ولذا فإن $2^n \equiv 2^{146} \equiv 2(2^{29})^5 \equiv 2 \pmod{1103}$. وبهذا نستنتج أن $2^n \equiv 2 \pmod{n}$ ومن ثم أن $n = 161038$ شبه أولي للأساس 2 □

سنبرهن الآن أن عدد الأعداد شبه الأولية للأساس 2 غير منته ونلفت الانتباه إلى أن 341 أصغرها وأن العدد 161038 الذي اكتشفه الرياضي لامير (*Lehmer*) عام ١٩٥٠م هو أصغر أشباه الأوليات الزوجية للأساس 2 .

مبرهنة (٣,٤٢)

(أ) إذا كان n عدداً مؤلفاً فإن 2^n-1 عدد مؤلف.

(ب) إذا كان n عدداً شبه أولي للأساس 2 فإن 2^n-1 شبه أولي للأساس 2 .

البرهان

(أ) لاحظ أولاً لكل $x\in\mathbb{Z}$ ولكل $m\in\mathbb{Z}^+$ أن:

$$x^m-1=(x-1)(x^{m-1}+x^{m-2}+\ldots+1)$$

الآن، إذا كان $n=ab$ حيث $1<a,b<n$ فبوضع $x=2^a$ و $m=b$ في المعادلة أعلاه نجد :

$$2^n-1=2^{ab}-1=(2^a-1)(2^{a(b-1)}+2^{a(b-2)}\ldots+1)$$

وبما أن $1<2^a-1<2^n-1$ فإننا نخلص إلى أن العدد 2^n-1 مؤلف.

(ب) لنفرض أن n شبه أولي للأساس 2 . بما أن n مؤلف فإن 2^n-1 مؤلف. سنبرهن الآن أن $2^{2^n-1}\equiv 2(\mathrm{mod}\ 2^n-1)$. بما أن n شبه أولي للأساس 2 فإن $2^n\equiv 2(\mathrm{mod}\ n)$. ومنه فإن $2^n=nk+2$ حيث $k\in\mathbb{Z}$. بوضع $x=2^n$ و $m=k$ في المعادلة المبينة في الفقرة (أ) نجد أن 2^n-1 يقسم $(2^n)^k-1$، أي أن 2^n-1 يقسم $2^{nk}-1$. وبالتالي فإن $2^{nk}\equiv 1(\mathrm{mod}\ 2^n-1)$. $2^{2^n-1}=2^{nk+1}=2\,2^{nk}\equiv 2(\mathrm{mod}\ 2^n-1)$

وبهذا نخلص إلى أن 2^n-1 شبه أولي للأساس 2 ◆

نتيجة (٣,٤٣)

يوجد عدد غير منته من الأعداد شبه الأولية للأساس 2 .

البرهان

بما أن $n_1=341$ شبه أولي للأساس 2 فنجد باستخدام المبرهنة (٣,٤٢) أن $n_2=2^{n_1}-1$ شبه أولي للأساس 2 . وبتطبيق المبرهنة مرة أخرى نجد أن $n_3=2^{n_2}-1$ شبه أولي للأساس 2 . وبالاستمرار نحصل على المتتالية غير المنتهية $n_1,n_2,n_3,\ldots$ من أشباه الأوليات للأساس 2 حيث $n_1=341$ ◆

تستخدم أشباه الأوليات لاختبار أولية العدد الفردي n ويتم ذلك النحو التالي:

(١) نقوم باختيار عدد عشوائي a حيث $1 \le a \le n-1$.

(٢) نقوم بحساب $d=(a,n)$.

(٣) إذا كان $d>1$ فإن n مؤلف.

(٤) إذا كان $d=1$ فإننا نقوم بحساب $a^{n-1} \pmod n$ (باستخدام خوارزمية التربيع والضرب).

(٥) إذا كان $a^{n-1} \not\equiv 1 \pmod n$ فإن n مؤلف.

(٦) إذا كان $a^{n-1} \equiv 1 \pmod n$ فإن n أولي (على الأرجح).

ملحوظات

(١) عند استخدامنا كلمة (عشوائي) فنعني بذلك أن العدد قد تم اختياره باستخدام برنامج يولد لنا متتالية من الأعداد بطريقة يصعب محاكاتها أو تخمينها.

(٢) لاحظ أنه إذا كان $a^{n-1} \not\equiv 1 \pmod n$ فمن المؤكد أن يكون n عدداً مؤلفاً. أما إذا كان $a^{n-1} \equiv 1 \pmod n$ فإن الاستنتاج على أن n عدداً أولياً في الخطوة (٦) ليس مؤكداً. وعلى الرغم من ضعف احتمالية أن يكون العدد الصحيح شبه أولي لأكثر من أساس بدون أن يكون أولياً فهناك في الواقع عدد غير منته من مثل هذه الأعداد، والتي نفرد لها البند الجزئي التالي:

(٣,٥,٣) أعداد كارمايكل (*Carmichael Numbers*)

تعريف (٣,١١)

ليكن n عدداً مؤلفاً. نقول إن n عدد كارمايكل إذا كان $a^{n-1} \equiv 1 \pmod n$ لكل عدد a أولي نسبياً مع n.

لقد بينا في المثال (٣,٣٠) أن العدد561 هو عدد كارمايكل حيث اكتشفه الرياضي كارمايكل في العام ١٩١٠م ومن هنا جاءت التـــسمية. وقـــد تـــساءل كارمايكل فيما إذا كان عدد مثل هذه الأعداد غير منته. فكثير من الحقائق تـــشير إلى أنها نادرة الورود، فمثلاً يوجد سبع من أعداد كارمايكل فقط أصغر من العدد 10^4 هي: $561, 1105, 1729, 2465, 2821, 6601, 8911$.

كما أن عدد أعداد كارمايكل التي تقل عن 10^9 يساوي8421 وأن عـــدد هـــذه الأعداد التي تقل عن 10^{15} يساوي 105212 ، على الرغم من كل هذا فلقد تم في العام ١٩٩٤م من إثبات أن عدد أعداد كارمايكل غير منته.

في المبرهنة التالية نقدم شرطاً كافياً ليكون العدد المؤلف n واحداً من أعداد كارمايكل.

مبرهنة (٣,٤٤)

إذا كان $n = p_1 p_2 \dots p_k$ حيـــث p_i أعـــداد أوليـــة مختلفـــة وكـــان $(p_i - 1) | (n-1)$ لكل i فإن n عدد كارمايكل.

البرهان

لنفرض أن $(a,n) = 1$. عندئذ $(a,p_i) = 1$ لكـــل $1 \le i \le k$. ولـــذا نجـــد باستخدام مبرهنة فيرمـــا الـــصغرى أن $a^{p_i - 1} \equiv 1 (\text{mod } p_i)$ لكـــل i. وبمـــا أن $(p_i - 1) | (n-1)$ فـــإن $n - 1 = (p_i - 1) m_i$ حيـــث $m_i \in \mathbb{Z}$. ومنـــه فـــإن $a^{n-1} = (a^{p_i - 1})^{m_i} \equiv 1 (\text{mod } p_i)$ لكل i. إذن، $a^{n-1} \equiv 1 (\text{mod } n)$ ونخلـــص إلى أن n عدد كارمايكل ◆

ملحوظة

عكس المبرهنة (٣,٤٤) صحيح أيضاً ولكننا نؤجل برهان ذلك إلى الفصل السابع [انظر التمرين (١) من التمارين المحلولة (٧,٣,١)].

مثال (٣,٣٧)

العدد $1729 = 7\times13\times19$ عدد كارمايكل.

الحل

لاحظ أن $1728 = 2^6\times3^3$ يقبل القسمة على كل من 6 ، 12 ، 18. ولذا فباستخدام المبرهنة (٣,٤٤) نجد أن 1729 عدد كارمايكل □

(٣,٥,٤) تمارين محلولة *(Solved Exercises)*

تمرين (١)

إذا كان p عدداً أولياً فأثبت أن:

(أ) $(a+b)^p \equiv a^p + b^p \pmod p$ لكل $a,b \in \mathbb{Z}$.

(ب) استخدم الفقرة (أ) والاستقراء الرياضي لإثبات مبرهنة فيرما الصغرى . أي أن $a^p \equiv a \pmod p$ لكل $a \in \mathbb{Z}^+$.

الحل

(أ) باستخدام مبرهنة ذات الحدين لدينا:

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \ldots + \binom{p}{p-1}ab^{p-1} + b^p$$

ولكن $\binom{p}{k} \equiv 0 \pmod p$ لكل $1 \le k \le p-1$. وبهذا يكون

$$(a+b)^p \equiv a^p + b^p \pmod p.$$

(ب) باستخدام الاستقراء الرياضي على a. من الواضح أن العبارة صحيحة عندما $a = 1$. لنفرض الآن العبارة صحيحة لكل $k \le a$. باستخدام الفقرة (أ) والاستقراء الرياضي نجد أن:

$(a+1)^p \equiv a^p + 1 \equiv a+1 \pmod p$. ولذا فإن العبارة صحيحة عند $a+1$. وبهذا يكون $a^p \equiv a \pmod p$ لكل $a \in \mathbb{Z}^+$ △

تمرين (٢)

إذا كان $n \in \mathbb{Z}$ فأثبت أن $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} \in \mathbb{Z}$.

الحل

بمـــا أن $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} = \frac{3n^5 + 5n^3 + 7n}{15}$ فيكفـــي إثبـــات أن $3n^5 + 5n^3 + 7n \equiv 0 \pmod{15}$. الآن باستخدام مبرهنة فيرما الصغرى لدينا:

$$3n^5 + 5n^3 + 7n \equiv 2n^3 + 7n \equiv 2n - 2n \equiv 0 \pmod 3$$

$$3n^5 + 5n^3 + 7n \equiv 3n + 2n \equiv 5n \equiv 0 \pmod 5$$

وبما أن $(3,5) = 1$ فإن $3n^5 + 5n^3 + 7n \equiv 0 \pmod{15}$ △

تمرين (٣)

إذا كان $n \mid (2^n - 1)$ فأثبت أن $n = 1$.

الحل

لنفرض أن $n \mid (2^n - 1)$ ولنفرض لغرض التناقض أن $n > 1$. ليكن p أصغر قاسم أولي للعدد n. باستخدام مبرهنة فيرما الصغرى نجد أن $2^{p-1} \equiv 1 \pmod p$. وبما أن $p \mid n$ و $n \mid (2^n - 1)$ فإن $p \mid (2^n - 1)$. ولذا فـــإن $2^n \equiv 1 \pmod p$. باستخدام المبرهنة (٣,٣٨) نجـــد أن $2^d \equiv 1 \pmod p$ حيـــث $d = (n, p-1)$. لاحظ أن $d = 1$، لأنه لو كان $d > 1$ فإنه يوجد قاسم للعدد n أكبر من 1 وأصغر من p وهذا يناقض اختيار العدد p. إذن، $d = 1$. وبالتالي فـــإن $2 \equiv 1 \pmod p$ وهذا مستحيل. ونخلص إلى أن $n = 1$ △

تمرين (٤)

جد أصغر عدد صحيح غير سالب k يحقق $18! \equiv k \pmod{437}$.

الحل

لاحظ أن $437 = 19 \times 23$. بإستخدام مبرهنة ويلسن نعلم أن $18! \equiv -1 \pmod{19}$ و $22! \equiv -1 \pmod{23}$.

ولذا فإن: $18! \equiv -1 \pmod{23}$. $22 \times 21 \times 20 \times 19 \times 18! \equiv (-1)(-2)(-3)(-4) \times 18!$

ومنه فإن $18! \equiv -1 \pmod{23}$. وبهذا نرى أن

$18! \equiv -1 \pmod{19 \times 23} \equiv -1 \pmod{437} \equiv 436 \pmod{437}$ △

تمرين (٥)

إذا كان كل من p و $p+2$ عدداً أولياً فأثبت أن

$4[(p-1)! + 1] + p \equiv 0 \pmod{p(p+2)}$.

الحل

باستخدام مبرهنة ويلسن لدينا $(p-1)! + 1 \equiv 0 \pmod{p}$. عندئذ ،

$4[(p-1)! + 1] + p \equiv 0 \pmod{p}$. كذلك ، باستخدام مبرهنة ويلسن مرة أخرى نجد $(p+1)! + 1 \equiv 0 \pmod{p+2}$. فنتوصل بملاحظة أن $p + 1 \equiv -1 \pmod{p+2}$ وأن $p \equiv -2 \pmod{p+2}$ إلى أن:

$$\begin{aligned} 4[(p-1)! + 1] + p &= 4(p-1)! + 4 + p \\ &\equiv 2(-1)(-2)(p-1)! + 2 + p + 2 \\ &\equiv 2(p+1)(p)(p-1)! + 2 + p + 2 \\ &\equiv 2(p+1)! + 2 + p + 2 \\ &\equiv 2(-1) + 2 + 0 \\ &\equiv 0 \pmod{p+2} \end{aligned}$$

إذن ، $4[(p-1)! + 1] + p \equiv 0 \pmod{p(p+2)}$ △

تمرين (٦)

(أ) إذا كان p عدداً أولياً حيث $p \nmid a$ وكان $n \equiv m \pmod{p-1}$ فأثبت أن $a^n \equiv a^m \pmod{p}$.

(ب) استخدم الفقرة (أ) لإيجاد أصغر عدد صحيح k يحقق $(55)^{142} \equiv k \pmod{143}$.

الحل

(أ) لنفرض أن $n > m$. بما أن $(p-1) \mid (n-m)$ فإن $n = m + k(p-1)$ حيث $k \in \mathbb{Z}$. وباستخدام مبرهنة فيرما الصغرى لدينا $a^{p-1} \equiv 1 \pmod{p}$. حينئذ:

$$a^n = a^{m+k(p-1)} = a^m a^{k(p-1)} = a^m \left(a^{p-1}\right)^k \equiv a^m \pmod{p}.$$

(ب) لاحظ أن $143 = 11 \times 13$. وبما أن $55 \equiv 0 \pmod{11}$ فإن $55^{142} \equiv 0 \pmod{11}$. الآن $142 \equiv 10 \pmod{12}$، ولذا بإستخدام الفقرة (أ) نجد أن $(55)^{142} \equiv (55)^{10} \pmod{13}$. لكن $55 \equiv 3 \pmod{13}$. وبهذا يكون

$$(55)^{142} \equiv (55)^{10} \equiv 3^{10} \equiv 3 \pmod{13}.$$

الآن ، باستخدام مبرهنة الباقي الصينية لحل التطابقين $(55)^{142} \equiv 0 \pmod{11}$ و $(55)^{142} \equiv 3 \pmod{13}$ نجد أن $(55)^{142} \equiv 55 \pmod{143}$ △

تمرين (٧)

أثبت عدم وجود حلول صحيحة للمعادلة $y^2 = x^3 + 23$.

الحل

بما أن $x \equiv 0,1,2,3 \pmod{4}$ فلدينا الحالات التالية:

(أ) $x \equiv 0 \pmod{4}$ أو $x \equiv 2 \pmod{4}$:

في هذه الحالة $x^3 \equiv 0 \pmod{4}$ ومن ثم فإن $y^2 = x^3 + 23 \equiv 3 \pmod{4}$

وهذا مستحيل لأن مربع أي عدد يطابق 0 أو 1 قياس 4.

(ب) $x \equiv 3 \pmod{4}$: في هذه الحالة لدينا :

$y^2 = x^3 + 23 \equiv 3^3 + 23 \equiv 3 + 3 = 6 \equiv 2 \pmod 4$ وهذا مستحيل أيضاً.

(ج) $x \equiv 1 \pmod 4$: في هذه الحالة لدينا :

$y^2 + 4 = x^3 + 3^3 = (x+3)(x^2 - 3x + 9)$.

لكن $x^2 - 3x + 9 \equiv 1 - 3 + 9 \equiv 7 \equiv -1 \pmod 4$. وبما أن $x^2 - 3x + 9 > 1$ فيوجد $p \mid (x^2 - 3x + 9)$ حيث $p \equiv -1 \pmod 4$ (لأنه لو كان $p \equiv 1 \pmod 4$ لكل $p \mid (x^2 - 3x + 9)$ لكان $x^2 - 3x + 9 \equiv 1 \pmod 4$).

الآن، $y^2 + 4 = (x+3)(x^2 - 3x + 9) \equiv 0 \pmod p$ حيث $p \equiv -1 \pmod 4$.

من هنا نرى أن $y^2 \equiv (-1) \times 2^2 \pmod p$ وبما أن $(2,p) = 1$ فإنه يوجد نظير ضربي 2^{-1} قياس p. إذن، $(2^{-1}y)^2 \equiv -1 \pmod p$. ومنه فإن $2^{-1}y$ حل للتطابق $z^2 \equiv -1 \pmod p$ وهذا مستحيل لأن $p \equiv -1 \pmod 4$. وبهذا نخلص إلى استحالة وجود حلول صحيحة للمعادلة $y^2 = x^3 + 23$ △

تمرين (٨)

أثبت صحة المبرهنة (٢,٢٠) التي تنص على: إذا كان p عدداً أولياً وكان q قاسماً أولياً لعدد ميرسين $M_p = 2^p - 1$ فإن $q = 2kp + 1$ حيث $k \in \mathbb{Z}$.

الحل الأول:

باستخدام مبرهنة فيرما لدينا $2^{q-1} \equiv 1 \pmod q$. وباستخدام الفرض لدينا $2^p \equiv 1 \pmod q$. ولذا بإستخدام المبرهنة (٣,٣٨) نجد أن $2^d \equiv 1 \pmod q$ حيث $d = (p, q-1)$. وبما أن p عدد أولي فإن $d = 1$ أو $d = p$.

إذا كان $d = 1$ فإن $2^1 \equiv 1 \pmod q$. ومنه فإن $q \mid 1$ وهذا مستحيل. ولذا فإن $d = p$. ومنه فإن $p \mid (q-1)$. وبما أن q فردي فإن $q-1$ زوجي. ويكون $2 \mid (q-1)$. إذن، $2p \mid (q-1)$. أي أن $q = 2kp + 1$ حيث $k \in \mathbb{Z}$.

الحل الثاني:

بما أن $2^p \equiv 1 (\mathrm{mod}\, q)$ فإن $ord_q(2) \mid p$. ولـــذا فـــإن $ord_q(2) = p$.
ولكن $ord_q(2) \mid \varphi(q)$. إذن، $p \mid (q-1)$. ومنه فـــإن $q = mp + 1$ وبمـــا أن q فردي فإن m زوجي. وبالتالي فإن $q = 2kp + 1$ حيث $k \in \mathbb{Z}$ △

تمرين (٩) [اختبار لوقا – *Lucas test*]

افرض أن $n \in \mathbb{Z}^+$. إذا وجد $a \in \mathbb{Z}$ حيـــث $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ ولكـــن $a^{\frac{n-1}{p}} \not\equiv 1 (\mathrm{mod}\, n)$ لكل قاسم أولي p للعدد $n-1$ فأثبت أن n عدد أولي.

الحل

بما أن $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ فإن $aa^{n-2} - kn = 1$ حيـــث $k \in \mathbb{Z}$. وعليـــه فإن $(a,n) = 1$. ولذا فإن $ord_n(a) \mid (n-1)$. لنفرض أن $p \mid (n-1)$ حيـــث p عدد أولي. بما أن $a^{\frac{n-1}{p}} \not\equiv 1 (\mathrm{mod}\, n)$ فإن $ord_n(a) \nmid (n-1)/p$ (لو كان الأمـــر غير ذلك لوجدنا أن $a^{ord_n(a)} \equiv 1 (\mathrm{mod}\, n)$).

الآن، بما أن $ord_n(a) \mid (n-1)$ وأن $ord_n(a) \nmid (n-1)/p$ لكل قاســـم أولي p للعدد $n-1$ فـــإن $ord_n(a) = n-1$. وبملاحظـــة أن $ord_n(a) \mid \varphi(n)$، نـــرى أن $\varphi(n) \mid (n-1)$. لكن بما أن $\varphi(n) \le n-1$ فيتوجب أن يكون $\varphi(n) = n-1$. وبالتالي فإن n أولي △

تمارين (٣,٥)

(١) جد أصغر عدد صحيح موجب k يحقق $3^{100} \equiv k (\mathrm{mod}\ 17)$.

(٢) جد باقي قسمة 2^{70} على 37.

(٣) جد أصغر عدد صحيح موجب k يحقق $2^{1000000} \equiv k (\mathrm{mod}\ 7)$.

(٤) جد باقي قسمة 13×12^{45} على 47.

(٥) أثبت أن $5555^{2222}+2222^{5555}\equiv0(\text{mod }7)$.

(٦) أثبت أن $a^{25}\equiv a(\text{mod }30)$ لكل $a\in\mathbb{Z}$.

(٧) إذا كان $(a,m)=1$ وكان $n_1\equiv n_2(\text{mod}\,\varphi(m))$ فأثبت أن $a^{n_1}\equiv a^{n_2}(\text{mod }m)$.

(٨) جد باقي قسمة $2^{1000000}$ على 77.

(٩) أثبت أن $a^{100}\equiv1(\text{mod }125)$ أو $a^{100}\equiv0(\text{mod }125)$ لكل $a\in\mathbb{Z}$.

(١٠) أثبت أن $9^{9^9}\equiv89(\text{mod }100)$.

(١١) إذا كان $a\nmid2$ و $a\nmid5$ فأثبت أن $a^{101}\equiv a(\text{mod }1000)$.

(١٢) إذا كان $(a,72)=1$ فأثبت أن $a^{12}\equiv1(\text{mod }72)$.

(١٣) إذا كان $(a,1729)=1$ فأثبت أن $a^{36}\equiv1(\text{mod }1729)$.

(١٤) أثبت أن $a^{20}\equiv a^4(\text{mod }4080)$ لكل $a\in\mathbb{Z}^+$.

(١٥) جد أصغر عدد صحيح موجب k يحقق $90!\equiv k(\text{mod }97)$.

(١٦) جد باقي قسمة العدد $82!/21!$ على 83.

(١٧) إذا كان n عدداً فردياً لا يقبل القسمة على 3 فأثبت أن $n^2\equiv1(\text{mod }24)$.

(١٨) أثبت أن $n^7\equiv n(\text{mod }42)$ لكل $n\in\mathbb{Z}^+$.

(١٩) إذا كان p و q عددين أوليين مختلفين حيث $a^p\equiv a(\text{mod }q)$ و $a^q\equiv a(\text{mod }p)$ فأثبت أن $a^{pq}\equiv a(\text{mod }pq)$. استنتج أن $2^{341}\equiv2(\text{mod }341)$.

(٢٠) إذا كان $n>4$ عدداً مؤلفاً فأثبت أن $(n-1)!\equiv0(\text{mod }n)$.

(٢١) جد جميع الأعداد الصحيحة $n>1$ التي تحقق التطابق $(n-1)!\equiv0(\text{mod }n(n+1))$.

(٢٢) إذا كان $p\neq q$ عددين أوليين فأثبت أن $p^{q-1}+q^{p-1}\equiv1(\text{mod }pq)$.

(٢٣) إذا كان $(m,n)=1$ فأثبت أن $m^{\varphi(n)}+n^{\varphi(m)}\equiv1(\text{mod}\,mn)$.

(٢٤) إذا كان p عدداً أولياً حيث $a^p+b^p=c^p$ فأثبت أن p يقسم $a+b-c$.

(٢٥) استخدم مبرهنة فيرما الصغرى لحل كل من التطابقين:

(أ) $x^{35}+5x^{19}+11x^{3}\equiv 0(\text{mod } 17)$.

(ب) $304x^{303}+204x^{202}-104x^{101}\equiv 0(\text{mod } 101)$.

(٢٦) إذا كان p عدداً أولياً فردياً وكان $(p-1)\mid k$ فأثبت أن:

$1^{k}+2^{k}+\ldots+(p-1)^{k}\equiv -1(\text{mod } p)$.

(٢٧) إذا كان p عدداً أولياً فردياً فأثبت أن $2(p-3)!\equiv -1(\text{mod } p)$.

(٢٨) إذا كانا $p\neq q$ عددين أوليين فرديين حيث $(p-1)\mid(q-1)$ وكان $(a,pq)=1$ فأثبت أن $a^{q-1}\equiv 1(\text{mod } pq)$.

(٢٩) إذا كان p عدداً أولياً فأثبت أن $a^{p}+(p-1)!a\equiv 0(\text{mod } p)$ لكل $a\in\mathbb{Z}^{+}$.

(٣٠) إذا كان p و q عددين أوليين مختلفين وكان $a\in\mathbb{Z}^{+}$ فأثبت أن:

$a^{p+q}-a^{p+1}-a^{q+1}+a^{2}\equiv 0(\text{mod } pq)$.

(٣١) إذا كان p و q عددين أوليين مختلفين وكان $a\in\mathbb{Z}^{+}$ فأثبت أن:

$a^{pq}-a^{p}-a^{q}+a\equiv 0(\text{mod } pq)$.

(٣٢) جد حل كل من التطابقات التالية إن أمكن ذلك:

(أ) $x^{2}\equiv -1(\text{mod } 37)$ (ب) $x^{2}\equiv -1(\text{mod } 103)$

(ج) $x^{2}\equiv -1(\text{mod } 41)$ (د) $x^{2}\equiv -1(\text{mod } 7)$

(٣٣) إذا كان p عدداً أولياً فردياً فأثبت أن

$[1\times 3\times 5\times\ldots\times(p-2)]^{2}\equiv[2\times 4\times 6\times\ldots\times(p-1)]^{2}\equiv(-1)^{\frac{p+1}{2}}(\text{mod } p)$

(٣٤) أثبت وجود عدد غير منته من الأعداد n بحيث يكون:

(أ) $n!-1$ مؤلف (ب) $n!+1$ مؤلف.

(٣٥) إذا كان p عدداً أولياً فأثبت أن $(p-s)!\equiv(-1)^{s}(\text{mod } p)$ لكل $1\leq s\leq p-1$ [إرشاد: استخدم الاستقراء الرياضي على s]

(٣٦) إذا كان p عدداً أولياً فأثبت أن $(p-1)!\equiv p-1(\text{mod } p(p-1))$.

(٣٧) إذا كان p عدداً أولياً وكان $a^p \equiv b^p \pmod p$ فأثبت أن $a^p \equiv b^p \pmod{p^2}$.

(٣٨) إذا كان p عدداً أولياً فردياً وكان $1 \le k \le p-1$ فأثبت أن:

$$\binom{p-1}{k} \equiv (-1)^k \pmod p$$

(٣٩) إذا كان $(a,m) = (a-1,m) = 1$ فأثبت أن:

$$1 + a + a^2 + \ldots + a^{\varphi(m)-1} \equiv 0 \pmod m.$$

(٤٠) إذا كان p عدداً أولياً حيث $p \mid (2^p + 1)$ فأثبت أن $p = 3$.

(٤١) لقد كتب أويلر في العام ١٧٣٢م العبارة التالية: لقد حصلت على بعض النتائج من المبرهنة الرائعة التالية وإنني متأكد من صحتها ولكن للأسف لا أملك برهاناً لها: " إذا كان $n+1$ عدداً أولياً ولا يقسم كل من a و b فإن $n+1$ يقسم $a^n - b^n$". فهل تستطيع أن تساعد أويلر؟

(٤٢) إذا كان p عدداً أولياً حيث $p \equiv 3 \pmod 4$ وكان $a^2 + b^2 \equiv 0 \pmod p$ فأثبت أن $a \equiv b \equiv 0 \pmod p$.

(٤٣) أثبت عدم وجود حلول صحيحة للمعادلة $x^2 + 1 = 23y$.

(٤٤) إذا كان p عدداً أولياً فردياً فأثبت أن $ord_p(a) = 2$ إذا وفقط إذا كان $a \equiv -1 \pmod p$.

(٤٥) إذا كان p عدداً أولياً فردياً حيث $a \not\equiv \pm 1 \pmod p$ وكان $a^r \equiv 1 \pmod p$ حيث $r < p-1$ فهل أن $r \mid (p-1)$؟

(٤٦) إذا كان $ab \equiv 1 \pmod n$ فأثبت أن $ord_n(a) = ord_n(b)$.

(٤٧) أثبت أن $n \mid \varphi(2^n - 1)$.

(٤٨) إذا كان p عدداً أولياً فردياً وكان $ord_p(a) = 2k$ فأثبت أن $a^k \equiv -1 \pmod p$.

(٤٩) إذا كان $ord_n(a) = n - 1$ فأثبت أن n عدد أولي.

(٥٠) (أ) ليكن $(a,n)=1$ وليكن $m \mid (t\varphi(n)+1)$ حيث $t \in \mathbb{Z}$. أثبت أن الحل الوحيد للتطابق $x^m \equiv a \pmod{n}$ هو a^k حيث $k=\dfrac{(t\varphi(n)+1)}{m}$.

(ب) استخدم الفقرة (أ) لايجاد الحل الوحيد لكل من التطابقين $x^{11} \equiv 3 \pmod{68}$ و $x^{13} \equiv 7 \pmod{68}$.

(٥١) إذا كان $d \mid \varphi(n)$ فهل من الضروري أن يوجد a بحيث يكون $ord_n(a)=d$؟

(٥٢) إذا كان $ord_n(a)=4k$ فأثبت أن $ord_n(-a)=4k$.

(٥٣) إذا كان كل من p و q عدداً أولياً فردياً حيث $p \mid (2^q+1)$ فأثبت أن $p=3$ أو أن $p=2kq+1$ حيث $k \in \mathbb{Z}$.

(٥٤) استخدم تمرين (٥٣) لتحليل العدد $2^{13}+1$.

(٥٥) إذا كان p قاسماً أولياً لعدد فيرما F_n فأثبت أن $ord_p(2)=2^{n+1}$.

(٥٦) استخدم التمرين (٥٥) لاثبات أن أي قاسم أولي p لعدد فيرما F_n يجب أن يكون على الصورة $2^{n+1}k+1$ حيث $k \in \mathbb{Z}$.

(٥٧) إذا كان $ord_p(a)=3$ حيث p عدد أولي فأثبت أن $ord_p(a+1)=6$.

(٥٨) إذا كان p قاسماً أولياً فردياً للعدد a^4+1 فأثبت $p=8k+1$.

(٥٩) إذا كان كل من p و q عدداً أولياً حيث $q=2p+1$ فأثبت $q \mid M_p$ أو أن $q \mid (M_p+2)$. استخدم ذلك لإثبات أن M_{23} عدد مؤلف.

(٦٠) هل تستطيع أن استنتاج أن M_{29} عدد مؤلف باستخدام التمرين (٥٩) فقط؟

(٦١) ليكن $a \in \mathbb{Z}$ وليكن $(a,n)=1$ حيث $n \geq 2$. أثبت أن n عدد أولي إذا وفقط إذا كان $(x+a)^n \equiv x^n+a \pmod{n}$ لكل $x \in \mathbb{Z}$.

(٦٢) أثبت أن كل من الأعداد التالية شبه أولي للأساس المبين:

(أ) 45 للأساس 17 (ب) 49 للأساس 18

(ج) 51 للأساس 35 (د) 55 للأساس 21

(هـ) 57 للأساس 20 (و) 65 للأساس 14

(٦٣) لنفرض أن n عدد مؤلف وأن $(a,n)=(b,n)=1$.

(أ) أثبت أن n شبه أولي للأساس a إذا وفقط إذا كان $ord_n(a)|(n-1)$.

(ب) إذا كان n شبه أولي لكل من الأساسين a و b فأثبت أن n شبه أولي لكل من الأساسين ab و ab^{-1}.

(٦٤) ليكن n شبه أولي للأساس b وليكن $(b-1,n)=1$. أثبت أن $N=\frac{b^n-1}{b-1}$ شبه أولي للأساس b وأن $(b-1,N)=1$.

(٦٥) أثبت أن $91=7\times13$ شبه أولي للأساس 3 ثم استنتج وجود عدد غير منته من أشباه الأوليات للأساس 3.

(٦٦) أثبت أن $217=7\times31$ شبه أولي للأساس 5 ثم استنتج وجود عدد غير منته من أشبه الأوليات للأساس 5.

(٦٧) أعط مثالاً على شبه أولي n للأساس b بحيث لا يكون $N=\frac{b^n-1}{b-1}$ شبه أولي للأساس b.

(٦٨) ليكن n عدداً مؤلفاً فردياً حيث $(a,n)=1$ وليكن p قاسماً أولياً للعدد n وليكن $m=\frac{n}{p}$.

(أ) أثبت أن n شبه أولي للأساس a إذا وفقط إذا كان $a^{m-1}\equiv1(\mathrm{mod}\ p)$.

(ب) إذا كان $n=3p$ حيث p عدد أولي أكبر من 3 فأثبت أن n لا يمكن أن يكون شبه أولي لأي من الأساسات 2 ، 5 أو 7.

(ج) إذا كان $n=5p$ حيث p عدداً أولياً أكبر من 5 فأثبت أن n لا يمكن أن يكون شبه أولي لأي من الأساسات 2 ، 3 أو 7.

(د) أثبت أن 91 هو أصغر شبه أولي للأساس 3.

(٦٩) إذا كان p عدداً أولياً فأثبت أن p^2 شبه أولي للأساس a إذا وفقط إذا كان $a^{p-1}\equiv1(\mathrm{mod}\ p^2)$.

(٧٠) إذا كان n عدداً صحيحاً موجباً بحيث يكون كل من الأعداد $6n+1$، $12n+1$ ، $18n+1$ عدداً أولياً فأثبت أن $m=(6n+1)(12n+1)(18n+1)$ عدد كارمايكل.

(٧١) بين أن كل من الأعداد التالية هو عدد كارمايكل:

$1105=5\times13\times17$ ، $1729=7\times13\times19$ ، $2465=5\times17\times29$ ،

$2821=7\times13\times31$ ، $6601=7\times23\times41$ ، $9811=7\times19\times67$.

(٣,٦) تطابقات كثيرات الحدود
Polynomial Congruences

سنقدم في هذا البند طريقة لحل تطابقات كثيرات الحدود، فنتناول على سبيل المثال، مسألة إيجاد جميع الحلول الصحيحة للتطابق $x^4+2x+36\equiv0(\text{mod }875)$. بدءاً نحتاج إلى بعض الحقائق عن كثيرات الحدود التي وسنفترض على الدوام في هذا البند أن جميع معاملات كثيرات الحدود الواردة أعداد صحيحة.

إذا كانت $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$ كثيرة حدود من الدرجة n فنقول إن b حل للمعادلة $f(x)=0$ إذا كان $f(b)=0$. كما نقول إن b حل للتطابق $f(x)\equiv0(\text{mod }m)$ إذا كان $f(b)\equiv0(\text{mod }m)$.

إذا كان $b\equiv c(\text{mod }m)$ وكان $f(b)\equiv0(\text{mod }m)$ فمن الواضح أن $f(c)\equiv0(\text{mod }m)$، وفي هذه الحالة نقول إن b و c حلان متطابقان للتطابق $f(x)\equiv0(\text{mod }m)$. أما إذا كان $b\not\equiv c(\text{mod }m)$ حيث $f(b)\equiv f(c)\equiv0(\text{mod }m)$ فإننا نسمي b و c حلين غير متطابقين للتطابق

$f(x) \equiv 0 (\mathrm{mod}\ m)$. هذا وسنرمز لدرجة كثيرة الحدود f بالرمز $\deg f$. إذا كانت f و g كثيرتي حدود حيث $\deg f = n$ و $\deg g = m$ فمن الممكن إثبات أن : $\deg(f+g) \le \max\{m,n\}$ و $\deg(fg) = m+n$.

وبإستخدام الاستقراء الرياضي على k يمكن التحقق من:

$$x^k - a^k = (x-a)(x^{k-1} + ax^{k-2} + a^2x^{k-3} + \ldots + a^{k-1}x + a^{k-1})$$

لكل $x, a \in \mathbb{Z}$. ونستنتج أن $x-a$ يقسم $x^k - a^k$ إذا كان $x \neq a$.

مبرهنة (٣,٤٥)

إذا كانت $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ كثيرة حدود من الدرجة n وكان $f(a) = 0$ فإن $x-a$ يقسم $f(x)$، أي $f(x) = (x-a)g(x)$ حيث $g(x)$ كثيرة حدود من الدرجة $n-1$.

البرهان

$$f(x) = f(x) - f(a) = a_n(x^n - a^n) + a_{n-1}(x^{n-1} - a^{n-1}) + \ldots + a_1(x-a).$$

وبما أن $x-a$ يقسم كل حد من حدود $f(x)$ فإن $x-a$ يقسم $f(x)$. كذلك، إذا كانت $g_k(x) = \dfrac{x^k - a^k}{x-a}$ وكانت $g(x) = \sum_{k=1}^{n} a_k g_k(x)$ فمن السهل أن نرى أن $f(x) = (x-a)g(x)$ وأن $\deg g = n-1$ ◆

نتيجة (٣,٤٦)

إذا كانت $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ فإن درجة كثيرة الحدود:

$f(x) = (x-a_1)(x-a_2)\ldots(x-a_n)$ تساوي n.

البرهان

نحصل على النتيجة باستخدام الاستقراء الرياضي على n وتطبيق المبرهنة (٣,٤٥) ◆

نتيجة (٣,٤٧)

إذا كانت $f(x)$ كثيرة حدود من الدرجة $n>0$ وكان $f(a)\equiv 0(\text{mod } m)$ فإن $f(x)\equiv(x-a)g(x)(\text{mod } m)$ حيث $\deg g=n-1$.

البرهان

بما أن $f(x)-f(a)\equiv f(x)(\text{mod } m)$ فنجد باستخدام المبرهنة (٣,٤٥) أن

- $f(x)\equiv(x-a)g(x)(\text{mod } m)$ حيث $\deg g=n-1$

تزودنا المبرهنة التالية بعدد الحلول غير المتطابقة قياس العدد الأولي p لكثيرة حدود من الدرجة n.

مبرهنة (٣,٤٨) [لاجرانج]

إذا كان p عدداً أولياً وكانت $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ كثيرة حدود من الدرجة $n>0$ وكان $a_n\not\equiv 0(\text{mod } p)$ فإنه يوجد على الأكثر n من الحلول غير المتطابقة قياس p للتطابق $f(x)\equiv 0(\text{mod } p)$.

البرهان

باستخدام الاستقراء الرياضي على n.

إذا كان $n=1$ فإن $f(x)=a_0+a_1x\equiv 0(\text{mod } p)$. أي $a_1x\equiv -a_0(\text{mod } p)$. وبما أن $(a_1,p)=1$ فهناك حل وحيد للتطابق. وتصح العبارة عند $n=1$.

لنفرض الآن أن العبارة صحيحة لجميع كثيرات الحدود من الدرجة k. ولتكن $f(x)$ كثيرة حدود من الدرجة $k+1$. ولنفرض لغرض التناقض أن $b_1,b_2,\ldots,b_{k+2}$ هي حلول غير متطابقة قياس p للتطابق $f(x)\equiv 0(\text{mod } p)$. الآن باستخدام النتيجة (٣,٤٧) لدينا $f(x)\equiv(x-b_{k+2})g(x)(\text{mod } p)$ حيث $\deg g=k$. ولذا فإن

$0 \equiv f(b_i) \equiv (b_i - b_{k+2})g(b_i) \pmod p$ لكل $1 \le i \le k+2$. الأمر الذي يؤكد أن $p \mid (b_i - b_{k+2})g(b_i)$. لكن، بما أن $b_i \not\equiv b_{k+2} \pmod p$ لكل $i \ne k+2$ فإن $p \mid g(b_i)$ لكل $i \ne k+2$. ومن ثم فإن عدد حلول التطابق $g(x) \equiv 0 \pmod p$ هو $k+1$ مما يناقض فرضية الاستقراء. وبالتالي فإن عدد حلول التطابق $f(x) \equiv 0 \pmod p$ لا يزيد عن $k+1$، وبهذا ينتهي البرهان ◆

ملحوظات

(١) لا يمكن الاستغناء عن الشرط القاضي بأن يكون p عدداً أولياً في مبرهنة لاجرانج، فمثلاً للتطابق $f(x) = 8x - 20 \equiv 0 \pmod{12}$ أربعة حلول غير متطابقة قياس 12 هي 1، 4، 7، 10 وذلك لأن $(8,20) = 4$.

(٢) من الواضح أيضاً أن للتطابق $f(x) \equiv 0 \pmod p$ على الأكثر p من الحلول غير المتطابقة قياس p حيث p عدد أولي مهما كانت درجة كثيرة الحدود f.

ننتقل الآن لدراسة كيفية إيجاد حلول التطابق $f(x) \equiv 0 \pmod m$ حيث $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ وحيث $a_n \not\equiv 0 \pmod m$.

لحل التطابق $f(x) \equiv 0 \pmod m$ لاحظ أولاً أنه إذا كان $r \equiv s \pmod m$ فإن $f(r) \equiv f(s) \pmod m$. ومن ثم فإن r حل للتطابق $f(x) \equiv 0 \pmod m$ إذا وفقط إذا كان s حلاً كذلك.

إذا كان p عدداً أولياً فإننا نجد جميع حلول $f(x) \equiv 0 \pmod p$ بتجريب كل عناصر نظام الرواسب التام $\{0,1,2,\ldots,p-1\}$. هذه الطريقة فعالة إذا كان العدد الأولي p صغير نسبياً. أما لإيجاد عدد حلول التطابق $f(x) \equiv 0 \pmod m$ حيث m مؤلف فمن الممكن كتابة $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$ والاستعانة بمبرهنة الباقي الصينية كما هو موضح في المبرهنة التالية:

مبرهنة (٣,٤٩)

لنفرض أن $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ ولنفرض أن للتطابقات:

$$f(x) \equiv 0 (\text{mod } p_1^{\alpha_1})$$
$$f(x) \equiv 0 (\text{mod } p_2^{\alpha_2})$$
$$\vdots$$
$$f(x) \equiv 0 (\text{mod } p_t^{\alpha_t})$$

k_1، k_2، ... ، k_t من الحلول غير المتطابقة على التوالي. عندئذ يوجد $k_1 k_2 \dots k_t$ من الحلول غير المتطابقة للتطابق $f(x) \equiv 0 (\text{mod } m)$.

البرهان

لنفرض أن r_1 حل للتطابق $f(x) \equiv 0 (\text{mod } p_1^{\alpha_1})$، r_2 حل للتطابق $f(x) \equiv 0 (\text{mod } p^{\alpha_2})$، ... ، r_t حل للتطابق $f(x) \equiv 0 (\text{mod } p_t^{\alpha_t})$.

باستخدام مبرهنة الباقي الصينية نرى أن للنظام:

$$x \equiv r_1 (\text{mod } p_1^{\alpha_1})$$
$$x \equiv r_2 (\text{mod } p_2^{\alpha_2})$$
$$\vdots$$
$$x \equiv r_t (\text{mod } p_t^{\alpha_t})$$

حل وحيد قياس $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$. وهذا الحل يزودنا بحل للتطابق $f(x) \equiv 0 (\text{mod } m)$. لذا فإن عدد الحلول غير المتطابقة قياس m للتطابق $f(x) \equiv 0 (\text{mod } m)$ يساوي $k_1 k_2 \dots k_t$ ◆

من المبرهنة (٣,٤٩) يتضح ان الاستراتيجية التي يجب علينا إتباعها لحل التطابق $f(x) \equiv 0 (\text{mod } m)$ تكون بتحليل $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ ومحاولة إيجاد حلول كل من التطابقات $f(x) \equiv 0 (\text{mod } p_i^{\alpha_i})$ ومن ثم استخدام مبرهنة الباقي الصينية. سنبين الآن كيفية الحصول على حلول التطابق $f(x) \equiv 0 (\text{mod } p_i^{\alpha_i+1})$ بمعرفة حلول التطابق $f(x) \equiv 0 (\text{mod } p_i^{\alpha_i})$. ولكننا نحتاج أولاً إلى مفهوم مشتقة كثيرة الحدود.

تعريف (٣,١٢)

إذا كانت $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_2x^2+a_1x+a_0$ كثيرة حدود فإن مشتقة f يرمز لها بالرمز $f'(x)$ وتعرف على النحو التالي:

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\ldots+2a_2x+a_1$$

مبرهنة (٣,٥٠)

افرض أن $k\in\mathbb{Z}^+$. إذا كان p عدداً أولياً وكانت $f(x)$ كثيرة حدود من الدرجة n فإن $f(x+p^kt)\equiv f(x)+f'(x)p^kt(\text{mod } p^{k+1})$.

البرهان

سنستخدم الاستقراء الرياضي على $\deg f=n$. من الواضح أن العبارة صحيحة عند $n=0$. لنفرض الآن أن العبارة صحيحة عند $n-1$. لاحظ أنه يمكن كتابة $f(x)$ على الصورة $f(x)=a+xg(x)$ حيث $a\in\mathbb{Z}$ و $g(x)$ كثيرة حدود من الدرجة $n-1$. باستخدام فرضية الاستقراء نجد أن: $g(x+p^kt)\equiv g(x)+g'(x)p^kt(\text{mod } p^{k+1})$. وبهذا نرى:

$$\begin{aligned}f(x+p^kt)&=a+(x+p^kt)g(x+p^kt)\\&\equiv a+(x+p^kt)[g(x)+g'(x)p^kt](\text{mod } p^{k+1})\\&\equiv a+xg(x)+(xg'(x)+g(x))p^kt\ (\text{mod } p^{k+1})\\&\equiv f(x)+f'(x)p^kt(\text{mod } p^{k+1})\end{aligned}$$

لأن $f(x)=a+xg(x)$ وأن $f'(x)=g(x)+xg'(x)$. ونخلص إلى أن العبارة صائبة عند n ◆

من الواضح أن أي حل للتطابق $f(x)\equiv 0(\text{mod } p^{k+1})$ هو أيضاً حل للتطابق $f(x)\equiv 0(\text{mod } p^k)$. سنبين الآن كيفية الحصول على حلول $f(x)\equiv 0(\text{mod } p^{k+1})$ بمعرفة حلول $f(x)\equiv 0(\text{mod } p^k)$.

مبرهنة (٣,٥١)

افرض أن $k \in \mathbb{Z}^+$ وأن p عدد أولي ولـيكن s حلاً للتطابق $f(x) \equiv 0 \pmod{p^k}$. عندئذ:

(أ) إذا كان $p \nmid f'(s)$ فهناك حل وحيد s_{k+1} للتطابق $f(x) \equiv 0 \pmod{p^{k+1}}$ يحقق $s_{k+1} \equiv s \pmod{p^k}$. وإضافة إلى ذلك فإن $s_{k+1} = s + p^k t$ حيث t هو الحل الوحيد للتطابق الخطي $f'(s)t \equiv -\frac{f(s)}{p^k} \pmod{p}$.

(ب) إذا كان $p \mid f'(s)$ وكان $p^{k+1} \mid f(s)$ فهناك p من الحلول للتطابق $f(x) \equiv 0 \pmod{p^{k+1}}$ كل منها يطابق s قياس p . وهذه الحلول تكون على الصورة $r_j = s + p^k j$ حيث $0 \le j \le p-1$.

(ج) إذا كان $p \mid f'(s)$ ولكن $p^{k+1} \nmid f(s)$ فلا يوجد أي حل للتطابق $f(x) \equiv 0 \pmod{p^{k+1}}$ يطابق s قياس p^k .

البرهان

لنفرض أن r حل للتطابق $f(x) \equiv 0 \pmod{p^{k+1}}$ حيث $r \equiv s \pmod{p^k}$. عندئذ، $r = s + p^k t$ حيث $t \in \mathbb{Z}$. ولذا فالمطلوب هو إيجاد قيم t بحيث يكون $s + p^k t$ حل للتطابق $f(x) \equiv 0 \pmod{p^{k+1}}$. أي $f(s + p^k t) \equiv 0 \pmod{p^{k+1}}$. ولكن باستخدام المبرهنة (٣,٥١) لدينا:

$$f(s + p^k t) = f(s) + f'(s)p^k t \equiv 0 \pmod{p^{k+1}}$$

وبما أن $f(s) \equiv 0 \pmod{p^k}$ فإن $\frac{f(s)}{p^k}$ عدد صحيح وأن:

$$f'(s)t \equiv -\frac{f(s)}{p^k} \pmod{p} \qquad (١)$$

لذا فالمطلوب إيجاد t الذي يحقق التطابق (١). الآن:

(أ) إذا كان $p \nmid f'(s)$ فإن $(p, f'(s)) = 1$. ولذا يكون للتطابق (١) حل وحيد قياس p.

(ب) إذا كان $p \mid f'(s)$ و $p^{k+1} \mid f(s)$ فإن كل من طرفي التطابق (١) يطابق 0 قياس p. ومن ثم فإن أي $0 \le t \le p-1$ يحقق (١). وبالتالي يكون لدينا p من الحلول كل منها على الصورة $s + p^k j$ ، $0 \le j \le p-1$.

(ج) إذا كان $p \mid f'(s)$ ولكن $p^{k+1} \nmid f(s)$ فإن $f'(s)t \equiv 0 \pmod{p}$. ولكن $\frac{f(s)}{p^k} \not\equiv 0 \pmod{p}$. وبهذا لا توجد قيم t تحقق التطابق (١) ونرى أن التطابق $f(x) \equiv 0 \pmod{p^{k+1}}$ غير قابل للحل ◆

ملحوظة

إذا كان $f(x) \equiv 0 \pmod{p^k}$ فإن $f(x) \equiv 0 \pmod{p}$. ولذا يكون من الواضح أنه إذا لم يوجد حل للتطابق $f(x) \equiv 0 \pmod{p}$ فليس هناك حل للتطابق $f(x) \equiv 0 \pmod{p^k}$ أيضاً.

نتيجة (٣,٥٢)

إذا كان $k \in \mathbb{Z}^+$ وكان p عدداً أولياً وكان s_1 حلاً للتطابق $f(x) \equiv 0 \pmod{p}$ حيث $p \nmid f'(s_1)$ فإنه يوجد حل وحيد s_k للتطابق $f(x) \equiv 0 \pmod{p^k}$ يحقق $s_k \equiv s_1 \pmod{p}$.

البرهان

بما أن $p \nmid f'(s_1)$ فباستخدام المبرهنة (٣,٥١) الفقرة (أ) يوجد حل وحيد s_2 للتطابق $f(x) \equiv 0 \pmod{p^2}$ حيث $s_2 \equiv s_1 \pmod{p}$. وبما أن $f'(s_1) \not\equiv 0 \pmod{p}$ فإن $f'(s_2) \not\equiv 0 \pmod{p}$. ولذا باستخدام المبرهنة (٣,٥١) الفقرة (أ) مرة أخرى نجد حلاً وحيداً s_3 للتطابق $f(x) \equiv 0 \pmod{p^3}$ حيث $s_3 \equiv s_2 \pmod{p^2}$. ولذا فإن $s_3 \equiv s_2 \pmod{p}$. ومنه فإن $s_3 \equiv s_1 \pmod{p}$.

وبالاستمرار على هذا المنوال نخلص إلى وجود حل وحيد s_k للتطابق $f(x)\equiv 0(\mathrm{mod}\ p^k)$ حيث $s_k \equiv s_1(\mathrm{mod}\ p)$ ◆

مما سبق نرى أن خطوات حل التطابق $f(x)\equiv 0(\mathrm{mod}\ p^k)$ تكون على النحو التالي:

(١) نجد جميع حلول التطابق $f(x)\equiv 0(\mathrm{mod}\ p)$.

(٢) لكل حل من الحلول s التي وجدناها في الخطوة (١) إما أن لا يكون هناك حل للتطابق $f(x)\equiv 0(\mathrm{mod}\ p^2)$ أو إن هناك حلاً واحداً أو هناك p من الحلول ولإيجاد هذه الحلول نقوم بحل التطابق الخطي $f'(s)t \equiv -\dfrac{f(s)}{p}(\mathrm{mod}\ p)$.

(٣) لكل حل من الحلول r التي وجدت في الخطوة (٢) يكون للتطابق $f(x)\equiv 0(\mathrm{mod}\ p^3)$ إما 0 أو 1 أو p من الحلول ولإيجاد هذه الحلول نقوم بحل التطابق الخطي $f'(r)t \equiv -\dfrac{f(r)}{p^2}(\mathrm{mod}\ p)$.

(٤) نكرر الخطوات السابقة.

مثال (٣,٣٨)

جد جميع حلول التطابق $f(x)=x^4+2x+36\equiv 0(\mathrm{mod}\ 5^3)$.

الحل

(١) نجد أولاً جميع حلول التطابق $f(x)\equiv 0(\mathrm{mod}\ 5)$. بتجريب عناصر نظام الرواسب التام $\{0,\pm 1,\pm 2\}$ قياس 5 نجد أن الحل الوحيد للتطابق هو $x\equiv -1(\mathrm{mod}\ 5)$.

(٢) ضع $s_1=-1$. $f'(x)=4x^3+2$. عندئذ، $f'(-1)=-2\not\equiv 0(\mathrm{mod}\ 5)$. ولذا باستخدام النتيجة (٣,٥٢) يكون للتطابق $f(x)\equiv 0(\mathrm{mod}\ 5^3)$ حل وحيد s_3 حيث $s_3\equiv -1(\mathrm{mod}\ 5)$.

(٣) لحل التطابق $f(x)\equiv 0(\mathrm{mod}\ 5^3)$ نبحث عن $s_2=-1+5t$ بحيث يكون t حلاً التطابق $f'(-1)t\equiv -\frac{f(-1)}{5}(\mathrm{mod}\ 5)$. أي بحيث $-2t\equiv -\frac{35}{5}\equiv -7(\mathrm{mod}\ 5)$. من الواضح أن الحل الوحيد هو $t=1$. ومن ثم فإن $s_2=-1+5t=4$.

(٤) الآن الحل الوحيد للتطابق $f(x)\equiv 0(\mathrm{mod}\ 5^3)$ هو $s_3=4+25t$ حيث t هو حل التطابق $f'(4)t\equiv -\frac{f(4)}{25}(\mathrm{mod}\ 5)$. ولكن $f'(4)\equiv f'(-1)\equiv -2(\mathrm{mod}\ 5)$ و $f(4)\equiv 50(\mathrm{mod}\ 125)$. إذن، للتطابق $-2t\equiv -2(\mathrm{mod}\ 5)$ حل وحيد هو $t=1$.

وبالتالي فإن $s_3=4+25t=29$ هو الحل الوحيد للتطابق $f(x)\equiv 0(\mathrm{mod}\ 5^3)$ □

مثال (٣,٣٩)

جد جميع حلول التطابق $f(x)=x^4+2x+36\equiv 0(\mathrm{mod}\ 875)$.

الحل

بما أن $875=5^3\times 7$ فإننا نبحث عن حلول كل من $f(x)\equiv 0(\mathrm{mod}\ 5^3)$ و $f(x)\equiv 0(\mathrm{mod}\ 7)$. لقد وجدنا في المثال (٣,٣٨) أن الحل الوحيد للتطابق الأول هو $s=29$. وأما التطابق الثاني فنجد بتجريب عناصر نظام الرواسب التام $\{0, \pm 1, \pm 2, \pm 3\}$ قياس 7 أن له حلان هما $r=-1, 2$.

بتطبيق مبرهنة الباقي الصينية لحل كل من النظامين

$$x\equiv 29(\mathrm{mod}\ 125) \qquad x\equiv 29(\mathrm{mod}\ 125)$$
$$\text{و}$$
$$x\equiv 2(\mathrm{mod}\ 7) \qquad x\equiv -1(\mathrm{mod}\ 7)$$

نخلص إلى أن أن كل من 279 و 779 حل للتطابق $f(x)\equiv 0(\mathrm{mod}\ 875)$ □

مثال (٣,٤٠)

جد جميع حلول التطابق $f(x)=x^3+2x^2+3x-22\equiv 0(\text{mod } 8)$.

الحل

(١) بتجريب عناصر نظام الرواسب التام $\{0,1\}$ قياس 2 نجد أن كل من $x\equiv 0(\text{mod } 2)$ و $x\equiv 1(\text{mod } 2)$ حل للتطابق $f(x)\equiv 0(\text{mod } 2)$.

(٢) لإيجاد حلول التطابق $f(x)\equiv 0(\text{mod } 2^2)$:

(أ) عند $s_1=0$. بما أن $f'(s_1)=f'(0)=3$ وأن $2\nmid 3$ فهناك حل وحيد s_2 للتطابق $f(x)\equiv 0(\text{mod } 4)$ على الصورة $s_2=s_1+2t$ حيث t هو حل التطابق $f'(0)t=-\frac{f(0)}{2}(\text{mod } 2)$. أي أن $3t\equiv 1(\text{mod } 2)$. ومنه فإن $t\equiv 1(\text{mod } 2)$. وبالتالي فإن $s_2=0+2\times 1=2$ هو الحل الوحيد للتطابق $f(x)\equiv 0(\text{mod } 4)$ في هذه الحالة.

(ب)عند $s_1=1$. بما أن $f'(s_1)=f'(1)=10$ وأن $f(s_1)=f(1)=-16$ فإن $2\mid 10$ و $4\mid -16$ ولذا فإنه يوجد حلان للتطابق $f(x)\equiv 0(\text{mod } 4)$ على الصورة $s_2=s_1+2t$ حيث $t=0,1$. أي أن $s_2=1+2\times 0=1$ و $s_2=1+2\times 1=3$ هما حلا التطابق $f(x)\equiv 0(\text{mod } 4)$ في هذه الحالة.

وبالتالي فإن جميع حلول التطابق $f(x)\equiv 0(\text{mod } 4)$ هي 1 ، 2 و 3 .

(٣) لإيجاد حلول التطابق $f(x)\equiv 0(\text{mod } 2^3)$.

(أ) عند $s_2=1$. في هذه الحالة $f(s_2)=f(1)=-16$ و $f'(1)=10$ وأن $2\mid 10$ و $8\mid -16$. ولذا فإنه يوجد حلان للتطابق $f(x)\equiv 0(\text{mod } 8)$ على الصورة $s_3=s_2+4t$ حيث $t=0,1$. ومن ثم فإن حلا التطابق $f(x)\equiv 0(\text{mod } 8)$ في هذه الحالة هما $s_3=1+4\times 0=1$ و $s_3=1+4\times 1=5$.

(ب) عند $s_2 = 2$. في هذه الحالة $f(s_2) = f(2) = 0$ و $f'(s_2) = f'(2) = 23$ وأن $2 \nmid 23$. ولذا فإنه يوجد حل وحيد للتطابق $f(x) \equiv 0 \pmod 8$ على الصورة $s_3 = s_2 + 4t$ حيث t هو حل التطابق $f'(2)t \equiv -\frac{f(2)}{4} \pmod 2$.
أي أن $23t \equiv 0 \pmod 2$. ومنه فإن $t = 0$. ولذا فإن الحل الوحيد للتطابق $f(x) \equiv 0 \pmod 8$ في هذه الحالة هو $s_2 = 2 + 4 \times 0 = 2$.

(ج) عند $s_2 = 3$. في هذه الحالة $f(s_2) = f(3) = -128$ و $f'(s_2) = f'(3) = 42$ وأن $2 \mid 42$ و $8 \mid -128$. ولذا فإنه يوجد حلان للتطابق $f(x) \equiv 0 \pmod 8$ على الصورة $s_3 = s_2 + 4t$ حيث $t = 0,1$. أي أن $s_3 = 3 + 4 \times 0 = 3$ و $s_3 = 3 + 4 \times 1 = 7$ هما حلا التطابق في هذه الحالة.
وبالتالي فإن جميع حلول التطابق $f(x) \equiv 0 \pmod 8$ هي: 1، 2، 3، 5، 7 □

مثال (٣,٤١)

جد جميع حلول التطابق $f(x) = x^3 + 2x^2 + 3x - 22 \equiv 0 \pmod{56}$.

الحل

بما أن $56 = 2^3 \times 7$ فعلينا إيجاد حلول كل من التطابقين $f(x) \equiv 0 \pmod 8$ و $f(x) \equiv 0 \pmod 7$. لقد وجدنا في المثال (٣,٤٠) أن حلول التطابق $f(x) \equiv 0 \pmod 8$ هي: 1، 2، 3، 5، 7. أما بالنسبة للتطابق $f(x) \equiv 0 \pmod 7$ فإننا نجد بتجريب عناصر نظام الرواسب التام $\{0, \pm 1, \pm 2, \pm 3\}$ قياس 7 أن له حلان هما 2- و 2.
ولذا فإن للتطابق $f(x) \equiv 0 \pmod{56}$ عشرة حلول نحصل عليها باستخدام مبرهنة الباقي الصينية لحل كل زوج من التطابقات:

$$x \equiv a(\text{mod } 8)$$
$$x \equiv b(\text{mod } 7)$$

حيث $a = 1, 2, 3, 5, 7$ و $b = -2, 2$. وبالتالي نجد أن جميع الحلول هي:

9 ، 33 ، 2 ، 26 ، 51 ، 19 ، 37 ، 5 ، 23 ، 47 قياس 56 □

(٣,٦,١) تمارين محلولة (Solved Excercises)

تمرين (١)

ليكن $k \in \mathbb{Z}^+$ وليكن p عدداً أولياً فردياً حيث $(a, p) = 1$. إذا كان للتطابق $x^2 \equiv a(\text{mod } p)$ حل فأثبت وجود حلين فقط للتطابق $x^2 \equiv a(\text{mod } p^k)$.

الحل

لنفرض أن s حل للتطابق $x^2 \equiv a(\text{mod } p)$. عندئذ $-s$ هو الحل الآخر ولدينا $s \not\equiv -s(\text{mod } p)$. الآن إذا كانت $f(x) = x^2 - a$ فإن $f'(s) = 2s$ وأن $p \nmid f'(s)$. ولذا بإستخدام النتيجة (٣,٥٢) الفقرة (أ) نرى أن للتطابق $f(x) = 0(\text{mod } p^k)$ حل وحيد s_k حيث $s_k \equiv s(\text{mod } p)$. وبالمثل فإن $-s$ يعطينا حل وحيد آخر △

تمرين (٢)

ليكن a عدداً صحيحاً فردياً.

(أ) أثبت وجود حل واحد فقط للتطابق $x^2 \equiv a(\text{mod } 2)$.

(ب) أثبت أن التطابق $x^2 \equiv a(\text{mod } 4)$ قابل للحل إذا وفقط إذا كان $a \equiv 1(\text{mod } 4)$. وفي هذه الحالة يوجد حلان فقط.

(ج) أثبت أن $x^2 \equiv a(\text{mod } 2^k)$ قابل للحل إذا وفقط إذا كان $a \equiv 1(\text{mod } 8)$ حيث $k \geq 3$.

الحل

(أ) بما أن a فردي فإن $a=2b+1$. ولذا فإن $x^2 \equiv a = 2b+1 \equiv 1 \pmod 2$.
وبالتالي فإن $s=1$ هو الحل الوحيد للتطابق.

(ب) لنفرض أن $x^2 \equiv a \pmod 4$ قابل للحل. بما أن $x^2 \equiv 1 \pmod 4$ أو $x^2 \equiv 0 \pmod 4$ و a فردي فنرى أن أن $a \equiv 1 \pmod 4$.
وبالعكس، إذا كان $a \equiv 1 \pmod 4$ فإن $x^2 \equiv 1 \pmod 4$ ونجد أن $x = \pm 1$ حلان للتطابق.

(ج) لنفرض أن $x^2 \equiv a \pmod{2^k}$ قابل للحل. بما أن a عدد فردي وأن $x^2 \equiv 0,1,4 \pmod 8$ فإن $x^2 \equiv 1 \pmod 8$. ولذا فإن $a \equiv 1 \pmod 8$.
وبالعكس، نفرض أن $a \equiv 1 \pmod 8$. سنستخدم الاستقراء الرياضي على k.
عندما $k=3$ نجد أن $x^2 \equiv 1 \pmod{2^3}$ قابل للحل، في الحقيقة كل من 1، 3 ، 5 ، 7 حل للتطابق.
لنفرض الآن أن s_0 حل للتطابق $x^2 \equiv a \pmod{2^k}$. حينئذ يوجد $b \in \mathbb{Z}$ حيث $s_0^2 = a + b2^k$. وبما أن a فردي فإن s_0 فردي ولذا يوجد حل وحيد t_0 للتطابق $s_0 t \equiv -b \pmod 2$. سنبرهن الآن أن $s_1 = s_0 + t_0 2^{k-1}$ حل للتطابق $x^2 \equiv a \pmod{2^{k+1}}$. الآن :

$$\begin{aligned} s_1^2 = (s_0 + t_0 2^{k-1})^2 &= s_0^2 + s_0 t_0 2^k + t_0^2 2^{2k-2} \\ &= a + b2^k + s_0 t_0 2^k + t_0^2 2^{2k-2} \\ &= a + (b + s_0 t_0)2^k + t_0^2 2^{k-3} 2^{k+1} \end{aligned}$$

وبما أن $2 \mid (b + s_0 t_0)$ فنرى أن $s_1^2 \equiv a \pmod{2^{k+1}}$. وبهذا تكون العبارة صحيحة عند $k+1$ △

تمرين (٣)

إذا كان a عدداً زوجياً حيث $a \not\equiv 0 \pmod{2^k}$ وكان $a = 2^b c$ حيث c فردي و b فردي فأثبت عدم وجود حلول للتطابق $x^2 \equiv a \pmod{2^k}$ لكل k.

الحل

لاحظ أن $b \le k-1$. إذا كان s حلاً للتطابق $x^2 \equiv a \pmod{2^k}$ فإن $2^k \mid (s^2-a)$. ومنه فإن $2^b \mid (s^2-a)$. وبما أن $2^b \mid a$ فإن $2^b \mid s^2$. فنرى أن $s^{b+1} \mid s^2$ (لأن b فردي). وبالتالي فإن $2^{b+1} \mid a$ وهذا تناقض. إذن، $x^2 \equiv a \pmod{2^k}$ غير قابل للحل △

تمرين (٤)

ليكن $a = 2^b c$ حيث c فردي، $b = 2t$ زوجي و $a \not\equiv 0 \pmod{2^k}$.

(أ) إذا كان $b \le k-3$ فإن $x^2 \equiv a \pmod{2^k}$ قابل للحل إذا وفقط إذا كان $c \equiv 1 \pmod 8$.

(ب) إذا كان $b = k-2$ فإن $x^2 \equiv a \pmod{2^k}$ قابل للحل إذا وفقط إذا كان $c \equiv 1 \pmod 4$.

(ج) إذا كان $b = k-1$ فإن $x^2 \equiv a \pmod{2^k}$ قابل للحل.

الحل

الحالة $b = 0$ ليست سوى التمرين(٢).

لنفرض الآن أن $b \neq 0$ وأن s حل للتطابق $x^2 \equiv a \pmod{2^k}$ حيث $0 < s < s^k - 1$. بما أن $2^k \mid (s^2-a)$ وأن $2^b \mid a$ فإن $2^b \mid s^2$. ولذا فإن $2^t \mid s$. بقسمة التطابق $s^2 \equiv a \pmod{2^k}$ على 2^b نحصل على التطابق المكافئ $\left(s/2^t\right)^2 \equiv c \pmod{2^{k-b}}$.

(أ) بما أن $b \le k-3$ فإن $k-b \ge 3$. وبما أن c فردي فنجد باستخدام التمرين (٢) أن للتطابق حل إذا وفقط إذا كان $c \equiv 1 \pmod 8$.

(ب) إذا كان $b=k-2$ فإننا نحصل على التطابق المكافئ $(s/2^t)^2 \equiv c \pmod 4$.
ولذا فإن للتطابق حل إذا وفقط إذا كان $c \equiv 1 \pmod 4$.

(ج) إذا كان $b=k-1$ فنحصل على التطابق المكافئ $(s/2^t)^2 \equiv c \equiv 1 \pmod 2$.
ولذا فإن $\frac{s}{2^t}=1+2j$. أي أن $s=1+2^{t+1}j$ حيث $0 \le j \le 2^t-1$ حلول للتطابق △

تمارين (٦, ٣)

حل كل من تطابقات التمارين من (١) إلى (١٠) :

(١) $2x-3 \equiv 0 \pmod{5^3}$.

(٢) $x^3-x^2+4x+1 \equiv 0 \pmod{5^3}$.

(٣) $x^3+4x^2+19x+1 \equiv 0 \pmod{5^2}$.

(٤) $x^{18}+4x^{14}+3x+10 \equiv 0 \pmod{21}$.

(٥) (أ) $5x^4+x^3-2x^2+1 \equiv 0 \pmod 5$.

(ب) $5x^4+x^3-2x^2+1 \equiv 0 \pmod{25}$.

(ج) $5x^4+x^3-2x^2+1 \equiv 0 \pmod{125}$.

(٦) (أ) $2x^3+4x^2-3x+2 \equiv 0 \pmod 7$.

(ب) $2x^3+4x^2-3x+2 \equiv 0 \pmod{49}$.

(ج) $2x^3+4x^2-3x+2 \equiv 0 \pmod{343}$.

(٧) $4x^4-x^3+3x^2+36 \equiv 0 \pmod{45}$.

(٨) (أ) $13x^7-42x+674 \equiv 0 \pmod{3^3}$.

(ب) $13x^7-42x+674 \equiv 0 \pmod{7^2}$.

(ج) $13x^7-42x+674 \equiv 0 \pmod{1323}$.

(٩) (أ) $x^6-2x^5-35\equiv 0(\text{mod } 5^3)$.

(ب) $x^6-2x^5-35\equiv 0(\text{mod } 7^2)$.

(ج) $x^6-2x^5-35\equiv 0(\text{mod } 6125)$.

(١٠) (أ) $x^2-31x-12\equiv 0(\text{mod } 4)$.

(ب) $x^2-31x-12\equiv 0(\text{mod } 9)$.

(ج) $x^2-31x-12\equiv 0(\text{mod } 36)$.

(١١) إذا كانت f و g كثيرتي حدود من الدرجة n ولهما الجذور نفسها قياس العدد الأولي p فهل من الضروري أن يكون $f(x)\equiv g(x)(\text{mod } p)$ لكل x؟ ماذا لو كان لهما المعامل المتقدم نفسه؟

(١٢) إذا كان لكل من كثيرتي الحدود في التمرين (١١) n من الجذور المختلفة ولهما المعامل المتقدم نفسه فهل يكون $f(x)\equiv g(x)\ (\text{mod } p)$ لكل x؟

(١٣) (أ) إذا كان $m=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$ عدداً فردياً فأثبت أن عدد حلول التطابق $x^2\equiv 1(\text{mod } m)$ يساوي 2^r.

(ب) جد أصغر عدد صحيح فردي m بحيث يكون عدد حلول التطابق $x^2\equiv 1(\text{mod } m)$ يساوي 16.

(ج) جد أصغر عدد صحيح زوجي m بحيث يكون عدد حلول التطابق $x^2\equiv 1(\text{mod } m)$ يساوي 16.

(١٤) ليكن p عدداً أولياً حيث $(a,p)=(n,p)=1$. أثبت وجود حل للتطابق $x^n\equiv a(\text{mod } p^k)$ إذا وفقط إذا وجد حل للتطابق $x^n\equiv a(\text{mod } p)$ لكل $k\in\mathbb{Z}^+$.

(١٥) أثبت أنه لكل عدد أولي p توجد كثيرة حدود درجتها p بحيث يكون التطابق $f(x)\equiv 0(\text{mod } p)$ غير قابل للحل.

(١٦) أثبت وجود حلين للتطابق $x^2+x+a\equiv 0(\text{mod } 2^k)$ إذا كان a زوجياً وعدم وجود حلول إذا كان a فردياً.

(١٧) ما هو العدد العشري المكون من خمس مراتب الذي يساوي الخمس مراتب الأولى من مربعه؟

(١٨) إذا كان p عدداً أولياً فردياً حيث $(a,p)=1$ فأثبت أن $x^2 \equiv a(\text{mod } p^k)$ قابل للحل إذا وفقط إذا كان $x^2 \equiv a(\text{mod } p^{k+1})$ قابلاً للحل لكل $k \in \mathbb{Z}^+$.

(١٩) إذا كان k عدداً زوجياً فأثبت أن عدد حلول التطابق $x^2 \equiv 0(\text{mod } 2^k)$ هو $k/2$ وهذه الحلول هي $2^{k/2}t$ حيث $0 \le t \le 2^{k/2}-1$.

(٢٠) إذا كان a عدداً فردياً و s حلاً للتطابق $x^2 \equiv a(\text{mod } 2^k)$ حيث $k \ge 3$ فأثبت أنه إما أن s أو أن $s+2^{k-1}$ وليس كلاهما حل للتطابق $x^2 \equiv a(\text{mod } 2^{k+1})$.

لكل من التمارين (٢١) إلى (٢٧) جد عدد حلول التطابق المعطى.

(٢١) $10x^4+4x+1 \equiv 0(\text{mod } 27)$.

(٢٢) $7x^2-17x-2 \equiv 0(\text{mod } 128)$.

(٢٣) $7x^5-3x^3+2x-5 \equiv 0(\text{mod } 27\times25\times49)$.

(٢٤) $3x^2+x+1 \equiv 0(\text{mod } 125)$.

(٢٥) $x^2-49 \equiv 0(\text{mod } 53^2\times61^4)$.

(٢٦) $x^2-851 \equiv 0(\text{mod } 5^2\times7^3\times11^4)$.

(٢٧) $x^2+1 \equiv 0(\text{mod } 5^3\times7^2)$.

نبذة عن حياة جاوس
Biography of Gauss

ولد : ١٧٧٧/٤/٣٠ م في ألمانيا.

توفي: ١٨٥٥/٨/٢٣ م في ألمانيا.







ظهرت عبقرية كارل فردريك جاوس مبكرة جداً حيث تكمن وهو في سن الثالثة من تصحيح خطأ في حسابات والده وفاجأ أستاذه وهو في السابعة من عمره بأنه استطاع جمع الأعداد من 1 إلى 100 بأقل من دقيقة وعندما سأل بعد ذلك عن السر وراء هذه السرعة اعترف أنه اكتشف النسق :

$$1+100=101, 2+99=101, \ldots, 50+51=100$$

وبما أنه يوجد 50 زوجاً من هذه الأعداد مجموع كل منها 101 فإن المجموع المطلوب هو $50\times101=5050$.

في سن العاشرة بدأ جاوس دراسة الجبر والتحليل وتمكن من اكتشاف العديد من النظريات وهو لا يزال في سن المراهقة، منها طريقة المربعات الصغرى، إنشاء مضلع منتظم ذو 17 ضلعاً باستخدام المسطرة والفرجار. حصل جاوس على الدكتوراه عام ١٧٩٩م من جامعة هيلمستاد تحت إشراف الرياضي فاف *(Pfaff)* وبرهن في رسالته المبرهنة الأساسية في الجبر، ومن حبه لهذه المبرهنة قدم لها أربع براهين مختلفة في أوقات مختلفة.

في العام ١٨٠١م وهو لا يزال شاباً يافعاً نشر كتابه المميز *(Disquisitiones Arithmetica)* في نظرية الأعداد وضع فيه كل ما كان معلوماً عن نظرية الأعداد بتنسيق ملفت للنظر وأضاف إليه أفكاراً أساسية من اكتشافه أهمها تقديم التطابق قياس n . وكان هذا الكتاب أحد العوامل الرئيسة لشهرته بين زملائه الرياضيين في العالم.

وفي العام ١٨٠١م نفسه لاحظ بعض الفلكيين سُيِّر يدعى سيريز *(Ceres)* ثلاث مرات قبل أن يختفي ولقد استطاع جاوس استخدام البيانات القليلة المتوفرة لحساب مدار سيريز بدقة متناهية بحيث تم اكتشاف السُيِّر في نهاية العام في المكان الذي حدده جاوس، وبهذا فقد اعتبر جاوس أحد العلماء العباقرة القلائل قبل أن يبلغ سن الخامسة والعشرين. في العام ١٨٠٧م عن جاوس أستاذاً في الفلك ومديراً للمركز الفلكي في جامعة جوتنجن. واستمر جاوس في اكتشافاته المميزة في جميع فروع الرياضيات، الفلك، الميكانيكا، الضوء، الجيوديسيا والمغناطيسية.

لقد تسبب أسلوب جاوس في تجاهله لاكتشافات زملاءه العلماء في عداوة الكثير منهم له وقد رفض الاشراف على الكثير من الرياضيين الشباب ومع ذلك انتقى بعض الطلاب المميزين مثل: ايزنستاين، ريمان، كومار، دريشليه، وديدكاند وقام بالإشراف عليهم.

وعلى الرغم من إنشغال جاوس في الكثير من علوم المعرفة إلا أنه أعطى نظرية الأعداد أولوية خاصة لديه وهو القائل بأن الرياضيات ملكة العلوم ونظرية الأعداد تاج على رأس هذه الملكة.

لقد نال جاوس التقدير المناسب لمكانته سواء قبل وفاته أم بعد مماته حيث أصدرت ألمانيا الشرقية في العام ١٩٧٧م طابع بريدي يحمل صورته والمضلع المنتظم الذي أنشأه، كما أصدرت ألمانيا في العام ١٩٨٩م ورقة نقد عليها صورته مع شكل لتوزيع جاوس.

نبذة عن حياة أويلر
Biography of Euler

ولد: ١٥/٤/١٧٠٧م في سويسراً.
توفي: ١٨/٩/١٧٨٣م في روسيا.



ترعرع ليونارد أويلر في بيت والـــده بول أويلر الذي درس علم اللاهوت وأصبح راهباً ولذا فإنه كان يشجع ابنه ليورناد ليسير على الدرب نفسه، حيث أرسله وهو في سن الثالثة عشر إلى جامعة بسل ليتخـــصص في علم اللاهوت والتقى هناك بأحـــد أشـــهر رياضي أوروبا في ذلك الوقت وهو جوهان برنولي والذي كان صديقاً لوالده، و لم يمض وقت طويل حتى أصبح أويلر صديقاً لولدي جوهان، نيقولا ودانيال برنـــولي ولاحظ جوهان قدرة أويلر الفريدة على التفكير في المسائل الرياضـــية وميلـــه لأن يصبح رياضياً، واستطاع جوهان إقناع صديقه بول بأن يسمح لأويلـــر بدراســـة الرياضيات بدلاً من اللاهوت وكان له ذلك، حيث أكمل دراسته في الرياضـــيات في العام ١٧٢٦م ونشر أول بحث له في الرياضيات في العام نفسه.

وفي العام ١٧٢٧م نال بحثه عن أفضل طريقة لترتيب سواري السفن بالجائزة الثانية المقدمة من الأكاديمية العلمية في باريس.

انتقل أويلر في العام ١٧٢٧م إلى روسيا ليعمل في الأكاديمية العلمية لسانت بطرس بيرغ أستاذاً للفيزياء لمدة ثلاث سنوات ثم استطاع الحصول على مقعد استاذ الرياضيات في الأكاديمية في العام ١٧٣٣م . وأثناء ذلك التقى نيقـــولا ودانيـــال برنولي وكذلك جولدباخ. قبل أويلر دعوة فرديك الكبير للذهاب إلى برلين للعمل

في الأكاديمية الملكية في عام ١٧٤١م وبعد أن أمضى ٢٥ عاماً في هذا المركز عاد إلى سانت بطرس بيرغ ومكث هناك حتى وافاه الأجل عام ١٧٨٣م.

يعد أويلر أكثر العلماء انتاجاً في مجال الرياضيات حتى يومنا هـذا، ولقـد اقترن اسمه بجميع فروع الرياضيات. وكانت له اسهامات كثيرة في نظرية الأعداد حيث استطاع أن يبرهن معظم النتائج التي ادعى فيرما صحتها و لم يقدم إثباتاً لها.

لم يتوقف أويلر عن التفكير والإنتاج رغم المصاعب الصحية التي واجهتـه وكان أشدها إصابته بالعمى في عام ١٧٦٦م ، وللتغلب على مشكلة الرؤيا استعان بمساعدين منهم إبنيه جوهان وكريستوف أويلر وزوج حفيدته الرياضي الـشاب وقتئذ فاص *(Fuss)* الذي عين مساعداً لأويلر في الأكاديمية.

الفصل الرابع

معادلات ديوفنتيّة خاصة
SPECIAL DIOPHANTINE EQUATIONAS

(٤,١) ثلاثيات فيثاغورس
Phythagorean Triples

اكتشف البابليون أن المثلث الذي أطوال أضلاعه 119 ، 120 ، 169 هو مثلث قائم الزاوية. والحقيقة أنهم اكتشفوا مثلثات أخرى قائمة الزوايا من بينها المثلثات التي أطوال أضلاعها :

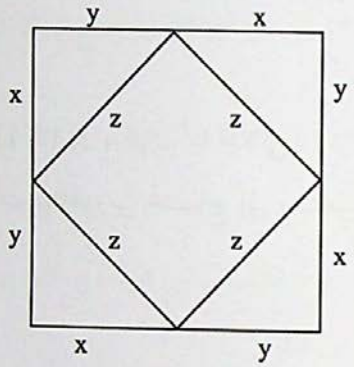
319 ، 360 ، 481
1679 ، 2400 ، 2929
1771 ، 2700 ، 3229
4601 ، 4800 ، 6649
4961 ، 6480 ، 8161

ومن المحتمل أنهم استخدموا هذه المثلثات لإيجاد قيم بعض الدوال المثلثية. ومن هذه الملاحظات استنتجوا علاقة تربط بين أضلاع مثلث قائم، فيه x ، y طولا ضلعي الزاوية القائمة و z طول وتره فوجدوا أن :

$$x^2 + y^2 = z^2$$

ولكن هذه الحقيقة لم تبرهن رياضياً إلى أن جاء الرياضي فيثاغورس *(Phythagoras)* الذي يعتقد أنه عاش في الفترة ما بين العام ٥٧٢ والعام ٥٠٠ قبل الميلاد ، حيث قام بتقديم برهان لهذه الحقيقة التي حملت اسمه بعد ذلك.

تعد مبرهنة فيثاغورس من المبرهنات التي لها العدد الأكبر من البراهين حيث زاد عدد براهينها المختلفة عن أربعمائة برهان. سنقدم هنا أحد البراهين الذي يمكن استنتاجه من الشكل التالي:



من الشكل أعلاه نلاحظ أن مساحة المربع الكبير هي :

$$(x+y)^2 = x^2 + 2xy + y^2$$

ولكن هذه المساحة تساوي مساحة المربع الصغير مضافاً إليها مساحات المثلثات الأربعة. أي أن :

$$x^2 + 2xy + y^2 = z^2 + 4(\frac{1}{2}xy)$$

وبهذا يكون $x^2 + y^2 = z^2$.

من الآن فصاعداً سنسمي المثلث القائم الزاوية الذي أطوال جميع أضلاعه أعداد صحيحة بمثلث فيثاغورس، فمن أجل إيجاد جميع مثلثات فيثاغورس يجب أن نجد جميع الثلاثيات x, y, z من الأعداد الصحيحة الموجبة التي تحقق المعادلة الديوفنتية التالية : $x^2 + y^2 = z^2$.

ونطلق على هذه الثلاثيات اسم ثلاثيات فيثاغورس ، وسنجدها جميعاً في هذا البند.

تعريف (٤,١)

نقول إن ثلاثي فيثاغورس x,y,z هو ثلاثي بدائي (*primitive triple*) إذا كان $(x,y,z)=1$.

مثال (٤,١)

الثلاثيان $3,4,5$ و $5,12,13$ بدائيان أما الثلاثي $6,8,10$ فهو غير بدائي □

لإيجاد جميع ثلاثيات فيثاغورس تحتاج إلى بعض التمهيديات نبدأها بالتمهيدية التالية:

تمهيدية (٤,١)

(أ) إذا كان x,y,z ثلاثي فيثاغورس فيوجد عدد صحيح $d>0$ وثلاثي فيثاغورس بدائي x_1,y_1,z_1 بحيث يكون $x=dx_1, y=dy_1, z=dz_1$.

(ب) إذا كان x_1,y_1,z_1 ثلاثي فيثاغورس بدائي وكان $d>0$ فإن dx_1, dy_1, dz_1 ثلاثي فيثاغورس .

البرهان

(أ) لنفرض أن x,y,z ثلاثي فيثاغورس وأن $(x,y,z)=d$. عندئذ: $x^2+y^2=z^2$ ونستطيع إيجاد أعداد صحيحة x_1,y_1,z_1 بحيث يكون $x=dx_1, y=dy_1, z=dz_1$ و $(x_1,y_1,z_1)=1$. من ذلك نجد أن $d^2x_1^2+d^2y_1^2=d^2z_1^2$. وبما أن $d>0$ فنرى $x_1^2+y_1^2=z_1^2$ وبهذا يكون x_1,y_1,z_1 ثلاثي فيثاغورس بدائي.

(ب) نفرض أن x_1,y_1,z_1 ثلاثي فيثاغورس بدائي. عندئذ:

$x_1^2+y_1^2=z_1^2$. وبالضرب بالعدد d^2 نحصل على $(dx_1)^2+(dy_1)^2=(dz_1)^2$.

إذن، dx_1,dy_1,dz_1 ثلاثي فيثاغورس ◆

من التمهيدية (٤,١) نلاحظ أنه لإيجاد جميع ثلاثيات فيثاغورس يكفي أن نجد جميع ثلاثيات فيثاغورس البدائية.

تمهيدية (٤,٢)

إذا كان x,y,z ثلاثي فيثاغورس بدائي فإن $(x,y)=(x,z)=(y,z)=1$.

البرهان

لنفرض أن $(x,y)>1$. حينئذ، يوجد عدد أولي p بحيث يكون $p\mid x$ و $p\mid y$. ولذا فإن $p\mid(x^2+y^2)$. وبما أن $x^2+y^2=z^2$ فإن $p\mid z^2$. ونرى أن $p\mid z$. وهذا يؤدي إلى أن $(x,y,z)>1$. مما يناقض كون الثلاثي x,y,z بدائياً. وبالطريقة نفسها يمكن إثبات أن $(x,z)=(y,z)=1$ ◆

تمهيدية (٤,٣)

إذا كان x,y,z ثلاثياً بدائياً لفيثاغورس فإما أن يكون x عدداً زوجياً و y عدداً فردياً أو يكون x عدداً فردياً و y عدداً زوجياً.

البرهان

باستخدام تمهيدية (٤,٢) نعلم أن $(x,y)=1$. وعليه فإنه لا يمكن أن يكون x و y زوجيين معاً. وإذا كان كل من x و y فردياً فإن $x^2 \equiv y^2 \equiv 1 \pmod 4$. ونرى $z^2 \equiv x^2+y^2 \equiv 2 \pmod 4$ وهذا مستحيل ◆

المبرهنة التالية تزودنا بوصف كامل لجميع ثلاثيات فيثاغورس البدائية.

مبرهنة (٤,٤)

تكون الأعداد الصحيحة الموجبة x,y,z حيث y زوجي، ثلاثي فيثاغورس بدائي إذا وفقط إذا وجد عددان صحيحان موجبان m و n أوليان نسبياً ويحققان

$$m>n,\ m \not\equiv n \pmod 2$$

$$x=m^2-n^2$$

$$y=2mn$$

$$z=m^2+n^2$$

البرهان

لنفرض أن x,y,z ثلاثي فيثاغورس بدائي حيث y عدد زوجي. باستخدام تمهيدية (٤,٣) يكون x عدداً فردياً. وعليه فإن z عدد فردي. وبهذا نرى أن $z+x$ و $z-x$ عددان زوجيان. ومن هذا يوجد عددان صحيحان موجبان r و s بحيث يكون $z+x=2r$ و $z-x=2s$. وبما أن $x^2+y^2=z^2$ فإن $y^2=(z+x)(z-x)=4rs$. أي أن $(y/2)^2=rs$. لاحظ أن $(r,s)=1$، ولرؤية ذلك نفرض أن $(r,s)=d$. حينئذ $d \mid r$ و $d \mid s$

ويكون $d \mid (r+s)=z$ و $d \mid (r-s)=x$. وهـذا يعـني أن $d \mid (x,z)=1$.
وبالتالي فإن $d=1$.

لدينا الآن $(r,s)=1,\ (y/2)^2=rs$. باستخدام مبرهنة (٢,٣) نستطيع إيجاد عددين صحيحين m و n بحيث يكون $r=m^2$ و $s=n^2$.

سنبرهن الآن أن العددين m و n يحققان الشروط المطلوبة في المبرهنة. لاحظ أولاً أن $(m,n)=1$، فلو كان $(m,n)>1$ لوجد عدد أولي p بحيث $p \mid m$ و $p \mid n$، ومنه $p \mid m^2$ و $p \mid n^2$. أي أن $p \mid r$ و $p \mid s$. وبالتالي فإن $(r,s)>1$ وهذا مستحيل. إذن، $(m,n)=1$. وعليه لا يمكن أن يكون m و n زوجيين في آن واحد. نلاحظ أيضاً أنه لا يمكن أن يكون m و n فرديين معاً، ولو تحقق ذلك لكانت الأعداد x,y,z كلها زوجية (انظر العلاقات (١) أدناه) وهذا يناقض كون $(x,y,z)=1$. إذن، $m \not\equiv n \pmod 2$. وأخيراً بكتابة كل من x,y,z بدلالة m و n نحصل على:

$$\begin{aligned} x &= r-s = m^2-n^2 \\ y &= \sqrt{4rs} = 2mn \\ z &= r+s = m^2+n^2 \end{aligned} \qquad (١)$$

لبرهان العكس نفرض أن شروط المبرهنة محققة. سنبرهن على أن x,y,z ثلاثي فيثاغورس بدائي. لاحظ أولاً أن:

$$x^2+y^2=(m^2-n^2)^2+(2mn)^2=(m^2+n^2)^2=z^2 .$$

يبقى إثبات أن $(x,y,z)=1$.

إذا كان $(x,y,z)=d>1$ فإنه يوجد عدد أولي p بحيث يكون $p \mid d$، وبما أن x عدد فردي فإن $p \neq 2$. وبما أن $p \mid x$ و $p \mid z$ فإن $p \mid (x+z)$. أي أن

$p \mid 2m^2$ وأن $p \mid (z-x)$. ونرى أن $p \mid 2n^2$. إذن، $p \mid m$ و $p \mid n$ وهـذا يناقض كون $(m,n)=1$. وبالتالي نخلص إلى أن $(x,y,z)=1$ ◆

نتيجة (٤,٥)

يكون الثلاثي (x,y,z) فيثاغورسياً إذا وفقط إذا كان:

$$x = t(m^2-n^2)$$
$$y = 2tmn$$
$$z = t(m^2+n^2)$$

حيث $t \geq 1$ ، $m > n$ ، $(m,n)=1$ ، $m \not\equiv n \pmod 2$.

البرهان

من تمهيدية (٤,١) يمكن كتابة $x = tx_1$ ، $y = ty_1$ ، $z = tz_1$ حيث (x_1,y_1,z_1) ثلاثي فيثاغورس بدائي. الآن نحصل على المطلوب بتطبيق المبرهنة (٤,٤) أعلاه ◆

الجدول التالي يعطينا بعض ثلاثيات فيثاغورس البدائية:

m	n	x	y	z	x^2	y^2	z^2
2	1	3	4	5	9	16	25
3	2	5	12	13	25	144	169
4	1	15	8	17	225	64	289
4	3	7	24	25	49	576	625
5	2	21	20	29	441	400	841
5	4	9	40	41	81	1600	1681
6	1	35	12	37	1225	144	1369
6	5	11	60	61	121	3600	3721

مثال (٤,٢)

جِدْ جميع ثلاثيات فيثاغورس البدائية التي فيها $x=15$.

الحل

بما أن $x=15$ فإن $(m+n)(m-n)=m^2-n^2=15$ ونرى أن

$(m-n=1$ و $m+n=15)$ أو $(m-n=3$ و $m+n=5)$.

ويحل كل زوج من هذه المعادلات آنياً نحصل على القيم:

$(n=7$ ، $m=8)$ أو $(n=1$ ، $m=4)$.

إذن، الثلاثيان البدائيان هما 15, 112, 113 أو 15, 8, 17 □

مثال (٤,٣)

جد جميع ثلاثيات فيثاغورس البدائية وغير البدائية والتي يكون فيها $y=28$.

الحل

بما أن $y=2mn=28$ فإن $mn=14$. ونرى أن قيم m و n التي تحقق شروط المبرهنة (٤,٤) هي $(n=1$، $m=14)$ و $(n=2$ ، $m=7)$. وهذا بدوره يعطينا الثلاثيين البدائيين 195, 28, 197 و 45, 28, 53.

إن جميع الثلاثيات يجب أن تحقق التالي:

$x=dx_1$ ، $y=dy_1$ ، $z=dz_1$ حيث x_1, y_1, z_1 ثلاثي بدائي.

وبما أن $y=28$ فإن $y_1 \mid 28$ وتكون جميع القيم الممكنة للعدد y_1 هي 1, 2, 4, 7, 14, 28. ويجب أن نجرب كلاً من هذه القواسم من حيث إمكانية كونه أحد أعداد ثلاثي بدائي. لنجرب القواسم الزوجية أولاً:

إذا كان أحد هذه القواسم عدداً من ثلاثي بدائي فيجب أن يكون على الصورة $2mn$.

إذا كان $2mn=2$ فإن $mn=1$. أي أن $n=1$ و $m=1$ وهذا مستحيل (لماذا؟).

إذا كان $2mn=4$ فإن $mn=2$. ومنه فإن $n=1$ و $m=2$. وعليه فإن 3, 4, 5 ثلاثي بدائي. وبضرب كل من أعداده بالعدد 7 نحصل على ثلاثي فيثاغورس 21, 28, 35.

إذا كان $2mn=14$ فإن $mn=7$ وهذا مستحيل (لماذا؟).

وإذا كان $2mn=28$ فإن $mn=14$. ولقد وجدنا أن ذلك يؤدي إلى الثلاثين البدائيين 195, 28, 197 و 45, 28, 53.

ننتقل الآن إلى القواسم الفردية:

أي قاسم فردي للعدد 28 والذي يكون أحد أعداد ثلاثي فيثاغورس يجب أن يكون على الصورة m^2-n^2.

إذا كان $m^2-n^2=1$ فإنه لا يمكن الحصول على ثلاثيات فيثاغورس في هذه الحالة.

أما إذا كان $m^2-n^2=7$ فإننا نجد أن $n=3$ ، $m=4$. وهذا يعطينا الثلاثي البدائي 7, 24, 25. وبالضرب بالعدد 4 نحصل على 28, 96, 100. وبما أننا نريد أن يكون $y=28$ فإننا نعيد ترتيب هذا الثلاثي لنحصل على 96, 28, 100. وبهذا نكون قد وجدنا جميع الثلاثيات عندما $y=28$ □

مثال (٤,٤)

إذا كان x,y,z ثلاثي فيثاغورس فأثبت أن $12 \mid xyz$.

الحل

من الواضح أنه يكفي إثبات أن $12 \mid xy$ حيث x, y, z ثلاثي فيثاغورس بدائي. باستخدام مبرهنة (٤,١) لدينا:

$$x = m^2 - n^2$$
$$y = 2mn$$
$$z = m^2 + n^2$$

حيث $m > n > 0$ و $(m,n) = 1$ و $m \not\equiv n \pmod 2$.

بما أن $m \not\equiv n \pmod 2$ فإن m زوجي أو n زوجي. أي أن $4 \mid y$.

إذا كان $3 \mid y$ فإن $3 \mid xy$. ولكون $(3,4) = 1$ نجد أن $12 \mid xy$.

لنفرض إذن أن $3 \nmid y$. عندئذ، $3 \nmid m$ و $3 \nmid n$. ونرى أن

$m^2 \equiv 1 \pmod 3$ و $n^2 \equiv 1 \pmod 3$. أي أن $m^2 - n^2 \equiv 0 \pmod 3$. وبهذا يكون $3 \mid (m^2 - n^2)$. أي أن $3 \mid x$. إذن، $3 \mid xy$. ويكون $12 \mid xy$ في هذه الحالة أيضاً □

(٤,١,١) تمارين محلولة *(Solved Exercises)*

تمرين (١)

جد جميع مثلثات فيثاغورس التي أطوال أضلاعها أعداد صحيحة بحيث تكون مساحتها تساوي محيطها.

الحل

لنفرض أن (x, y, z) ثلاثي فيثاغورس . عندئذ:

$$x = k(m^2 - n^2)$$
$$y = k(2mn)$$
$$z = k(m^2 + n^2)$$

وبما أن المساحة تساوي المحيط فإن :

$$\frac{1}{2}xy = x + y + z$$

ومنه فإن $k^2 mn(m^2 - n^2) = k(2m^2 + 2mn)$. وبقسمة طرفي المعادلة على $km(m+n)$ نحصل على:

$$kn(m-n) = 2$$

إذا كان $k = 1$ فإن ($n = 1$ و $m - n = 2$) أو ($n = 2$ و $m - n = 1$). ولذا فإن ($n = 1$ و $m = 3$) أو ($n = 2$ و $m = 3$) . وبهذا نحصل على الثلاثين $(8,6,10)$ و $(5,12,13)$.

إما إذا كان $k = 2$ فإن $n(m-n) = 1$. ولذا فإن $n = 1$ و $m - n = 1$. أي أن $n = 1$ و $m = 2$. ونحصل على الثلاثي $(6,8,10)$. ولذا (باستثناء ترتيب x و y) فإنه يوجد ثلاثيان فقط هما $(6,8,10)$ و $(5,12,13)$ △

تمرين (٢)

هل تستطيع إيجاد ثلاثي فيثاغورس بدائي (x, y, z) بحيث يكون $x - y = c^2 > 1$.

الحل

لنفرض أن $x - y = c^2$. حينئذ :

$$m^2 - n^2 - 2mn = c^2 \Rightarrow (m-n)^2 - 2n^2 = c^2$$
$$\Rightarrow (m-n)^2 - c^2 = 2n^2$$

$$\Rightarrow (m-n-c)\,(m-n+c)=2n^2$$

وبوضع $m-n-c=2$ و $m-n+c=n^2$ والطرح نجد أن $n^2-2=2c$. الآن بأخذ n زوجي فإننا نستطيع أن نجد قيمة للعدد c. على سبيل المثال، إذا كان $n=4$ فإن $c=7$. ولذا فإن $m=n+c+2=13$. وبالتالي فإن $x=m^2-n^2=153$ و $y=2mn=104$ $\triangle$

تمرين (٣)

جد جميع ثلاثيات فيثاغورس (x,y,z) التي تحقق $z=y+1$.

الحل

بما أن $z=y+1$ فمن الواضح أن الثلاثيات يجب أن تكون بدائية. ولذا فإن $x=m^2-n^2$ و $y=2mn$ و $z=m^2+n^2=y+1$. ومنه فإن $y=m^2+n^2-1=2mn$ ومن ثم $(m-n)^2=1$. أي أن $m-n=1$. ونرى أن $m=n+1$. وبهذا يكون

$$x=(n+1)^2-n^2=2n+1$$
$$y=2mn=2(n+1)=2n^2+2n$$
$$z=y+1=2n^2+2n+1 \quad \triangle$$

تمارين (١,٤)

(١) جد جميع ثلاثيات فيثاغورس التي أحد أعدادها يساوي 18.

(٢) جد جميع ثلاثيات فيثاغورس البدائية إذا علمت أن $y=24$.

(٣) جد جميع ثلاثيات فيثاغورس البدائية إذا علمت أن $x=21$.

(٤) جد جميع ثلاثيات فيثاغورس البدائية إذا علمت أن $z = 125$.

(٥) جد جميع ثلاثيات فيثاغورس إذا علمت أن $y = 16$.

(٦) جد جميع ثلاثيات فيثاغورس إذا علمت أن $x = 35$.

(٧) جد جميع ثلاثيات فيثاغورس حيث $x < y$ و $z = 481$.

(٨) إذا كان (x, y, z) ثلاثي فيثاغورس فأثبت أن 60 يقسم xyz.

(٩) إذا كان $n = 1$ أو $n = 2$ فأثبت استحالة وجود ثلاثي فيثاغورس بحيث يكون n أحد أعداده.

(١٠) إذا كان $k \geq 3$ فأثبت أن k أحد أعداد ثلاثي فيثاغورس.

(١١) أثبت أن $(3,4,5)$ هو ثلاثي فيثاغورس البدائي الوحيد التي تكون أعداده متتالية حسابية.

(١٢) أثبت أن $(3k, 4k, 5k)$ هو ثلاثي فيثاغورس الوحيد التي تكون أعداده متتالية حسابية .

(١٣) إذا كان $y \equiv 2 \pmod 4$ فأثبت أنه لا يمكن أن يكون (x, y, z) ثلاثي فيثاغورس بدائي.

(١٤) إذا كان p عدداً أولياً يمثل طول الوتر في مثلث فيثاغورس فأثبت أن $p \equiv 1 \pmod 4$.

(١٥) أثبت أن طول نصف قطر الدائرة المرسومة داخل مثلث فيثاغورس يجب أن يكون عدداً صحيحاً.

(١٦) إذا كان مجموع عددين صحيحين متتالين مربعاً كاملاً فأثبت أن العدد الأصغر طول ضلع مثلث فيثاغورس والعدد الأكبر طول وتره.

(١٧) إذا كان $p > 2$ عدداً أولياً فأثبت أنه يوجد ثلاثي فيثاغورس بدائي (x, y, z) حيث $x = p$.

(١٨) جد جميع ثلاثيات فيثاغورس (x, y, z) التي تحقق $z = y + 2$.

(٤,٢) مجموع المربعات
Sums of Squares

هدفنا الأساس في هذا البند هو إيجاد الأعداد الصحيحة n التي يمكن كتابتها كمجموع مربعين، ثلاثة مربعات أو أربعة مربعات، أي محاولة إيجاد حل لكل من المعادلات الديوفنتية:

$$x^2 + y^2 = n \ ، \ x^2 + y^2 + z^2 = n \ ، \ x^2 + y^2 + z^2 + t^2 = n \ .$$

(٤,٢,١) مجموع مربعين *(Sum of Two Squares)*

نقدم في هذا البند الجزئي الشرط اللازم والكافي لكتابة عدد صحيح غير سالب كمجموع مربعين، كما نقدم خوارزمية لإنجاز ذلك.

مبرهنة (٤,٦)

(أ) إذا كان كل من m و n مجموع مربعين فإن mn كذلك.

(ب)إذا كان كل من m و n مجموعة أربعة مربعات فإن mn كذلك.

البرهان

(أ) لنفرض أن $m=a^2+b^2$ و $n=c^2+d^2$. عندئذ:

$$\begin{aligned} mn &= (a^2+b^2)(c^2+d^2) = a^2c^2+a^2d^2+b^2c^2+b^2d^2 \\ &= (a^2c^2-2abcd+b^2d^2)+(a^2d^2+2abcd+b^2c^2) \\ &= (ac-bd)^2+(ad+bc)^2 \end{aligned}$$

وبما أن $ac-bd, ad+bc \in \mathbb{Z}$ فإن mn مجموع مربعين.

(ب) لنفرض أن $m=a_1^2+b_1^2+c_1^2+d_1^2$ وأن $n=a_2^2+b_2^2+c_2^2+d_2^2$.

من السهل أن نرى الآن أن:

$$\begin{aligned} mn &= (a_1a_2-b_1b_2-c_1c_2-d_1d_2)^2+(a_1b_2+b_1a_2+c_1d_2-d_1c_2)^2 \\ &+(a_1c_2-b_1d_2+c_1a_2+d_1b_2)^2+(a_1d_2+b_1c_2-c_1b_2+d_1a_2)^2 \end{aligned}$$

وبالتالي فإن mn مجموع أربعة مربعات ◆

باستخدام الاستقراء الرياضي والمبرهنة (٤,٦) نحصل مباشرة على النتيجة التالية:

نتيجة (٤,٧)

(أ) إذا كان كل من $n_1, n_2, \ldots, n_k$ مجموع مربعين فإن $n_1n_2 \ldots n_k$ مجموع مربعين لكل $k \geq 1$.

(ب) إذا كان كل من $n_1, n_2, \ldots, n_k$ مجموع أربعة مربعات فإن $n_1n_2 \ldots n_k$ مجموع أربعة مربعات لكل $k \geq 1$ ◆

ملحوظات

(١) إذا كان كل من m و n مجموع ثلاث مربعات فإنه ليس بالضرورة أن يكون mn مجموعاً لثلاث مربعات، على سبيل المثال، $3=1^2+1^2+1^2$ و $5=2^2+1^2+0^2$ ولكن لا يمكن كتابة $15=5\times3$ كمجموع ثلاث مربعات.

(٢) لاحظ أنه بوضع $-b$ بدلاً b في الفقرة (أ) من المبرهنة (٤,٦) نحصل على المساواة: $(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$

(٣) لاحظ أنه بوضع $-d_1,-c_1,-b_1$ بدلاً من d_1,c_1,b_1 على التوالي في الفقرة (ب) من المبرهنة (٤,٦). نحصل على المتطابقة :

$$(a_1^2+b_1^2+c_1^2+d_1^2)(a_2^2+b_2^2+c_2^2+d_2^2)$$
$$=(a_1a_2+b_1b_2+c_1c_2+d_1d_2)^2+(a_1b_2-b_1a_2+c_1d_2-d_1c_2)^2$$
$$+(a_1c_2+b_1d_2-c_1a_2-d_1b_2)^2+(a_1d_2-b_1c_2+c_1b_2-d_1a_2)^2$$

تقترح علينا المبرهنة (٤,٦) أنه لكي نحدد ما إذا كان العدد الصحيح n مجموعاً لمربعين هو كتابته أولاً كحاصل ضرب أعداد أولية وإذا كان كل من الأعداد الأولية مجموعاً لمربعين فإننا نخلص إلى أن n مجموع مربعين. ولكن للأسف ليست جميع الأعداد الأولية مجموعاً لمربعين. فمثلاً لا يمكن كتابة العدد الأولي 3 كمجموع مربعين. والمبرهنة التالية تزودنا بجميع الأعداد الأولية التي يمكن كتابتها كمجموع مربعين.

مبرهنة (٤,٨)

(أ) إذا كان $p\equiv 1(\mathrm{mod}\ 4)$ عدداً أولياً فيوجد عددان صحيحان غير سالبين x و y يحققان

$$x^2+y^2=kp \quad ، \quad 1\le k\le \frac{p-1}{4}$$

(ب) إذا كان p عدداً أولياً فإنه يكتب كمجموع مربعين بطريقة وحيدة إذا وفقط إذا كان $p=2$ أو $p\equiv 1(\mathrm{mod}\ 4)$.

البرهان

(أ) نختار عدداً a بحيث يكون التطابق $x^2 \equiv a \pmod{p}$ غير قابل للحل [سنرى في الفصل السابع أن مثل هذه الأعداد موجودة وعددها $\frac{p-1}{2}$ ، ولذا فإنه ليس بالأمر الصعب إيجادها].

لنفرض الآن أن $r \equiv a^{\frac{p-1}{4}} \pmod{p}$ وأن $x = \min\{r, p-r\}$. عندئذ، باستخدام معيار أويلر لدينا :

$$x^2 \equiv r^2 \equiv a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

ومنه فإن $x^2+1 = kp$. وبوضع $y = 1$ نجد أن $x^2 + y^2 = kp$.

وأخيراً ، $kp = x^2 + 1 \le \left(\frac{p-1}{2}\right)^2 + 1 \le p\frac{(p-1)}{4}$. ويكون $k \le \frac{p-1}{4}$.

(ب) لنفرض أولاً أن $p = x^2 + y^2$ حيث $x, y \in \mathbb{Z}$. بما أن $a^2 \equiv 0 \pmod{4}$ أو $a^2 \equiv 1 \pmod{4}$ لكل $a \in \mathbb{Z}$ فإن $p = x^2 + y^2 \not\equiv 3 \pmod{4}$. وعليه فإن $p = 2$ أو $p \equiv 1 \pmod{4}$.

لبرهان العكس، لاحظ أولاً أن $2 = 1^2 + 1^2$. ولذا نفرض أن $p \equiv 1 \pmod{4}$.

باستخدام الفقرة (أ) يوجد عددان صحيحان x_1 و y_1 بحيث يكون:

$$x_1^2 + y_1^2 = k_1 p \quad ، \quad 1 \le k_1 \le \frac{p-1}{4}$$

إذا كان $k_1 = 1$ فإن $x_1^2 + y_1^2 = p$ وينتهي البرهان. أما إذا كان $k_1 \ne 1$ فإننا ندرس الحالتين k_1 زوجي و k_1 فردي.

الحالة k_1 زوجي:

في هذه الحالة $x_1 \equiv y_1 \pmod 2$ (لماذا ؟) . ومن ثم فإن كل من $\frac{x_1+y_1}{2}$ و $\frac{x_1-y_1}{2}$ عدد صحيح.

الآن، بوضع $x_2=\frac{|x_1+y_1|}{2}$ ، $y_2=\frac{|x_1-y_1|}{2}$ نجد أن:

$$x_2^2+y_2^2=\frac{(x_1+y_1)^2}{4}+\frac{(x_1-y_1)^2}{4}=\frac{x_1^2+y_1^2}{2}=\frac{k_1}{2}=k_2p$$

حيث $1\le k_2\le \frac{k_1}{2}$.

الحالة k_1 فردي:

في هذه الحالة نختار عددين صحيحين m_1 و n_1 بحيث يكون:

$$m_1\equiv x_1 \pmod{k_1}\text{ ، }n_1\equiv y_1 \pmod{k_1}\text{ ، }|m_1|<\frac{k_1}{2}\text{ ، }|n_1|<\frac{k_1}{2}$$

عندئذ ، $m_1^2+n_1^2\equiv x_1^2+y_1^2\equiv 0 \pmod{k_1}$ ونرى أن $m_1^2+n_1^2=k_2k_1$.

لاحظ أن $k_2\neq 0$. لأنه لو كان $k_2=0$ فإن $m_1=n_1=0$. ومنه فإن $x_1\equiv y_1\equiv 0 \pmod{k_1}$. أي أن $x_1=k_1t_1$ و $y_1=k_1s_1$ حيث $t_1,s_1\in\mathbb{Z}$.

الآن : $k_1p=x_1^2+y_1^2=k_1^2(t_1^2+s_1^2)$. ومنه فإن $p=k_1(t_1^2+s_1^2)$. وبما أن p أولي و $k_1>1$ فإن $t_1^2+s_1^2=1$ ويكون $p=k_1$ مما يناقض الفرض. ولذا فإن $1\le k_2\le\frac{k_1}{2}$. لدينا أيضاً:

$$m_1x_1+n_1y_1\equiv x_1^2+y_1^2\equiv 0 \pmod{k_1}$$
$$m_1y_1-n_1x_1\equiv x_1y_1-y_1x_1\equiv 0 \pmod{k_1}$$

وعليه فإن كل من $x_2=\frac{|m_1x_1+n_1y_1|}{k_1}$ و $y_2=\frac{|m_1y_1-n_1x_1|}{k_1}$

عدد صحيح وأن:

$$x_2^2+y_2^2=\frac{(m_1x_1+n_1y_1)^2}{k_1^2}+\frac{(m_1y_1-n_1x_1)^2}{k_1^2}$$
$$=\frac{(m_1^2+n_1^2)(x_1^2+y_1^2)}{k_1^2}$$
$$=\frac{(k_2k_1)\,(k_1p)}{k_1^2}=k_2p$$

حيث $1\le k_2<\frac{k_1}{2}$.

الآن ، إذا كان $k_2=1$ في أي من الحالتين فإننا نتوقف ونكون قد حصلنا على x و y بحيث يكون $x^2+y^2=p$.

أما إذا كان $k_2>1$ فإننا نكرر الخطوات لنحصل مرة أخرى على:

$$x_3^2+y_3^2=k_3p \quad ، \quad 1\le k_3<\frac{k_2}{2} .$$

وبما أن $k_1>k_2>k_3>\ldots\ge 1$ فإنه لا بد من وجود $t\ge 1$ حيث $k_t=1$ ونحصل على x_t و y_t بحيث يكون $x_t^2+y_t^2=p$.

ولبرهان الوحدانية نفرض أن:

$p=x^2+y^2=r^2+s^2$ حيث $x>y>0$ ، $r>s>0$. عندئذ :

$$x^2\equiv -y^2 \pmod p$$
$$s^2\equiv -r^2 \pmod p$$

وبما أن: $0<x,y,r,s<\sqrt{p}$

فإن : $-p<xs-yr<p$

$0<xs+yr<2p$

الآن: $x^2s^2-y^2r^2=(xs-yr)\,(xs+yr)\equiv 0 \pmod p$.

ولذا فإن $p\mid(xs-yr)$ أو $p\mid(xs+yr)$.

إذا كان $p \mid (xs-yr)$ فإن $xs-yr=0$. ومنه فإن $xs=yr$. أي أن $yr \mid s$. وبما أن $(s,r)=1$ (لأن $s^2+r^2=p$) فإن $y \mid s$. وبالمثل $s \mid y$. وبالتالي فإن $s=y$. ومن ثم $x=r$.

أما إذا كان $p \mid (xs+yr)$ فإن $xs+yr=p$. ومنه فإن:

$$p^2+(xr-ys)^2=(xs+yr)^2+(xr-ys)^2=(x^2+y^2)(r^2+s^2)=p^2$$

ولذا فإن $xr-ys=0$. ومن ثم فإن $xr=ys$.

وبصورة مماثلة لما هو مبين أعلاه نجد أن $y=s$ وأن $x=r$ ◆

مثال (٤,٥)

اكتب العدد الأولي $p=397$ كمجموع مربعين.

الحل

لاحظ أن التطابق $x^2 \equiv 5 \pmod{397}$ غير قابل للحل (سنبين ذلك في الفصل السابع). ولذا فإننا نختار $a=5$. الآن ، باستخدام خوارزمية التربيع والضرب نجد أن:

$$r=5^{\frac{397-1}{4}}=5^{99} \equiv 334 \pmod{397} \quad .$$

ولذا فإن $x_1=\min\{334,\ 397-334\}=63$. وبوضع $y_1=1$ نحصل على:

$$x_1^2+y_1^2=(63)^2+1^2=3970=10\times 397$$

أي أن $k_1=10$. الآن :

$$x_2=\frac{|x_1+y_1|}{2}=\frac{63+1}{2}=32$$

$$y_2=\frac{|x_1-y_1|}{2}=\frac{63-1}{2}=31$$

$$x_2^2+y_2^2=(32)^2+(31)^2=1985=5\times 397$$

وبهذا نرى أن $k_2=5$. بما أن k_2 فردي فنختار m_2 و n_2 بحيث يحققان $m_2\equiv 32(\text{mod }5)$ و $n_2\equiv 31(\text{mod }5)$. من الواضح أن $m_2=2$ و $n_2=1$ يفيان بالغرض. الآن:

$$x_3=\frac{|m_2x_2+n_2y_2|}{k_2}=\frac{64+31}{5}=19$$

$$y_3=\frac{|m_2y_2-n_2x_2|}{k_2}=\frac{62-32}{5}=6$$

$$x_3^2+y_3^2=(19)^2+6^2=397$$

ونكون قد انتهينا □

ملحوظات

(١) من الممكن كتابة العدد الأولي $p\equiv 1(\text{mod }4)$ كمجموع مربعين باستخدام خوارزمية أخرى على النحو التالي:

نقوم باختيار a ، r ، x_1 ، y_1 كما في المبرهنة (٤,٨) . إذا كان $p=x_1^2+1$ فإننا نتوقف. أما إذا كان غير ذلك فإننا نستخدم خوارزمية إقليدس لحساب (p,x_1) . إذا كان r_i هو أول باقي يحقق $r_i<\sqrt{p}$ فإن $p=r_i^2+r_{i+1}^2$ (انظر [129]) لتبرير الخوارزمية.

فمثلا لكتابة $p=397$ كمجموع مربعين، نقوم باستخدام خوارزمية القسمة لحساب $(397,63)$ فنجد أن:

$$397=6\times 63+19$$

$$63=3\times 19+6$$

وبما أن $19<\sqrt{397}\approx 19.92$ فإن :

$$397=(19)^2+6^2$$

(٢) من الممكن استخدام المبرهنة (٤,٨) لاختبار أولية الأعداد التي على الصورة $4k+1$. على سبيل المثال، إذا كان $n=53461$ فإن $n \equiv 1 \pmod 4$. إذا كان n أولياً فإنه يمكن كتابته بطريقة وحيدة كمجموع مربعين. ولكن:

$$n = 53461 = (10)^2 + (231)^2 = (105)^2 + (206)^2$$

ولذا فإن n مؤلف.

إذا كان n مربعاً كاملاً فإن $n = m^2 + 0^2$ حيث $m \in \mathbb{Z}$. ولذا فإنه يمكن كتابة n كمجموع مربعين. أما إذا لم يكن n مربعاً كاملاً فنجد باستخدام المبرهنة الأساسية في الحساب انه يمكن كتابة n بطريقة وحيدة على النحو التالي:

$n = k^2 p_1 p_2 \dots p_t$ حيث $k > 0$ و $p_1, p_2 \dots p_t$ أعداد أولية جميعها مختلفة. والمبرهنة التالية تزودنا بالشرط اللازم والكافي لكتابة العدد الصحيح غير المربع كمجموع مربعين.

مبرهنة (٤,٩)

إذا كان $n = k^2 p_1 p_2 \dots p_t$ حيث $k \in \mathbb{Z}^+$ و $p_1, p_2, \dots, p_t$ أعداد أولية مختلفة فإن n مجموع مربعين إذا وفقط إذا كان $p_i \not\equiv 3 \pmod 4$ لكل $1 \le i \le t$.

البرهان

لنفرض أولاً أنه يوجد $a,b \in \mathbb{Z}$ حيث $n = a^2 + b^2$ ، ولنفرض أن $d = (a,b)$. ومنه فإن $a = dx$ و $b = dy$ حيث $x,y \in \mathbb{Z}$ و $(x,y) = 1$. ولذا فإن $n = d^2(x^2+y^2) = d^2 r$ حيث $r = x^2 + y^2$. الآن، بما أن $p_i \mid n$ وأن $(p_i, d) = 1$ فإن $p_i \mid r$. وبما أن $(x,r) = 1$ (لأن $(x,y) = 1$) فيوجد نظير

ضربي للعدد x قياس r. ونرى أن $xz \equiv 1 \pmod{r}$. ولذا فإن $xzy \equiv y \pmod{r}$. أي أن $xm \equiv y \pmod{r}$ حيث $m = zy$. الآن :

$$r = x^2 + y^2 \equiv x^2 + x^2 m^2 \equiv x^2(1+m^2) \equiv 0 \pmod{r}$$

وبهذا نرى $1+m^2 \equiv 0 \pmod{r}$. وبما أن $p_i \mid r$ فإن $1+m^2 \equiv 0 \pmod{p_i}$. وباستخدام المبرهنة (٢,٢٠) نخلص إلى أن $p_i \equiv 1 \pmod{4}$. ويكون $p_i \not\equiv 3 \pmod{4}$ لكل $1 \le i \le t$.

لبرهان العكس، نفرض أن $p_i \not\equiv 3 \pmod{4}$. عندئذ، $p_i = 2$ أو $p_i \equiv 1 \pmod{4}$. وباستخدام المبرهنة (٤,٨) نجد أن p_i مجموعاً لمربعين. وباستخدام النتيجة (٤,٧) نجد أن $p_1 p_2 \dots p_t = a^2 + b^2$. وبالتالي فإن:

$$n = k^2 p_2 p_2 \dots p_t = k^2(a^2+b^2) = (ka)^2 + (kb)^2 .$$

ونخلص إلى أن n مجموع مربعين ◆

مثال (٤,٦)

اكتب العدد $n = 53461 = 193 \times 277$ كمجموع مربعين.

الحل

بما أن $193 \equiv 277 \equiv 1 \pmod{4}$ فإنه يمكن كتابة n كمجموع مربعين، الآن، باستخدام المبرهنة (٤,٨) نجد أن:

$$193 = 7^2 + 12^2 \quad \text{و} \quad 277 = 9^2 + 14^2 .$$

ويكون $n = 53461 = (7^2+12^2)(9^2+14^2) = 105^2 + 206^2$ □

(٤,٢,٢) مجموع ثلاث مربعات (Sum of Three Squares)

إذا كان كل من n و m مجموعاً لثلاث مربعات فلقد بينا في الملحوظات السابقة أنه ليس بالضرورة أن يكون mn مجموعاً لثلاث مربعات.

ولذا فإننا لا نستطيع استخدام المبرهنة (٤,٦) لمعرفة الأعداد الصحيحة التي يمكن كتابتها كمجموع ثلاث مربعات. وعليه فإن مسألة كتابة الأعداد كمجموع ثلاث مربعات أصعب من مسألة كتابتهم كمجموع مربعين.

مبرهنة (٤,١٠)

(أ) إذا كان $n \equiv 7 \pmod 8$ فإنه لا يمكن كتابة n كمجموع ثلاث مربعات.

(ب) إذا كان $n = 4^m(8k+7)$ حيث m و k عددان صحيحان غير سالبين فإنه لا يمكن كتابة n كمجموع ثلاث مربعات.

البرهان

(أ) بما أن $x^2 \equiv 0,1,4 \pmod 8$ لأي عدد صحيح x فنرى أن مجموع أي ثلاث مربعات لا يمكن أن يطابق 7 قياس 8. وبالتالي لا يمكن كتابة $n \equiv 7 \pmod 8$ كمجموع ثلاث مربعات.

(ب) باستخدام الاستقراء الرياضي على m.

باستخدام الفقرة (أ) نجد أن العبارة صحيحة عندما $m = 0$. لنفرض الآن أن العبارة صحيحة عند m. ولنفرض لغرض التناقض أن $4^{m+1}(8k+7) = a^2+b^2+c^2$. حينئذ، $a^2+b^2+c^2 \equiv 0 \pmod 4$. وبهذا يكون كل من a و b و c عدد زوجي. أي أن $a = 2x$ و $b = 2y$ و $c = 2z$ حيث $x,y,z \in \mathbb{Z}$. ونرى أن $4^m(8k+7) = x^2+y^2+z^2$. ومنه فإن $4^{m+1}(8k+7) = 4x^2+4y^2+4z^2$. وهذا يناقض فرضية الاستقراء ◆

لقد بين كل من ليجندر (*Legendre*) وجاوس (*Gauss*) أن عكس المبرهنة (٤,١٠) صحيح أيضاً. إلا أن البرهان يحتاج إلى مفهوم الصيغ التربيعية التي تخرجنا عن نطاق الكتاب ولذا فإننا نقدمها دون برهان.

مبرهنة (٤,١١)

إذا كان $n \in \mathbb{Z}^+$ فإنه من الممكن كتابة n كمجموع ثلاث مربعات إذا وفقط إذا لم يكن n على الصورة $4^m(8k+7)$.

البرهان

انظر [9] ◆

(٤,٢,٣) مجموع أربع مربعات (*Sum of Four Squares*)

إذا حاولنا كتابة جميع الأعداد الأولية p حيث $1 < p < 90$ كمجموع مربعات أربعة أعداد. أي $p = a^2 + b^2 + c^2 + d^2$ حيث $a \geq b \geq c \geq d \geq 0$ فإننا نجد أننا نستطيع ذلك كما هو مبين في الجدول التالي:

p	a	b	c	d	p	a	b	c	d
2	1	1	0	0	41	5	4	0	0
3	1	1	1	0	43	5	3	3	0
5	2	1	0	0	47	6	3	1	1
7	2	1	1	1	53	7	2	0	0
11	3	1	1	0	59	5	5	3	0
13	3	2	0	0	61	6	5	0	0
17	4	1	0	0	67	7	3	3	0
19	3	3	1	0	71	7	3	3	2
23	3	3	2	1	73	8	3	0	0
29	5	2	0	0	79	6	5	3	3
31	5	2	1	1	83	8	3	3	1
37	6	1	0	0	89	9	2	2	0

سنبرهن أنه من الممكن كتابة أي عدد أولي كمجموع أربع مربعات ومن ثم نستخدم النتيجة (٤,٧) لإثبات أنه من الممكن كتابة أي عدد صحيح غير سالب كمجموع أربع مربعات.

مبرهنة (٤,١٢)

إذا كان $p \equiv 3 \pmod 8$ عدداً أولياً فإنه لا يوجد حل للتطابق $x^2 \equiv 2 \pmod p$.

البرهان

لاحظ أن :

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! = (2)(4)(6) \ldots \left(\frac{p-3}{2}\right)\left(-\frac{p-1}{2}\right) \ldots (-5)(-3)(-1)$$

$$\equiv (-1)^{\frac{p+1}{4}} \left(\frac{p-1}{2}\right)! \pmod p$$

ولذا فإن $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{4}} \pmod p$. وبما أن $p \equiv 3 \pmod 8$ فإن $\frac{p+1}{4}$ عدد فردي. وعليه فإن $2^{\frac{p-1}{2}} \equiv -1 \pmod p$. وباستخدام معيار أويلر نجد أن التطابق $x^2 \equiv 2 \pmod p$ غير قابل للحل ◆

مبرهنة (٤,١٣)

إذا كان $p \equiv 7 \pmod 8$ عدداً أولياً فإنه يوجد عدد أولي q بحيث يكون $q \not\equiv 3 \pmod 4$ ويكون التطابق $x^2 \equiv q \pmod p$ غير قابل للحل.

البرهان

بما أن $(2p-1, 4p) = 1$ (لماذا؟) فيوجد استناداً إلى المبرهنة (٢,١٠) عدد غير منته من الأوليات التي على الصورة $(2p-1)k + 4p$ حيث $k \in \mathbb{Z}$. لنفرض الآن أن q هو أصغر هذه الأوليات. وبما أن $p = 8r + 7$ حيث $r \in \mathbb{Z}$ فنرى أن:

$$\begin{aligned} q = (2p-1)k + 4p &\equiv (2p-1) \pmod{4p} \\ &\equiv (2p-1) \pmod 4 \\ &\equiv (16r+13) \pmod 4 \\ &\equiv 1 \pmod 4 \\ &\not\equiv 3 \pmod 4 \end{aligned}$$

أيضاً، $q \equiv (2p-1) \pmod p \equiv -1 \pmod p$.

وبما أن $p \equiv 7 \pmod 8$ فنرى أن $p \equiv 3 \pmod 4$ ويكون التطابق $x^2 \equiv q \equiv -1 \pmod p$ غير قابل للحل ◆

نتيجة (٤,١٤)

إذا كان $p \equiv 3 \pmod 4$ فيوجد عدد أولي q بحيث يكون $q \not\equiv 3 \pmod 4$ والتطابق $x^2 \equiv q \pmod p$ غير قابل للحل.

البرهان

بما أن $p \equiv 3 \pmod 4$ فإن $p \equiv 3 \pmod 8$ أو $p \equiv 7 \pmod 8$. ومن ثم فإننا نحصل على $q = 2$ باستخدام المبرهنة (٤,١٢) إذا كان $p \equiv 3 \pmod 8$. أما إذا كان $p \equiv 7 \pmod 8$ فنحصل على q من المبرهنة (٤,١٣) ◆

مبرهنة (٤,١٥)

إذا كان $p \equiv 3 \pmod 4$ عدداً أولياً فتوجد أعداد a, b, c, d, k تحقق $|a|, |b|, |c| < \frac{p}{2}$ و $a^2 + b^2 + c^2 + d^2 = kp$ و $0 < k < \frac{3p}{4}$.

البرهان

بما أن $p \equiv 3 \pmod 4$ فنجد استناداً إلى النتيجة (٤,١٤) عدد أولي q بحيث يكون $q \not\equiv 3 \pmod 4$ والتطابق $x^2 \equiv q \pmod p$ غير قابل للحل. وباستخدام

معيار أويلر نجد أن $q^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. ونرى أن

$q^{\frac{p+1}{2}} = q^{\frac{p-1}{2}} q \equiv -q \pmod{p}$.

ومنه فإن $\left(q^{\frac{p+1}{4}}\right)^2 + q = q^{\frac{p+1}{2}} + q \equiv 0 \pmod{p}$.

الآن، بما أن $q \neq 3 \pmod 4$ فنجد استناداً إلى المبرهنة (٤,٨) أن $q = r^2 + s^2$.

وعليه فإن:

$$\left(q^{\frac{p+1}{4}}\right)^2 + r^2 + s^2 + 0^2 \equiv 0 \pmod{p}$$

وباختيار $a \equiv q^{\frac{p+1}{4}}$ ، $b \equiv r \pmod{p}$ ، $c \equiv s \pmod{p}$ ، $d = 0$ ، $|a| < \frac{p}{2}$ ،

$|b| < \frac{p}{2}$ ، $|c| < \frac{p}{2}$ نجد أن $a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{p}$. ويكون

$a^2 + b^2 + c^2 + d^2 = kp$. كذلك، $0 < kp = a^2 + b^2 + c^2 + d^2 < 3\left(\frac{p}{2}\right)^2$.

ونرى أن $0 < k < \frac{3p}{4}$ ◆

مبرهنة (٤,١٦)

إذا كان $p \equiv 3 \pmod 4$ فإنه يوجد أعداد صحيحة a,b,c,d حيث $p = a^2 + b^2 + c^2 + d^2$.

البرهان

باستخدام المبرهنة (٤,١٥) يوجد $a_1,b_1,c_1,d_1 \in \mathbb{Z}$ حيث

$a_1^2 + b_1^2 + c_1^2 + d_1^2 = k_1 p$ ، $0 < k_1 < \frac{3p}{4}$.

إذا كان $k_1 = 1$ فإننا نكون قد انتهينا. لنفرض أن $k_1 > 1$.

الحالة الأولى: k_1 زوجي.

في هذه الحالة لدينا $a_1 \equiv b_1 \pmod 2$ و $c_1 \equiv d_1 \pmod 2$. وبوضع:

$$a_2=\frac{|a_1+b_1|}{2}$$

$$b_2=\frac{|a_1-b_1|}{2}$$

$$c_2=\frac{|c_1+d_1|}{2}$$

$$d_2=\frac{|c_1-d_1|}{2}$$

نجد أن $a_2^2+b_2^2+c_2^2+d_2^2=\frac{1}{2}(a_1^2+b_1^2+c_1^2+d_1^2)=\frac{1}{2}k_1p=k_2p$

حيث $k_2=\frac{1}{2}k_1$.

الحالة الثانية : k_1 فردي

في هذه الحالة نختار أعداداً m_1,n_1,r_1,s_1 حيث :

$$m_1\equiv a_1(\text{mod } k_1) \quad , \quad |m_1|<\frac{k_1}{2}$$

$$n_1\equiv b_1(\text{mod } k_1) \quad , \quad |n_1|<\frac{k_1}{2}$$

$$r_1\equiv c_1(\text{mod } k_1) \quad , \quad |r_1|<\frac{k_1}{2}$$

$$s_1\equiv d_1(\text{mod } k_1) \quad , \quad |s_1|<\frac{k_1}{2}$$

وبهذا نرى أن $m_1^2+n_1^2+r_1^2+s_1^2\equiv a_1^2+b_1^2+c_1^2+d_1^2\equiv 0(\text{mod}\,k_1)$

أي أن: $m_1^2+n_1^2+r_1^2+s_1^2=k_2k_1$.

لاحظ أن $k_2\neq 0$. لأنه لو كان $k_2=0$ فإن:

$$m_1=n_1=r_1=s_1=0\Rightarrow a_1\equiv b_1\equiv c_1\equiv d_1\equiv 0(\text{mod } k_1)$$

$$\Rightarrow k_1^2\,|\,(a_1^2+b_1^2+c_1^2+d_1^2)$$

$$\Rightarrow k_1^2\,|\,k_1p$$

$$\Rightarrow k_1\,|\,p$$

وهذا مستحيل لأن $0<k_1<p$. أيضاً:

$$m_1^2+n_1^2+r_1^2+s_1^2<4(\frac{k_1}{2})^2 \Rightarrow k_2k_1<k_1^2 \Rightarrow k_2<k_1$$

كذلك :

$$a_1m_1+b_1n_1+c_1r_1+d_1s_1 \equiv a_1^2+b_1^2+c_1^2+d_1^2 \equiv 0(\text{mod } k_1)$$
$$a_1n_1-b_1m_1+c_1s_1-d_1r_1 \equiv a_1b_1-b_1a_1+c_1d_1-d_1c_1 \equiv 0(\text{mod } k_1)$$
$$a_1r_1-b_1s_1-c_1m_1+d_1n_1 \equiv a_1c_1-b_1d_1-c_1a_1+d_1b_1 \equiv 0(\text{mod } k_1)$$
$$a_1s_1+b_1r_1-c_1n_1-d_1m_1 \equiv a_1d_1+b_1c_1-c_1b_1-d_1a_1 \equiv 0(\text{mod } k_1)$$

الآن بوضع:

$$a_2=\frac{|a_1m_1+b_1n_1+c_1r_1+d_1s_1|}{k_1}$$
$$b_2=\frac{|a_1n_1-b_1m_1+c_1s_1-d_1r_1|}{k_1}$$
$$c_2=\frac{|a_1r_1-b_1s_1-c_1m_1+d_1n_1|}{k_1}$$
$$d_2=\frac{|a_1s_1+b_1r_1-c_1n_1-d_1m_1|}{k_1}$$

نجد أن:

$$a_2^2+b_2^2+c_2^2+d_2^2=\frac{1}{k_1^2}(a_1^2+b_1^2+c_1^2+d_1^2)(m_1^2+n_1^2+r_1^2+s_1^2)$$
$$=\frac{1}{k_1^2}(k_1p)(k_2k_1)$$
$$=k_2p$$

حيث $1\le k_2<k_1$.

أخيراً، إذا كان $k_2=1$ في أي من الحالتين نتوقف ونكون حصلنا على المطلوب.
أما إذا كان $k_2>1$ فإننا نكرر الخطوتين مرة أخرى لنحصل على :
$a_3^2+b_3^2+c_3^2+d_3^2=k_3p$ ، $1\le k_3<k_2$. وهكذا .

وبما أن $k_1 > k_2 > k_3 > \ldots \geq 1$ فإنه لا بد من وجود $t \geq 1$ حيث $k_t = 1$ ويكون

$a_t^2 + b_t^2 + c_t^2 + d_t^2 = p$ ◆

نتيجة (٤,١٧)

يمكن كتابة أي عدد أولي p كمجموع أربع مربعات.

البرهان

إذا كان $p = 2$ فإن $p = 1^2 + 1^2 + 0^2 + 0^2$.

أما إذا كان $p \equiv 1 \pmod 4$ فإنه من الممكن كتابة p كمجموع مربعين $p = a^2 + b^2$. ويكون $p = a^2 + b^2 + 0^2 + 0^2$.

وأخيراً إذا كان $p \equiv 3 \pmod 4$ فإنه من الممكن كتابته كمجموع أربع مربعات استناداً إلى المبرهنة (٤,١٦) ◆

نتيجة (٤,١٨)

إذا كان $n \in \mathbb{Z}^+$ فيمكن كتابة n كمجموع أربع مربعات.

البرهان

إذا كان $n = 1$ فإن $n = 1^2 + 0^2 + 0^2 + 0^2$. أما إذا كان $n \geq 2$ فنجد استناداً إلى النتيجة (٤,٧) والنتيجة (٤,١٧) أن n مجموعاً لأربع مربعات ◆

ملحوظة

لاحظ أنه عند كتابة $n \in \mathbb{Z}^+$ كمجموع أربع مربعات فمن الممكن أن يكون واحد منها على الأقل صفراً. على سبيل المثال لا يمكن كتابة العدد 5 كمجموع أربع مربعات جميعها ليست أصفاراً.

مثال (٤,٧)

اكتب $p = 103$ كمجموع أربع مربعات.

الحل

نقوم أولاً باختيار أصغر عدد أولي $q \not\equiv 3 \pmod 4$ بحيث يكون التطـــابق $x^2 \equiv q \pmod{103}$ غير قابل للحل. بالتجريب نجد أن $q = 5$. ونرى أن

$$5^{\frac{103+1}{4}} = 5^{26} \equiv 60 \pmod{103}$$

$$a_1 = \min\{5^{26}, 103 - 5^{26}\} = 43$$

$$q = 5 = 1^2 + 2^2$$

إذن، $a_1 = 43$ ، $b_1 = 1$ ، $c_1 = 2$ ، $d_1 = 0$. أي أن:

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 = (43)^2 + 1^2 + 2^2 + 0^2 = 1854 = 18 \times 103$$

وعليه فإن $k_1 = 18$. الآن بوضع:

$$a_2 = \frac{|43+1|}{2} = 22 \quad ، \quad b_2 = \frac{|43-1|}{2} = 21$$

$$c_2 = \frac{|2+0|}{2} = 1 \quad ، \quad d_2 = \frac{|2-0|}{2} = 1$$

نجد أن:

$$a_2^2 + b_2^2 + c_2^2 + d_2^2 = 927 = 9 \times 103$$

وعليه فإن $k_2 = 9$. الآن:

$$a_2 \equiv 4 \pmod 9 \quad ، \quad b_2 \equiv 3 \pmod 9$$

$$c_2 \equiv 1 \pmod 9 \quad ، \quad d_2 \equiv 1 \pmod 9$$

ولذا فإن: $m_2 = 4$ ، $n_2 = 3$ ، $r_2 = 1$ ، $s_2 = 1$. ونرى أن

$$a_3 = \frac{|22 \times 4 + 21 \times 3 + 1 \times 1 + 1 \times 1|}{9} = 17$$

$$b_3 = \frac{|22 \times 3 - 21 \times 4 + 1 \times 1 - 1 \times 1|}{9} = 2$$

$$c_3 = \frac{|22 \times 1 - 21 \times 1 - 1 \times 4 + 1 \times 3|}{9} = 0$$

$$d_3 = \frac{|22 \times 1 + 21 \times 1 - 1 \times 3 - 1 \times 4|}{9} = 4$$

$$a_3^2 + b_3^2 + c_3^2 + d_3^2 = (17)^2 + 2^2 + 0^2 + 4^2 = 309 = 3 \times 103$$

وعليه فإن $k_3=3$. الآن:

$$a_3\equiv 2\equiv -1(\text{mod }3)\ ،\ b_3\equiv 2\equiv -1(\text{mod }3)$$

$$c_3\equiv 0(\text{mod }3)\ ،\ d_3\equiv 1(\text{mod}3)$$

ولذا فإن : $m_3=n_3=-1$ ، $r_3=0$ ، $s_3=1$. ونرى أن

$$a_4=\frac{|17\times(-1)+2\times(-1)+0\times 0+4\times 1|}{3}=5$$

$$b_4=\frac{|17\times(-1)-2\times(-1)+0\times 1-4\times 0|}{3}=5$$

$$c_4=\frac{|17\times 0-2\times 1-0\times(-1)+4\times(-1)|}{3}=2$$

$$d_4=\frac{|17\times 1+2\times 0-0\times(-1)-4\times(-1)|}{3}=7$$

ويكون:

$$\square\quad a_4^2+b_4^2+c_4^2+d_4^2=5^2+5^2+2^2+7^2=103$$

ملحوظة

لاحظ أن البرهان الذي قدمناه لكتابة العدد الصحيح الموجب n كمجموع أربع مربعات يبين لنا الخطوات اللازمة لتنفيذ ذلك، والتمرين المحلول (١) يزودنا ببرهان قصير يعتمد على المبرهنة (٤,١١) .

(٤,٢,٤) تمارين محلولة (*Solved Exercises*)

تمرين (١)

استخدام المبرهنة (٤,١١) لكتابة أي عدد صحيح موجب كمجموع أربع مربعات .

الحل

لنفرض أن $n\in\mathbb{Z}^+$.

إذا كان $n \neq 4^m(8k+7)$ حيث $m \geq 0$ و $k \geq 0$ فنجد استناداً إلى المبرهنة (٤,١١) أن n مجموع ثلاث مربعات ومن ثم فهو مجموع أربع مربعات.

أما إذا كان $n = 4^m(8k+7)$ فإن

$$n - 4^m = 4^m(8k+6) = a^2 + b^2 + c^2$$

وبهذا نرى أن $n = a^2 + b^2 + c^2 + (2^m)^2$ مجموعاً لأربع مربعات $\triangle$

تمرين (٢)

أثبت امكانية كتابة أي عدد صحيح n كفرق بين مربعين إذا وفقط إذا كان $n \not\equiv 2 \pmod 4$.

الحل

لنفرض أولاً أن $n = a^2 - b^2$. بما أن مربع أي عدد يطابق 0 أو 1 قياس 4 فإن $a^2 - b^2$ يطابق 0، 1 أو 1− قياس 4 وبهذا يكون $n = a^2 - b^2 \not\equiv 2 \pmod 4$. وبالعكس، إذا كان n فردياً فإن كل من $n-1$ و $n+1$ زوجي وأن $n = (\frac{n+1}{2})^2 - (\frac{n-1}{2})^2$. أما إذا كان $n \equiv 0 \pmod 4$ فإن

$$n = (\frac{n}{4}+1)^2 - (\frac{n}{4}-1)^2 \quad \triangle$$

تمرين (٣)

(أ) إذا كان $n = a^2 + b^2$ وكان $p \equiv 3 \pmod 4$ قاسماً أولياً للعدد n فأثبت أن $p \mid a$ و $p \mid b$.

(ب) إذا كان $p \equiv 3 \pmod 4$ عدداً أولياً فأثبت أنه لا يمكن كتابة p^2 كمجموع مربعين كلاهما لا يساوي صفراً.

الحل

(أ) لنفرض أن p لا يقسم a. عندئذ ، $(a,p)=1$. ومن ثم يوجد $s\in\mathbb{Z}$ حيث $as\equiv 1(\text{mod } p)$. وبما أن $p \mid n$ فإن $n=a^2+b^2\equiv 0(\text{mod } p)$. ومنه فإن $(sa)^2+(sb)^2\equiv 0(\text{mod } p)$. أي أن $(sb)^2\equiv -1(\text{mod } p)$ وهذا مستحيل لأن $p\equiv 3(\text{mod } 4)$. وبهذا التناقض نرى أن p يقسم a. وبالمثل p يقسم b .

(ب) لنفرض أن $p^2=a^2+b^2$. باستخدام الفقرة (أ) نجد أن $p \mid a$. وإذا كان $a\neq 0$ فإن $a^2\geq p^2$. وبالتالي فإن $b=0$ △

تمرين (٤)

إذا كان $n=a^2+b^2=c^2+d^2$ حيث $a\geq b\geq 0$ و $c\geq d\geq 0$ و $a>c$ وكان $d=(ac-bd,n)$ فأثبت أن d قاسم فعلي للعدد n.

الحل

بما أن $a^2\equiv -b^2(\text{mod } n)$ وأن $c^2\equiv -d^2(\text{mod } n)$ فإن $a^2c^2\equiv b^2d^2(\text{mod } n)$. ومنه فإن n يقسم $(ac+bd)(ac-bd)$. وبما أن $n^2=(a^2+b^2)(c^2+d^2)=(ab+cd)^2+(ad-bc)^2$ وأن $ad>bc$ فإن $ac+bd<n$. وبما أن $0<ac-bd<n$ فإننا نخلص إلى وجود قاسم مشترك غير صفري للعددين $ac-bd$ و n. ومن ثم فإن $d=(ac-bd,n)$ قاسم فعلي للعدد n △

تمرين (٥)

إذا كان $n>169$ فأثبت أنه يمكن كتابته كمجموع خمس مربعات غير صفرية.

الحل

لنفرض أن $k=n-169$. حينئذ، باستخدام النتيجة (٤,١٨) نجد أن $k=a^2+b^2+c^2+d^2$ حيث $a,b,c,d\in\mathbb{Z}$.

إذا كانت جميعها ليست أصفاراً فإن $n=a^2+b^2+c^2+d^2+(13)^2$.

إذا كان واحد فقط منها يساوي صفراً وليكن $d=0$ فإن:

$$n=a^2+b^2+c^2+169=a^2+b^2+c^2+5^2+12^2$$

إذا كان إثنان فقط منها أصفاراً وليكونا $d=c=0$ فإن :

$$n=a^2+b^2+169=a^2+b^2+3^2+4^2+12^2.$$

وأخيراً إذا كان ثلاث منها أصفاراً ولتكن $b=c=d=0$ فإن

$$n=a^2+169=a^2+4^2+4^2+4^2+11^2 \qquad \triangle$$

تمارين (٤,٢)

(١) اكتب كل من الأعداد التالية كمجموع مربعين (إن أمكن ذلك):

(أ) 98 (ب) 343 (ج) 735

(د) 1428 (س) 4680 (ص) 5525

(م) 14365 (هـ) 229320 (و) 16660

(٢) أثبت أن العدد الأولي p يكون على الصورة $4k+1$ إذا وفقط إذا كان p يقسم $n^2+(n+1)^2$ حيث $n\in\mathbb{Z}^+$.

(٣) أثبت أنه يوجد على الأقل عدد واحد من بين الأعداد المتتالية $n,n+1,n+2,n+3$ بحيث لا يمكن كتابته كمجموع مربعين لكل $n\in\mathbb{Z}^+$.

(٤) إذا كان p عدداً أولياً حيث $2p-1$ مربعاً كاملاً فأثبت أن p مجموع لمربعين.

(٥) إذا كان $n=2\times3^2\times5^3\times13^5$ فهل يوجد مثلث فيثاغورس بدائي بحيث يكون n طول ضلع الوتر؟

(٦) أثبت أنه لا يمكن كتابة $9k+3$ أو $9k+6$ كمجموع مربعين.

(٧) إذا كان $n\equiv7(\mathrm{mod}\,8)$ فأثبت أنه لا يمكن كتابته كمجموع ثلاث مربعات كسرية.

(٨) إذا كان $n\geq1$ فأثبت أنه إما أن n أو أن $2n$ مجموع ثلاث مربعات.

(٩) أثبت أنه يمكن كتابة أي عدد فردي موجب كمجموع أربع مربعات أحدها 0 أو 1.

(١٠) إذا كان n عدداً فردياً موجباً فأثبت أن $n=r^2+s^2+2t^2$.

(١١) أثبت وجود عدد غير منته من الأعداد الأولية p التي تحقق $p=a^2+b^2+c^2+1$.

(٤,٣) المعادلة الديوفنتية $x^4+y^4=z^4$

The Diophantine Equation $x^4+y^4=z^4$

كتب فيرما على هامش إحدى صفحات نسخته من كتاب ديافنتس العبارة التالية : " من المستحيل كتابة مكعب كحاصل جمع مكعبين، وكذلك من المستحيل كتابة عدد مرفوع إلى القوة أربعة كحاصل جمع عددين مرفوعين للقوة أربعة. وبصورة عامة أي عدد مرفوع لأي قوة n، $n>2$ كحاصل جمع عددين مرفوعين للقوة نفسها. لدي برهان لهذه الحقيقة المذهلة، ولكن يؤسفني أن مساحة الهامش صغيرة جداً بحيث لا تتسع لكتابة البرهان".

الاعتقاد السائد الآن أن البرهان الذي كان لدى فيرما هو برهان خاطيء وذلك استناداً إلى المحاولات الجادة بعد فيرما من كبار علماء الرياضيات لإيجاد طريقة بسيطة "كما ادعى" لإثبات أن:

"لا يوجد حل غير تافه للمعادلة الديوفنتيّة : $x^n+y^n=z^n$ ، $n>2$"

وبالرغم من هذا فإن استحالة وجود حل للمعادلة أعلاه يسمى إلى الآن "مبرهنة فيرما الكبرى"، وذلك لتمييزها عن مبرهنة فيرما الصغرى التي سبق أن درسناها في الفصل الثالث من هذا الكتاب. في الحقيقة أن التسمية الصحيحة لهذه العبارة يجب أن تكون "حدس فيرما"

لقد خصص عدد كبير من علماء الرياضيات الكثير من الوقت لمحاولة حل حدس فيرما، وكانت محصلة هذا العمل هو برهان بعض الحالات الخاصة للحدس. ومن الجدير بالذكر هنا أن الأكاديمية العلمية الألمانية خصصت قبل الحرب العالمية الأولى مبلغ مائة ألف مارك جائزة تشجيعية لمن يستطيع حل حدس فيرما. ولقد

حاول كثير من الهواة حل هذا الحدس طمعاً في الحصول على هذه الجائزة، وقُدِّم للأكاديمية أكثر من ألفي محاولة لحله إلا أن أحداً لم يفلح في الحصول على الجائزة.

ولقد تمكن الرياضي أندرو وايلز (Andrew Wiles) من جامعة برنستون بمساعدة أحد تلامذته السابقين ريتشارد تايلر (Richard Taylor) من برهان حدس فيرما في العام ١٩٩٤م.

في هذا البند سنبرهن على حدس فيرما في الحالة $n=4$. وسنستخدم طريقة للبرهان ثمّ اكتشافها بوساطة فيرما نفسه وتعرف بطريقة فيرما غير المنتهية التناقص. وباختصار شديد فإنه يمكن وصف هذه الطريقة على النحو التالي:

إذا أردنا أن نبرهن أن علاقة ما على مجموعة الأعداد الصحيحة الموجبة مستحيلة، نفرض العكس، أي نفرض وجود بعض الأعداد الصحيحة الموجبة التي تجعل العلاقة صحيحة. ومن مبدأ الترتيب الحسن يوجد عدد أصغر موجب يحقق العلاقة، بيد أن باستطاعتنا إيجاد عدد أصغر من ذلك، وهذا ينافي مبدأ الترتيب الحسن، مما يعني أن الفرضية خاطئة.

قبل أن نستخدم طريقة فيرما غير المنتهية التناقص لإثبات أن المعادلة

$$x^4+y^4=z^4$$

غير قابلة للحل في مجموعة الأعداد الصحيحة ، دعنا نطبق الطريقة على مثال أسهل.

مثال (٤,٨)

أثبت أنه لا يمكن إيجاد ثلاثي فيثاغورس (x,y,z) حيث $x=y$.

الحل

نستخدم طريقة فيرما غير المنتهية التناقص. ولذا نفرض أن (x,y,z) ثلاثي فيثاغورس حيث $x=y$. عندئذ ، $x^2+y^2=2x^2=z^2$. ولذا فإن z^2 ومن ثم z عدد زوجي وليكن $z=2z_1$. إذن، $2x^2=4z_1^2$. أي أن $x^2=2z_1^2$. ولذا فإن x^2 ومن ثم x زوجي وليكن $x=2x_1$. إذن، $2x_1^2=z_1^2$. وبهذا يكون (x_1,x_1,z_1) ثلاثي فيثاغورس آخر فيه $x_1<x$. وبالاستمرار على هذا المنوال نحصل على متتالية غير منتهية من الثلاثيات (x_i,y_i,z_i) التي تحقق:

$$x>x_1>x_2>...$$

وهذا مستحيل □

ملحوظة

لاحظ أن المثال (٤,٨) يبين لنا أن $\sqrt{2}$ عدد غير كسري، لأنه لو كان $\sqrt{2}=\frac{z}{x}$ حيث $x,z\in\mathbb{Z}$ فإن $z^2=2x^2=x^2+x^2$ وهذا ما بينا استحالته في المثال (٤,٨).

الآن سنطبق طريقة فيرما غير المنتهية التناقص للبرهنة على استحالة حل المعادلة الديوفنتيّة $x^4+y^4=z^2$. لنلاحظ أولاً ما يلي:

إذا كان x_0,y_0,z_0 حلاً للمعادلة $x^4+y^4=z^2$ فإن $-x_0,-y_0,-z_0$ حل أيضاً. لذلك يكفي أن نبرهن استحالة الحل على $\mathbb{Z}^+$.

تمهيدية (٤,١٩)

إذا كان x_0,y_0,z_0 حلاً للمعادلة $x^4+y^4=z^2$ فنستطيع إيجاد حل آخر x_1,y_1,z_1 للمعادلة نفسها بحيث يكون $(x_1,y_1)=1$.

البرهان

لنفرض أن x_0,y_0,z_0 حل للمعادلة ولنفرض أن $(x_0,y_0)=d$. عندئذ: $x_0=dx_1,y_0=dy_1$، $x_1,y_1\in\mathbb{Z}$ و $(x_1,y_1)=1$. بما أن $x_0^4+y_0^4=z_0^2$ فإن $d^4(x_1^4+y_1^4)=(dx_1)^4+(dy_1)^4=z_0^2$ ونرى أن $d^4\mid z_0^2$. ومن ثم فإن $d^2\mid z_0$ (لماذا؟). أي يوجد عدد صحيح موجب z_1 بحيث إن $z_0=d^2z_1$. وبالتعويض عن قيمة z_0 نجد أن $d^4(x_1^4+y_1^4)=d^4(z_1^2)$. ويكون $x_1^4+y_1^4=z_1^2$ ◆

مبرهنة (٤,٢٠)

لا يوجد حلول صحيحة غير تافهة للمعادلة $x^4+y^4=z^2$.

البرهان

لنفرض أن x_0,y_0,z_0 حل للمعادلة. باستخدام التمهيدية (٤,١٩) والملحوظة التي تسبقها نستطيع اعتبار $x_0,y_0,z_0\in\mathbb{Z}^+$ بحيث إن $(x_0,y_0)=1$.

سنبرهن على وجود حل آخر x_1,y_1,z_1 يحقق $(x_1,y_1)=1$ و $z_1<z_0$. بما أن $x_0^4+y_0^4=z_0^2$ فإن $(x_0^2)^2+(y_0^2)^2=z_0^2$. ومنه نجد أن x_0^2,y_0^2,z_0 ثلاثي فيثاغورس. لاحظ أن $(x_0^2,y_0^2)=1$. لأنه لو كان $(x_0^2,y_0^2)>1$ فإننا نستطيع إيجاد عدد أولي p بحيث إن $p\mid x_0^2$ و $p\mid y_0^2$. ومن ثم $p\mid x_0$ و $p\mid y_0$ وهذا مستحيل لأن $(x_0,y_0)=1$.

إذن، (x_0^2, y_0^2, z_0) ثلاثي فيثاغورس بدائي. باستخدام مبرهنة (٤,٤) يوجد عددان صحيحان موجبان أوليان نسبياً m، n يحققان :

$m > n$ ، $m \not\equiv n \pmod 2$ وكذلك $z_0 = m^2 + n^2$ ، $y_0^2 = 2mn$ ، $x_0^2 = m^2 - n^2$.

وبما أن $x_0^2 + n^2 = m^2$ وأن $(m,n) = 1$ فإن x_0, n, m ثلاثي فيثاغورس بدائي. وباستخدام مبرهنة (٤,٤) مرة أخرى نستطيع إيجاد عددين صحيحين موجبين أوليين نسبياً r أو s يحققان:

$r > s$ ، $r \not\equiv s \pmod 2$ وكذلك $x_0 = r^2 - s^2, n = 2rs, m = r^2 + s^2$.

لاحظ أن n زوجي، لذا فإن m فردي. من $(m,n) = 1$ نستنتج أن $(m,2n) = 1$.

وبما أن $y_0^2 = (2n)m$ فإننا نستطيع استخدام مبرهنة (٢,٣) لإيجاد عددين صحيحين موجبين z_1 ، w يحققان $m = z_1^2$ و $2n = w^2$. ومن ذلك نرى أن w زوجي. إذن $w = 2u$ ، $u \in \mathbb{Z}^+$. ويكون لدينا

$u^2 = \frac{w^2}{4} = \frac{n}{2} = rs$ ، $(r,s) = 1$. باستخدام مبرهنة (٢,٣) مرة أخرى نستطيع إيجاد عددين صحيحين موجبين x_1 ، y_1 يحققان $r = x_1^2$ ، $s = y_1^2$ ، $(x_1, y_1) = 1$. وبالتالي فإن $x_1^4 + y_1^4 = z_1^2$. وعلاوة على ذلك فإن $z_1 \le z_1^4 = m^2 < m^2 + n^2 = z_0$.

لتكن $S = \{z : x^4 + y^4 = z^2, z > 0\}$.

إن وجود حل للمعادلة $x^4 + y^4 = z^2$ يعني أن $S \neq \phi$. من مبدأ الترتيب الحسن يوجد عنصر أصغر z_0 في S. وبهذا نحصل على التناقض: $z_1 \in S$ و $z_1 < z_0$ ◆

نتيجة (٤,٢١)

لا يوجد حل غير تافه للمعادلة الديوفنتيّة $x^4+y^4=z^4$.

البرهان

لنفرض أن x_0,y_0,z_0 حل للمعادلة $x^4+y^4=z^4$. عندئذ يكون: x_0,y_0,z_0^2 حلاً للمعادلة $x^4+y^4=z^2$ وهذا يناقض مبرهنة (٤,٢٠) ◆

نتيجة (٤,٢٢)

إذا كان العدد $n>2$ عدداً مضاعفاً للعدد 4 فإنه لا يوجد حل غير تافه للمعادلة $x^n+y^n=z^n$.

البرهان

بما أن العدد n من مضاعفات العدد 4 فإن $n=4k$ و $k\geq 1$. عندئذٍ نستطيع كتابة المعادلة $x^n+y^n=z^n$ على الصورة المكافئة:

$$(x^k)^4+(y^k)^4=(z^k)^4$$

إذا كان x_0,y_0,z_0 حلاً للمعادلة $x^n+y^n=z^n$ فمن الواضح أن x_0^k,y_0^k,z_0^k حل للمعادلة $x^4+y^4=z^4$ وهذا يناقض النتيجة (٤,٢١) ◆

ملحوظة

لاحظ أن أي عدد صحيح $n>2$ إما أن يكون قوة للعدد 2 أو يقبل القسمة على عدد أولي فردي. إذا كان $n>2$ ويساوي قوة للعدد 2 فإن $4\mid n$ ، لذا فإنه من نتيجة (٤,٢٢) لا يوجد حل للمعادلة $x^n+y^n=z^n$. الحالة الأخرى هي أن يوجد عدد أولي فردي p يقسم n. أي أن $n=pk$ و $k\geq 1$ عندئذ نستطيع كتابة المعادلة $x^n+y^n=z^n$ على الصورة:

$$.(x^k)^p+(y^k)^p=(z^k)^p$$

الآن إذا كان x_1,y_1,z_1 حلاً للمعادلة $x^n+y^n=z^n$ فإن x_1^k,y_1^k,z_1^k يكون حلاً للمعادلة $(x^k)^p+(y^k)^p=(z^k)^p$. مما سبق نستنتج أنه لحل حدس فيرما يكفي أن نبرهن أن المعادلة $x^p+y^p=z^p$ ليس لها حل لجميع الأعداد الأولية الفردية p.

ننتقل الآن إلى استخدام طريقة فيرما غير المنتهية التناقص لإثبات أن المعادلة الديوفنتيّة $x^4-y^4=z^2$ ليس لها حل.

مبرهنة (٤,٢٣)

لا يوجد حل غير تافه للمعادلة الديوفنتيّة $x^4-y^4=z^2$.

البرهان

لنفرض أن x_0,y_0,z_0 حل للمعادلة. باستخدام تمهيدية (٤,١٩) نستطيع اعتبار $x_0,y_0,z_0\in\mathbb{Z}^+$ بحيث إن $(x_0,y_0)=1$. سنبرهن على وجود حل آخر x_1,y_1,z_1 يحقق $(x_1,y_1)=1$ و $x_1<x_0$. وسيتم ذلك بدراسة الحالتين التاليتين:

الحالة الأولى: y_0 عدد فردي.

بما أن $(x_0^2)^2=(y_0^2)^2+z_0^2$ وأن $(x_0^2,y_0^2)=1$ فإن y_0^2,z_0,x_0^2 ثلاثي فيثاغورس بدائي حيث y_0^2 عدد فردي. وباستخدام مبرهنة (٤,٤) نستطيع إيجاد عددين صحيحين موجبين t و s يحققان:

$$s\not\equiv t\pmod 2\ ،\ s>t\ ،\ (s,t)=1$$

$$.y_0^2=s^2-t^2\ ,\ z_0=2st\ ,\ x_0^2=s^2+t^2$$

ومنه نجد أن $s^4-t^4=(s^2+t^2)(s^2-t^2)=(x_0y_0)^2$. أي أن $z_1=x_0y_0$ ، $y_1=t$ ، $x_1=s$ حل موجب للمعادلة $x^4-y^4=z^2$ وأن $0<x_1=s<\sqrt{s^2+t^2}=x_0$.

الحالة الثانية: y_0 عدد زوجي.

في هذه الحالة y_0^2,z_0,x_0^2 ثلاثي فيثاغورس بدائي، y_0^2 عدد زوجي. باستخدام مبرهنة (٤,٤) يوجد عددان صحيحان موجبان t و s يحققان:

$(s,t)=1$ ، $s>t$ ، $s\not\equiv t(\text{mod }2)$ ، $x_0^2=s^2+t^2$ ، $y_0^2=2st$ ، $z_0=s^2-t^2$.

لنفرض أولاً أن s زوجي و t فردي. بما أن $y_0^2=2st$ وأن $(2s,t)=1$ فباستخدام مبرهنة (٢,٣) يوجد عددان صحيحان a، b بحيث إن $2s=a^2$ وإن $t=b^2$.

بما أن a زوجي فإن $a=2c$ حيث $c\in\mathbb{Z}^+$ ، أي أن $s=2c^2$ ، ونرى أن

$$x_0^2=s^2+t^2=(2c^2)^2+(b^2)^2$$

من هذه المعادلة نستطيع استنتاج أن $x_0,b^2,2c^2$ ثلاثي فيثاغورس بدائي، وباستخدام مبرهنة (٤,٤) يوجد عددان صحيحان موجبان m و n يحققان

$(m,n)=1$ ، $m>n$ ، $n\not\equiv m(\text{mod }2)$ و

$x_0=m^2+n^2$ ، $2c^2=2mn$ ، $b^2=m^2-n^2$.

بما أن $(m,n)=1$ ، $c^2=mn$ فإنه باستخدام مبرهنة (٢,٣) يوجد عددان صحيحان موجبان e ، f بحيث إن $m=e^2$ و $n=f^2$. ومنه $b^2=m^2-n^2=e^4-f^4$. وبالتالي فإن $z_1=b$ ، $y_1=f$ ، $x_1=e$ حل للمعادلة $x^4-y^4=z^2$ حيث $0<x_1=\sqrt{m}<m^2+n^2=x_0$.

أما الحالة s فردي ، t زوجي فهي مشابهة.

لتكن $S=\{x:x^4-y^4=z^2,z>0\}$.

إن وجود حل للمعادلة $x^4-y^4=z^2$ يعني أن $S\neq\phi$. من المبدأ الترتيب الحسن يوجد عنصر أصغر x_0 في S.

ولكن الذي ورد أعلاه يثبت أن $x_1\in S$ وأن $x_1<x_0$ وهذا تناقض ◆

(٤,٣,١) تمارين محلولة (Solved Exercises)

تمرين (١)

أثبت أن مساحة أي مثلث فيثاغورس لا يمكن أن تكون مربعاً كاملاً.

الحل

لنفرض أن (x,y,z) مثلث فيثاغورس طول وتره z. ولنفرض أن مساحته مربعاً كاملاً. ولذا فإن $\frac{1}{2}xy=s^2$ حيث $s\in\mathbb{Z}^+$. ومنه فإن $2xy=4s^2$. وبما أن $x^2+y^2=z^2$ فإننا نجد أن:

$$x^2+2xy+y^2=z^2+4s^2$$
$$x^2-2xy+y^2=z^2-4s^2$$

أي أن:

$$(x+y)^2=z^2+4s^2$$
$$(x-y)^2=z^2-4s^2$$

وبضرب المعادلتين الأخيرتين نحصل على:

$$(x^2-y^2)^2=z^4-16s^4=z^4-(2s)^4$$

وبالتالي فإننا نخلص إلى وجود حل للمعادلة $a^4-b^4=c^2$ وهذا مستحيل △

تمرين (٢)

جد جميع حلول نظام المعادلات الديوفنتية

$$x^2+y^2=z^2-1$$
$$x^2-y^2=w^2-1$$

الحل

بوضع $x=2n^2$ و $y=2n$ نجد أن:

$$z=4n^4+4n^2+1=(2n^2+1)^2$$
$$w=4n^4-4n^2+1=(2n^2-1)^2$$

ولذا فإن مجموعة الحل هي:

$$\{(2n^2,2n,2n^2+1,2n^2-1):n\in\mathbb{Z}^+\}$$

ونخلص إلى وجود عدد غير منته من الحلول △

تمرين (٣)

(أ) أثبت عدم وجود حلول صحيحة موجبة للمعادلة الديوفنتية $x^4-2y^2=1$.

(ب) أثبت أن الحل الموجب الوحيد للمعادلة الديوفنتية $x^4-2y^2=-1$ هو $x=y=1$.

الحل

(أ) إذا كان $x^4-2y^2=1$ فإن $2y^2=x^4-1$. ولذا فإن $4y^4=x^8-2x^4+1$. وبإضافة $4x^4$ لطرفي المعادلة نحصل على $4(y^4+x^4)=(x^4+1)^2$. ولذا فإن x^4+1 عدد زوجي . ومنه فإن للمعادلة الديوفنتية $y^4+x^4=((x^4+1)/2)^2$ حل وهذا مستحيل.

(ب) بصورة مماثلة للفقرة (أ) نحصل على المعادلة الديوفنتية $y^4 - x^4 = z^2$ حيث $z = 2/(x^4+1)$. وحلول هذه المعادلة هي $x = \pm 1$، $y = \pm 1$ ، $z = 0$.
وبالتالي فإن الحل الموجب الوحيد هو $x = y = 1$ △

تمارين (٤,٣)

(١) استخدم طريقة فيرما غير المنتهية التناقص لإثبات استحالة وجود ثلاثي فيثاغورس (x, y, z) حيث $z = 2y$ ثم استنتج أن $\sqrt{3}$ عدد غير كسري.

(٢) استخدم طريقة فيرما غير المنتهية التناقص لإثبات استحالة وجود ثلاثي فيثاغورس (x, y, z) حيث $x = 2y$. ثم استنتج أن $\sqrt{5}$ عدد غير كسري.

(٣) إذا كان p عدداً أولياً وكان $x^{p-1} + y^{p-1} = z^{p-1}$ فأثبت أن $p \mid xyz$.

(٤) إذا كان p عدداً أولياً وكان $x^p + y^p = z^p$ فأثبت أن $p \mid (x + y - z)$.

(٥) إذا كان (x, y, z) ثلاثي فيثاغورس فأثبت أنه لا يمكن أن يكون حل للمعادلة $x^n + y^n = z^2$ حيث $n \geq 3$.

(٦) إذا كان $x^5 + y^5 = z^5$ فأثبت أنه واحداً على الأقل من الأعداد x أو y أو z يقبل القسمة على 5.

(٧) أثبت عدم وجود حلول صحيحة موجبة للمعادلة $x^4 - 4y^4 = z^2$.

(٨) أثبت عدم وجود حلول صحيحة موجبة للمعادلة $x^4 - y^4 = 2z^2$.

(٩) أثبت عدم وجود حلول صحيحة موجبة للمعادلة $x^4 + 4y^4 = z^2$.

(١٠) جد عدد غير منته من الحلول للمعادلة $x^4 + y^4 = 2z^2$.

(١١) جد عدد غير منته من الحلول للمعادلة $x^4+3y^4=z^4$.

(١٢) جد عدد غير منته من الحلول للمعادلة $x^2+y^2=z^3$.

(١٣) أثبت أنه لا يمكن إيجاد عددين صحيحين a و b بحيث يكون كل من a^2+b^2 و a^2-b^2 مربعاً كاملاً.

(١٤) إذا كان (x,y,z) ثلاثي فيثاغورس فأثبت واحداً على الأكثر من بين الأعداد x أو y أو z يكون مربعاً كاملاً.

(١٥) إذا كان $d>0$ مربعاً كاملاً فأثبت عدم وجود حلول صحيحة موجبة للمعادلة $x^2-dy^2=1$.

(١٦) إذا كان $x^2-2y^2=1$ فأثبت أن:

(أ) $(3,2)$ حل للمعادلة.

(ب) إذا كان (x_0,y_0) حل للمعادلة فأثبت أن $(3x_0+4y_0,2x_0+3y_0)$ حل للمعادلة.

(ج) استنتج وجود عدد غير منته من الحلول للمعادلة.

(١٧) أثبت استحالة وجود مثلث فيثاغورس تكون مساحته مثلي مربع كامل.

(١٨) أثبت عدم وجود حل للنظام :

$$x^2+y^2=z^2$$
$$x^2-y^2=w^2$$

(١٩) أثبت عدم وجود حل للنظام :

$$x^2+2y^2=w^2$$
$$x^2+y^2=z^2$$

(٢٠) أثبت وجود عدد غير منته من الحلول للنظام:

$$x^2+y^2=z^2+1$$
$$x^2-y^2=w^2+1$$

نبذة عن حياة فيرما

Biography of Ferma



ولد : ١٦٠١/٨/١٧م في فرنسا.

توفي: ١٦٦٥/١/١٢م في فرنسا.

ولد بيير فيرما *(Pierre de Fermat)* بمدينة تولوز الفرنسية لأب غني وتلقى علومه في جامعة تولوز ثم أكمل دراسته في القانون في جامعة أورليتر وحصل على شهادة في القانون المدني وشغل منصباً في القضاء في مدينة تولوز وتدرج في هذا المنصب إلى أن أصبح رئيساً للقضاة في العام ١٦٥٢م.

وفي تقرير كتبه أحد رؤساءه عنه يقول فيه: يعد فيرما من الرجال ذوي المعرفة الواسعة وله اتصالات كثيرة مع المثقفين في أماكن كثيرة، ولكنه دائماً مشغول البال وتقاريره عن القضايا التي يبت فيها في المحكمة ينقصها الدقة وتوحي بتشويش أفكار كاتبها.

لا شك أن تقرير رئيس فيرما فيه جانب من الصواب إذ أن فيرما كان مشغول البال بهوايته المفضلة ألا وهي الرياضيات. وعلى الرغم من اسهامات فيرما الكثيرة في فروع الرياضيات المختلفة إلا أنه لم ينشر أي من أبحاثه في أي مجلة متخصصة، بل اكتفى بمراسلة العديد من علماء الرياضيات واطلاعهم على اكتشافاته الرياضية والتشاور معهم في بعض المسائل.

لقد أغنى فيرما فروعاً كثيرة في الرياضيات وكانت أبحاثه على درجة كبيرة من الأهمية لكي يعتبره العلماء أعظم رياضي فرنسي في القرن السابع عشر. ومن

أهم اسهامات فيرما الكثيرة في فروع الرياضيات وضعه لنظرية الأعداد بمفهومها الحديث. ويعتقد أن للترجمة اللاتينية لكتاب علم الحساب *(Arithmetica)* للرياضي ديوفنتاس الفضل الكثير في اهتمام فيرما بنظرية الأعداد. ولقد وجد العديد من اكتشافات فيرما في نظرية الأعداد مكتوبة على هامش نسخته من كتاب علم الحساب، أهم هذه الاكتشافات هو عدم وجود حل موجب للمعادلة الديوفنتية $x^n + y^n = z^n$ حيث $n > 2$ والتي تعرف بمبرهنة فيرما الكبرى.

نبذة عن حياة وايلز

Biography of Wiles



ولد: عام ١٩٥٣م في كامبرج، بريطانيا .

حصل أندرو وايلز على شهادة البكالوريوس في الرياضيات من جامعة أوكسفورد وشهادة الدكتوراة من جامعة كامبريج عام ١٩٨٠م. وشغل منصب أستاذ في جامعة هارفرد قبل أن ينتقل إلى وظيفته الحالية كأستاذ الرياضيات في جامعة برنستون.

في حزيران من عام ١٩٩٣م ومن ضمن محاضرة كان يلقيها وايلز في جامعة كامبريج في بريطانيا حول بعض الخصائص الحسابية لنوع خاص من المنحنيات الجبرية شعر الحاضرون أن وايلز في نهاية محاضرته بصدد إعلان نتيجة مهمة جداً والتي يمكن استنتاجها من إحدى المبرهنات التي برهنها. و لم يخب ظن الحاضرون إذ أعلن وايلز عن توصله إلى إثبات لمبرهنة فيرما الكبرى والتي استعصت على جميع محاولات أشهر الرياضيين لما يزيد عن ثلاثة قرون.

لقد بلغ جو الإثارة في قاعة المحاضرات درجة وصفها أحدهم بقوله "عندما اقترب وايلز من نهاية محاضرته شعرنا وكأننا نحلق فوق الأثير" . وقد انتشر الخبر بسرعة عبر وكالات الأنباء العالمية ومحطات الإذاعة والتلفاز. وقد نشرت صحيفة التايم التي تصدر في نيويورك الخبر في صفحتها الأولى، وبلغت الإثارة في الوسط الرياضي إلى الحد الذي قام فيه مجموعة من الرياضيين باستئجار قاعة سينما في سان

فرانسيسكو تتسع لألف ومائتين شخص لإتاحة الفرصة لأكبر عدد من المهتمين بحضور المحاضرة وكانت تباع التذاكر بخمسة دولارات ومع تزايد الطلب عليها بلغ سعرها خمس وعشرون دولاراً في السوق السوداء.

بعد حوالي أربعة شهور من محاضرة وايلز وبتفحص البرهان الذي زاد عن 200 صفحة تبين أن هناك خطأ في البرهان ليعيد مبرهنة فيرما الكبرى إلى مرتبة الحدس مرة أخرى. ولكن وايلز لم ييأس ودأب على تصحيح الخطأ بالتعاون مع أحد طلابه السابقين ريتشارد تايلر *(Richard Taylor)* الذي راجع البرهان وبسط العديد من خطواته. وأعلن عن صحة البرهان في أكتوبر ١٩٩٤م وبهذا طويت صفحة هذه المعضلة التي خلفها لنا فيرما.

لقد نال وايلز عدة جوائز عن إنجازه العلمي أهمها جائزة الملك فيصل العالمية.

الفصل الخامس

الدوال العددية
ARITHMETIC FUNCTIONS

(٥,١) الدوال الضربية
Multiplicative Functions

يرتبط مع العدد الصحيح الموجب n العديد من الخواص العددية، فمثلاً يمكن أن نسأل عن عدد قواسم n الموجبة، أو مجموع هذه القواسم، أو عن عدد الأعداد الأولية نسبياً مع n . إن أي من هذه الخواص دالة مداها مجموعة جزئية من الأعداد الصحيحة. مثل هذه الدوال تسمى الدوال العددية وهي مجموعة من الدوال تهتم نظرية الأعداد بدراسة خواصها. بصورة عامة، تعرف الدالة العددية على أنها متتالية من الأعداد المركبة (a_n) . أي أنها دالة $f:\mathbb{Z}^+\to\mathbb{C}$ حيث $f(n)=a_n$.

إن جل اهتمامنا بدراسة الدوال العددية ينصب في إيجاد صيغة بسيطة لحساب قيمة هذه الدوال عند أي عدد صحيح موجب. ويوجد العديد من الدوال العددية التي تتمتع بصفات خاصة تسهل علينا هذه المهمة مثل الدوال الضربية والتي نعرفها على النحو التالي:

تعريف (٥,١)

إذا كانت f دالة عددية غير صفرية فنقول إن f دالة ضربية (*multiplicative*) إذا كان $f(mn)=f(m)f(n)$ لكل $m,n\in\mathbb{Z}^+$ حيث $(m,n)=1$.

كما نقول إن f دالة ضربية تماماً (*completely multiplicative*) إذا كان $f(mn)=f(m)f(n)$ لكل $m,n\in\mathbb{Z}^+$.

مثال (٥,١)

كل من الدوال العددية التالية ضربية تماماً:

(أ) $U(n)=1$ لكل $n\in\mathbb{Z}^+$.

(ب) $E(n)=n$ لكل $n\in\mathbb{Z}^+$.

(ج) $I(n)=\begin{cases}1, & n=1\\ 0, & n>1\end{cases}$ لكل $n\in\mathbb{Z}^+$ □

مثال (٥,٢)

دالة مانجولد (*Mangoldt*) المعرفة على النحو التالي:

$\Lambda(n)=\begin{cases}\ln(p) & , \ n=p^m\\ 0 & , \ n\neq p^m\end{cases}$ حيث p عدد أولي

دالة غير ضربية لأنه على سبيل المثال:

$\Lambda(2\times5)=\Lambda(10)=0\neq\Lambda(2)\times\Lambda(5)=\ln(2)\times\ln(5)$ □

للحقيقة يوجد اختبار سهل لإثبات أن الدالة غير ضربية هو:

مبرهنة (٥,١)

إذا كانت f دالة ضربية فإن $f(1)=1$.

البرهان

ليكن $n \in \mathbb{Z}^+$ حيث $f(n) \neq 0$. بما أن $(n,1)=1$ فنرى أن

$f(n)=f(n\times 1)=f(n)f(1)$. وبهذا يكون $f(1)=1$ ◆

إذا كانت f دالة ضربية فالمبرهنة التالية تبين لنا أنه لحساب $f(n)$ حيث $n=p_1^{k_1}p_2^{k_2}\dots p_t^{k_t}$ يكفي أن نحسب القيم $f(p_i^{k_i})$.

مبرهنة(٢,٥)

إذا كانت f دالة ضربية وكانت $n_1,n_2,\dots,n_r$ أعداداً صحيحة موجبة أولية نسبياً زوجاً زوجاً فإن:

$$f(n_1n_2\dots n_r)=f(n_1)f(n_2)\dots f(n_r)$$

البرهان

باستخدام الاستقراء الرياضي على r . بما أن f دالة ضربية وأن $(n_1,n_2)=1$ فإن $f(n_1n_2)=f(n_1)f(n_2)$. لذا فالعبارة صحيحة عند $r=2$.

لنفرض الآن أن العبارة صحيحة عند $r=k$. سنبرهن صحة العبارة عند $r=k+1$.

بما أن $(n_1n_2\dots n_k,n_{k+1})=1$ فإن:

$$f(n_1n_2\dots n_k\, n_{k+1})=f(n_1n_2\dots n_k)f(n_{k+1})$$.

ولكن باستخدام فرضية الاستقراء لدينا:

$$f(n_1n_2\dots n_k)=f(n_1)f(n_2)\dots f(n_k)$$

ونرى أن

$$f(n_1n_2\dots n_kn_{k+1})=f(n_1)f(n_2)\dots f(n_k)f(n_{k+1})$$

إذن، العبارة صحيحة عند $r=k+1$ ◆

بتطبيق المبرهنة (٢,٥) نحصل مباشرة على النتيجة الهامة التالية:

نتيجة (٥,٣)

إذا كانت f دالة ضربية وكان $n=p_1^{k_1}p_2^{k_2}\dots p_t^{k_t}$ فإن

◆ $f(n)=f(p_1^{k_1})f(p_2^{k_2})\dots f(p_t^{k_t})$

مبرهنة (٥,٤)

إذا كانت f دالة عددية فإن $\sum_{d|n}f(d)=\sum_{d|n}f(\frac{n}{d})$ حيث $\sum_{d|n}$ تعني أن المجموع مأخوذ على جميع قواسم n الموجبة.

البرهان

لنفرض أن $d_1<d_2<\dots<d_k$ هي جميع قواسم n الموجبة. عندئذ من الواضح أن $\frac{n}{d_1}=d_k,\frac{n}{d_2}=d_{k-1},\dots,\frac{n}{d_k}=d_1$. ولذا فإن:

$$\begin{aligned}\sum_{d|n}f(\frac{n}{d})&=f(\frac{n}{d_1})+f(\frac{n}{d_2})+\dots+f(\frac{n}{d_k})\\&=f(d_k)+f(d_{k-1})+\dots+f(d_1)\\&=\sum_{d|n}f(d)\end{aligned}$$

ونستنتج أن المجموعين متساويين ◆

مبرهنة (٥,٥)

إذا كانت كل من f و g دالة عددية فإن:

$$\sum_{\substack{d|m\\e|n}}f(d)g(e)=\left[\sum_{d|m}f(d)\right]\left[\sum_{e|n}g(e)\right]$$

البرهان

لنفرض أن $d_1,d_2,\dots,d_s$ و $e_1,e_2,\dots,e_t$ هي جميع القواسم الموجبة للعددين m و n على التوالي. عندئذ

$$\sum_{\substack{d|m\\ e|n}} f(d)g(e) = \sum_{j=1}^{s}\sum_{k=1}^{t} f(d_j)g(e_k)$$

$$= \sum_{j=1}^{s} f(d_j)g(e_1) + \sum_{j=1}^{s} f(d_j)g(e_2) + \ldots + \sum_{j=1}^{s} f(d_j)g(e_t)$$

$$= \left[\sum_{j=1}^{s} f(d_j)\right]\left[\sum_{k=1}^{t} g(e_k)\right]$$

$$= \left[\sum_{d|m} f(d)\right]\left[\sum_{e|n} g(e)\right]$$

◆ لاحظ أن جل ما استخدمناه هو خاصية توزيع الضرب على الجمع

المبرهنة التالية تبين لنا إحدى الخواص المهمة جداً للدوال الضربية.

مبرهنة (٥,٦)

إذا كانت f دالة ضربية وكان $G(n) = \sum_{d|n} f(d)$ فإن G دالة ضربية أيضاً.

البرهان

لنفرض أن $m,n \in \mathbb{Z}^+$ حيث $(m,n)=1$. ولنفرض أن $d \mid mn$. باستخدام المبرهنة (٢,٤) يوجد عددان وحيدان $d_1,d_2 \in \mathbb{Z}^+$ حيث $d_1 \mid m$ و $d_2 \mid n$ و $d = d_1d_2$ و $(d_1,d_2)=1$. من هذا نجد أن:

$$G(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m\\ d_2|n}} f(d_1d_2) =$$

$$\sum_{\substack{d_1|m\\ d_2|n}} f(d_1)f(d_2) = \sum_{d_1|m} f(d_1)\sum_{d_2|n} f(d_2) = G(m)G(n)$$

◆ وبهذا تكون G دالة ضربية

ملحوظة

سنبرهن لاحقاً في هذا الفصل أن عكس المبرهنة (٥,٦) صحيح أيضاً.

نقدم الآن بعض الدوال العددية الهامة.

تعريف (٥,٢)

إذا كان $n \in \mathbb{Z}^+$ فإننا نرمز لعدد قواسم n الموجبة بالرمز $\tau(n)$ ولمجموع هذه القواسم بالرمز $\sigma(n)$. وإذا كان $k \in \mathbb{N}$ فنرمز لمجموع قواسم n الموجبة مرفوعة للقوة k بالرمز $\sigma_k(n)$. أي أن:

$$\tau(n)=\sum_{d|n}1 \quad \text{و} \quad \sigma(n)=\sum_{d|n}d \quad \text{و} \quad \sigma_k(n)=\sum_{d|n}d^k$$

مبرهنة(٥,٧)

كل من τ ، σ و σ_k دالة ضربية.

البرهان

بما أن $U(n)=1$ و $E(n)=n$ و $f(n)=n^k$ دوال ضربية فنجد باستخدام المبرهنة (٥,٦) أن الدوال τ و σ و σ_k ضربية ◆

ملحوظة

لاحظ أن جميع الدوال τ و σ و σ_k ليست ضربية تماماً، على سبيل المثال:

$$4=\tau(8)\neq\tau(2)\tau(4)=2\times3=6$$
$$15=\sigma(8)\neq\sigma(2)\sigma(4)=3\times7=21$$
$$85=\sigma_2(8)\neq\sigma_2(2)\sigma_2(4)=5\times21=105$$

نستخدم الآن النتيجة (٥,٣) لإيجاد صيغة مناسبة لحساب كل من $\tau(n)$ و $\sigma(n)$ و $\sigma_k(n)$.

مبرهنة (٥,٨)

إذا كان p عدداً أولياً وكان $\alpha \in \mathbb{Z}^+$ فإن:

(أ) $\tau(p^\alpha)=\alpha+1$.

(ب) $\sigma(p^\alpha)=1+p+p^2+...+p^\alpha=\frac{p^{\alpha+1}-1}{p-1}$.

(ج) $\sigma_k(p^\alpha)=\frac{p^{(\alpha+1)k}-1}{p^k-1}$.

البرهان

لاحظ أن قواسم p^α الموجبة هي $1,p,p^2,...,p^\alpha$ وعددها $\alpha+1$. وينتج عن ذلك أن $\tau(p^\alpha)=\alpha+1$.

كما أن مجموع هذه القواسم هو متتالية هندسية حدها الأول 1 وحدها الأخير هو p^α. وعليه فإن $\sigma(p^\alpha)=\frac{p^{\alpha+1}-1}{p-1}$. وأخيراً :

$$\sigma_k(p^\alpha)=\sum_{d|p^\alpha} d^k=1+p^k+p^{2k}+...+p^{\alpha k}=\frac{p^{(\alpha+1)k}-1}{p^k-1}$$

باستخدام النتيجة (٥,٣) والمبرهنة (٥,٨) نحصل مباشرة على الصيغ التالية لحساب $\tau(n)$ و $\sigma(n)$ و $\sigma_k(n)$.

نتيجة (٥,٩)

إذا كان $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_t^{\alpha_t}$ فإن:

(أ) $\tau(n)=\prod_{i=1}^{t}(\alpha_i+1)$.

(ب) $\sigma(n)=\prod_{i=1}^{t}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$.

(ج) $\sigma_k(n)=\prod_{i=1}^{t}\frac{p_i^{(\alpha_i+1)k}-1}{p_i^k-1}$.

البرهان

نحصـــل على برهان الفقرات الثلاث مباشرة من النتيجـــة (٥,٣) والمبرهنـــة (٥,٨) ◆

مثال (٥,٣)

احسب كل من $\tau(1125)$ ، $\sigma(1125)$ ، $\sigma_2(1125)$.

الحل

بما أن $1125 = 3^2 \times 5^3$ فإن:

$$\tau(1125) = (2+1)(3+1) = 12$$

$$\sigma(1125) = \frac{3^3-1}{3-1} \cdot \frac{5^4-1}{5-1} = 13 \times 156 = 2028$$

$$\sigma_2(1125) = \frac{3^6-1}{3^2-1} \cdot \frac{5^8-1}{5^2-1} = 91 \times 16276 = 1481116 \quad \square$$

مثال (٥,٤)

جد جميع الأعداد الصحيحة $n < 100$ التي تحقق $\tau(n) = 12$.

الحل

لنفرض أن $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$. عندئذ :

$$\tau(n) = (\alpha_1+1)(\alpha_2+1) \dots (\alpha_t+1) = 12$$

الآن : $12 = 4 \times 3 = 2 \times 2 \times 3 = 6 \times 2 = 12 \times 1$.

إذا كان $12 = 4 \times 3$ فـــإن $\alpha_1 = 3$ و $\alpha_2 = 2$. ولـــذا فـــإن $n = p_1^3 p_2^2$. وبمـــا أن $n < 100$ فإن القيمة الوحيدة في هذه الحالة هي $2^3 \times 3^2 = 72$.

إذا كان $12 = 2 \times 2 \times 3$ فـــإن $\alpha_1 = \alpha_2 = 1$ وأن $\alpha_3 = 2$. ونجـــد $n = p_1 p_2 p_3^2$. وقيم n في هذه الحالة هي:

$n = 3 \times 5 \times 2^2 = 60$ ، $n = 3 \times 7 \times 2^2 = 84$ ، $n = 2 \times 5 \times 3^2 = 90$.

إذا كان $12=6\times2$ فإن $\alpha_1=5$ و $\alpha_2=1$. ويكون $n=p_1^5p_2$. وقيمة n الوحيدة في هذه الحالة هي $n=2^5\times3=96$.

وأخيراً، إذا كان $12=12\times1$ فإن $\alpha_1=11$ و $\alpha_2=0$. ومنه فإن $n=p_1^{11}>100$ في هذه الحالة. وبالتالي نجد أن جميع قيم $n<100$ التي تحقق $\tau(n)=12$ هي:

60 ، 72 ، 84 ، 90 ، 96 □

مثال (٥,٥)

جد جميع قيم n التي تحقق $\sigma(n)=60$.

الحل

إذا كان $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_t^{\alpha_t}$ فإن $\sigma(n)=N_1N_2\dots N_t$ حيث $N_i=1+p_i+p_i^2+\dots+p_i^{\alpha_i}$ يقسم 60 لكل $1\le i\le t$. ولكن قواسم 60 هي:

1، 2 ، 3 ، 4 ، 5 ، 6 ، 10 ، 12 ، 15 ، 20 ، 30 ، 60 . الآن:

$N_i\neq1$ لكل عدد أولي p_i

$N_i\neq2$ لكل عدد أولي p_i.

$N_i=3$ إذا وفقط إذا كان $p_i=2$ وفي هذه الحالة $N_i=1+2$.

$N_i=4$ إذا وفقط إذا كان $p_i=3$ وفي هذه الحالة $N_i=1+3$.

$N_i\neq5$ لكل عدد أولي p_i .

$N_i=6$ إذا وفقط إذا كان $p_i=5$. وفي هذه الحالة $N_i=1+5$.

$N_i\neq10$ لكل عدد أولي p_i.

$N_i=12$ إذا وفقط إذا كان $p_i=11$ وفي هذه الحالة $N_i=1+11$.

$N_i=15$ إذا وفقط إذا كان $p_i=2$ وفي هذه الحالة $N_i=1+2+2^2+2^3$.

$N_i=20$ إذا وفقط إذا كان $p_i=19$ وفي هذه الحالة $N_i=1+19$.

$N_i=30$ إذا وفقط إذا كان $p_i=29$ وفي هذه الحالة $N_i=1+29$.

$N_i=60$ إذا وفقط إذا كان $p_i=59$ وفي هذه الحالة $N_i=1+59$.

الآن: $60=3\times20=4\times15=60\times1$

ولذا فإن: $\sigma(n)=60=(1+2)(1+19)=(1+3)(1+2+2^2+2^3)=(1+59)$.

ومنه فإن $n=2\times19$ أو $n=3\times2^3$ أو $n=59$. ونستنتج أن

$n=38$ أو $n=24$ أو $n=59$ هي جميع حلول المعادلة $\sigma(n)=60$ □

(٥,١,١) تمارين محلولة (*Solved Exercises*)

تمرين (١)

جد جميع الأعداد الصحيحة n بحيث يكون $\tau(n)$ عدداً فردياً.

الحل

إذا كان $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_t^{\alpha_t}$ فإن $\tau(n)=(\alpha_1+1)(\alpha_2+1)\dots(\alpha_t+1)$.

الآن $\tau(n)$ فردياً إذا وفقط إذا كان α_i+1 فردياً لكـــل $1\le i\le t$. أي أن $\tau(n)$ فردي إذا وفقط إذا كان α_i زوجياً لكل $1\le i\le t$. وبهذا يكون:

$$n=p_1^{2a_1}p_2^{2a_2}\dots p_t^{2a_t}=(p_1^{a_1}p_2^{a_2}\dots p_t^{a_2})^2$$

أي أن n مربع كامل △

تمرين (٢)

صنف جميع الأعداد الصحيحة الموجبة n حيث $\tau(n)=4$.

الحل

إذا كان $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_t^{\alpha_t}$ فـــإن $\tau(n)=(\alpha_1+1)(\alpha_2+1)\dots(\alpha_t+1)$.

وبمـــا أن $\tau(n)=4$ فـــإن $\alpha_1+1=\alpha_2+1=2$ أو أن $\alpha_1+1=1$ ، $\alpha_2+1=4$.

ونستنتج أن $n=p_1^3$ أو أن $n=p_1p_2$ △

تمرين (٣)

أثبت أن $\left[\sum_{d|n}\tau(d)\right]^2=\sum_{d|n}(\tau(d))^3$.

الحل

بما أن $\tau(n)$ دالة ضربية فإن $(\tau(n))^3$ دالة ضربية. وعليه فإن $\sum_{d|n}(\tau(d))^3$ دالة ضربية. كذلك $\left[\sum_{d|n}\tau(d)\right]^2$ دالة ضربية. ولذا فإنه يكفي إثبات صحة المتطابقة في الحالة $n=p^k$ حيث p عدد أولي. الآن ، الطرف الأيسر للمتطابقة يساوي:

$$\left[\sum_{d|p^k}\tau(d)\right]^2=\left[\sum_{i=0}^{k}\tau(p^i)\right]^2=\left[\sum_{i=0}^{k}(i+1)\right]^2=\left[\sum_{i=1}^{k+1}i\right]^2=\left[\frac{(k+1)(k+2)}{2}\right]^2$$

وأما الطرف الأيمن فهو:

$$\sum_{d|p^k}(\tau(d))^3=\sum_{i=0}^{k}(\tau(p^i))^3=\sum_{i=0}^{k}(i+1)^3=\sum_{i=1}^{k+1}i^3=\left[\frac{(k+1)(k+2)}{2}\right]^2 .$$

وبهذا فإن المتطابقة صحيحة عندما $n=p^k$ وهذا ينهي البرهان △

تمرين (٤)

إذا كان $n\in\mathbb{Z}^+$ فأثبت أن n عدد مؤلف إذا وفقط إذا كان $\sigma(n)>n+\sqrt{n}$.

الحل

لنفرض أولاً أن n عدد مؤلف. عندئذ، $n=ab$ حيث $1<a\le b<n$. ومنه فإن $a\ge\sqrt{n}$ أو أن $b\ge\sqrt{n}$. ويكون:

$$\sigma(n)\ge 1+a+b+n>1+\sqrt{n}+n>\sqrt{n}+n .$$

لبرهان العكس، نفرض أن $\sigma(n)>n+\sqrt{n}$ ونفرض لغرض التناقض أن n عدد أولي. عندئذ: $\sigma(n)=n+1\le n+\sqrt{n}$ وهذا تناقض. إذن، n مؤلف △

تمرين (٥)

إذا كان $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_t^{\alpha_t}$ فأثبت أن:

(أ) $\sum_{d|n}\frac{1}{d}=\frac{\sigma(n)}{n}$ (ب) $\prod_{i=1}^{t}(1-\frac{1}{p_i})<\frac{n}{\sigma(n)}<1$ (ج) $\sum_{k=1}^{n}\frac{1}{k}\le\frac{\sigma(n!)}{n!}$.

الحل

(أ) $\sum_{d|n}\frac{1}{d}=\sum_{d|n}\frac{1}{\frac{n}{d}}=\sum_{d|n}\frac{d}{n}=\frac{1}{n}\sum_{d|n}d=\frac{\sigma(n)}{n}$.

(ب) بما أن $\sigma(n)>n$ فإن $\frac{n}{\sigma(n)}<1$. كما أن:

$$\sigma(n)\prod_{i=1}^{t}(1-\frac{1}{p_i})=\prod_{i=1}^{t}\frac{(p_i^{\alpha_i+1}-1)}{p_i-1}\times\frac{p_i-1}{p_i}=\prod_{i=1}^{t}\frac{p_i^{\alpha_i+1}-1}{p_i}$$

$$=\prod_{i=1}^{t}(p_i^{\alpha_i}-\frac{1}{p_i})<\prod_{i=1}^{t}p_i^{\alpha_i}=n$$

وبالتالي نخلص إلى أن $\prod_{i=1}^{t}(1-\frac{1}{p_i})<\frac{n}{\sigma(n)}<1$.

(ج) باستخدام الفقرة (أ) لدينا:

$$\frac{\sigma(n!)}{n!}=\sum_{d|n!}\frac{1}{d}\ge 1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}=\sum_{k=1}^{n}\frac{1}{k}\quad\triangle$$

تمارين (١,٥)

(١) احسب $\tau(5112)$ ، $\sigma(5112)$ ، $\sigma_2(5112)$.

(٢) احسب $\tau(509)$ ، $\tau(20!)$ ، $\tau(1128)$.

(٣) احسب $\sigma(509)$ ، $\tau(20!)$ ، $\sigma(1128)$.

(٤) احسب $\sigma_2(4)$ ، $\sigma_2(9)$ ، $\sigma_2(36)$.

(٥) احسب $\sigma_3(4)$ ، $\sigma_3(9)$ ، $\sigma_3(36)$.

(٦) أثبت أن $\sigma(n)=2n$ لكل من $n=496$ و $n=8128$.

(٧) أثبت أن $\sigma(n)=3n$ لكل من $n=120$ و $n=672$.

(٨) أثبت أن $\sigma(n)=m^2$ لكل من $n=66$ و $n=4479865$.

(٩) أثبت أن $\sigma[(3^3\times5\times11\times13\times41\times47)^3]=m^2$.

(١٠) أثبت أن $\sigma[(7\times11\times29\times163\times191\times439)^2]=m^3$.

(١١) أثبت أن $\sigma[(3\times7\times11\times29\times37)^2]=m^2$.

(١٢) جد أصغر عدد صحيح موجب n يحقق:

(أ) $\tau(n)=100$ (ب) $\tau(n)=14$

(١٣) جد جميع الأعداد الصحيحة الموجبة n التي تحقق:

(أ) $\sigma(n)=52$ (ب) $\sigma(n)=36$

(ج) $\sigma(n)=72$ (د) $\sigma(n)=51$

(هـ) $\sigma(n)=42$ (و) $\sigma(n)=91$

(١٤) صنف جميع الأعداد الصحيحة n التي تحقق:

(أ) $\tau(n)=2$ (ب) $\tau(n)=3$

(١٥) جد جميع الأعداد الصحيحة n بحيث يكون $\sigma(n)$ عدداً فردياً.

(١٦) أثبت أن $\prod_{d\mid n} d=n^{\tau(n)/2}$ لكل $n>1$.

(١٧) أثبت أن $\sigma(p)=p+1$ إذا وفقط إذا كان p عدداً أولياً.

(١٨) لكل $k>1$ أثبت وجود عدد غير منته من الأعداد n التي تحقق $\tau(n)=k$.

(١٩) هل يوجد $k\in\mathbb{Z}^+$ بحيث يكون للمعادلة $\sigma(n)=k$ عدد غير منته من الحلول؟

(٢٠) أثبت أن $\tau(2^n-1)\geq\tau(n)$ لكل $n>1$.

(٢١) أثبت أن $\tau(n)=\tau(n+1)=\tau(n+2)=\tau(n+3)$ لكل من $n=3655$ و $n=4503$.

(٢٢) أثبت أن $\sigma(n)=\sigma(n+1)$ لكل من $n=957$ و $n=14206$.

(٢٣) أثبت أن $\tau(n)\leq2\sqrt{n}$ لكل $n\geq1$.

(٢٤) إذا كان n عدداً صحيحاً خال من المربعات وكان عدد قواسمه الأولية يساوي r فأثبت أن $\tau(n)=2^r$.

(٢٥) أثبت وجود عدد غير منته من الأعداد m و n بحيث يكون $\sigma(m^2)=\sigma(n^2)$ [ارشاد : $m=5k$ و $n=4k$ حيث k يحقق $(k,10)=1$].

(٢٦) إذا كان p و $p+2$ عددين أوليين فأثبت أن $\sigma(p+2)=\sigma(p)+2$.

(٢٧) إذا كان p عدداً أولياً حيث $p\equiv 1(\text{mod } 4)$ فأثبت أن $\sigma(p^\alpha)\equiv \alpha+1(\text{mod } 4)$.

(٢٨) إذا كان $\sigma(n)$ عدداً أولياً فأثبت أن $n=p^k$ حيث $k\in\mathbb{Z}^+$ و p عدد أولي.

(٢٩) إذا كان $\tau(n)=q$ عدداً أولياً فأثبت أن $n=p^{q-1}$ حيث p عدد أولي.

(٣٠) إذا كانت $f(n)=n^k$ حيث $k\in\mathbb{Z}^+$ فأثبت أن f دالة ضربية تماماً.

(٣١) إذا كانت كل من f و g دالة ضربية وكان $f(p^k)=g(p^k)$ لكل عدد أولي p وكل $k\geq 1$ فأثبت أن $f=g$.

(٣٢) إذا كانت كل من f و g دالة ضربية فأثبت أن كل من fg و $\frac{f}{g}$ دالة ضربية. هل $f+g$ ضربية؟

(٣٣) لتكن f الدالة العددية المعرفة كما يلي:

$$f(n)=\begin{cases}0\ , & n=2k\\ 1\ , & n=2k+1\end{cases}$$

. ولتكن $G(n)=\sum_{d|n} f(d)$.

(ا) أثبت أن f دالة ضربية (ب) أثبت أن G دالة ضربية.

(ج) احسب $G(n)$ حيث $n\in\mathbb{Z}^+$ (د) احسب $G(220)$.

(٣٤) لتكن f دالة عددية معرفة على النحو التالي:

$$f(n)=\begin{cases}1\ , & n=1\\ 2^r\ , & n=p_1^{\alpha_1}p_2^{\alpha_2}\ \dots\ p_r^{\alpha_r}\end{cases}$$

(أ) أثبت أن f دالة ضربية.

(ب) أثبت أن $G(n)=\sum_{d|n} f(d)$ دالة ضربية.

(ج) جد صيغة مناسبة للدالة $G(n)$ باستخدام تحليل العدد n .

(٣٥) لتكن f دالة عددية معرفة على النحو التالي:

$$f(n)=\begin{cases}0\ ,\ n=2k\\ 1\ ,\ n\equiv 1(\text{mod }4)\\ -1\ ,\ n\equiv 3(\text{mod }4)\end{cases}$$

أثبت أن f دالة ضربية.

(٣٦) لنفرض أن $\tau_1(n)=\sum_{d|n}1$ إذا كان $d\equiv 1(\text{mod }4)$. وأن $\tau_3(n)=\sum_{d|n}1$ إذا كان $d\equiv 3(\text{mod }4)$. ولتكن $g(n)=\tau_1(n)-\tau_3(n)$. أثبت أن g دالة ضربية وجد صيغة مناسبة للدالة $g(n)$ باستخدام تحليل العدد n .

(٣٧) أثبت أن $\sum_{d|n}\sigma(d)=\sum_{d|n}\frac{n}{d}\tau(d)$ [إرشاد: كل من الدالتين ضربية].

(٣٨) أثبت أن $\sum_{d|n}\frac{n}{d}\sigma(d)=\sum_{d|n}d\tau(d)$.

(٣٩) إذا كان $n\in\mathbb{Z}^+$ فإن دالة ليوفيل (*Liouville's function*) تعرف على النحو التالي:

$$\lambda(n)=\begin{cases}1\ ,\ n=1\\ (-1)^{k_1+k_2+\dots+k_t}\ ,\ n=p_1^{k_1}p_2^{k_2}\dots p_t^{k_t}\end{cases}$$

(أ) أثبت أن λ دالة ضربية تماماً.

(ب) أثبت أن $\sum_{d|n}\lambda(d)=1$ إذا كان n مربعاً كاملاً وأن $\sum_{d|n}\lambda(d)=0$ إذا لم يكن n مربعاً كاملاً.

(٤٠) إذا كانت g دالة ضربية فأثبت أن كلاً من $f(n)=\sum_{d^2|n}g(d^2)$ و $h(n)=\sum_{d^2|n}g(\frac{n}{d^2})$ دالة ضربية.

(٥,٢) الأعداد التامة
Perfect Numbers

تقسم الأعداد الصحيحة الموجبة إلى ثلاثة أنواع، الأعداد الناقصة *(deficient nmbers)* ، الأعداد التامة *(perfect numbers)* والأعداد الزائدة *(abundant numbers)* . وبما أن الإنسان بطبيعة تكوينه يسعى إلى الكمال (الذي لن يناله بطبيعة الحال) فإن اهتمام الرياضيين انصب على إيجاد الأعداد التامة. ومع ذلك فإنهم لم يستطيعوا اكتشاف الكثير منها حيث أن عدد الأعداد التامة المكتشفة لتاريخ كتابة هذا الكتاب هو 38 عدداً وجميع هذه الأعداد زوجية. (انظر البند (٢,٣)) .

على الرغم من أن إقليدس هو أول من اكتشف صيغة للعدد التام الزوجي إلا أن إثبات ذلك تم بعد ألفي عام حيث برهن أويلر أن هذه الصيغة هي الوحيدة التي تزودنا بالأعداد التامة الزوجية.

تعريف (٥,٣)

نقول إن العدد $n \in \mathbb{Z}^+$ ناقص إذا كان $\sigma(n) < 2n$. ونقول إنه زائداً إذا كان $\sigma(n) > 2n$. كما نقول إنه عدداً تاماً إذا كان $\sigma(n) = 2n$.

مثال (٥,٦)

(أ) العدد 14 عدداً ناقصاً لأن:

$$\sigma(14) = \sigma(2)\sigma(7) = 3 \times 8 = 24 < 2 \times 14 = 28$$

كما أن العدد 21 عدداً ناقصاً لأن:

$$\sigma(21) = \sigma(3)\sigma(7) = 4 \times 8 = 32 < 2 \times 21 = 42$$

(ب) العدد 12 عدداً زائداً لأن:

$$\sigma(12) = \sigma(4)\sigma(3) = 7 \times 4 = 28 > 2 \times 12 = 24 \ .$$

كما أن العدد 105 عدداً زائداً لأن:

$$\sigma(105)=\sigma(3\times5\times7)=\sigma(3)\sigma(5)\sigma(7)=4\times6\times8=288>2\times105$$

(ج) كل من الأعداد 6 ، 28 ، 496 ، 8128 عدداً تاماً لأن:

$$\sigma(6)=\sigma(2)\sigma(3)=3\times4=12=2\times6 \quad .$$

$$\sigma(28)=\sigma(4)\sigma(7)=7\times8=56=2\times28 \quad .$$

$$\sigma(496)=\sigma(2^4\times31)=\frac{2^5-1}{2-1}.\frac{31^2-1}{31-1}=31\times32=2\times496 \quad .$$

$$\sigma(8128)=\sigma(2^6\times127)=\frac{2^7-1}{2-1}.\frac{127^2-1}{127-1}=127\times128=2\times8128 \quad \square$$

لاحظ أن جميع الأعداد التامة المقدمة في المثال السابق هي أعداد زوجية يمكن كتابتها على الصورة $2^{p-1}M_p$ حيث p عدد أولي و M_p عدد ميرسين أولي. سنبرهن الآن أن هذه هي بالفعل الصيغة العامة للأعداد التامة الزوجية.

مبرهنة (٥,١٠)

(أ) [إقليدس]: إذا كان $n=2^{p-1}M_p$ حيث p عدداً أولياً و M_p عدد ميرسين أولي فإن n عدد تام.

(ب) [أويلر] : إذا كان n عدداً تاماً زوجياً فإن $n=2^{p-1}M_p$ حيث p عدد أولي و M_p عدد ميرسين أولي.

البرهان

(أ)

$$\sigma(n)=\sigma(2^{p-1}M_p)=\sigma(2^{p-1}(2^p-1))$$

$$=\sigma(2^{p-1})\sigma(2^p-1)=\frac{2^p-1}{2-1}.2^p$$

$$=2^p(2^p-1)=2\times2^{p-1}M_p=2n$$

وبهذا يكون n عدداً تاماً.

(ب) بما أن n عدد زوجي فإن $n=2^{p-1}m$ حيث $p\in\mathbb{Z}^+$ ، $p\geq2$ و m عدد فردي. وبما أن n تام فإن:

$$2n = 2^p m = \sigma(n) = \sigma(2^{p-1}m) = \sigma(2^{p-1})\sigma(m) = (2^p - 1)\sigma(m)$$

إذن، $(2^p - 1)\sigma(m) = 2^p m$ (١)

ومنه فإن $2^p m \mid (2^p - 1)$. وبما أن $(2^p - 1, 2^p) = 1$ فإن $m \mid (2^p - 1)$. أي أن $m = (2^p - 1)k$ حيث $k \in \mathbb{Z}$. وبالتعويض في المعادلة (١) نجد أن: $\sigma(m) = 2^p k$. وعليه فإن:

$$n = 2^{p-1}m = 2^{p-1}(2^p - 1)k$$

سنبرهن الآن أن $k = 1$. إذا كان $k > 1$ فإن كل من 1 ، k ، m قواسم للعدد m. ولذا فإن:

$$\sigma(m) \geq m + k + 1 = (2^p - 1)k + k + 1 = 2^p k + 1 > \sigma(m)$$

وهذا مستحيل. إذن، $k = 1$. وعليه فإن:

$$n = 2^{p-1}(2^p - 1) \quad ، \quad \sigma(2^p - 1) = 2^p \quad ، \quad m = 2^p - 1$$

سنبرهن الآن أن $2^p - 1$ عدد أولي. إذا كان $2^p - 1$ مؤلفاً فإن له قاسماً r يحقق $1 < r < 2^p - 1$. وحينئذ :

$$\sigma(2^p - 1) \geq 2^p - 1 + r + 1 = 2^p + r > 2^p = \sigma(2^p - 1)$$

وهذا مستحيل. إذن، $2^p - 1$ عدد أولي. وبالتالي فإن p عدد أولي أيضاً ◆

نستنتج من المبرهنة (٥,١٠) وجود تقابل بين أعداد ميرسين الأولية M_p والأعداد التامة الزوجية. وكما بينا في البند (٢,٣) فإن أعداد ميرسين الأولية التي تم اكتشافها حتى تاريخ كتابة هذا الكتاب هي 38 عدداً. وعلى الرغم من ذلك فهناك دلائل قوية توحي بوجود عدد غير منته من الأعداد التامة الزوجية وما زلنا ننتظر البرهان. أما بالنسبة للأعداد التامة الفردية فلم يتوصل أحد إلى اكتشاف أي منها، وإذا افترضنا وجود عدد تام فردي n فلقد تم التوصل إلى اكتشاف العديد من خواص هذا العدد منها:

(١) يوجد للعدد n ثمانية قواسم أولية على الأقل.

(٢) يحتوي تحليل العدد n على 29 عدداً أولياً على الأقل (ليست بالضرورة مختلفة).

(٣) يتكون n من 300 مرتبة عشرية على الأقل.

(٤) يوجد قاسم أولي p للعدد n حيث $p > 10^{20}$.

(٥) يمكن كتابة n على الصورة $n = p_1^{k_1} p_2^{2\alpha_2} p_3^{2\alpha_3} \dots p_t^{2\alpha_t}$ حيث p_i أعداد أولية فردية مختلفة وحيث $p_1 \equiv k_1 \equiv 1 \pmod 4$.

سنقدم هنا برهاناً للخاصية الخامسة.

مبرهنة(٥,١١) [أويلر]

إذا كان n عدداً تاماً فردياً فإن $n = p_1^{k_1} p_2^{2\alpha_2} p_3^{2\alpha_3} \dots p_t^{2\alpha_t}$ حيث $p_1 \equiv k_1 \equiv 1 \pmod 4$ وحيث p_i جميعها أعداد أولية فردية مختلفة.

البرهان

لنفرض أن $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$. بما أن n عدد تام فإن:

$$2n = \sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) \dots \sigma(p_t^{k_t})$$

وبما أن n فردي فإن $n \equiv 1 \pmod 4$ أو $n \equiv 3 \pmod 4$. وفي كلتا الحالتين نجد أن $\sigma(n) = 2n \equiv 2 \pmod 4$. ولذا فإن $2 \mid \sigma(n)$ ولكن $4 \nmid \sigma(n)$. ومنه نجد أن واحداً فقط من الأعداد $\sigma(p_i^{k_i})$ يجب أن يكون زوجياً (ولكنه لا يقبل القسمة على 4) وليكن $\sigma(p_1^{k_1})$ وأما باقي الأعداد فهي فردية.

الآن، لكل p_i نعلم أن $p_i \equiv 1 \pmod 4$ أو أن $p_i \equiv 3 \pmod 4$.

إذا كان $p_i \equiv 1 \pmod 4$ فإن:

$$\sigma(p_i^{k_i}) = 1 + p_i + p_i^2 + \dots + p_i^{k_i}$$
$$\equiv 1 + 1 + 1^2 + \dots + 1^{k_i} \equiv k_i + 1 \pmod 4$$

وبما أن $\sigma(p_1^{k_1}) \equiv 2 \pmod 4$ فإن $k_1 \equiv 1 \pmod 4$. وبما أن $\sigma(p_i^{k_i}) \equiv 1 \pmod 4$ أو $\sigma(p_i^{k_i}) \equiv 3 \pmod 4$ لكل $2 \le i \le t$ فإن $k_i \equiv 0 \pmod 4$ أو

$k_i \equiv 2(\text{mod } 4)$. أي أن k_i عدد زوجي لكل $2 \le i \le t$. وبالتالي فإن العدد n على الصورة المطلوبة في هذه الحالة.

أما إذا كان $p_i \equiv 3(\text{mod } 4)$ فإن:

$$\begin{aligned}\sigma(p_i^{k_i}) &= 1 + p_i + p_i^2 + \ldots + p_i^{k_i} \\ &\equiv 1 + (-1) + (-1)^2 + \ldots + (-1)^{k_i} (\text{mod } 4) \\ &= \begin{cases} 0(\text{mod } 4) & , k_i \text{ فردي} \\ 1(\text{mod } 4) & , k_i \text{ زوجي} \end{cases}\end{aligned}$$

بما أن $\sigma(p_i^{k_i}) \equiv 2(\text{mod } 4)$ فإن $p_1 \not\equiv 3(\text{mod } 4)$. ولذا فإن $p_1 \equiv 1(\text{mod } 4)$. كذلك ، إذا كان $\sigma(p_i^{k_i}) \equiv 0(\text{mod } 4)$ فإن 4 يقسم $\sigma(p_i^{k_i})$ وهذا مستحيل.

إذن، نخلص إلى أنه إذا كان $p_i \equiv 3(\text{mod } 4)$ حيث $2 \le i \le t$ فإن $\sigma(p_i^{k_i}) \equiv 1(\text{mod } 4)$. ومنه فإن k_i زوجي. وبالتالي يكون n على الصورة المطلوبة في هذه الحالة أيضاً ◆

(٥,٢,١) تمارين محلولة (*Solved Exercises*)

تمرين (١)

إذا كان n عدداً تاماً زوجياً فأثبت أن $n \equiv 6(\text{mod } 10)$ أو أن $n \equiv 8(\text{mod } 10)$.

الحل

باستخدام المبرهنة (٥,١٠) نجد أن $n = 2^{p-1}(2^p - 1)$ حيث كل من p و $2^p - 1$ عدداً أولياً. إذا كان $p = 2$ فإن $n = 6$. وبهذا يكون $n \equiv 6(\text{mod } 10)$.

لنفرض الآن أن p عدد فردي . عندئـذ ، $p \equiv 1 \pmod 4$ أو $p \equiv 3 \pmod 4$.
سـنبرهن الآن أن $n \equiv 6 \pmod{10}$ في حالـة كـون $p \equiv 1 \pmod 4$ وأن $n \equiv 8 \pmod{10}$ في حالة كون $p \equiv 3 \pmod 4$.

الحالة $p = 4k+1$: في هذه الحالة لدينا

$$2^{p-1} = 2^{4k} = 16^k \equiv 6 \pmod{10} .$$

وإن: $$2^p - 1 = 2 \times 2^{p-1} - 1 \equiv 2 \times 6 - 1 \equiv 1 \pmod{10}$$

وبهذا يكون $n \equiv 6 \pmod{10}$.

أما في الحالة $p = 4k+3$ فلدينا:

$$2^{p-1} = 2^{4k+2} = 4 \times 16^k \equiv 4 \times 6 \equiv 4 \pmod{10} .$$

وإن: $$2^p - 1 = 2 \times 2^{p-1} - 1 \equiv 2 \times 4 - 1 \equiv 7 \pmod{10} .$$

وبهذا يكون $n \equiv 4 \times 7 \equiv 28 \equiv 8 \pmod{10}$ △

تمرين (٢)

أثبت وجود عدد غير منته من الأعداد الناقصة.

الحل

يوضع $n = p^k$ حيث p عدد أولي فردي و $k \geq 1$. نجد أن:

$$2p^k - \sigma(p^k) = 2p^k - \frac{p^{k+1}-1}{p-1} = \frac{2p^k(p-1) - p^{k+1} + 1}{p-1}$$

$$= \frac{p^k(p-2)+1}{p-1} > 0$$

ولذا فإن $\sigma(p^k) < 2p^k$. إذن، $n = p^k$ عدد ناقص لكل عـدد أولي فـردي p ولكل $k \geq 1$. وهذا يضمن وجود عدد غير منته من الأعداد الناقصة △

تمرين (٣) [ثابت بن قرة]

إذا كان $m,n\in\mathbb{Z}^+$ فنقول إن m و n عددان متحابان (*amicable pair*) إذا كان $\sigma(m)=m+n=\sigma(n)$.

لنفرض أن $p=3\times2^{k-1}-1$ ، $q=3\times2^{k}-1$ ، $r=9\times2^{2k-1}-1$ أعداداً أولية حيث $k>1$. أثبت أن $m=2^k r$ و $n=2^k pq$ عددان متحابان.

الحل

$$\begin{aligned}\sigma(n)&=\sigma(2^k)\sigma(p)\sigma(q)\\&=(2^{k+1}-1)(3\times2^{k-1})(3\times2^{k})=9\times2^{2k-1}(2^{k+1}-1)\\\sigma(m)&=\sigma(2^k)\sigma(r)=(2^{k+1}-1)(9\times2^{2k-1})\\n+m&=2^k[3\times2^{k-1}-1)(3\times2^{k}-1)+(9\times2^{2k-1}-1)]\\&=2^k[9\times2^{2k-1}-3\times2^{k-1}-3\times2^{k}+1+9\times2^{2k-1}-1]\\&=2^k[9\times2^{2k}-3\times2^{k-1}(1+2)]\\&=2^k[9\times2^{2k}-9\times2^{k-1}]\\&=9\times2^{k}\times2^{k-1}(2^{k+1}-1)\\&=9\times2^{2k-1}(2^{k+1}-1)\end{aligned}$$

وبهذا نرى أن $\sigma(n)=n+m=\sigma(m)$ ويكون العددان متحابان △

تمرين (٤)

إذا كان $n\in\mathbb{Z}^+$ فيعرف الوسط التوافقي (*harmonic mean*) $H(n)$ لقواسم العدد n كالتالي: $\dfrac{1}{H(n)}=\dfrac{1}{\tau(n)}\sum_{d\mid n}\dfrac{1}{d}$.

(أ) أثبت أن H دالة ضربية.

(ب) إذا كان $m=2^{p-1}(2^p-1)$ عدداً تاماً فأثبت أن $H(m)=p$ ،

الحل

(أ) باستخدام التمرين المحلول (٥) من تمارين (٥,١,١) لدينا:

$\sum_{d|n}\frac{1}{d}=\frac{\sigma(n)}{n}$. ولذا فإن $H(n)=\frac{n\tau(n)}{\sigma(n)}$.

وبما أن كل من τ و σ و $f(n)=n$ دالة ضربية فإن $H(n)$ دالة ضربية.

(ب) $\triangle\ H(m)=\frac{m\tau(m)}{\sigma(m)}=\frac{m\times p\times 2}{2m}=p$

تمارين (٢,٥)

(١) أثبت أن كل من الأعداد التالية عدداً تاماً:

33550336 ، 8589869056 ، 137438691328 ، $2^{30}(2^{31}-1)$.

(٢) هل $2^{10}(2^{11}-1)$ عدداً تاماً ؟

(٣) هل $2^{28}(2^{29}-1)$ عدداً تاماً ؟

(٤) إذا كان p عدداً أولياً وكان $k\geq 1$ فأثبت أن p^k لا يمكن أن يكون عدداً تاماً.

(٥) إذا كان n عدداً تاماً فأثبت أن $\sum_{d|n}\frac{1}{d}=2$.

(٦) إذا كان n عدداً تاماً وكان m قاسماً فعلياً للعدد n فأثبت أن m لا يمكن أن يكون عدداً تاماً.

(٧) إذا كان n عدداً تاماً أو زائداً فأثبت أن kn عدد زائد لكل $k>1$.

(٨) أثبت أن كل زوج من الأزواج التالية عددان متحابان:

(أ) 220 و 284 (ب) 1184 و 1210 (ج) 79750 و 88730

(د) 10744 و 10856 (هـ) 1111448537712 و 118853793424

(٩) إذا كان n عدداً تاماً زوجياً فأثبت أن $n\equiv 6(\mathrm{mod}\ 10)$ أو أن $n\equiv 28(\mathrm{mod}\ 100)$.

(١٠) إذا كان $n>6$ عدداً تاماً زوجياً فأثبت أن $n\equiv 1(\mathrm{mod}\ 9)$.

(١١) إذا كان كل من p و q عدداً أولياً حيث $pq\neq 6$ فأثبت أن pq عدد ناقص.

(١٢) هل يوجد $k \in \mathbb{Z}^+$ بحيث يكون $3\times5^k\times7$ عدداً زائداً ؟

(١٣) إذا كان n عدداً زائداً وكان $(m,n)=1$ فأثبت أن mn عدد زائد.

(١٤) إذا كان $n=2^{k-1}(2^k-1)$ حيث 2^k-1 مؤلف فأثبت أن n عدد زائد.

(١٥) إذا كان $n=3\times2^k$ حيث $k>1$ فأثبت أن n عدد زائد . استنتج وجود عدد غير منته من الأعداد الزائدة الزوجية.

(١٦) إذا كان $k>1$ حيث k لا يقبل القسمة على كل من 2 ، 3 ، 5 ، 7 فأثبت أن العدد $n=945k$ زائد. استنتج وجود عدد غير منته من الأعداد الزائدة الفردية.

(١٧) إذا كان $n>6$ عدداً تاماً زوجياً فأثبت أن $n\equiv1(\text{mod }6)$.

(١٨) إذا كان n عدداً تاماً فردياً فأثبت أن $n=p^km^2$ حيث p عدد أولي لا يقسم m و $p\equiv k\equiv1(\text{mod }4)$. على وجه الخصوص $n\equiv1(\text{mod }4)$.

(١٩) إذا كان n عدداً تاماً فردياً فأثبت أن $n=pm^2$ حيث p عدد أولي.

(٢٠) إذا كان n عدداً تاماً فردياً فأثبت أن له على الأقل ثلاث قواسم أولية مختلفة.

(٢١) ليكن $n\in\mathbb{Z}^+$. نقول إن n عدد تام من الرتبة k إذا كان $\sigma(n)=kn$. أثبت أن:

(أ) 672 عدد تام من الرتبة 3 (ب) 30240 عدد تام من الرتبة 4

(ج) $14182439040=2^7\times3^4\times5\times7\times11^2\times17\times19$ عدد تام من الرتبة 5.

(د) $2^{23}\times3^7\times5^3\times7^4\times11^2\times13^2\times17^2\times31\times41\times61\times241\times307\times467\times2801$ عدد تام من الرتبة 6.

(٢٢) إذا كان n عدداً تاماً من الرتبة 3 وكان $3\nmid n$ فأثبت أن $3n$ عدد تام من الرتبة 4.

(٥,٣) صيغة موبياس للتعاكس

Möbius Inversion Formula

لتكن f دالة عددية ولتكن $G(n)=\sum_{d|n} f(d)$. بينا في البند (٥,١) أنه إذا كانت f دالة ضربية فإن G كذلك، ولذا ، باستخدام تحليل n إلى قوى عوامله الأولية يكون بالإمكان إيجاد صيغة مناسبة لحساب $G(n)$. في هذا البند سنبرهن العكس، أي أننا سوف نثبت أنه إذا كانت $G(n)=\sum_{d|n} f(d)$ حيث G دالة ضربية فإن f كذلك، كما أننا سنجد صيغة للدالة f بدالة G.

تعريف (٥,٤)

ليكن $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_t^{\alpha_t}$. يرمز لدالة موبياس (*Möbius function*) بالرمز μ وتعرف على النحو التالي:

$$\mu(n)=\begin{cases}1 & , \ n=1\\ (-1)^t & , \ 1\le i\le t \ \text{ لكل } \ \alpha_i=1 \ \text{ إذا كان}\\ 0 & , \ \alpha_i>1 \ \text{ اذا وجد } i \ \text{ حيث}\end{cases}$$

مثال (٥,٧)

بما أن $28=2^2\times 7$ فإن $\mu(28)=0$.

وبما أن $35=5\times 7$ فإن $\mu(35)=(-1)^2=1$.

وبما أن $30=2\times 3\times 5$ فإن $\mu(30)=(-1)^3=-1$ □

مبرهنة (٥,١٢)

(أ) الدالة μ دالة ضربية.

(ب) الدالة $G(n)=\sum_{d|n}\mu(d)$ دالة ضربية.

(ج) $G(n)=I(n)$.

البرهان

(أ) لنفرض أن $m,n \in \mathbb{Z}^+$ حيث $(m,n)=1$. لدينا الحالات الثلاث التالية:

(١) $n=1$ أو $m=1$ ولنعالج فقط الحالة $n=1$. في هذه الحالة لدينا:

$$\mu(mn)=\mu(m)=\mu(m)\times 1=\mu(m)\mu(1)=\mu(m)\mu(n)$$

(٢) $m=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_t^{\alpha_t}$ و $n=q_1^{\beta_1}q_2^{\beta_2}\dots q_s^{\beta_s}$ حيث على الأقل $\alpha_i>1$ أو $\beta_j>1$ ، ولنفرض أن $\alpha_i>1$. عندئذ:

$$\mu(mn)=0=0\times\mu(n)=\mu(m)\mu(n)$$

(٣) $m=p_1p_2\dots p_t$ و $n=q_1q_2\dots q_s$. عندئذ:

$$\mu(mn)=(-1)^{t+s}=(-1)^t(-1)^s=\mu(m)\mu(n)\ .$$

وبالتالي فإن μ ضربية.

(ب) بما أن μ ضربية فباستخدام المبرهنة (٥,٦) نجد أن G دالة ضربية أيضاً.

(ج) إذا كان $n=1$ فإن $G(n)=\sum_{d|n}\mu(d)=\mu(1)=1$.

وإذا كان $n>1$ وكان $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_t^{\alpha_t}$ هو تحليل n إلى قوى عواملـــه الأوليـــة فإن: $G(p_i^{\alpha_i})=\mu(1)+\mu(p_i)+\mu(p_i^2)+\dots+\mu(p_i^{\alpha_i})=1-1+0+\dots+0=0$

ونرى أن $G(n)=G(p_1^{\alpha_1})G(p_2^{\alpha_2})\dots G(p_t^{\alpha_t})=0\times 0\times\dots\times 0=0$.

وبهذا نخلص إلى أن $G(n)=I(n)$ ◆

مبرهنة (٥,١٣) [صيغة موبياس للتعاكس]

إذا كانت كل من f و G دالة عددية حيث $G(n)=\sum_{d|n}f(d)$ فإن:

$$f(n)=\sum_{d|n}G(d)\mu\left(\frac{n}{d}\right)=\sum_{d|n}\mu(d)G\left(\frac{n}{d}\right)$$

البرهان

باستخدام المبرهنة (٥,٤) نجد أن:

$$\sum_{d|n} G(d)\mu(\frac{n}{d}) = \sum_{d|n} \mu(d)\, G(\frac{n}{d}) .$$

الآن : $$\sum_{d|n} \mu(d)G(\frac{n}{d}) = \left(\sum_{d|n} \mu(d)\right)\left(\sum_{c|\frac{n}{d}} f(c)\right) = \sum_{d|n}\sum_{c|\frac{n}{d}} \mu(d)f(c) .$$

ولكن $d \mid n$ و $c \mid \frac{n}{d}$ إذا وفقط إذا كان $c \mid n$ و $d \mid \frac{n}{c}$ (تحقق من ذلك).

ويكون

$$\sum_{d|n}\sum_{c|\frac{n}{d}} \mu(d)f(c) = \sum_{c|n}\sum_{d|\frac{n}{c}} f(c)\mu(d)$$

$$= \left(\sum_{c|n} f(c)\right)\left(\sum_{d|\frac{n}{c}} \mu(d)\right) = \left(\sum_{c|n} f(c)\right) I(\frac{n}{c})$$

ولكن باستخدام المبرهنة (٥,١٢) نعلم أن:

$$I(\frac{n}{c}) = \begin{cases} 1 & , \ \frac{n}{c} = 1 \\ 0 & , \ \frac{n}{c} > 1 \end{cases}$$

وبهذا يكون $\left(\sum_{c|n} f(c)\right) I(\frac{n}{c}) = \sum_{n=c} f(c) = f(n)$.

ونستنتج أن $\sum_{d|n} \mu(d)G(\frac{n}{d}) = f(n)$ ◆

ملحوظة

سنبرهن في البند (٥,٤) أن عكس المبرهنة (٥,١٣) صحيح أيضاً.

نتيجة (٥,١٤)

(أ) $\sum_{d|n} \mu(\frac{n}{d})\tau(d) = 1$ (ب) $\sum_{d|n} \mu(\frac{n}{d})\sigma(d) = n$.

البرهان

(أ) بما أن $\tau(n)=\sum_{d|n}1$ فباستخدام صيغة موبياس للتعاكس نجد أن:

$$1=\sum_{d|n}\mu(\frac{n}{d})\tau(d)$$

(ب) بما أن $\sigma(n)=\sum_{d|n}d$ فإنه باستخدام صيغة موبياس للتعاكس مرة أخرى نجد أن:

$$n=\sum_{d|n}\mu(\frac{n}{d})\sigma(d) \quad \blacklozenge$$

النتيجة التالية هي عكس المبرهنة (٥,٦).

نتيجة (٥,١٥)

إذا كان $G(n)=\sum_{d|n}f(d)$ وكانت G دالة ضربية فإن f دالة ضربية.

البرهان

لنفرض أن $m,n\in\mathbb{Z}^+$ حيث $(m,n)=1$. بما أن $G(n)=\sum_{d|n}f(d)$ فباستخدام صيغة موبياس للتعاكس نجد أن $f(n)=\sum_{d|n}\mu(d)G(\frac{n}{d})$. الآن :

$$f(mn)=\sum_{d|mn}\mu(d)G(\frac{mn}{d})$$

ولكن باستخدام المبرهنة (٢,٤) نعلم أن $d\mid mn$ إذا وفقط إذا وجد $d_1\mid m$ و $d_2\mid n$ حيث $d=d_1d_2$ و $(d_1,d_2)=1$. وبهذا يكون :

$$f(mn)=\sum_{\substack{d_1|m\\ d_2|n}}\mu(d_1d_2)G(\frac{mn}{d_1d_2})$$

$$=\sum_{d_1|m}\mu(d_1)G(\frac{m}{d_1})\sum_{d_2|n}\mu(d_2)G(\frac{n}{d_2}) \qquad \text{(لماذا؟)}$$

$$=f(m)f(n)$$

إذن، f دالة ضربية $\blacklozenge$

في المثال التالي نبين كيفية الاستفادة من صيغة موبياس للتعاكس لإيجاد صيغة ملائمة للدالة f حيث $G(n)=\sum_{d|n} f(d)$.

مثال (٥,٨)

جد صيغة لقيمة $f(n)$ إذا علمت أن $\sum_{d|n} f(d)=n^2$.

الحل

لنفرض أن $G(n)=n^2$. بما أن G ضربية فإن f ضربية، وباستخدام صيغة موبياس للتعاكس لدينا :

$$f(n)=\sum_{d|n}\mu(d)G(\frac{n}{d})=\sum_{d|n}\frac{n^2}{d^2}\mu(d)$$

لنفرض الآن أن $n=p_1^{k_1}p_2^{k_2}\ldots p_t^{k_t}$. عندئذ

$$f(p_i^{k_i})=p_i^{2k_i}[1\times\mu(1)+\frac{1}{p_i^2}\mu(p_i)+\frac{1}{p_i^4}\mu(p_i^2)+\ldots+\frac{1}{p_i^{2k_i}}\mu(p_i^{k_i})]$$

$$=p_i^{2k_i}[1-\frac{1}{p_i^2}+0+\ldots+0]$$

$$=p_i^{2k_i}(1-\frac{1}{p_i^2})$$

ونخلص إلى أن $f(n)=\prod_{i=1}^{t}p_i^{2k_i}(1-\frac{1}{p_i^2})=n^2\prod_{i=1}^{t}(1-\frac{1}{p_i^2})$ □

(٥,٣,١) تمارين محلولة (*Solved Exercises*)

تمرين (١)

لتكن $\Lambda(n)$ دالة مانجولد.

(أ) أثبت أن $\sum_{d|n}\Lambda(d)=\ln(n)$.

(ب) أثبت أن $\Lambda(n)=\sum_{d|n}\ln(d)\mu(\frac{n}{d})=-\sum_{d|n}\ln(d)\mu(d)$.

الحل

(أ) إذا كان $n=1$ فإن $\sum_{d|n}\Lambda(d)=\Lambda(1)=0\times\ln 1$. لنفرض الآن أن $n=p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}$. عندئذ $\ln(n)=\sum_{i=1}^{r}a_i\ln p_i$.

الآن ، نحصل على الحدود غير الصفرية في المجموع $\sum_{d|n}\Lambda(d)$ من القواسم d التي على الصورة p_i^k حيث $k=1,2,\ldots,a_i$ و $i=1,2,\ldots,r$. وعليه نجد أن:

$$\begin{aligned}\sum_{d|n}\Lambda(d)&=\sum_{i=1}^{r}\sum_{k=1}^{a_i}\Lambda(p_i^k)\\&=\sum_{i=1}^{r}\sum_{k=1}^{a_i}\ln p_i\\&=\sum_{i=1}^{r}a_i\ln p_i=\ln(n)\end{aligned}$$

(ب) بما أن $\ln(n)=\sum_{d|n}\Lambda(d)$ فنجد باستخدام صيغة موبياس للتعاكس أن:

$$\begin{aligned}\Lambda(n)&=\sum_{d|n}\mu(d)\ln(\frac{n}{d})\\&=\sum_{d|n}\mu(d)[\ln(n)-\ln(d)]\\&=\ln(n)\sum_{d|n}\mu(d)-\sum_{d|n}\mu(d)\ln(d)\\&=\ln(n)I(n)-\sum_{d|n}\mu(d)\ln(d)\end{aligned}$$

ولكن $\ln(n)I(n)=0$ لكل $n\in\mathbb{Z}^+$. إذن، $\Lambda(n)=-\sum_{d|n}\mu(d)\ln(d)$ △

تمرين (٢)

إذا كانت F دالة ضربية فأثبت أن $\sum_{d|n}\mu(d)F(d)=\prod_{p|n}(1-F(p))$.

الحل

بما أن F دالة ضربية فإن $g(n)=\sum_{d|n}\mu(d)F(d)$ دالة ضربية. الآن

$$g(p^k)=\sum_{d|p^k}\mu(d)F(d)=\mu(1)F(1)+\mu(p)F(p)+0=1-F(p)$$

وبهذا يكون $g(n)=\prod_{p|n}g(p^k)=\prod_{p|n}(1-F(p))$ △

تمرين (٣)

أثبت أن $\sum_{d|n}\frac{\mu^2(d)}{d}=\prod_{p|n}(1+\frac{1}{p})$.

الحل

لنفرض أن $F(n)=\frac{\mu(n)}{n}$. بما أن F دالة ضربية فنجد باستخدام التمـــرين (٢) أعلاه أن :

$$\sum_{d|n}\frac{\mu^2(d)}{d}=\sum_{d|n}\mu(d)F(d)=\prod_{p|n}(1-F(p))=\prod_{p|n}(1-\frac{\mu(p)}{p})$$

ولكن $\mu(p)=-1$. إذن، $\sum_{d|n}\frac{\mu^2(d)}{d}=\prod_{p|n}(1+\frac{1}{p})$ △

تمارين (٣,٥)

(١) أثبت أن $\sum_{k=1}^{n}\mu(k!)=1$ لكل $n\geq 3$.

(٢) أثبت أن $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3)=0$.

(٣) أثبت أن $\sum_{d|n}\frac{\mu(d)}{d}=\prod_{p|n}(1-\frac{1}{p})$ حيث p أولي.

(٤) إذا كان $n=p_1^{\alpha_1}p_1^{\alpha_2}\ldots p_k^{\alpha_k}$ هو تحليل n إلى قوى عوامله الأولية فأثبت أن:

(أ) $\sum_{d|n}|\mu(d)|=2^k$.

(ب) $\sum_{d|n}\mu(d)\tau(d)=(-1)^k$.

(ج) $\sum_{d|n}\mu(d)\sigma(d)=(-1)^k p_1p_2\ldots p_k$.

(د) $\sum_{d|n}d\,\mu(d)=\prod_{i=1}^{k}(1-p_i)$.

(هـ) $\sum_{d|n}\mu(d)\lambda(d)=2^k$ حيث $\lambda(n)$ هي دالة ليوفيل.

(٥) إذا كان $n=p_1^{\alpha_1}p_1^{\alpha_2}\ldots p_k^{\alpha_k}$ هو تحليل n إلى قوى عوامله الأولية فجد صيغة لكل من :

(أ) $\sum_{d|n}\frac{\mu^2(d)}{\tau(d)}$ (ب) $\sum_{d|n}\frac{\mu^2(d)}{\sigma(d)}$.

(٦) إذا كان $n=p_1^{\alpha_1}p_1^{\alpha_2}\ldots p_k^{\alpha_k}$ هو تحليل n إلى قوى عوامله الأولية وكان $G(n)=\sum_{d|n}f(d)$ فجد صيغة للقيمة $f(n)$ إذا علمت أن:

(أ) $G(n)=n$

(ب) $G(n)=\mu(n)$

(ج) $G(n)=(\mu(n))^2$

(د) $G(n)=1$ إذا كان n فردياً و $G(n)=0$ إذا كان n زوجياً.

(٥,٤) دالة أويلر
Euler Function

سبق وأن قدمنا في البند (٣,١) دالة أويلر ورمزنا لها بالرمز φ وعرفنا $\varphi(n)$ على أنه عدد عناصر أي نظام رواسب مختزل قياس n. وهذا يساوي أيضاً عدد الأعداد التي لا تزيد عن n وأولية نسبياً مع n. أي أن $\varphi(n)=|U_n|$.

تعد دالة أويلر من أهم الدوال العددية ولذا فإننا نفرد هذا البند لدراستها، حيث سنبرهن أنها دالة ضربية ونجد صيغة لقيمة $\varphi(n)$ باستخدام تحليل n إلى قوى عوامله الأولية، كما سندرس بعض خواصها المهمة. وفي نهاية البند نحاول إلقاء بعض الضوء على كيفية حل المعادلة $\varphi(x)=m$.

مبرهنة (٥,١٦)

إذا كان p عدداً أولياً فإن $\varphi(p^k)=p^k-p^{k-1}$.

البرهان

الأعداد التي لا تزيد عن p^k وليست أولية نسبياً مع p^k هي: $p,2p,3p,\ldots,(p^{k-1})p$ وعددها p^{k-1} إذن، عدد الأعداد التي لا تزيد عن p^k وأولية نسبياً مع p^k يساوي p^k-p^{k-1}. ونستنتج أن $\varphi(p^k)=p^k-p^{k-1}$ ◆

نتيجة (٥,١٧)

$\varphi(p)=p-1$ إذا وفقط إذا كان p عدداً أولياً.

البرهان

لنفرض أن $\varphi(p)=p-1$. إذا كان p مؤلفاً فإنه يوجد $d \mid p$ حيث $1<d<p$. وبما أن $\varphi(p)\le p-1$ بالتعريف فإننا نجد أن $\varphi(p)\le p-2$ وهذا مستحيل. إذن، p مؤلف. برهان العكس نحصل عليه مباشرة بتطبيق المبرهنة (٥,١٦) ◆

مبرهنة (٥,١٨)

إذا كان $n \in \mathbb{Z}^+$ فإن $\sum_{d|n} \varphi(d) = n$.

البرهان

لنفرض أن $A = \{1, 2, \ldots, n\}$. لكل $d|n$ ضع $A(d) = \{a \in A : (a,n) = d\}$. بما أن القاسم المشترك الأعظم لعددين وحيد فإنه من الواضح أن $A(d) \cap A(d') = \phi$ لكل $d \neq d'$. ومن ذلك نرى أن $\{A(d)\}$ تجزئ للمجموعة A. ومنه فإن $|A| = |\bigcup_{d|n} A(d)| = \sum_{d|n} |A(d)|$.

وبما أن $(a,n) = d$ إذا وفقط إذا كان $(a/d, n/d) = 1$ فنجد أن $A(d) = \{a \in A : (a/d, n/d) = 1\}$. أي أن $A(d)$ هي الأعداد التي لا تزيد عن $\frac{n}{d}$ وأولية نسبياً مع $\frac{n}{d}$. ولذا فإن $|A(d)| = \varphi(\frac{n}{d})$. وبالتالي فإن

$$n = \sum_{d|n} |A(d)| = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d) \quad \blacklozenge$$

مثال (٥,٩)

في هذا المثال نوضح برهان المبرهنة (٥,١٨) عندما $n = 14$. قواسم العدد 14 هي: 1 ، 2 ، 7 ، 14. ولذا فإن $A(1) = \{1,3,5,9,11,13\}$ ، $A(2) = \{2,4,6,8,10,12\}$ ، $A(7) = \{7\}$ و $A(14) = 14$. وبهذا يكون

$$|A(1)| = \varphi(14) = 6 \quad ، \quad |A(2)| = \varphi(7) = 6 \quad ،$$
$$|A(7)| = \varphi(2) = 1 \quad ، \quad |A(14)| = \varphi(1) = 1$$

ومن ذلك نجد أن:

$$\sum_{d|14} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(7) + \varphi(14) = 6 + 6 + 1 + 1 = 14 \quad \square$$

نتيجة (٥,١٩)

إذا كان $n \in \mathbb{Z}^+$ فإن $\varphi(n) = \sum_{d|n} d\,\mu(\frac{n}{d}) = \sum_{d|n} \mu(d)\frac{n}{d}$.

البرهان

باستخدام المبرهنة (٥,١٨) لدينا $\sum_{d|n} \varphi(d) = n$. وباستخدام صيغة موبياس للتعاكس نجد أن $\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = \sum_{d|n} \mu(\frac{n}{d})d$ ◆

سنبرهن الآن أن φ دالة ضربية ونقدم برهانين لذلك.

مبرهنة (٥,٢٠)

φ دالة ضربية.

البرهان الأول

باستخدام المبرهنة (٥,١٨) لدينا $\sum_{d|n} \varphi(d) = n$. وبما أن $G(n) = n$ دالة ضربية فنجد باستخدام النتيجة (٥,١٥) أن φ دالة ضربية.

البرهان الثاني

لنفرض أن $m,n \in \mathbb{Z}^+$ حيث $(m,n)=1$. الآن ، $x \in \mathbb{Z}^+$ أولي نسبياً مع mn إذا وفقط إذا كان x أولي نسبياً مع كل من m و n. لنفرض أن $a < m$ حيث $(a,m)=1$. من الواضح أن متتالية الأعداد : $a, a+m, a+2m, \ldots, a+(n-1)m$ هي نظام رواسب تام قياس n لأنه لو كان $a+jm \equiv a+km \pmod n$ فإن $jm \equiv km \pmod n$. وبما أن $(m,n)=1$ فنجد $j \equiv k \pmod n$ وهذا مستحيل. وبما أن $\{0, 1, 2, \ldots n-1\}$ نظام رواسب تام قياس n فإن كل من أعداد المتتالية يطابق عدداً أصغر من n قياس n . ولذا فإن عدد الأعداد الأولية نسبياً مع n في هذه المتتالية هو $\varphi(n)$. ولكن عدد جميع هذه المتتاليات هو $\varphi(m)$. وبهذا يوجد $\varphi(m)\varphi(n)$ عدداً أولي نسبياً مع كل من m و

n وأصغر من mn. ولكن كل من هذه الأعداد أولي نسبياً مع mn. إذن، نستنتج أن $\varphi(mn)=\varphi(m)\varphi(n)$ ◆

نتيجة (٥,٢١)

إذا كان $n>2$ فإن $\varphi(n)$ عدد زوجي.

البرهان

إذا كان n لا يحتوي على قواسم أولية فردية فإن $n=2^k$ حيث $k\geq 2$. وبهذا يكون فإن $\varphi(n)=\varphi(2^k)=2^{k-1}$ وهذا عدد زوجي. أما إذا كان n يحتوي على قاسم أولي فردي p فإن $n=p^k m$ حيث $(p^k,m)=1$. ومنه نجد أن $\varphi(n)=\varphi(p^k)\varphi(m)=p^{k-1}(p-1)\varphi(m)$. وهذا عدد زوجي لأن $p-1$ قاسم زوجي ◆

نتيجة (٥,٢٢)

إذا كان $\{a_1,a_2,\ldots,a_{\varphi(n)}\}$ نظام رواسب مختزل قياس n وكان $n>2$ فإن $a_1+a_2+\ldots+a_{\varphi(n)}\equiv 0 \pmod n$.

البرهان

بما أن $(a_i,n)=1$ إذا وفقط إذا كان $(n-a_i,n)=1$ لكل $1\leq i\leq\varphi(n)$

فإن: $\{a_1,a_2,\ldots,a_{\varphi(n)}\}=\{n-a_1,n-a_2,\ldots,n-a_{\varphi(n)}\}$.

ولذا فإن: $a_1+a_2+\ldots+a_{\varphi(n)}=(n-a_1)+(n-a_2)+\ldots+(n-a_{\varphi(n)})$.

ومنه فإن: $2(a_1+a_2+\ldots+a_{\varphi(n)})=n\varphi(n)$.

أي أن: $a_1+a_2+\ldots+a_{\varphi(n)}=\frac{1}{2}n\varphi(n)$.

وبما أن $\varphi(n)$ زوجي فنجد

$a_1+a_2+\ldots+a_{\varphi(n)}\equiv 0 \pmod n$ ◆

نجد الآن صيغة لقيمة $\varphi(n)$ ونقدم لذلك برهانين.

نتيجة (٥,٢٣)

إذا كان $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ تحليل n إلى قوى عوامله الأولية فإن:

$$\varphi(n) = \prod_{i=1}^{t} (p_i^{k_i} - p_i^{k_i - 1}) = n \prod_{i=1}^{t} (1 - \frac{1}{p_i}) .$$

البرهان الأول

باستخدام المبرهنة (٥,١٦) لدينا $\varphi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i - 1}$.

وبما أن φ ضربية فإن:

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \dots \varphi(p_t^{k_t}) \\
&= (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1}) \dots (p_t^{k_t} - p_t^{k_t - 1}) \\
&= p_1^{k_1} p_2^{k_2} \dots p_t^{k_t} (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_t}) \\
&= n \prod_{i=1}^{t} (1 - \frac{1}{p_i})
\end{aligned}$$

البرهان الثاني

باستخدام النتيجة (٥,١٩) لدينا $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$. ولكن

$$\begin{aligned}
\varphi(p_i^{k_i}) &= \mu(1) p_i^{k_i} + \mu(p_i) p_i^{k_i - 1} + \mu(p_i^2) p_i^{k_i - 2} + \dots + \mu(p_i^{k_i}) \mu(1) \\
&= p_i^{k_i} - p_i^{k_i - 1} + 0 + \dots + 0 \\
&= p_i^{k_i} - p_i^{k_i - 1} = p_i^{k_i} (1 - \frac{1}{p_i})
\end{aligned}$$

وبما أن φ ضربية فنستنتج أن

◆ $\varphi(n) = \prod_{i=1}^{t} (p_i^{k_i} - p_i^{k_i - 1}) = n \prod_{i=1}^{t} (1 - \frac{1}{p_i})$

مثال (٥,١٠)

جد كل من $\varphi(7865)$ و $\varphi(39616304)$.

الحل

بما أن $7865 = 5\times11^2\times13$ فإن:

$$\varphi(7865) = 7865\,(1-\frac{1}{5})(1-\frac{1}{11})(1-\frac{1}{13}) = 5280 .$$

وبما أن $39616304 = 2^4\times7^2\times13^3\times23$ فإن:

$$\varphi(39616304) = 39616304(1-\frac{1}{2})(1-\frac{1}{7})(1-\frac{1}{13})(1-\frac{1}{23}) = 14990976 \quad \square$$

(٥,٤,١) حل المعادلة $\varphi(x)=m$ $\qquad$ **(Solving $\varphi(x)=m$)**

إذا كان $m\in\mathbb{Z}^+$ فلدينا الحالات التالية لحل المعادلة $\varphi(x)=m$.

(أ) $m=1$: في هذه الحالة $x=1$ و $x=2$ هما الحلان الوحيدان.

(ب) $m>1$ عدد فردي. باستخدام النتيجة (٥,٢١) نعلم أن $\varphi(x)$ عدد زوجي. ولذا فإنه لا يوجد حل للمعادلة في هذه الحالة.

(ج) $m>1$ عدد زوجي: في الحقيقة لا توجد صيغة عامة لحل المعادلة $\varphi(x)=m$ في هذه الحالة ولكننا سنحاول تقديم طريقة يمكن استخدامها لإيجاد جميع الحلول.

لنفرض أن $x=\prod_{i=1}^{t}p_i^{k_i}$ هو تحليل x إلى قوى عواملـه الأولية وأن $\varphi(x)=m$. عندئذ:

$$\varphi(x)=\prod_{i=1}^{t}(p_i^{k_i}-p_i^{k_i-1})=\prod_{i=1}^{t}p_i^{k_i-1}(p_i-1)=\prod_{i=1}^{t}p_i^{k_i-1}d_i$$
$$=\prod_{i=1}^{t}p_i^{k_i}(\frac{d_i}{p_i})=x\prod_{i=1}^{t}\frac{d_i}{p_i}=m$$

وبهذا نجد أن $x=m\prod_{i=1}^{t}p_i \;/\; \prod_{i=1}^{t}d_i$ حيث $d_i=p_i-1$ لكل $1\le i\le t$.

لاحظ أن d_i يجب أن يحقق:

(١) d_i+1 عدد أولي.

(٢) d_i قاسم موجب للعدد m .

(٣) $m \,/\, \prod_{i=1}^{t} d_i$ عدد صحيح أي قاسم أولي له يجب أن يكون أحد قواسم $\prod_{i=1}^{t} p_i$ الأولية.

مثال (٥,١١)

جد جميع حلول المعادلة $\varphi(x)=80$.

الحل

القواسم الموجبة للعدد 80 هي: $1,2,4,5,8,10,16,20,40,80$. ولكن قيم d_i المختلفة هي: $1,2,4,10,16,40$ لأن هذه هي فقط القواسم التي يكون فيها d_i+1 عدداً أولياً. ولذا فإن قيم $\prod_{i=1}^{t} d_i$ التي تحقق الشروط الثلاث أعلاه هي:

1×4 ، 1×10 ، 1×40 ، 2×40 ، $1\times2\times4$ ، $1\times2\times10$ ،

$1\times2\times40$، $1\times4\times10$ ، $2\times4\times10$ ، $1\times2\times4\times10$.

والجدول التالي يبين قيم x التي تحقق $\varphi(x)=80$:

$\prod_{i=1}^{t} d_i$	$80/\prod_{i=1}^{t} d_i$	$\prod_{i=1}^{t} p_i$	$80\prod_{i=1}^{t} p_i \,/\, \prod_{i=1}^{t} d_i = x$
1×4	$2^2\times5$	2×5	$2^3\times5^2 = 200$
1×10	2^3	2×11	$2^4\times11 = 176$
1×40	2	2×41	$2^2\times41 = 164$
2×40	1	3×41	$3\times41 = 123$
$1\times2\times4$	2×5	$2\times3\times5$	$2^2\times3\times5^2 = 300$
$1\times2\times10$	2^2	$2\times3\times11$	$2^3\times3\times11 = 264$
$1\times2\times40$	1	$2\times3\times41$	$2\times3\times41 = 246$
$1\times4\times10$	2	$2\times5\times11$	$2^2\times5\times11 = 220$
$2\times4\times10$	1	$3\times5\times11$	$3\times5\times11 = 165$
$1\times2\times4\times10$	1	$2\times3\times5\times11$	$2\times3\times5\times11 = 330$

□

ملحوظة

إذا علمنا مسبقاً عدد حلول المعادلة $\varphi(x)=m$ فإنه من الممكن كتابة $x=n_1n_2\dots n_k$ حيث $(n_i,n_j)=1$ لكل $i\neq j$. ومنه فإن $\varphi(x)=\varphi(n_1)\varphi(n_2)\dots\varphi(n_k)$. ولذا فنبحث عن القيم $\varphi(n_1),\varphi(n_2),\dots,\varphi(n_k)$ بحيث يكون $\varphi(n_1)\varphi(n_2)\dots\varphi(n_k)=m$ وحيث n_i أولية نسبياً زوجاً زوجاً . سنوضح ذلك في المثال التالي:

مثال (٥,١٢)

جد جميع حلول المعادلة $\varphi(x)=16$ إذا علمت أن عددها 6 .

الحل

لاحظ أن:

$$\varphi(1)\varphi(17)=1\times16=16$$
$$\varphi(1)\varphi(32)=1\times16=16$$
$$\varphi(2)\varphi(17)=1\times16=16$$
$$\varphi(5)\varphi(8)=4\times4=16$$
$$\varphi(3)\varphi(16)=2\times8=16$$
$$\varphi(5)\varphi(12)=4\times4=16$$

وبهذا تكون حلول المعادلة $\varphi(x)=16$ هي:

$$1\times17=17\ ،\ 1\times32=32\ ،\ 2\times17=34\ ،\ 5\times8=40\ ،$$
$$3\times16=48\ ،\ 5\times12=60\ \square$$

(٥,٤,٢) تمارين محلولة *(Solved Exercises)*

تمرين (١)

أثبت أن $\varphi(2n)=\varphi(n)$ إذا وفقط إذا كان n عدداً فردياً.

الحل

لنفرض أن $\varphi(2n)=\varphi(n)$. ولنفرض لغرض التناقض أن n عدد زوجي. عندئذ، $n=2^k m$ حيث m عدد فردي و $k\geq 1$. ومنه فإن $\varphi(2n)=\varphi(2^{k+1})\varphi(m)=2^k\varphi(m)$ وإن $\varphi(n)=\varphi(2^k)\varphi(m)=2^{k-1}\varphi(m)$.

ومن ثم فإن $\varphi(2n)\neq\varphi(n)$ وهذا تناقض. وبهذا يكون n عدداً فردياً.

وبالعكس، لنفرض أن n عدد فردي. حينئذ $(2,n)=1$ ويكون

$$\triangle\quad \varphi(2n)=\varphi(2)\varphi(n)=1\times\varphi(n)=\varphi(n)$$

تمرين (٢)

أثبت أن $\varphi(mn)=m\varphi(n)$ إذا وفقط إذا كان كل قاسم أولي للعدد m هو قاسم أولي للعدد n. ومن ثم استنتج أن $\varphi(n^k)=n^{k-1}\varphi(n)$ لكل $k\geq 1$.

الحل

لنفرض أن $N_k=\prod_{p|k}(1-\frac{1}{p})$. ولنفرض أولاً أن كل قاسم أولي للعدد m يقسم العدد n. حينئذ، من الواضح أن $N_{mn}=N_n$. وبالتالي فإن $\varphi(mn)=mnN_{mn}=m(nN_n)=m\varphi(n)$.

وبالعكس ، لنفرض أن $\varphi(mn)=m\varphi(n)$. عندئذ

$$mn\prod_{p|mn}(1-\frac{1}{p})=m\,(n\prod_{p|n}(1-\frac{1}{p}))$$

ومنه فإن $N_{mn}=N_n$. ولنفرض لغرض التناقض أن p قاسم أولي للعدد m ولكن p لا يقسم n. من هذا يكون $(1-\frac{1}{p})$ أحد قواسم N_{mn} ولكنه لا يقسم N_n وهذا مستحيل لأن $N_{mn}=N_n$.

وأخيراً ، بما أن أي قاسم أولي للعدد n^{k-1} هو قاسم أولي للعدد n فنجد أن

$$\triangle\quad \varphi(n^k)=\varphi(n^{k-1}n)=n^{k-1}\varphi(n)$$

تمرين (٣)

أثبت أن $\varphi(mn)=\frac{\varphi(m)\varphi(n)d}{\varphi(d)}$ حيث $d=(m,n)$.

الحل

لنفرض أن $N_k=\prod_{p|k}(1-\frac{1}{p})$. عندئذ :

$$\frac{\varphi(mn)}{mn}=N_{mn}=\frac{N_m N_n}{N_d}=\frac{\frac{\varphi(m)}{m}\frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}}$$

وبهذا يكون $\varphi(mn)=\frac{\varphi(m)\varphi(n)d}{\varphi(d)}$ △

تمرين (٤)

أثبت أن $\frac{n}{\varphi(n)}=\sum_{d|n}\frac{\mu^2(d)}{\varphi(d)}$.

الحل

لنفرض أن $G(n)=\frac{\mu(n)}{\varphi(n)}$. بما أن كل من μ و φ دالة ضربية فإن G دالة ضربية. ولذا باستخدام تمرين (٢) من التمارين المحلولة (١,٣,٥) نجد أن:

الآن: $\sum_{d|n}\mu(d)G(d)=\prod_{p|n}(1-G(p))$.

$$\sum_{d|n}\frac{\mu^2(d)}{\varphi(d)}=\sum_{d|n}\mu(d)G(d)=\prod_{p|n}(1-G(p))$$

$$=\prod_{p|n}(1-\frac{\mu(p)}{\varphi(p)})=\prod_{p|n}(1-\frac{-1}{p-1})$$

$$=\prod_{p|n}(\frac{p}{p-1})$$

ومن ناحية أخرى لدينا:

$$\frac{n}{\varphi(n)}=\frac{n}{n\prod_{p|n}(1-\frac{1}{p})}=\prod_{p|n}(\frac{p}{p-1})$$

وبهذا يكون $\frac{n}{\varphi(n)}=\sum_{d|n}\frac{\mu^2(d)}{\varphi(d)}$ △

تمرين (٥)

إذا كان m عدداً زوجياً فأثبت وجود عدد منته من الحلول للمعادلة $\varphi(x)=m$.

الحل

لنفرض أن $x=p_1^{a_1}p_2^{a_2}\dots p_t^{a_t}$. عندئذ، $\prod_{i=1}^{t}(p_i^{a_i}-p_i^{a_i-1})=m$. وبما أنه يوجد عدد منته من الطرق لتحليل m كحاصل ضرب أعداد صحيحة فنخلص إلى وجود عدد منته من الأعداد x التي تحقق $\varphi(x)=m$ △

تمرين (٦)

إذا كان $m=2^k b$ حيث b عدد فردي وكان $\varphi(x)=m$ فأثبت أنه يوجد على الأكثر k قاسم أولي فردي للعدد x.

الحل

إذا كان $x=p_1^{a_1}p_2^{a_2}\dots p_t^{a_t}$ فإن

$$\varphi(x)=p_1^{a_1-1}p_2^{p_2-1}\dots p_t^{a_t-1}(p_1-1)(p_2-1)\dots(p_t-1)=2^k b.$$

إذا كان p_i قاسماً أولياً فردياً للعدد x فإن $p_i - 1$ يسهم بقاسم يساوي 2 على الأقل في قيمة $\varphi(x)$. وبما أنه يوجد بالضبط k من قواسم m كل منها يساوي 2 فمن الواضح أن عدد القواسم الفردية للعدد x هي على الأكثر k △

تمرين (٧)

جد جميع قيم x بحيث لا يقبل العدد $\varphi(x)$ القسمة على العدد 4 .

الحل

لنفرض أولاً أن $x = 2^a$ حيث $a \geq 1$. بما أن $\varphi(x) = 2^{a-1}$ وأن 4 لا يقسم $\varphi(x)$ فإن $a = 1$ أو إن $a = 2$. ولذا فإن $x = 2$ أو $x = 4$.

لنفرض الآن أن $x = 2^a m$ حيث $m > 1$ عدد فردي.

بما أن 4 لا يقسم $\varphi(x)$ فباستخدام التمرين (٦) السابق يوجد على الأكثر قاسم أولي فردي واحد للعدد x. ولذا فإن $x = 2^a p^k$ حيث $k \geq 1$ و p عدد أولي فردي.

إذا كان $p \equiv 1 \pmod 4$ فإن $4 \mid (p-1)$. ولذا فإن $p \equiv 3 \pmod 4$. وفي هذه الحالة يقبل $\varphi(p^k)$ القسمة على 2 ولا يقبل القسمة على 4. وبالتالي فإن a يجب أن يجعل $\varphi(2^a)$ فردي. أي أن $a = 0$ أو $a = 1$. ومن ثم فإن $x = p^k$ أو $x = 2p^k$.

وبالتالي فإن جميع قيم x بحيث 4 لا يقسم $\varphi(x)$ هي:

1 ، 2 ، 4 ، p^k ، $2p^k$ حيث p عدد أولي على الصورة $4t+3$ △

تمارين (٤,٥)

(١) جد قيمة كل مما يلي:

(أ) $\varphi(5040)$ (ب) $\varphi(496125)$

(ج) $\varphi(2003)$ (د) $\varphi(8316)$

(هـ) $\varphi(30030)$ (و) $\varphi(10!)$

(٢) أثبت أن $\varphi(5188)=\varphi(5187)=\varphi(5186)$.

(٣) جد جميع قيم x التي تحقق المعادلة $\varphi(x)=m$ لكل مما يلي:

(أ) $\varphi(x)=24$ (ب) $\varphi(x)=30$

(ج) $\varphi(x)=72$ (د) $\varphi(x)=243$

(٤) أثبت عدم وجود حل للمعادلة $\varphi(x)=2\times 7^m$ حيث $m\geq 1$ [إرشاد: استخدم التمرين (٧) من التمارين المحلولة (١,٤,٥)]

(٥) أثبت عدم وجود حل للمعادلة $\varphi(x)=2\times 13^m$ حيث $m\geq 1$.

(٦) أثبت عدم وجود حل للمعادلة $\varphi(x)=2\times 11^{2m}$ حيث $m\geq 1$.

(٧) أثبت عدم وجود حل للمعادلة $\varphi(x)=2\times 3^{4m+3}$ حيث $m\geq 1$.

(٨) جد جميع قيم n التي تحقق $\varphi(n)=n-2$.

(٩) إذا كان $d \mid n$ فأثبت أن $\varphi(d)\mid\varphi(n)$.

(١٠) إذا كان n عدداً زوجياً فأثبت أن $\varphi(n)=\frac{n}{2}$ إذا وفقط إذا كان $n=2^k$ حيث $k\geq 1$.

(١١) إذا كان $\varphi(n)$ يقسم $n-1$ فأثبت أن n خالٍ من المربعات.

(١٢) أثبت أن $\frac{\varphi(n)}{n}=\frac{\varphi(m)}{m}$ إذا وفقط إذا كانت قواسم m الأولية هي قواسم n الأولية نفسها.

(١٣) جد أصغر عدد صحيح موجب n يحقق $\frac{\varphi(n)}{n}<\frac{1}{4}$.

(١٤) جد جميع قيم n التي تحقق التطابق $\varphi(n)\equiv 2(\mathrm{mod}\ 4)$.

(١٥) أثبت أن $\varphi(n)=\frac{n}{3}$ إذا وفقط إذا كان $n=2^k\times 3^m$ حيث $k\geq 1$ و $m\geq 1$.

(١٦) أثبت أن $\varphi(n)\mid n$ إذا وفقط إذا كان $n=1$ أو $n=2^k$ أو $n=2^k3^j$ حيث $k,j\in\mathbb{Z}^+$.

(١٧) إذا كان $6 \mid n$ فأثبت أن $\varphi(n) \le \frac{n}{3}$.

(١٨) أثبت أنه يوجد عدد غير منته من الأعداد الصحيحة n بحيث يكون $\varphi(n)$ مربعاً كاملاً.

(١٩) أثبت أن $\varphi(n^2)+\varphi((n+1)^2) < 2n^2$ لكل $n \ge 3$.

(٢٠) إذا كان p عدداً أولياً حيث $2p+1$ مؤلف فأثبت استحالة وجود حل للمعادلة $\varphi(x) = 2p$.

(٢١) استخدم التمرين (٢٠) لإثبات وجود عدد غير منته من الأعداد الزوجية m التي تجعل المعادلة $\varphi(x) = m$ مستحيلة الحل.

(٢٢) جد عدد غير منته من الأعداد الصحيحة n التي تحقق $\varphi(n) = \varphi(n+2)$ [إرشاد: $n = 2(2p-1)$ حيث كل من p و $2p-1$ أولي فردي].

(٢٣) أثبت أن $\frac{1}{2}\sqrt{n} \le \varphi(n) \le n$ لكل $n \in \mathbb{Z}^+$.

(٢٤) إذا كان $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ فأثبت أن $\varphi(n) \ge \frac{n}{2^t}$.

(٢٥) إذا كان n عدداً مؤلفاً فأثبت أن $\varphi(n) \le n - \sqrt{n}$.

(٢٦) أثبت أن $\sigma(n)\varphi(n) \ge n^2 \prod_{p \mid n} (1-\frac{1}{p^2})$.

(٢٧) أثبت أن $\tau(n)\varphi(n) \ge n$.

(٢٨) إذا كان $\varphi(n)+\sigma(n) = n\tau(n)$ فأثبت أن n عدد أولي.

(٢٩) (أ) إذا كانت $p_1, p_2, \dots p_t$ أعداد أولية مختلفة وكان $N = p_1 p_2 \dots p_t$ فأثبت وجود عدد أولي $p \mid \varphi(N)$ حيث $p \ne p_i$ لكل $1 \le i \le t$.

(ب) استخدم الفقرة (أ) لإثبات وجود عدد غير منته من الأعداد الأولية.

(٣٠) إذا كان p عدداً أولياً وكان $k \ge 2$ فأثبت أن $\varphi(\varphi(p^k)) = p^{k-2}(\varphi(p-1)^2$.

(٣١) أثبت أن:

$$\sum_{d|n}(-1)^{\frac{n}{d}}\varphi(d)=\begin{cases}0 & , \quad n \quad \text{زوجي}\\ -n & , \quad n \quad \text{فردي}\end{cases}$$

(٣٢) أثبت أن $\sum_{d|n}\mu(d)\varphi(d)=\prod_{p|n}(2-p)$.

(٣٣) إذا كان $n=p_1^{k_1}p_2^{k_2}\dots p_t^{k_t}$ فأثبت أن:

$$\sum_{d|n}d\,\varphi(d)=\prod_{i=1}^{t}\left(\frac{p_i^{2k_i+1}+1}{p_i+1}\right).$$

(٣٤) إذا كان $n=p_1^{k_1}p_2^{k_2}\dots p_t^{k_t}$ فأثبت أن:

$$\sum_{d|n}\frac{\varphi(d)}{d}=\prod_{i=1}^{t}\left(\frac{1+k_i(p_i-1)}{p_i}\right).$$

(٥,٥) ضرب دريشليه
The Dirichlet Product

لقد تعرضنا في البنود السابقة من هذا الفصل إلى أمثلة لمجموع دوال عددية على القواسم الموجبة لعدد n. وفي هذا البند نقدم تعميم لهذه المفاهيم.

تعريف (٥,٥)

إذا كانت كل من f و g دالة عددية فإننا نعرف ضرب دريشليه أو التلاف (Dirichlet product or convolution) $f*g$ على النحو التالي:

$$(f*g)(n)=\sum_{d|n}f(d)\,g\left(\frac{n}{d}\right)=\sum_{de=n}f(d)\,g(e)$$ حيث $e=\frac{n}{d}$.

مثال(٥,١٣)

لقد بينا في المبرهنة (٥,١٨) أن $n=\sum_{d|n}\varphi(d)$. ولذا باستخدام الدالتين $U(n)=1$ و $E(n)=n$ نجد أن $E(n)=\sum_{d|n}\varphi(d)\,U(\frac{n}{d})$ لكل $n\in\mathbb{Z}^+$. أي أن $\varphi*U=E$ □

مثال (٥,١٤)

لقد أثبتنا في المبرهنة (٥,١٢) أن $I(n)=\sum_{d|n}\mu(d)\,U(\frac{n}{d})$. من هذا نرى أن $\mu*U=I$ □

مثال (٥,١٥)

لقد أثبتنا في النتيجة (٥,٢٠) أن $\varphi(n)=\sum_{d|n}\mu(d)\frac{n}{d}=\sum_{d|n}d\,\mu(\frac{n}{d})$.

إذن، $E*\mu=\mu*E=\varphi$ □

مثال (٥,١٦)

لقد أثبتنا في النتيجة (٥,١٤) أن $U(n)=\sum_{d|n}\mu(\frac{n}{d})\tau(d)$ وأن $E(n)=\sum_{d|n}\mu(\frac{n}{d})\sigma(d)$. إذن، $\mu*\tau=U$ و $\mu*\sigma=E$ □

مثال (٥,١٧)

لاحظ أن $\tau(n)=\sum_{d|n}1=\sum_{d|n}U(d)\,U(\frac{n}{d})$. عندئذ، $\tau=U*U$.

كذلك $\sigma(n)=\sum_{d|n}d=\sum_{d|n}E(d)U(\frac{n}{d})$. ونستنتج أن $\sigma=E*U$ □

تزودنا المبرهنة التالية بالخواص الجبرية الأساسية لضرب دريشليه.

مبرهنة (٥,٢٤)

إذا كانت f ، g ، h دوال عددية فإن:

(١) $f*g=g*f$.

(٢) $(f*g)*h=f*(g*h)$.

(٣) $f*I=I*f=f$.

البرهان

(١)

$$(f*g)(n)=\sum_{de=n}f(d)g(e)=\sum_{ed=n}g(e)f(d)=\sum_{de=n}g(d)f(e)=(g*f)(n)$$

(٢)

$$((f*g)*h)(n)=\sum_{dc=n}(f*g)(d)h(c)$$

$$=\sum_{dc=n}\left(\sum_{ab=d}f(a)f(b)\right)h(c)$$

$$=\sum_{abc=n}f(a)g(b)h(c)$$

وبالمثل ،

$$(f*(g*h))(n)=\sum_{ae=n}f(a)(g*h)(e)$$

$$=\sum_{ae=n}f(a)\left(\sum_{ab=e}g(b)\,h(c)\right)$$

$$=\sum_{abc=n}f(a)\,g(b)\,h(c)$$

ونستنتج أن $(f*g)*h=f*(g*h)$.

(٣) لاحظ أن $(f*I)(n)=\sum_{de=n}f(d)I(e)=\sum_{d=n}f(d)=f(n)$

لأن $I(e)=1$ إذا كان $e=1$ وأن $I(e)=0$ إذا كان $e\neq 1$.

إذن، $f*I=f$. وبما أن $*$ إبدالية فإن $f=f*I$ أيضاً ◆

إذا كانت f دالة عددية حيث $f(1)\neq 0$ فإن المبرهنة التالية تبين لنا أن للدالة f معكوس بالنسبة لضرب دريشليه $*$.

مبرهنة (٥,٢٥)

لتكن f دالة عددية حيث $f(1)\neq 0$ ولتكن g الدالة العددية المعرفة استقرائياً على النحو التالي:

$$g(1)=\frac{1}{f(1)} \text{ و } g(n)=-\frac{1}{f(1)}\sum_{\substack{d|n\\ d<n}} g(d)\,f\left(\frac{n}{d}\right) \text{ لكل } n>1 .$$

عندئذ، $f*g=g*g=I$.

البرهان

بما أن $*$ عملية إبدالية فإنه يكفي إثبات أن

$$(f*g)(n)=\sum_{d|n} g(d)f\left(\frac{n}{d}\right)=I(n)=\begin{cases}1 & ,n=1\\ 0 & ,n>1\end{cases} .$$ الآن

$$(g*f)(1)=\sum_{d|n} g(d)\,f\left(\frac{1}{d}\right)=g(1)f(1)=\frac{1}{f(1)}f(1)=1=I(1) .$$

وإذا كان $n>1$ فإن:

$$(g*f)(n)=\sum_{d|n} g(d)\,f\left(\frac{n}{d}\right)=g(n)f(1)+\sum_{\substack{d|n\\ d<n}} g(d)f\left(\frac{n}{d}\right)$$

$$=-\frac{f(1)}{f(1)}\sum_{\substack{d|n\\ d<n}} g(d)f\left(\frac{n}{d}\right)+\sum_{\substack{d|n\\ d<n}} g(d)f\left(\frac{n}{d}\right)$$

$$=0=I(n)$$

ونخلص إلى أن $g*f=I$ ◆

تعريف (٥,٦)

تسمى الدالة g المعرفة في المبرهنة (٥,٢٥) معكوس الدالة f ويرمز لها عادة بالرمز f^{-1} .

مبرهنة (٥,٢٦)

إذا كانت كل من f و g دالة عددية حيث $f(1)\neq 0$ و $g(1)\neq 0$ فإن $(f*g)(1)\neq 0$.

البرهان

◆ $(f*g)(1)=\sum_{d|n} f(d)g(\frac{1}{d})=f(1)g(1)\neq 0$

ملحوظات

(١) لتكن G مجموعة جميع الدوال العددية f حيث $f(1)\neq 0$. من المبرهنات (٥,٢٤)، (٥,٢٥) ، (٥,٢٦) نجد أن $(G,*)$ زمرة إبدالية محايدها الدالة I.

(٢) لاحظ أننا نستطيع استخدام مفهوم ضرب دريشليه لتقديم برهان قصير لصيغة موبياس للتعاكس كالتالي:

بما أن $G(n)=\sum_{d|n} f(d)$ فإن $G=f*U$. وبذلك يكون

$$G*\mu=(f*U)*\mu=f*(U*\mu)=f*I=f$$.

أي أن $f(n)=\sum_{d|n} G(d)\mu(\frac{n}{d})$.

المبرهنة التالية هي عكس صيغة موبياس للتعاكس .

مبرهنة (٥,٢٧)

إذا كان $f(n)=\sum_{d|n} G(d)\ \mu(\frac{n}{d})$ فإن $G(n)=\sum_{d|n} f(d)$.

البرهان

لاحظ أن $f = G * \mu$. عندئذ:

$$f * U = (G * \mu) * U = G * (\mu * U) = G * I = G.$$

ونخلص إلى أن $\sum_{d|n} f(d) = G(n)$ ◆

تمارين (٥,٥)

(١) أثبت أن $\varphi * U = E$ إذا وفقط إذا كان $E * \mu = \mu * E = \varphi$.

(٢) إذا كانت كل من f و g دالة عددية حيث $f(1) \neq 0$ و $g(1) \neq 0$ فأثبت أن $(f * g)^{-1} = f^{-1} * g^{-1}$

(٣) إذا كانت كل من f و g دالة ضربية فأثبت أن $f * g$ دالة ضربية.

(٤) إذا كانت كل من f و g دالة ضربية تماماً فهل من الضروري أن تكون $f * g$ دالة ضربية تماماً؟

(٥) إذا كانت كل من g و $f * g$ دالة ضربية فأثبت أن f دالة ضربية.

(٦) إذا كان f دالة ضربية فأثبت أن f^{-1} دالة ضربية.

(٧) لتكن f دالة ضربية. أثبت أن f دالة ضربية تماماً إذا وفقط إذا كان $f^{-1}(n) = \mu(n) f(n)$ لكل $n \geq 1$.

(٨) أثبت أن $\varphi^{-1}(n) = \prod_{p|n} (1-p)$.

(٩) أثبت أن $\lambda^{-1}(n) = |\mu(n)|$ لكل $n \geq 1$ حيث λ هي دالة ليوفيل.

(١٠) أثبت أن $\sigma_k^{-1} = \mu E^k * \mu$.

(١١) إذا كانت كل من f و g دالة عددية وكانت h دالة ضربية تماماً فأثبت أن $(fh) * (gh) = (f * g)h$.

(١٢) إذا كانت f دالة ضربية وكان n خال من المربعات فأثبت أن $\sum_{d|n} f(d) = \prod_{p|n} (1 + f(p))$.

نبذة عن حياة ميرسين
Biography of Mersenne



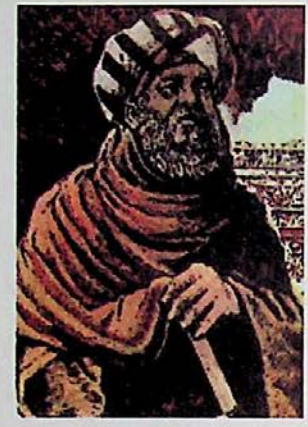
ولد : ١٥٨٨/٩/٨م في فرنسا.
توفي: ١٦٤٨/٩/١م في فرنسا.

درس مارين ميرسين علـــوم اللاهـــوت في السوربون وبعد أن تخرج عام ١٦١١م عين راهبـــاً في القصر الملكي في باريس.

كان بيته في باريس المكان المفـــضل لإلتقـــاء الرياضيين أمثال فيرما، باسكال، جاسندي، روبرفال وبيوجراند الذين أصبحوا فيما بعد نواة الأكاديمية الفرنسية. لعب ميرسين دوراً ريادياً في الاتصال مع رياضي أوروبا المشهورين لمناقشة المسائل الرياضية المطروحة في تلك الحقبة من الزمن.

كان اهتمام ميرسين منصباً على دراسة الأعداد الأولية ومحاولته إيجاد صـــيغة لتمثيل جميع الأعداد الأولية، ومع أنه فشل في ذلك إلا أن أعـــداده $M_p = 2^p - 1$ حيث p عدد أولي لا زالت تلعب دوراً مهماً في اكتشاف أعداد أولية كبيرة جداً.

نبذة عن حياة ثابت بن قرة
Biography of Thabit-ibn Qurra



ولد : عام ٨٢٦ م في حران (تركيا اليوم).
توفي: ٩٠١/٢/١٨ م في بغداد.

درس ثابت بن قرة الفلك والرياضيات وكان يتقن عدة لغات منها العربية والسريانية واليونانية. وأثناء زيارة محمد بن موسى بن شاكر إلى حران، التقى ثابت بن قرة وأعجب بقدرته في اجادة اللغات ومعلوماته الرياضية وأقنعه بالسفر معه إلى بغداد لمتابعة دراسته في الفلك والرياضيات.

وفي بغداد تقرب من مجلس الخليفة العباسي المعتضد بالله الذي كان له اهتمامات خاصة بالعلم والعلماء وكلفه بترجمة كتب اليونانيين في الرياضيات والمنطق والطب. ومن ضمن هذه الترجمات المهمة ترجمته لكتاب العناصر لإقليدس، ويعتقد الكثير من المؤرخين أن الترجمات العربية المختلفة لكتاب العناصر اعتمدت في الأساس على ترجمة ثابت بن قرة.

لم يقتصر نشاط ثابت بن قرة على ترجمة كتب اليونانيين بل كانت له اسهامات مهمة جداً في مختلف العلوم وعلى وجه الخصوص كانت له اهتمامات خاصة في الرياضيات حيث كتب عنه أحد المؤرخين :

لعب ثابت بن قرة دوراً رياديا في اكتشاف وبلورة الكثير من المفاهيم الرياضية كبناء الأعداد الحقيقية الموجبة من الأعداد الطبيعية، اكتشافاته في التفاضل والتكامل، الهندسة التحليلية والهندسة اللاإقليدية. كما يعد مؤسساً لعلم الاستاتيكا.

ومن أهم اكتشافات ثابت بن قرة في نظرية الأعداد هو وضعه صيغة للأعداد المتحابة.

الفصل السادس

الكسور المتواصلة
CONTINUED FRACTIONS

ليكن لدينا العدد الكسري $\frac{4756}{1121}$. باستخدام خوارزمية إقليدس لدينا:

$$4756 = 4\times1121+272$$
$$1121 = 4\times272+33$$
$$272 = 8\times33+8$$
$$33 = 4\times8+1$$

أي أن : $\frac{4756}{1121}=4+\frac{272}{1121}$ ، $\frac{1121}{272}=4+\frac{33}{272}$ ، $\frac{272}{33}=8+\frac{8}{33}$ ، $\frac{33}{8}=4+\frac{1}{8}$.

ولذا فإننا نستطيع كتابة العدد الكسري $\frac{4756}{1121}$ كالتالي:

$$\frac{4756}{1121}=4+\frac{272}{1121}$$
$$=4+\frac{1}{4+\frac{33}{272}}$$
$$=4+\frac{1}{4+\frac{1}{8+\frac{8}{33}}}$$

$$= 4 + \cfrac{1}{4 + \cfrac{1}{8 + \cfrac{1}{4 + \cfrac{1}{8}}}}$$

ويسمى هذا التمثيل، الكسر المتواصل للعدد $\frac{4756}{1121}$، واختصاراً نكتبه على الصورة $[4; 4, 8, 4, 8]$.

في هذا الفصل سندرس كيفية تمثيل أي عدد حقيقي على شكل كسر متواصل. لقد رأينا في المثال السابق ارتباط مفهوم الكسور المتواصلة مع خوارزمية إقليدس مما يرجح أن أول استخدام لهذا المفهوم يرجع إلى حقبة زمنية قديمة، إلا أن الشكل الحالي للكسور المتواصلة ظهر في القرن السادس عشر عندما استخدمه الرياضي الايطالي رافائيل بومبالي (*Rafael Bombelli*) لتقريب الجذور التربيعية. ولقد بين أويلر في العام ١٧٣٠م العلاقة بين الكسور المتواصلة واستخدام الأعداد الكسرية للتقريب حيث أثبت، مستخدماً خوارزمية إقليدس أن الكسر المتواصل لأي عدد كسري يجب أن يكون منتهياً. كما استخدم أويلر الكسور المتواصلة في العام ١٧٥٩م لإيجاد حلول لمعادلة بيل (*Pell*) المشهورة $x^2 - dy^2 = 1$. وفي العام ١٧٦٦م درس لاجرانج (*Lagrange*) الكسور المتواصلة الدورية. كما بين كل من لاجرانج وأويلر أن لمفهوم الكسور المتواصلة العامة تطبيقات هامة في التحليل. على سبيل المثال، إن الخوارزميات المستخدمة في الآلات الحاسبة لتقريب الدوال المتسامية مثل e^x و $\sin x$ ترجع أصولها إلى مفهوم الكسور المتواصلة.

(٦,١) الكسور المتواصلة المنتهية
Finite Continued Fractions

تعريف (٦,١)

لتكن $a_1, a_2, \ldots, a_n$ متتالية منتهية من الأعداد الحقيقية الموجبة وليكن a_0 عدداً حقيقياً. نعرف الكسر المتواصل المنتهي $[a_0; a_1, a_2, \ldots, a_n]$ على أنه

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\vdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

وإذا كانت a_i جميعها أعداداً صحيحة فإن الكسر المتواصل يسمى كسراً متواصلاً منتهياً بسيطاً *(finite simple continued fraction)* .

مثال (٦,١)

لقد بينا في بداية هذا الفصل أن $[4; 4, 8, 4, 8]$ كسراً متواصلاً منتهياً بسيطاً للعدد $\frac{4756}{1121}$. وبما أن $\frac{1}{8} = \frac{1}{7 + \frac{1}{1}}$ فإن $[4; 4, 8, 4, 7, 1]$ كسراً متواصلاً منتهياً بسيطاً آخر للعدد $\frac{4756}{1121}$ □

سنبرهن الآن على وجود كسر متواصل منته بسيط لأي عدد كسري.

مبرهنة (٦,١)

إذا كان r عدد كسرياً فإن له كسر متواصل منته بسيط.

البرهان

إذا كان r عدداً صحيحاً فمن الواضح أن $r=[r]$. لنفرض إذن أن $r=\frac{a}{b}$ حيث $a\in\mathbb{Z}$ و $b\in\mathbb{Z}^+$. باستخدام خوارزمية إقليدس نحصل على:

$$a=q_0b+r_1 \quad ، \quad 0<r_1<b .$$
$$b=q_1r_1+r_2 \quad ، \quad 0<r_2<r_1 .$$
$$r_1=q_2r_2+r_3 \quad ، \quad 0<r_3<r_2 .$$
$$\vdots$$
$$r_{n-2}=q_{n-1}r_{n-1}+r_n \quad ، \quad 0<r_n<r_{n-1}$$
$$r_{n-1}=q_nr_n+0 .$$

لاحظ أولاً أن كل من $r_k>0$ ، ولذا فإن $q_1,q_2,\dots,q_n$ جميعها موجبة.

لاحظ أيضاً أنه بإمكاننا كتابة المعادلات أعلاه على الصورة:

$$\frac{a}{b}=q_0+\frac{r_1}{b}=q_0+\frac{1}{\frac{b}{r_1}}$$
$$\frac{b}{r_1}=q_1+\frac{r_2}{r_1}=q_1+\frac{1}{\frac{r_1}{r_2}}$$
$$\frac{r_1}{r_2}=q_2+\frac{r_3}{r_2}=q_2+\frac{1}{\frac{r_2}{r_3}}$$
$$\vdots$$
$$\frac{r_{n-1}}{r_n}=q_n$$

وبالتعويض المتتابع نجد أن:

$$\frac{a}{b}=q_0+\cfrac{1}{\cfrac{b}{r_1}}$$

$$=q_0+\cfrac{1}{q_1+\cfrac{1}{\cfrac{r_1}{r_2}}}$$

$$=q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\cfrac{1}{\cfrac{r_2}{r_3}}}}$$

$$\vdots$$

$$=q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+}}}$$

$$\vdots$$

$$\cfrac{1}{q_{n-1}+\cfrac{1}{q_n}}$$

◆ وينتج عن ذلك أن $\frac{a}{b}=[q_0;q_1,q_2,\dots,q_n]$ كسر متواصل منته بسيط للعدد $\frac{a}{b}$

سنبرهن الآن وجود كسران متواصلان منتهيان بسيطان فقط لأي عدد كسري. ولكننا نحتاج أولاً إلى المبرهنة التالية:

مبرهنة (٦,٢)

إذا كان r عدداً كسرياً وكان

$r=[a_0; a_1, a_2, \dots, a_n]=[b_0; b_1, b_2, \dots, b_m]$ حيث a_i و b_i جميعها أعداد صحيحة موجبة (ما عدا ربما a_0 و b_0) وكان $a_n>1$ و $b_m>1$ فإن $m=n$ وإن $a_i=b_i$ لكل $0\le i\le n$.

البرهان

إذا كان r عدداً صحيحاً فإن $n=m=0$. لأنه لو كان $n>0$ فإن

$a_0<r<[a_0; a_1, a_2, \dots, a_n]=a_0+\dfrac{1}{[a_1, a_2, \dots, a_n]}<a_0+1$ وهذا مستحيل. وبالمثل $m=0$. ومن ثم فإن $a_0=b_0=r$.

لنفرض الآن أن r ليس عدداً صحيحاً. ولذا فإن $m\ge 1$ ، $n\ge 1$ وأن

$$r=a_0+\frac{1}{[a_1, a_2, \dots, a_n]}=b_0+\frac{1}{[b_1, b_2, \dots, b_m]}.$$

من الواضح أن $\dfrac{1}{[a_1, a_2, \dots, a_n]}>0$ وأن $\dfrac{1}{[b_1, b_2, \dots, b_n]}>0$. وبما أن $a_n>1$ فإن $a_1>1$ أو أن $n\ge 2$. ولذا فإن $\dfrac{1}{[a_1, a_2, \dots, a_n]}<1$. وبالمثل ، $\dfrac{1}{[b_1, b_2, \dots, b_m]}<1$. ومنه فإن $a_0<r<a_0+1$ وإن $b_0<r<b_0+1$. ومن ثم فإن $a_0=b_0=[r]$. وبالتالي فإن $[a_1, a_2, \dots, a_n]=[b_1, b_2, \dots, b_n]$. وبفرض أن $n\ge m$ والاستمرار نخلص إلى أن $a_1=b_1$ ، $a_2=b_2$ ، ... ، $a_{m-1}=b_{m-1}$ وأن $b_m=[b_m]=[a_m, a_{m-1}, \dots, a_n]$. وبما أن m عدد صحيح فإننا نجد (كما في الفقرة الأولى من البرهان) أن $n=m$ وأن $a_m=b_m$ ◆

مبرهنة (٦,٣)

يوجد بالضبط كسران متواصلان منتهيان بسيطان لكل عدد كسري r.

البرهان

إذا كان $r=1$ فإن $1=[1]=[0;1]$ الكسران المتواصلان المنتهيان البسيطان الوحيدان للعدد r. إذا كان $r\in\mathbb{Z}$ و $r\neq 1$ فباستخدام المبرهنة (٢,٥) نجد أن $[r]$ هو الكسر المتواصل المنته البسيط الوحيد حيث $r>1$. كما أن $[r-1;1]$ تمثيل آخر. ولذا فللعدد r تمثيلان فقط.

لنفرض الآن أن $r=\frac{a}{b}$ عدداً كسرياً وأن $r\notin\mathbb{Z}$. باستخدام المبرهنة (٦,١) نجد أن $\frac{a}{b}=[q_0;q_1,q_2,\dots,q_n]$ حيث $q_n\in\mathbb{Z}^+$. من الواضح أن $q_n\neq 1$. ولذا فإن $q_n=(q_n-1)+\frac{1}{1}$ وأن $\frac{a}{b}=[q_0;q_1,q_2,\dots,q_n-1]$. وباستخدام المبرهنة (٦,٢) نخلص إلى أن هذان هما التمثيلان الوحيدان للعدد $\frac{a}{b}$ ◆

نقدم الآن طريقة سهلة لإيجاد العدد الكسري بمعرفة الكسر المتواصل المنته البسيط الذي يمثله.

تعريف (٦,٢)

لتكن... $a_0,a_1,a_2,$ متتالية من الأعداد الصحيحة الموجبة (ما عدا ربما a_0).
نعرف المتتاليتين (p_k) و (q_k) استقرائياً على النحو التالي:

- $p_{-1}=1$ ، $p_0=a_0$ و $p_k=a_k\,p_{k-1}+p_{k-2}$ لكل $k\geq 1$.
- $q_{-1}=0$ ، $q_0=1$ و $q_k=a_k\,q_{k-1}+q_{k-2}$ لكل $k\geq 1$.

مبرهنة (٦,٤)

إذا كانت ... $a_0,a_1,a_2,$ متتالية من الأعداد الصحيحة الموجبة (ما عدا ربما a_0) وكان x عدداً حقيقياً موجباً فإن $[a_0;a_1,\dots,a_{k-1},x]=\frac{xp_{k-1}+p_{k-2}}{xq_{k-1}+q_{k-2}}$

وعلى وجه الخصوص $[a_0;a_1,\dots,a_{k-1},a_k]=\frac{p_k}{q_k}$.

البرهان

باستخدام الاستقراء الرياضي على k. عندما $k=1$ لدينا:

$$\frac{xp_0+p_{-1}}{xq_0+q_{-1}}=\frac{xa_0+1}{x}=a_0+\frac{1}{x}=[a_0;x]\ .$$

ولذا فالعبارة صحيحة عند $k=1$.

لنفرض الآن أن العبارة صحيحة عند $k-1$. أي أن

$$[a_0;a_1,\ldots,a_{k-1},x]=\frac{xp_{k-1}+p_{k-2}}{xq_{k-1}+q_{k-2}}\ .$$

الآن :

$$[a_0;a_1,\ldots,a_{k-1},a_k,x]=[a_0;a_1,\ldots,a_{k-1},a_k+\frac{1}{x}]$$

$$=\frac{(a_k+\frac{1}{x})p_{k-1}+p_{k-2}}{(a_k+\frac{1}{x})q_{k-1}+q_{k-2}}$$

$$=\frac{xa_kp_{k-1}+p_{k-1}+xp_{k-2}}{xa_kq_{k-1}+q_{k-1}+xq_{k-2}}$$

$$=\frac{x(a_kp_{k-1}+p_{k-2})+p_{k-1}}{x(a_kq_{k-1}+q_{k-2})+q_{k-1}}$$

$$=\frac{xp_k+p_{k-1}}{xq_k+q_{k-1}}$$

إذن، العبارة صحيحة عند k. وأخيراً :

◆ $$[a_0;a_1,a_2,\ldots,a_k]=\frac{a_kp_{k-1}+p_{k-2}}{a_kq_{k-1}+q_{k-2}}=\frac{p_k}{q_k}$$

مثال(٦,٢)

استخدم المبرهنة (٦,٤) لحساب $[-4;2,5,2,1]$.

الحل

k	a_k	p_k	q_k	p_k/q_k
0	−4	−4	1	−4/1
1	2	$(2)(-4)+1=-7$	$(2)(1)+0=2$	−7/2
2	5	$(5)(-7)+(-4)=-39$	$(5)(2)+1=11$	−39/11
3	2	$(2)(-39)+(-7)=85$	$(2)(11)+2=24$	−85/24
4	1	$(1)(-85)+(39)=124$	$(1)(24)+11=35$	−124/35

وبذلك نجد أن $[-4;2,5,2,1]=\frac{p_4}{q_4}=-\frac{124}{35}$ □

تتمتع المتتاليتان المقدمتان في التعريف (٦,٢) ببعض الخصائص الأساسية التي تقدمها لنا المبرهنة التالية.

مبرهنة (٦,٥)

إذا كانت (a_k) ، (p_k) ، (q_k) كما في التعريف (٦,٢) فإن:

(١) $q_k \geq 2^{\frac{k-1}{2}}$ لكل $k \geq 2$.

(٢) $p_k q_{k-1}-p_{k-1} q_k=(-1)^{k-1}$ لكل $k \geq 0$.

(٣) $(p_k, q_k)=1$ لكل $k \geq 0$.

(٤) $p_k\ q_{k-2}-p_{k-2}\ q_k=(-1)^k a_k$ لكل $k \geq 0$.

البرهان

(١) باستخدام الاستقراء الرياضي على k . من الواضح أن العبارة صحيحة عند $k=2$ و $k=3$. لنفرض أن العبارة صحيحة لكل k حيث $2\le k\le n$. عندئذ،

$$q_{n+1}=a_{n+1}q_n+q_{n-1}\ge 2q_{n-1}\ge 2\times 2^{\frac{n-2}{2}}=2^{\frac{n}{2}}.$$

ولذا فالعبارة صحيحة عند $n+1$.

(٢) باستخدام الاستقراء الرياضي على k.

من الواضح أن العبارة صحيحة عند $k=0$. لنفرض أن العبارة صحيحة عند $k=m$. الآن

$$\begin{aligned}p_{m+1}q_m-p_mq_{m+1}&=(ap_m+p_{m-1})q_m-p_m(a_{m+1}q_m+q_{m-1})\\&=-(p_mq_{m-1}-p_{m-1}q_m)\\&=-(-1)^{m-1}=(-1)^m\end{aligned}$$

ولذا فالعبارة صحيحة عند $k=m+1$.

(٣) لنفرض أن $(p_k,q_k)=d$. بما أن $d\mid p_k$ و $d\mid q_k$ فإن $d\mid(-1)^{k-1}$. وبما أن $d>0$ فإن $d=1$.

(٤) باستخدام الفقرة (٢) نجد لكل $k\ge 0$ أن:

$$\begin{aligned}p_kq_{k-2}-p_{k-2}q_k&=(a_kp_{k-1}+p_{k-2})q_{k-2}-p_{k-2}(a_kq_{k-1}+q_{k-2})\\&=a_k(p_{k-1}q_{k-2}-p_{k-2}q_{k-1})\\&=(-1)^{k-2}a_k=(-1)^ka_k\end{aligned}$$

وبهذا نكون قد أنهينا البرهان ◆

تعريف (٦,٣)

ليكن $[a_0;a_1,a_2,\dots,a_n]$ كسراً متواصلاً. يعرف المقارب (*convergent*) من الرتبة c_k حيث $k\ge n$ بأنه الكسر المتواصل $c_k=[a_0;a_1,a_2,\dots,a_k]$.

لاحظ أن $c_k = \frac{p_k}{q_k}$.

المبرهنة التالية تستخدم المقاربات من الرتب الفردية والزوجية لتقريب الكسر المتواصل.

مبرهنة (٦,٦)

إذا كان $[a_0; a_1, a_2, \dots, a_n]$ كسراً متواصلاً وكانت (p_k) و (q_k) المتتاليتين المقدمتين بالتعريف (٦,٢) فإن:

(١) $c_k - c_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$ لكل $1 \le k \le n$.

(٢) $c_k - c_{k-2} = \frac{(-1)^k a_k}{q_k q_{k-2}}$ لكل $2 \le k \le n$.

(٣) $c_0 < c_2 < c_4 < \dots$

(٤) $c_1 > c_3 > c_5 > \dots$.

(٥) $c_{2j} \le [a_0; a_1, a_2, \dots, a_n] \le c_{2i+1}$ لكل $0 \le j \le [n/2]$ ولكل $0 \le i \le [n-1/2]$. تكون المتباينة اليسرى مساواة إذا كان n زوجياً وتكون المتباينة اليمنى مساواة إذا كان n فردياً.

البرهان

(١) باستخدام الفقرة (٢) من المبرهنة (٦,٥) لدينا :

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1} \cdot$$

وبقسمة طرفي المعادلة على $q_k q_{k-1}$ عندما $k \ge 1$ نحصل على

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$. أي أن $c_k - c_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$.

(٢) باستخدام الفقرة (٤) من المبرهنة (٦,٥) لدينا

$p_k q_{k-2} - p_{k-2} q_k = (-1)^k a_k$. وبقسمة طرفي المعادلة على $q_k q_{k-2}$ عندما $k \geq 1$ نحصل على $\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^k a_k}{q_k q_{k-2}}$. أي أن

$$c_k - c_{k-2} = \frac{(-1)^k a_k}{q_k q_{k-2}} .$$

(٣) إذا كان $2 \leq k \leq n$ وكان k زوجياً فإن $k-2 \geq 0$ زوجياً. ولذا فإن $(-1)^k = 1$. وباستخدام الفقرة (٢) نجد أن $c_k - c_{k-2} = \frac{a_k}{q_k q_{k-2}} > 0$ لأن a_k و $q_k q_{k-2}$ موجبان لكل $k \geq 1$. وبالتالي فإن $c_{k-2} < c_k$.

(٤) إذا كان $3 \leq k \leq n$ وكان k فردياً فإن $k-2 \geq 1$ فردياً. ولذا فإن $(-1)^k = -1$. وباستخدام الفقرة (٢) نجد أن $c_k - c_{k-2} < 0$. وبالتالي فإن $c_k < c_{k-2}$.

(٥) إذا كان n فردياً فنجد باستخدام الفقرة (١) أن $c_n > c_{n-1}$. ونرى أن $[a_0; a_1, a_2, \dots, a_n]$ حيث c_{n-1} أكبر مقارب رتبته زوجية.

أما إذا كان n زوجياً فنجد باستخدام الفقرة (١) أن $[a_0; a_1, a_2, \dots, a_n] = c_n < c_{n-1}$. حيث c_{n-1} أصغر مقارب رتبته فردية ◆

(٦,١,١) تمارين محلولة (*Solved Exercises*)

تمرين (١)

(أ) ليكن $\frac{a}{b} = [a_0; a_1, a_2, \dots, a_n]$ حيث $(a,b) = 1$ و $b > 0$. إذا كان n عدداً فردياً فأثبت أن $x = cq_{n-1}$ و $y = -cp_{n-1}$ حل للمعادلة الديوفنتية $ax + by = c$ وإذا كان n عدداً زوجياً فأثبت أن $x = -cq_{n-1}$ و $y = cp_{n-1}$ حل للمعادلة.

(ب) استخدم الفقرة (أ) لحل المعادلة $26x - 55y = 1$.

الحل

(أ) بما أن $\frac{a}{b}=\frac{p_n}{q_n}$ وأن $(a,b)=(p_n,q_n)=1$ وأن $q_n>0$ فإن $a=p_n$ و $b=q_n$. ولكن باستخدام المبرهنة (٦,٥) نعلم أن $p_n q_{n-1}-p_{n-1}q_n=(-1)^{n-1}$. وبهذا يكون $aq_{n-1}-b_{n-1}=(-1)^{n-1}$. الآن:

إذا كان n فردياً فإن $a(cq_{n-1})+b(-cp_{n-1})=c$. ويكون $x=cq_{n-1}$ و $y=-cp_{n-1}$ حل للمعادلة.

أما إذا كان n زوجياً فإن $a(-cq_{n-1})+b(cp_{n-1})=c$ ويكون $x=-cq_{n-1}$ و $y=cp_{n-1}$ حل للمعادلة.

(ب) بما أن $26x-55y=1$ فإن $-26x+55y=-1$ وأن $a=-26$ و $b=55$.

وبإيجاد الكسر المتواصل للعدد $\frac{-26}{55}$ نجد أن:

$$-26=(-1)\times 55+29$$
$$55=1\times 29+26$$
$$29=1\times 26+3$$
$$26=8\times 3+2$$
$$3=1\times 2+1$$
$$2=2\times 1+0$$

عندئذ، $\frac{-26}{55}=[-1;1,8,1,2]$. الآن:

k	a_k	p_k	q_k	p_k/q_k
0	−1	−1	1	−1/1
1	1	(1)(−1)+1=0	(1)(1)+0=1	0/1
2	1	(1)(0)+−1=−1	(1)(1)+1=2	−1/2
3	8	(8)(−1)+0=−8	(8)(2)+1=17	−8/17
4	1	(1)(−8)+(−1)=−9	(1)(17)+2=19	−9/19
5	2	(2)(−9)+(−8)=−26	(2)(19)+17=55	−26/55

من ذلك نرى أن $x_0 = cq_4 = (-1)(19) = -19$ و $y_0 = -cp_4 = (1)(-9) = -9$

حل للمعادلة الديوفنتية ، ويكون الحل العام هو:

$$\triangle \quad x = x_0 + \frac{b}{d}k = -19 + 55k \;،\; y = y_0 - \frac{a}{d}k = -9 + 26k$$

تمرين (٢)

أثبت أن $q_k \geq f_k$ لكل $k \geq 0$ حيث f_k هو عدد فيبوناتشي وأن $c_k = \frac{p_k}{q_k}$ هو المقارب ذو الرتبة k في الكسر المتواصل البسيط $[a_0; a_1, a_2, \ldots, a_n]$.

الحل

باستخدام الاستقراء الرياضي على k.

بما أن $q_0 = 1$ فإن $q_0 = f_0 = 1$. وبما أن $q_1 = a_0 \geq 1$ فإن $q_1 \geq f_1$. ولذا فإن العبارة صحيحة عند $k = 0,1$.

لنفرض أن العبارة صحيحة لكل $k < n$ حيث $n \geq 2$. بما أن $a_n \geq 1$ فإن

$$q_n = a_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2} \geq f_{n-1} + f_{n-2} = f_n$$

وبهذا تكون العبارة صحيحة عند n $\triangle$

تمارين (٦,١)

(١) جد الكسرين المتواصلين المنتهيين البسيطين لكل من الأعداد الكسرية التالية:

(أ) $\frac{355}{113}$ (ب) $\frac{5}{32}$ (ج) $\frac{158}{49}$

(د) $\frac{-19}{51}$ (هـ) $\frac{-43}{1001}$ (و) $\frac{48}{1003}$

(٢) جد العدد الكسري الذي يمثل الكسر المتواصل المنته البسيط .

(أ) $[-3;4,2,5]$ (ب) $[1;1,1,1,1,1]$ (ج) $[4;2,1,3,1,2,4]$

(د) $[0;1,2,3,4,3,2,1]$ (هـ) $[3;7,15,1]$ (و) $[1;1,1]$

(٣) احسب المقاربات لكل من الأعداد الكسرية في التمرين (١).

(٤) احسب المقاربات لكل من الكسور المتواصلة في التمرين (٢).

(٥) استخدم الكسور المتواصلة لحل كل من المعادلات الديوفنتية التالية:

(أ) $89x-25y=3$ (ب) $377x-120y=-3$

(ج) $98x+263y=1$ (د) $1255x+177y=-1$

(٦) استخدم الاستقراء الرياضي لإثبات أن أي كسر متواصل منته بسيط يمثل عدداً كسرياً.

(٧) ليكن c_k المقارب ذو الرتبة k للكسر المتواصل $[a_0; a_1, a_2, \dots, a_n]$. إذا كان $a_0 \geq 1$ فأثبت أن $\frac{q_k}{q_{k-1}} = [a_k; a_{k-1}, \dots, a_2, a_1]$.

(٨) ليكن $\frac{a}{b}$ عدداً كسرياً حيث $(a,b)=1$ وليكن $\frac{a}{b} = [a_0; a_1, \dots, a_n]$ حيث $a_i \in \mathbb{Z}^+$.

(أ) إذا كان n فردياً فأثبت أن الكسر المتواصل للعدد $\frac{a}{b}$ متناظراً (أي $a_0 = a_n, a_1 = a_{n-1}, \dots$) إذا وفقط إذا كان $a \mid (b^2+1)$.

(ب) إذا كان n زوجياً فأثبت أن الكسر المتواصل للعدد $\frac{a}{b}$ متناظراً إذا وفقط إذا كان $a \mid (b^2-1)$.

(٩) جد كسراً متواصلاً منتهياً بسيطاً للعدد $\frac{f_n}{f_{n-1}}$ حيث f_n عدد فيبوناتشي.

(٦,٢) الكسور المتواصلة غير المنتهية
Infinite Continued Fractions

لقد بينا في البند (٦,١) أن الكسر المتواصل المنته البسيط يمثل عدداً كسرياً. سنبرهن في هذا البند أن الكسر المتواصل غير المنته البسيط يمثل عدداً غير كسري. وبالعكس كل عدد غير كسري يمكن تمثيله على شكل كسر متواصل غير منتـــه بسيط.

مبرهنة (٦,٧)

إذا كانت $a_0, a_1, a_2, \ldots$ متتالية غير منتهية من الأعداد الصحيحة الموجبـــة (ما عدا ربما a_0) وكان c_k هو المقارب ذو الرتبة k فإن $\lim_{k\to\infty} c_k$ موجـــودة وأن $c_{2i} < \lim_{k\to\infty} c_k < c_{2j+1}$ لكل $i \geq 0$ وكل $j \geq 0$.

البرهان

باستخدام المبرهنة (٦,٦) نعلم أن $\{c_{2k}\}$ متتالية تزايدية محدودة من الأسفل وأ، $\{c_{2k+1}\}$ متتالية تناقصية محدودة من الأعلى، ولذا فإن كـــل مـــن $\lim_{k\to\infty} c_{2k}$ و $\lim_{k\to\infty} c_{2k+1}$ موجودة. سنبرهن الآن أن هاتين النهايتين متساويتان. باستخدام المبرهنة (٦,٦) لـــديـنا $c_{2k+1} - c_{2k} = \frac{1}{q_{2k+1}q_{2k}}$. وبمـــا أن $q_{2k} \geq 2^{\frac{2k-1}{2}}$ فـــإن $\lim_{k\to\infty}(c_{2k+1} - c_{2k}) = 0$. وبهـــذا نـــرى أن $\lim_{k\to\infty} c_{2k+1} = \lim_{k\to\infty} c_{2k}$. وأخـــيراً إذا كانـــت $\alpha = \lim_{k\to\infty} c_k$ فمـــن الواضـــح أن $\alpha = \lim_{k\to\infty} c_{2k} = \lim_{k\to\infty} c_{2k+1}$ وأن $c_{2i} < \alpha < c_{2j+1}$ ◆

تعريف (٦,٤)

لتكن... $a_0, a_1, a_2,$ متتالية غير منتهية من الأعداد الصحيحة الموجبة (ما عدا ربما a_0) وليكن c_k المقارب ذو الرتبة k. نعرف الكسر المتواصل غير المنته البسيط $[a_0; a_1, a_2, ...]$ على أنه القيمة $\lim_{k\to\infty} c_k$.

سنبرهن الآن أن قيمتي كسران متواصلان غير منتهيين بسيطان مختلفان يجب أن تكونا مختلفتان ولكننا نحتاج قبل ذلك إلى المبرهنة التالية.

مبرهنة (٦,٨)

إذا كانت $\alpha = [a_0; a_1, a_2, ...]$ فإن $[\alpha] = a_0$ وأن $\alpha = a_0 + \frac{1}{[a_1; a_2, ...]}$.

حيث $[\alpha]$ هو أكبر عدد صحيح لا يزيد عن α.

البرهان

من الواضح أن $a_0 = c_0 < \alpha < c_1 = a_0 + \frac{1}{a_1}$. وبما أن $a_1 \geq 1$ فإن $a_0 < \alpha < a_0 + 1$. أي أن $[\alpha] = a_0$. وإذا كان $k \geq 1$ فإن

$$c_k = [a_0; a_1, ..., a_k] = a_0 + \frac{1}{[a_1; a_2, ..., a_k]}.$$

إذن، $\alpha = \lim_{k\to\infty} c_k = a_0 + \frac{1}{[a_1; a_2, ...]}$ ◆

مبرهنة (٦,٩)

ليكن كل من $\alpha = [a_0; a_1, a_2, ...]$ و $\beta = [b_0; b_1, b_2, ...]$ كسراً متواصلاً غير منته بسيط. إذا كان $\alpha = \beta$ فإن $a_i = b_i$ لكل $i \geq 0$.

البرهان

باستخدام المبرهنة (٦,٨) نعلم أن:

$$\alpha = a_0 + \frac{1}{[a_1; a_2, \ldots]}$$

$$\beta = b_0 + \frac{1}{[b_1; b_2, \ldots]}$$

وبما أن $\alpha = \beta$ فإن $a_0 = b_0$ وأن $[a_1; a_2, \ldots] = [b_1; b_2, \ldots]$. وبالاستمرار نجد أن $a_i = b_i$ لكل $i \geq 0$ ◆

مبرهنة (٦,١٠)

إذا كان $\alpha = [a_0; a_1, a_2, \ldots]$ فإن α عدد غير كسري.

البرهان

لنفرض أن α عدد كسري وليكن $\alpha = \frac{a}{b}$ حيث $a \in \mathbb{Z}$ و $b \in \mathbb{Z}^+$. إذا كان k زوجياً فنجد باستخدام المبرهنة (٦,٧) أن $c_k < \alpha < c_{k+1}$. ونرى أن

$$0 < \frac{a}{b} - \frac{p_k}{q_k} < \frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} = \frac{1}{q_k q_{k+1}}.$$

ومنه فإن $0 < aq_k - bp_k < \frac{b}{q_{k+1}}$. وإذا كان k كبير ما فيه الكفاية فإن $0 < aq_k - bp_k < 1$ وهذا مستحيل لأن $aq_k - bp_k \in \mathbb{Z}$. إذن، α عدد غير كسري ◆

مثال (٦,٣)

جد العدد غير الكسري الذي يمثل الكسر المتواصل $[1; 2, 1, 2, 1, 2, \ldots]$.

الحل

لنفرض أن العدد المطلوب هو α . وحينئذ :

$$\alpha = 1 + \frac{1}{[2; 1, 2, 1, 2, \ldots]}$$

$$= 1 + \frac{1}{2 + \frac{1}{[1, 2, 1, 2, \ldots]}}$$

$$= 1 + \frac{1}{2 + \frac{1}{\alpha}} = \frac{3\alpha + 1}{2\alpha + 1}$$

ونحصل على المعادلة $2\alpha^2 - 2\alpha - 1 = 0$. وبحل المعادلة نجد أن $\alpha = \frac{1 \pm \sqrt{3}}{2}$. وبما أن $\alpha > 0$ فإننا نخلص إلى أن $\alpha = \frac{1 + \sqrt{3}}{2}$ □

فيما تبقى من هذا البند سنبرهن أن عكس المبرهنة (٦,١٠) صحيح أيضاً. أي سنبرهن أن أي عدد غير كسري يمكن تمثيله بكسر متواصل غير منته بسيط ونقدم طريقة لإيجاد هذا التمثيل.

تعريف (٦,٥)

ليكن $\alpha = \alpha_0$ عدداً غير كسري. نعرف المتتالية $\{a_k\}$ استقرائياً على النحو التالي:

$$a_k = [\alpha_k] \quad \text{و} \quad \alpha_{k+1} = \frac{1}{\alpha_k - a_k} \quad \text{لكل } k \geq 0 .$$

ملحوظة

بما أن α_0 غير كسري فإن $0 < \alpha_0 - a_0 < 1$. ولذا فإن $\alpha_1 = \frac{1}{\alpha_0 - a_0} > 1$ عدد غير كسري وإن $\alpha_0 = a_0 + \frac{1}{\alpha_1} = [a_0; \alpha_1]$. وبالمثل، بما أن $a_1 = [\alpha_1]$ فإن $\alpha_2 = \frac{1}{\alpha_1 - a_1} > 1$ عدد غير كسري وإن $\alpha_1 = a_1 + \frac{1}{\alpha_2}$. ولذا فإن

$[a_0;a_1,\alpha_2]=\alpha_0$. وبصورة عامة نجد أن $\alpha_0=[a_0;a_1,\ldots,a_k,\alpha_{k+1}]$ لكل $k\geq 0$.

مبرهنة (٦,١١)

إذا كان α عدداً غير كسري وكان a_i و α_i هي كما في التعريف (٦,٥) فإن $\alpha-c_k=\dfrac{(-1)^k}{q_k(\alpha_{k+1}q_k+q_{k-1})}$.

البرهان

بما أن $\alpha=[a_0;a_1,\ldots,a_k,\alpha_{k+1}]$ لكل $k\geq 0$ فنجد باستخدام المبرهنة (٦,٤) أن:

$$\begin{aligned}\alpha-c_k&=\frac{\alpha_{k+1}p_k+p_{k-1}}{\alpha_{k+1}q_k+q_{k-1}}\\&=\frac{\alpha_{k+1}p_kq_k+q_kp_{k-1}-\alpha_{k+1}p_kq_k-p_kq_{k-1}}{q_k(\alpha_{k+1}q_k+q_{k-1})}\\&=\frac{-(p_kq_{k-1}-q_kp_{k-1})}{q_k(\alpha_{k+1}q_k+q_{k-1})}\end{aligned}$$

ولكن باستخدام المبرهنة (٦,٥) نعلم أن $p_kq_{k-1}-p_{k-1}q_k=(-1)^{k-1}$.

إذن، $\alpha-c_k=\dfrac{(-1)^k}{q_k(\alpha_{k+1}q_k+q_{k-1})}$ ◆

المبرهنة التالية تضمن لنا وجود كسراً متواصلاً غير منته بسيط لأي عدد غير كسري.

مبرهنة (٦,١٢)

إذا كان α عدداً غير كسري وكان a_i و α_i هي كما في التعريف (٦,٥) فإن $\alpha=[a_0;a_1,a_2,\ldots]$. وبصورة عامة $\alpha_k=[a_k;a_{k+1},a_{k+2},\ldots]$ لكل $k\geq 0$.

البرهان

استناداً إلى الملحوظة المقدمة أعلاه نجد أن α_k عدد غير كسري لكل $k \geq 0$ ولذا فإن $0 < \alpha_k - a_k < 1$ وأن $\alpha_{k+1} > 1$ و $a_{k+1} \geq 1$ لكل $k \geq 0$. وباستخدام المبرهنة (٦,١١) نجد أن $\lim_{k\to\infty} c_k = \alpha$. أي أن $\alpha = [a_0; a_1, a_2, \ldots]$. وأخيراً لإثبات أن $\alpha_k = [a_k; a_{k+1}, a_{k+1}, \ldots]$ لكل $k \geq 1$، نتبنى البرهان السابق مبتدئين بالعدد α_k بدلاً من $\alpha = \alpha_0$ ◆

مثال (٦,٤)

جد الكسر المتواصل غير المنته للعدد $\alpha = \alpha_0 = \sqrt{35}$.

الحل

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{\sqrt{35}+5}{10} \quad , \quad a_0 = [\alpha_0] = 5 .$$

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \sqrt{35}+5 \quad , \quad a_1 = [\alpha_1] = 1 .$$

$$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{\sqrt{35}+5}{10} \quad , \quad a_2 = [\alpha_2] = 10 .$$

بما أن $\alpha_3 = \alpha_1$ فمن الواضح أن:

$$a_3 = a_1, a_4 = a_2, \ldots$$

وبالتالي فإن العدد $\sqrt{35}$ دوري وأن :

□ $\sqrt{35} = [5; 1, 10, 1, 10, 1, 10, \ldots]$

(٦,٢,١) التقريب الكسري للأعداد غير الكسرية

Rational Approximation to Irrational Numbers

إذا كان α عدداً غير كسري وكان c_k المقارب ذو الرتبة k في الكسر المتواصل الذي يمثل α فإن المتتالية $\{c_k\}$ تقاربية وتقترب من α. أي أن مقاربات α تزودنا بتقريب جيد للعدد α. بالتحديد لدينا المبرهنة التالية.

مبرهنة (٦,١٣)

إذا كان c_k هو المقارب ذو الرتبة k للعدد غير الكسري α فإن

$$|\alpha - c_k| < \frac{1}{q_k q_{k+1}} < \frac{1}{q_k^2}$$ لكل $k \geq 0$.

البرهان

باستخدام المبرهنة (٦,١١) نعلم أن $|\alpha - c_k| < \dfrac{1}{q_k(\alpha_{k+1}q_k + q_{k-1})}$. وبما أن $a_{k+1} < \alpha_{k+1}$ وأن $a_{k+1}q_k + q_{k-1} = q_{k+1}$ فنجد أن $|\alpha - c_k| < \dfrac{1}{q_k q_{k+1}}$.

ولكن $q_{k+1} > q_k$. وبهذا يكون $|\alpha - c_k| < \dfrac{1}{q_k q_{k+1}} < \dfrac{1}{q_k^2}$ ◆

مبرهنة (٦,١٤)

إذا كان α عدداً غير كسري فإن:

(أ) $|q_{k+1}\alpha - p_{k+1}| < |q_k\alpha - p_k|$ لكل $k \geq 0$.

(ب) $|\alpha - c_{k+1}| < |\alpha - c_k|$ لكل $k \geq 0$.

البرهان

(أ) استناداً إلى المبرهنة (٦,١٣) نجد أن:

$$|\alpha - p_{k+1}/q_{k+1}| = |\alpha - c_{k+1}| < \frac{1}{q_{k+1}\, q_{k+2}}$$. عندئذ: $\dfrac{|q_{k+1}\alpha - p_{k+1}|}{q_{k+1}}$

$|q_{k+1}\alpha - p_{k+1}| < 1/q_{k+2}$ واستناداً إلى المبرهنة (٦,١١) لدينا:

$$\frac{|q_k\alpha - p_k|}{q_k} = |\alpha - p_k/q_k| = |\alpha - c_k| = \frac{1}{q_k(\alpha_{k+1}q_k + q_{k-1})}$$

وعليه فإن $|q_k\alpha - p_k| = \dfrac{1}{\alpha_{k+1}q_k + q_{k-1}}$. وبما أن $[\alpha_{k+1}] = a_{k+1}$ فنجد

$$\alpha_{k+1}q_k + q_{k-1} < a_{k+1}q_k + q_{k-1}$$

$$= q_{k+1} < q_{k+1} + q_k \le a_{k+2}q_{k+1} + q_k = q_{k+2}$$

وبهذا نخلص إلى أن: $|q_k\alpha - p_k| > 1/q_{k+2} > |q_{k+1}\alpha - p_{k+1}|$.

(ب) باستخدام الفقرة (أ) لدينا :

$$|\alpha - c_{k+1}| = \frac{1}{q_{k+1}}|q_{k+1}\alpha - p_{k+1}| < \frac{1}{q_{k+1}}|q_k\alpha - p_k| \le \frac{1}{q_k}|q_k\alpha - p_k| = |\alpha - c_k|$$

تزودنا الكسور المتواصلة بطريقة فعالة لتمثيل العدد غير الكسري α لأنها تقدم لنا أفضل تقريب كسري للعدد α وهذا ما سندرسه فيما تبقى من هذا البند.

مبرهنة (٦,١٥)

ليكن $\alpha = [a_0; a_1, a_2, \ldots]$ الكسر المتواصل للعدد غير الكسري α. إذا كان a و b عددين صحيحين حيث $b > 0$ وكان k عدداً صحيحاً موجباً يحقق $|b\alpha - a| < |q_k\alpha - p_k|$ فإن $b \ge q_{k+1}$.

البرهان

لنفرض لغرض التناقض أن $b < q_{k+1}$. ولنعتبر نظام المعادلات الديوفنتية:

$$p_k x + p_{k+1} y = a$$
$$q_k x + q_{k+1} y = b$$

بضرب المعادلة الأولى بالعدد q_k والثانية بالعدد p_k ومن ثم طرح المعادلة الثانية من الأولى نجد أن:

$$(p_{k+1}q_k - p_kq_{k+1})y = aq_k - bp_k$$

ولكن $p_{k+1}q_k - p_kq_{k+1} = (-1)^k$. فنجد $y = (-1)^k(aq_k - bp_k)$.

وبالمثل نجد أن $x = (-1)^k(pb_{k+1} - aq_{k+1})$. وبهذا يكون

$$|b\alpha - a| = |q_kx + q_{k+1}y)\alpha - (p_kx + p_{k+1})|$$
$$= |x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})|$$

سنبرهن الآن أن $x(q_k\alpha - p_k)$ و $y(q_{k+1}\alpha - p_{k+1})$ لهما الإشارة نفسها وذلك بإثبات أن إشارتي x و y مختلفتان وكذلك إشارتي $q_k\alpha - p_k$ و $q_{k+1}\alpha - p_{k+1}$ مختلفتان.

لاحظ أولاً أن $x \neq 0$. لأنه لو كان $x = 0$ فإن $bp_{k+1} = aq_{k+1}$. وبما أن $(q_{k+1}, p_{k+1}) = 1$ فإن $q_{k+1} \mid b$. ومنه فإن $q_{k+1} \leq b$ مما يناقض فرضيتنا. وعليه فإن $x \neq 0$.

لاحظ أيضاً أن $y \neq 0$. لأنه لو كان $y = 0$ فإن $a = p_kx$ و $b = q_kx$. ولذا فإن $|b\alpha - a| = |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k|$ مما يناقض الفرض. إذن، $y \neq 0$.

لنفرض الآن أن $y < 0$. بما أن $q_kx = b - q_{k+1}y$ وأن $b > 0$ ، $q_{k+1} > 0$ و $q_k > 0$ فإن $x > 0$.

وإذا كان $y > 0$ وأن $a_{k+1}y \geq q_{k+1} > b$ فإن $q_kx < 0$. ولذا فإن $x < 0$.

وأخيراً بما أن $\frac{p_{k+1}}{q_{k+1}} < \alpha < \frac{p_k}{q_k}$ أو أن $\frac{p_k}{q_k} < \alpha < \frac{p_{k+1}}{q_{k+1}}$ فإن $q_k\alpha - p_k$ و $q_{k+1}\alpha - p_{k+1}$ مختلفا الإشارة.

وبهذا نخلص إلى أن للمقدارين $x(q_k\alpha-p_k)$ و $y(q_{k+1}\alpha-p_{k+1})$ الإشارة نفسها. الآن

$$\begin{aligned}|b\alpha-a| &= |x(q_k\alpha-p_k)+y(q_{k+1}\alpha-p_{k+1})|\\ &= |x|\,|q_k\alpha-p_k|+|y|\,|q_{k+1}\alpha-p_{k+1}|\\ &\geq |x|\,|q_k\alpha-p_k| \geq |q_k\alpha-p_k|\end{aligned}$$

وهذا تناقض. وبالتالي فإن $b \geq q_{k+1}$ ◆

تبين لنا المبرهنة التالية أن المقارب c_k للعدد غير الكسري α هو أفضل تقريب كسري للعدد α من بين جميع الأعداد الكسرية التي مقاماتها أصغر من أو تساوي q_k.

مبرهنة (٦,١٦)

إذا كان $\alpha=[a_0;a_1,a_2,\ldots]$ عدداً غير كسري وكان $\frac{a}{b}$ عدداً كسرياً حيث $b>0$ وكان $k\in\mathbb{Z}^+$ حيث $|\alpha-\frac{a}{b}|<|\alpha-\frac{p_k}{q_k}|$ فإن $b>q_k$.

البرهان

لنفرض لغرض التناقض أن $b\leq q_k$. بما أن $|\alpha-\frac{a}{b}|<|\alpha-\frac{p_k}{q_k}|$ فإن $|b\alpha-a|<|q_k\alpha-p_k|$. ولذا باستخدام المبرهنة (٦,١٥) نجد أن $b\geq q_{k+1}$. وبهذا يكون $q_{k+1}\leq q_k$ وهذا مستحيل. وبالتالي نستنتج أن $b>q_k$ ◆

مثال (٦,٥)

ليكن $\alpha=\frac{1+\sqrt{5}}{2}$. لاحظ أن $a_0=[a_0]=1, \alpha_1=\frac{1}{\alpha_0-a_0}=\frac{1+\sqrt{5}}{2}$. حينئذ، $\alpha=\frac{1+\sqrt{5}}{2}=[1;1,1,1,\ldots]=1.618033\ldots$ من الواضح أن α دوري وأن α.

الجدول التالي يبين لنا قيم c_k و $\alpha-c_k$ حيث $0\leq k\leq 6$.

k	a_k	p_k	q_k	$c_k = p_k / q_k$	$\alpha - c_k$
0	1	1	1	$1/1 = 1$	0.6180...
1	1	2	1	$2/1 = 2$	−0.3819...
2	1	3	2	$3/2 = 1.5$	0.1180...
3	1	5	3	$5/3 = 1.666...$	−0.0486...
4	1	8	5	$8/5 = 1.6$	0.0180...
5	1	13	8	$13/8 = 1.625...$	−0.0069...
6	1	21	13	$21/13 = 1.615...$	0.0026...

وكما هو متوقع فإن c_k يتناوب في كونه أصغر من α وأكبر من α وأنه كلما ازداد k فإن c_k يقترب أكثر فأكثر من α □

مثال (٦,٦)

جد الكسر المتواصل للعدد غير الكسري $\pi = \alpha$.

الحل

$$a_0 = [\alpha_0] = 3 \ , \ \alpha_1 = \frac{1}{\alpha_0 - a_0} = 7.0625133 .$$

$$a_1 = [\alpha_1] = 7 \ , \ \alpha_2 = \frac{1}{\alpha_1 - a_1} = 15.9965959 .$$

$$a_2 = [\alpha_2] = 15 \ , \ \alpha_3 = \frac{1}{\alpha_2 - a_2} = 1.0034157 .$$

$$a_3 = [\alpha_3] = 1 \ , \ \alpha_4 = \frac{1}{\alpha_3 - a_3} = 292.7655078 .$$

$$a_4 = [\alpha_4] = 292 \ , \ \alpha_5 = \frac{1}{\alpha_4 - a_4} = 1.3063224 .$$

ولذا فإن $\pi = [3; 7, 15, 1, 292, \ldots]$.

الجدول التالي يبين لنا قيم c_k حيث $0 \le k \le 4$.

k	a_k	p_k	q_k	$c_k = p_k / q_k$
0	3	3	1	$3/1 = 3$
1	7	22	7	$22/7 = 3.142857$
2	15	333	106	$333/106 = 3.141509$
3	1	355	113	$355/113 = 3.141592$
4	292	5	103993	$103933/33102 = 3.141592$

ولذا فإن $\frac{22}{7}$ هو أفضل تقريب كسري للعدد π مقامه أقل من 106 □

لقد بينا في المبرهنة (٦,١٣) أنه إذا كان α عدداً غير كسري فإن المسافة بين المقارب c_k و α أقل من $\frac{1}{q_k^2}$ ، كما بينت لنا المبرهنة (٦,١٦) أن أفضل تقريب كسري للعدد α مقامه معلوم يجب أن يكون أحد مقاربات العدد α. والمبرهنة التالية تبين لنا أنه إذا كان العدد الكسري $\frac{a}{b}$ قريباً من α فإن $\frac{a}{b}$ يجب أن يكون أحد مقاربات العدد α، وسنستخدم هذه المبرهنة لاحقاً في هذا الفصل حيث تزودنا بالعلاقة بين الكسور المتواصلة ومعادلة بيل (*Pell's equation*).

مبرهنة (٦,١٧)

إذا كان α عدداً غير كسري وكان $\frac{a}{b}$ عدداً كسرياً حيث $b > 0$ وكان $|\alpha - \frac{a}{b}| < \frac{1}{2b^2}$ فإن $\frac{a}{b} = c_k$ حيث $k \geq 0$.

البرهان

لنفرض أن $\frac{a}{b} \neq c_k$ لكل $k \geq 0$. عندئذ، $aq_k \neq bp_k$ لكل $k \geq 0$. لكن $q_k \geq k$ لكل $k \geq 0$ و $q_k < q_{k+1}$ لكل $k \geq 1$. ولذا فيوجد $k \geq 1$ حيث $q_k \leq b < q_{l+1}$. الآن:

$$|\frac{a}{b}-\frac{p_k}{q_k}|=|\frac{aq_k-bp_k}{bq_k}|=\frac{|aq_k-bp_k|}{bq_k}\geq\frac{1}{bq_k} \qquad (١)$$

وبما أن $aq_k \neq bp_k$ فإن:

$$|a/b-p_k/q_k|\leq|a/b-\alpha|+|\alpha-p_k/q_k|<1/2b^2+|\alpha-p_k/q_k| \quad (٢)$$

وبما أن $b<q_{k+1}$ فإننا نجد باستخدام المبرهنة (٦,١٥) أن $|q_k\alpha-p_k|\geq|b\alpha-a|$، وبما أن $|\alpha-\frac{a}{b}|<\frac{1}{2b^2}$ فإن $|b\alpha-a|<\frac{1}{2b}$.

ولذا فإننا نحصل على:

$$|\alpha-\frac{p_k}{q_k}|=\frac{|q_k\alpha-p_k|}{q_k}\leq\frac{1}{2bq_k} \qquad (٣)$$

من المتباينات (١) ، (٢) و (٣) نحصل على:

$$\frac{1}{bq_k}\leq|a/b-p_k/q_k|<\frac{1}{2b^2}+\frac{1}{2bq_k}$$

ويضرب طرفي المتباينة بالعدد $2b^2q_n$ والتبسيط نحصل على $b<q_k$ وهذا تناقض.

إذن، يوجد $k\geq 0$ حيث $\frac{a}{b}=\frac{p_k}{q_k}$ ◆

(٦,٢,٢) تمارين محلولة (Solved Exercises)

تمرين (١)

إذا كان $a^2\equiv -1(\mathrm{mod}\ n)$ حيث $n>1$ وكان $c_k=\frac{p_k}{q_k}$ المقارب ذو الرتبة k في الكسر المتواصل للعدد $\frac{a}{n}$ حيث $q_k<\sqrt{n}\leq q_{k+1}$ فأثبت أن n مجموع مربعين. بالتحديد $n=(aq_k-np_k)^2+q_k^2$.

الحل

بما أن $a^2 \equiv -1 \pmod{n}$ فإن $(aq_k - np_k)^2 + q_k^2 \equiv 0 \pmod{n}$.

وباستخدام المبرهنة (٦,١٣) لدينا $|a/b - p_k/q_k| \le \frac{1}{q_k q_{k+1}}$.

ونرى أن $|aq_k - np_k| \le \frac{n}{q_{k+1}}$. وبما أن $q_{k+1} \ge \sqrt{n}$ فإن $|aq_k - np_k| \le \sqrt{n}$. وبما أن $(aq_k - np_k)^2 + q_k^2 < 2n$ فإن $q_k < \sqrt{n}$. وبما أن $q_k \ge 1$ فإننا نخلص إلى أن $(aq_k - np_k)^2 + q_k^2$ عدد صحيح موجب مضاعف للعدد n وأقل من $2n$. وبهذا يكون $(aq_k - np_k)^2 + q_k^2 = n$ △

تمرين (٢)

ليكن $\frac{a}{b} < \alpha < \frac{c}{d}$ حيث α عدد غير كسري، $a, b, c, d \in \mathbb{Z}^+$ و $bc - ad = 1$. أثبت أن $\frac{a}{b}$ أو $\frac{c}{d}$ مقارب للعدد α. هل يمكن أن يكون كلاهما مقاربان للعدد α ؟

الحل

باستخدام المبرهنة (٦,١٧) يكفي أن نثبت أن $|\alpha - \frac{a}{b}| < \frac{1}{2b^2}$ أو أن $|\alpha - \frac{c}{d}| < \frac{1}{2d^2}$. لنفرض لغرض التناقض أن $|\alpha - \frac{a}{b}| > \frac{1}{2b^2}$ وأن $|\alpha - \frac{c}{d}| > \frac{1}{2d^2}$. حينئذ،

$$\frac{1}{bd} = \frac{bc - ad}{bd} = \frac{c}{d} - \frac{a}{b} = |\alpha - \frac{a}{b}| + |\alpha - \frac{c}{d}| > \frac{1}{2b^2} + \frac{1}{2d^2}.$$

وبضرب طرفي المتباينة بالعدد $2b^2d^2$ نحصل على $2bd > b^2 + d^2$. أي أن $(b-d)^2 < 0$ وهذا مستحيل.

من الممكن أن يكون كلاً من $\frac{a}{b}$ و $\frac{c}{d}$ مقارباً. لأنه لو أخذنا k فردياً فإن

$p_k q_{k+1} - p_{k-1} q_k = 1$ وإن $\frac{p_{k-1}}{q_{k-1}} < \alpha < \frac{p_k}{q_k}$ △

تمرين (٣)

إذا كان $a,b \in \mathbb{Z}^+$ حيث $\pi < \frac{a}{b} < \frac{22}{7}$ فأثبت أن $b \geq 113$.

الحل

لاحظ أن $\pi = [3; 7, 15, 1, 292, \ldots]$ وأن $\frac{p_3}{q_3} = \frac{355}{113}$. لنفرض أن $\frac{a}{b} < \frac{355}{113}$. عندئذ ، $|\pi - \frac{355}{113}| < |\pi - \frac{a}{b}|$. ومن ثم باستخدام المبرهنة (٦,١٦) نجد أن $b > 113$.

لنفرض الآن أن $\frac{a}{b} \geq \frac{355}{113}$. حينئذ، $\pi < \frac{355}{113} \leq \frac{a}{b} < \frac{22}{7}$. إذا كان $\frac{a}{b} = \frac{355}{113}$ فإن $b \geq 113$. أما إذا كان $\frac{a}{b} > \frac{355}{113}$ فإن $|\frac{a}{b} - \frac{22}{7}| < \frac{22}{7} - \frac{355}{113} = \frac{1}{7 \times 113}$. وبالضرب بالعدد $7b$ نحصل على $0 < |7a - 22b| < \frac{b}{113}$. وبما أن $7a - 22b \neq 0$ فإن $|7a - 22b| \geq 1$. ونستنتج أن $\frac{b}{113} > 1$. أي أن $b > 113$ △

تمرين (٤)

إذا كان $\alpha > 1$ عدداً حقيقياً حيث $\alpha = [a_0; a_1; a_2, \ldots]$ فأثبت أن $\frac{1}{\alpha} = [0; a_0, a_1, a_2, \ldots]$. وإذا كان $\frac{p_k}{q_k}$ و $\frac{P_k}{Q_k}$ المقارب ذو الرتبة k لكل من α و $\frac{1}{\alpha}$ على التوالي فأثبت أن $\frac{P_k}{Q_k} = \frac{q_{k-1}}{p_{k-1}}$.

الحل

باستخدام المبرهنة (٦,٨) لدينا :

$$[0; a_0, a_1, a_2, \ldots] = 0 + \frac{1}{[a_0; a_1, a_2, \ldots]} = \frac{1}{\alpha}$$

ولذا فإن $\frac{P_k}{Q_k} = [0; a_0, a_1, a_2, \ldots, a_{k-1}] = \frac{1}{[a_0; a_1, a_2, \ldots a_{k-1}]} = \frac{q_{k-1}}{p_{k-1}}$ △

تمرين (٥)

إذا كان $\alpha = [a_0; a_1, a_2, \ldots]$ فأثبت أن $\lim_{k\to\infty} c_k = \alpha$ إذا وفقط إذا كان $\lim_{k\to\infty} q_k\, q_{k+1} = \infty$.

الحل

باستخدام المبرهنة (٦,٧) نعلم أن $\lim_{k\to\infty} c_k = \alpha$ إذا وفقط إذا كان $\lim_{k\to\infty} c_k = \lim_{k\to\infty} c_{k+1} = \alpha$. ولكن باستخدام المبرهنة (٦,٦) لدينا

$$c_{k+1} - c_k = \frac{(-1)^k}{q_{k+1} q_k}.$$

وبهذا نرى أن $\lim_{k\to\infty} c_k = \alpha$ إذا وفقط إذا كان $\lim_{k\to\infty} q_k q_{k+1} = \infty$ △

تمرين (٦,٢)

(١) جد كسراً متواصلاً لكل من الأعداد غير الكسرية التالية:

(أ) $\sqrt{6}$ (ب) $\sqrt{5}$ (ج) $\sqrt{15}$

(د) $\sqrt[3]{2}$ (هـ) $\frac{e^2-1}{e^2+1}$ (و) 2π

(٢) جد العدد غير الكسري الذي يمثل الكسر المتواصل التالي:

(أ) $[2; 2, 2, 2, \ldots]$ (ب) $[2; 1, 2, 1, 2, \ldots]$

(ج) $[-1; 3, 2, 3, 2, 3, 2, \ldots]$ (د) $[1; 3, 3, 3, \ldots]$

(٣) أثبت أن $e=[2;1,2,1,1,4,1,1,6,1,1,8,1,\dots]$.

(٤) إذا كان α عدداً حقيقياً وكان $\alpha=[1;2;3,a]$ حيث $a\geq 1$ فجد α.

(٥) ليكن $\alpha=[a_0;a_1,a_2,\dots]$ و $\beta=[b_0;b_1,b_2,\dots]$ حيث $a_i=b_i$ لكل $0\leq i\leq n-1$ و $a_n\neq b_n$. أثبت أن:

(أ) إذا كان n زوجياً فإن $\alpha>\beta$ إذا وفقط إذا كان $a_n>b_n$.

(ب) إذا كان n فردياً فإن $\alpha>\beta$ إذا وفقط إذا كان $b_n>a_n$.

(٦) ليكن $\alpha=[a_0;a_1,\dots,a_{n-1}]$ و $\beta=[a_0;a_1,\dots,a_{n-1},b_n,\dots]$.

أثبت أن $\alpha>\beta$ إذا وفقط إذا كان n عدداً زوجياً. [إرشاد: استخدم التمرين (٥)].

(٧) بين ما إذا كان $\alpha>\beta$ أو $\alpha<\beta$ لكل مما يلي:

(أ) $\alpha=[1;2,3,4,5]$ و $\beta=[1;2,3,5,4,\dots]$

(ب) $\alpha=[1;2,3,4,5]$ و $\beta=[1;2,3,5,4,\dots]$.

(ج) $\alpha=[1;2,3,4,5,6,\dots]$ و $\beta=[1;2,3,4]$.

(د) $\alpha=[292;1,15,7]$ و $\beta=[292;1,1,\dots]$.

(هـ) $\alpha=[292;1,15,7,\dots]$ و $\beta=[292;1,15]$.

(٨) جد أفضل تقريب كسري $\frac{a}{b}$ للعدد $\sqrt{2}$ مقامه أصغر من أو يساوي 70. ثم بدون حساب $\sqrt{2}-\frac{a}{b}$ أثبت أن $|\sqrt{2}-\frac{a}{b}|<0.000085$.

(٩) إذا علمت أن $\sqrt{18}=[4;4,8,4,8,\dots]$ فجد جميع الأعداد الكسرية $\frac{a}{b}$ حيث $(a,b)=1$ و $10<b<1000$ و $|\sqrt{18}-\frac{a}{b}|<\frac{1}{5b^2}$.

(١٠) إذا كان $|\sqrt{18}-\frac{140}{33}|<|\sqrt{18}-\frac{a}{b}|$ فأثبت أن $b\geq 48$.

(١١) هل $\frac{22}{9}$ أحد مقاربات $\sqrt{6}$؟ أجب على ذلك دون حساب مقاربات $\sqrt{6}$.

(١٢) جد أفضل تقريب كسري للعدد $\frac{\sqrt{6}-4}{2}$ مقامة لا يزيد عن 369.

(١٣) إذا كان $\sqrt{2} < \frac{a}{b} < \frac{99}{70}$ حيث كل من a و b عدد صحيح موجب فأثبت أن $b > 169$.

(١٤) إذا كان α عدداً غير كسري وكان $a \in \mathbb{Z}$ و $b \in \mathbb{Z}^+$ حيث $|\alpha - \frac{p_k}{q_k}| < |\alpha - \frac{a}{b}|$ فأثبت أن $b > \frac{1}{2} q_{k+1}$.

(١٥) إذا كان $|\sqrt{2} - \frac{41}{29}| < |\sqrt{2} - \frac{a}{b}|$ فاستخدم التمرين (١٤) لاثبات أن $b \geq 36$.

(١٦) إذا كان $\pi < \frac{a}{b} < \frac{22}{7}$ فأثبت أن $b > 106$.

(١٧) إذا كان $|\pi - \frac{a}{b}| < |\pi - \frac{355}{113}|$ فأثبت أن $b > 655|$. ثم جد أفضل تقريب كسري للعدد π من بين جميع الأعداد الكسرية التي مقاماتها لا تزيد عن $|655|$.

(١٨) إذا علمت أن $\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, \ldots]$ فجد أفضل تقريب كسري للعدد π من بين جميع الأعداد الكسرية التي مقاماتها لا تزيد عن 130000.

(١٩) إذا كان $\alpha = [a_0; a_1, a_2, \ldots]$ عدداً غير كسري وكان $a \in \mathbb{Z}$ و $b \in \mathbb{Z}^+$ حيث $\frac{p_k}{q_k} < \frac{a}{b} < \alpha$ أو $\alpha < \frac{a}{b} < \frac{p_k}{q_k}$ فأثبت أن $b > q_{k+1}$.

(٢٠) إذا كان α عدداً غير كسري فأثبت أن $|\alpha - \frac{p_k}{q_k}| < \frac{1}{2q_k q_{k+1}}$ لكل $k \geq 0$.

(٢١) جد عدداً كسرياً $\frac{a}{b}$ يحقق $|\pi - \frac{a}{b}| < |\pi - \frac{22}{7}|$ و $b < 106$ [إرشاد: استخدم تمرين (٢٠)].

(٢٢) إذا كان α عدداً غير كسري وكان $|b\alpha - a| \geq \frac{1}{b}$ حيث $(a,b) = 1$ و $b \geq 1$ فأثبت أنه لا يمكن أن يكون $\frac{a}{b}$ مقارباً للعدد α.

(٢٣) إذا كان α عدداً غير كسري فأثبت أن $|\alpha-\frac{p_k}{q_k}|>\frac{1}{q_k(q_k+q_{k+1})}$.

(٢٤) إذا كان α عدداً غير كسري فأثبت أن $|\alpha-\frac{p_k}{q_k}|<\frac{1}{2q_k^2}$ أو أن $|\alpha-\frac{p_{k+1}}{q_{k+1}}|<\frac{1}{2q_{k+1}^2}$.

(٢٥) إذا كان α عدداً غير كسري فأثبت أنه لكل $\varepsilon>0$ يوجد $k\geq 1$ حيث $|\alpha-\frac{p_k}{q_k}|>\frac{1-\varepsilon}{q_k^2}$.

(٢٦) أثبت أنه يوجد عدد غير منته من المقاربات $\frac{p_k}{q_k}$ للعدد غير الكسري α التي تحقق $|\alpha-\frac{p_k}{q_k}|<\frac{1}{\sqrt{5}\,q_k^2}$. [إرشاد: أثبت أن على الأقل واحد من بين ثلاث مقاربات متتالية يحقق المتباينة].

(٦,٣) الكسور المتواصلة الدورية
Periodic Continued Fractions

ندرس في هذا البند الكسور المتواصلة للأعداد التي على الصورة $\frac{a+\sqrt{d}}{b}$ حيث $a,b\in\mathbb{Z}$ و $d\in\mathbb{Z}^+$ ليس مربعاً كاملاً (أي أن $\sqrt{d}$ عدد غير كسري). سنبرهن أن الكسور المتواصلة التي تمثل مثل هذه الأعداد هي كسور دورية، وبالعكس، أي كسر متواصل دوري يجب أن يكون تمثيلاً لعدد على الصورة أعلاه.

تعريف (٦,٦)

نقول إن الكسر المتواصل غير المنته البسيط $[a_0; a_1, a_2, a_3, \dots]$ كسراً دورياً إذا وجد عددان صحيحان $K \geq 0$ و $m \geq 1$ حيث $a_k = a_{k+m}$ لكل $k \geq K$. ويسمى أصغر عدد صحيح m دورة *(period)* الكسر المتواصل. كما نقول إن الكسر المتواصل دوري تماماً *(purely periodic)* إذا وجد $m \geq 1$ حيث $a_k = a_{k+m}$ لكل $k \geq 0$.

ملحوظة

إذا كان $[a_0; a_1, a_2, a_3 \dots]$ دوري ودورته m فإننا نكتب

$$[a_0; a_1, a_2, \dots] = [a_0; a_1, \dots, a_n, \overline{c_0, c_1, \dots, c_{m-1}}].$$

وإذا كان دوري تماماً فإننا نكتب $[a_0; a_1, a_2, \dots] = \overline{[a_0; a_1, a_2, \dots, a_{m-1}]}$.

مثال (٦,٧)

لقد وجدنا في المثال (٦,٤) أن $\sqrt{35} = [5; 1, 10, 1, 10, \dots]$. ولذا فإن $\sqrt{35}$ دوري ودورته 2 . أي أن $\sqrt{35} = [5; \overline{1,10}]$. كما وجدنا في المثال (٦,٥) أن $\frac{1+\sqrt{5}}{2} = [1; 1, 1, 1, \dots]$. ولذا فإن $\frac{1+\sqrt{5}}{2}$ دوري تماماً وأن $\frac{1+\sqrt{5}}{2} = [\bar{1}]$ □

تعريف (٦,٧)

نقول إن العدد غير الكسري α عدداً تربيعياً *(quadratic irrational)* إذا كان α جذراً للمعادلة التربيعية $ax^2 + bx + c = 0$ حيث $a,b,c \in \mathbb{Z}$ و $a \neq 0$.

مثال (٦,٨)

العدد $\alpha = \frac{1+\sqrt{5}}{2}$ غير كسري وهو جذراً للمعادلة $x^2 - x - 1 = 0$. وبهذا يكون α عدد غير كسري تربيعي □

مبرهنة (٦,١٨)

يكون العدد الحقيقي α عدداً غير كسري تربيعي إذا وفقط إذا وكان $\alpha=\frac{r+\sqrt{d}}{s}$ حيث $r,d,s\in\mathbb{Z}$ ، $d>0$ ، $s\neq 0$ و d ليس مربعاً كاملاً.

البرهان

لنفرض أولاً أن α عدد غير كسري تربيعي. حينئذ، يوجد $a,b,c\in\mathbb{Z}$ حيث $a\alpha^2+b\alpha+c=0$. وبحل هذه المعادلة نرى أن $\alpha=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$. وبما أن α عدد غير كسري فإن $b^2-4ac>0$ ليس مربعاً كاملاً وأن $a\neq 0$. بوضع $r=-b$ ، $d=b^2-4ac$ ، $s=2a$ أو $r=b$ ، $d=b^2-4ac$ ، $s=-2a$ نرى أن $\alpha=\frac{r+\sqrt{d}}{s}$.

لبرهان العكس، نفرض أن $\alpha=\frac{r+\sqrt{d}}{s}$ حيث $r,d,s\in\mathbb{Z}$ ، $d>0$ و $s\neq 0$ و d ليس مربعاً كاملاً . عندئذ، α عدد غير كسري و α جذراً للمعادلة $s^2x^2-2rsx+(r^2-d)=0$. وبالتالي فإن α عدد غير كسري تربيعي ◆

ملحوظة

لاحظ أن $s\mid(d-r^2)$ في المبرهنة (٦,١٨). وإذا حصل وأن كان $\alpha=\frac{r+\sqrt{d}}{s}$ حيث $s\nmid(d-r^2)$ فإن $\alpha=\frac{R+\sqrt{D}}{S}$ حيث $D=ds^2$ ، $R=r\mid s\mid$ و $S=s\mid s\mid$ وأن $S\mid(D-R^2)$.

نقدم الآن خوارزمية لحساب الكسر المتواصل للعدد غير الكسري التربيعي.

مبرهنة (٦,١٩)

ليكن $\alpha=\alpha_0=\frac{r_0+\sqrt{d}}{s_0}$ عدد غير كسري تربيعي حيث d ليس مربعاً كاملاً و $s_0\mid(d-r_0^2)$. ضع $a_0=[\alpha_0]$ ، $\alpha_{k+1}=\frac{1}{\alpha_k-a_k}$ و $a_{k+1}=[\alpha_{k+1}]$

لكل $k \geq 0$. ولنفرض أن $r_{k+1} = a_k s_k - r_k$ و $s_{k+1} = \frac{d - r_{k+1}^2}{s_k}$. عندئذ لكل $k \geq 0$ لدينا:

(أ) كل من r_k و s_k عدداً صحيحاً وأن $s_k \neq 0$.

(ب) $s_k \mid (d - r_k^2)$.

(ج) $\alpha_k = \frac{r_k + \sqrt{d}}{s_k}$. ومن ثم فإن $a_k = [\frac{r_k + \sqrt{d}}{s_k}]$.

البرهان

باستخدام الاستقراء الرياضي على k.

من الواضح أن العبارات صحيحة عند $k = 0$. لنفرض الآن أن العبارات صحيحة عند k. من الواضح أن r_{k+1} عدد صحيح وأن $r_{k+1} \equiv -r_k \pmod{s_k}$. ولذا فإن $d - r_{k+1}^2 \equiv d - r_k^2 \equiv 0 \pmod{s_k}$. ومن ثم فإن $s_{k+1} = \frac{d - r_{k+1}^2}{s_k}$ عدد صحيح وأن $s_{k+1} \neq 0$ لأن d ليس مربعاً كاملاً. كما أن $d - r_{k+1}^2 = s_k s_{k+1}$. ومنه فإن $s_{k+1} \mid (d - r_{k+1}^2)$. وأخيراً ، بما أن $\alpha_k = \frac{r_k + \sqrt{d}}{s_k}$ فإن:

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k} = \frac{s_k}{r_k + \sqrt{d} - a_k s_k} = \frac{s_k}{-r_{k+1} + \sqrt{d}}$$

$$= \frac{s_k (r_{k+1} + \sqrt{d})}{d - r_{k+1}^2} = \frac{r_{k+1} + \sqrt{d}}{s_{k+1}}$$

ولذا فإن جميع العبارات صحيحة عند $k+1$ ◆

ملحوظات

إذا كان $\alpha = \frac{r_0 + \sqrt{d}}{s_0}$ عدداً غير كسري تربيعي فإننا نستطيع تبسيط حساب الكسر المتواصل للعدد α بملاحظة ما يلي:

(١) $a_k=[\alpha_k]=[\frac{r_k+\sqrt{d}}{s_k}]=[\frac{r_k+d_0}{s_k}]$ حيث $d_0=[\sqrt{d}]$. ولرؤية ذلك لاحظ $d_0<\sqrt{d}<d_0+1$ وأنه باستخدام خوارزمية القسمة نجد أن $r_k+d_0=qs_k+t$ حيث $0\le t\le s_k-1$. ولذا فإن $qs_t+t<\sqrt{d}+r_k<qs_k+t+1$. ومنه فإن

$$q\le q+\frac{t}{sk}<\frac{\sqrt{d}+r_k}{s_k}<q+\frac{t+1}{s_k}\le q+1$$

وبالتالي فإن $[\frac{\sqrt{d}+r_k}{s_k}]=[\frac{d_0+r_k}{s_k}]$.

(٢) $s_{k+1}=s_{k-1}+a_k(r_k-r_{k+1})$. ولإثبات ذلك لاحظ أن $s_ks_{k+1}=d-r_{k+1}^2$ وأن $s_{k-1}s_k=d-r_k^2$. وبالطرح نحصل على:

$(r_k-r_{k+1})(r_k+r_{k+1})=r_k^2-r_{k+1}^2=s_k(s_{k+1}-s_{k-1})$. ولكن $r_k+r_{k+1}=a_ks_k$. ومن ثم فإن $s_k(s_{k+1}-s_{k-1})=a_ks_k(r_k-r_{k+1})$.

وبالتالي فإن $s_{k+1}=s_{k-1}+a_k(r_k-r_{k+1})$.

مثال (٦,٩)

جد الكسر المتواصل للعدد $\alpha=\alpha_0=\frac{7-\sqrt{11}}{3}$.

الحل

بما أن $\frac{7-\sqrt{11}}{3}=\frac{-7+\sqrt{11}}{-3}$ وأن 3- لا يقسم 7^2-11 ، بضرب البسط والمقام بالعدد 3 نحصل على $\alpha=\alpha_0=\frac{-21-\sqrt{99}}{-9}$. ولذا فإن

$a_0=[\alpha_0]=1$ ، $d=99$ ، $d_0=9$ ، $r_0=-21$ ، $s_0=-9$ ، $s_1=5$. الآن

k	$r_{k+1}=a_k s_k - r_k$	$s_{k+1}=s_{k-1}+a_k(r_k-r_{k+1})$	$a_{k+1}=[\frac{r_{k+1}+d_0}{s_{k+1}}]$
0	-21	-9	1
1	12	5	4
2	8	7	2
3	6	9	1
4	3	10	1
5	7	5	3
6	8	7	

وبما أن $r_6=r_2$ و $s_6=s_2$ فنجد $\frac{7-\sqrt{11}}{3}=[1;\overline{4,2,1,1,3}]$ □

تعريف (٦,٨)

إذا كان $\alpha=\frac{r+\sqrt{d}}{s}$ عدداً غير كسري تربيعي فإننا نعرف مرافق α (*conjugate*) بأنه العدد $\alpha'=\frac{r-\sqrt{d}}{s}$.

المبرهنة التالية تزودنا بالخصائص الأساسية للمرافق.

مبرهنة (٦,٢٠)

ليكن كل من α و β عدداً غير كسري تربيعي. عندئذ:

(١) إذا كان α جذراً للمعادلة $ax^2+bx+c=0$ فإن α' هو الجذر الآخر.

(٢) $(\alpha+\beta)'=\alpha'+\beta'$.

(٣) $(\alpha-\beta)'=\alpha'-\beta'$.

(٤) $(\alpha\beta)'=\alpha'\beta'$.

(٥) $(\frac{\alpha}{\beta})'=\frac{\alpha'}{\beta'}$.

البرهان

◆ يترك كتمرين للقارئ

سنبرهن الآن الخاصية الأساسية للكسور المتواصلة الدورية والتي تنسب إلى لاجرانج (*Lagrange*). ولكننا نحتاج قبل ذلك للمبرهنة التالية.

مبرهنة (٦,٢١)

ليكن α عدداً غير كسري تربيعي وليكن $r,s,t,u \in \mathbb{Z}$. عندئذ:

إما أن $\frac{r\alpha+s}{t\alpha+u}$ عدد كسري أو أنه عدد غير كسري تربيعي.

البرهان

بما أن α عدد غير كسري تربيعي فإن $\alpha=\frac{a+\sqrt{b}}{c}$ حيث $a,b,c \in \mathbb{Z}$ ،

$b>0$ ، $c\neq 0$ و b ليس مربعاً كاملاً. الآن

$$\frac{r\alpha+s}{t\alpha+u}=\frac{\frac{r(a+\sqrt{b})}{c}+s}{\frac{t(a+\sqrt{b})}{c}+u}$$

$$=\frac{(ar+cs)+r\sqrt{b}}{(at+cu)+t\sqrt{b}}$$

$$=\frac{[(ar+cs)+r\sqrt{b}]\,[(at+cu)-t\sqrt{b}]}{(at+cu)^2-t^2b}$$

$$=\frac{[(ar+cs)(at+cu)]-[r(at+cu)=t(ar+cs)]\sqrt{b}}{(at+cu)^2t^2b}$$

ولذا فباستخدام المبرهنة (٦,١٨) نجد أن $\frac{r\alpha+s}{t\alpha+u}$ عدد غير كسري تربيعي إلا إذا كان معامل $\sqrt{b}$ صفراً فيكون في هذه الحالة عدد كسري ◆

مبرهنة (٦,٢٢) [مبرهنة لاجرانج]

يكون الكسر المتواصل غير المنته البسيط للعدد غير الكسري α دورياً إذا وفقط إذا كان α عدداً تربيعياً.

البرهان

لنفرض أولاً أن $\alpha=[a_0; a_1, \dots, a_n, \overline{c_0, c_1, \dots, c_{m-1}}]$ عدد غير كسري دوري. ولنفرض أن $\beta=[\overline{c_0; c_1, \dots, c_{m-1}}]$. باستخدام المبرهنة (٦,٤) نجد أن

$$\beta=\frac{\beta p_{m-1}+p_{m-2}}{\beta q_{m-1}+q_{m-2}}$$

حيث $\frac{p_{m-1}}{q_{m-1}}$ و $\frac{p_{m-2}}{q_{m-2}}$ مقاربات للكسر المتواصل $[c_0; c_1, \dots, c_{m-1}]$. وبهذا يكون

$$\beta^2 q_{m-1}+(q_{m-2}-p_{m-1})\beta-p_{m-1}=0 .$$

وبما أن β عدد غير كسري (تمثيله غير منته) فنخلص إلى أن β عدد غير كسري تربيعي.

الآن: $\alpha=[a_0; a_1, \dots, a_n, \beta]$. باستخدام المبرهنة (٦,٤) نجد أن:

$$\alpha=\frac{\beta p_n+p_{n-1}}{\beta q_n+q_{n-1}}$$

حيث $\frac{p_n}{q_n}$ و $\frac{p_{n-1}}{q_{n-1}}$ مقاربان للكسر المتواصل $[a_0; a_1, \dots, a_n]$.

بما أن β عدد غير كسري تربيعي فإننا نجد باستخدام المبرهنة (٦,٢١) أن α عدد غير كسري تربيعي.

ولبرهان العكس، نفرض أن α عدد غير كسري تربيعي. باستخدام الخوارزمية المقدمة في المبرهنة (٦,١٩) نجد أن $\alpha=[a_0; a_1, a_2, a_3, \dots]$. ولإثبات أن هذا التمثيل دورياً سنجد عدد صحيح $m \geq 1$ حيث $a_{m+t}=a_{n+t}$ لكل $n>m$ ولكل $t \in \mathbb{Z}^+$.

سنبرهن أولاً على وجود $m \in \mathbb{Z}^+$ حيث $\alpha'_m<0$ (α'_m هو مرافق α_m).

باستخدام المبرهنة (٦,١١) لدينا $\alpha-\frac{p_k}{q_k}=\frac{(-1)^k}{q_k(\alpha_{k+1}q_k+q_{k-1})}$.

ولذا فإن $\alpha' - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k(\alpha'_{k+1}q_k + q_{k-1})}$. ومنه فإن

$$(\alpha - \frac{p_k}{q_k})(\alpha' - \frac{p_k}{q_k}) = \frac{1}{q_k^2(\alpha_{t+1}q_k + q_{k-1})(\alpha'_{k+1}q_k + q_{k-1})} .$$

بما أن $\alpha' \neq \alpha$ وأن $\frac{p_k}{q_k}$ يتقارب إلى α فيوجد k حيث $\alpha' < \frac{p_k}{q_k} < \alpha$ أو $\alpha < \frac{p_k}{q_k} < \alpha'$. ولذا فإن $(\alpha - \frac{p_k}{q_k})(\alpha' - \frac{p_k}{q_k}) < 0$. ومنه فإن $\alpha'_{k+1}q_k + q_{k-1} < 0$. وبالتالي إذا كان $m = k+1$ فنجد أن $\alpha'_m < 0$.

سنبرهن الآن أن $-1 < \alpha'_{m+1} < 0$. بما أن $\alpha_{m+1} = \frac{1}{\alpha_m - a_m}$ فإن $\alpha'_{m+1} = \frac{1}{\alpha'_m - a_m} < 0$. وبما أن $a_m \geq 1$ فإن $\alpha'_{m+1} > -1$. إذن، $-1 < \alpha'_{m+1} < 0$.

ولذا فإننا نخلص إلى أنه إذا كان $\alpha'_m < 0$ فإن $-1 < \alpha'_n < 0$ لكل $n > m$.

لنفرض الآن أن k كبير ما فيه الكفاية حيث $-1 < \alpha'_k < 0$. عندئذ، $\alpha_k = \frac{r_k + \sqrt{d}}{s_k}$ فإن $\alpha_k - \alpha'_k = \frac{2\sqrt{d}}{s_k} > 1$. ومنه فإن $0 < s_k < 2\sqrt{d}$. وبما أن $\alpha_k \alpha'_k = \frac{r_k^2 - d}{s_k^2}$. ولهذا نرى $r_k^2 < 0$. أي أن $-\sqrt{d} < r_k < \sqrt{d}$. ولذا، عندما يكون k كبير جداً فإن عدد القيم المختلفة للزوج r_k, s_k يكون على الأكثر $2d$. وبهذا نستطيع إيجاد $m, n \in \mathbb{Z}$ يحققان $m < n$، $r_n = r_m$ و $s_n = s_m$. ومن ثم فإن $a_{m+t} = a_{n+t}$ لكل $t \in \mathbb{Z}^+$، ونخلص إلى أن الكسر المتواصل للعدد α دوري ◆

مثال (٦,١٠)

جد العدد غير الكسري α الذي تمثيله الدوري $[1;\overline{1,4,8}]$.

الحل

لنفرض أن $\beta=[\overline{4;8}]$. عندئذ، $\alpha=[1;1,\beta]=1+\frac{1}{1+\frac{1}{\beta}}=1+\frac{\beta}{\beta+1}$.

ولكن $\beta=4+\frac{1}{8+\frac{1}{p}}=4+\frac{\beta}{8\beta+1}$. ونرى أن $2\beta^2-8\beta-1=0$. وبحل المعادلة

نجد أن $\beta=\frac{4+3\sqrt{2}}{2}$. وبهذا يكون $\alpha=1+\frac{\beta}{\beta+1}=1+\frac{1+\sqrt{2}}{3}=\frac{4+\sqrt{2}}{3}$ □

(٦,٣,١) الكسور المتواصلة الدورية تماماً

(Purely Periodic Continued Fractions)

سنصنف الآن الأعداد غير الكسرية التي تكون كسورها المتواصلة دورية تماما.

تعريف (٦,٩)

نقول إن العدد غير الكسري التربيعي α مختزل *(Reducible)* إذا كان $\alpha>1$ و $-1<\alpha'<0$.

مثال (٦,١١)

إذا كان $\alpha=\frac{4+3\sqrt{2}}{2}$ فإن $\alpha>1$ وإن $\alpha'=\frac{4-3\sqrt{2}}{2}$. ولذا فإن $-1<\alpha'=-0.1213\ldots<0$. ويكون α مختزلاً. لاحظ أن $\alpha=[\overline{4;8}]$ (انظر المثال (٦,١٠)) □

مبرهنة (٦,٢٣)

ليكن α عدداً غير كسري تربيعي. عندئذ $\alpha=[\overline{a_0;a_1,a_2,\ldots,a_{m-1}}]$ إذا وفقط إذا كان α مختزلاً. إضافة إلى ذلك $\frac{-1}{\alpha'}=[\overline{a_{m-1};a_{m-2},\ldots,a_1,a_0}]$.

البرهان

لنفرض أولاً أن $\alpha=[a_0; a_1, a_2, \dots]$ مختزل ولنفرض أن α_k هي كما في التعريف (٦,٥). بما أن $\alpha_{k+1}=\frac{1}{\alpha_k-a_k}$ فإن $\alpha'_{k+1}=\frac{1}{\alpha'_k-a_k}$.

لاحظ أنه إذا كان $\alpha'_k<0$ فإن $-1<\alpha'_{k+1}<0$ (لأن $a_k\geq 1$). ولذا إذا كان α_k مختزلاً فإن α_{k+1} كذلك. ولكن $\alpha=\alpha_0$ مختزلاً. وبهذا يكون α_n مختزلاً لكل n.

الآن، بما أن $\alpha_{k+1}=\frac{1}{\alpha'_k-a_k}$ فإن $\alpha'_k=a_k+\frac{1}{\alpha_{k+1}}$. وبوضع $\beta_i=-\frac{1}{\alpha'_i}$ نحصل على $\beta_{k+1}=a_k+\frac{1}{\beta_k}$. لاحظ أن $0<\beta_k<1$. ولذا فإن $a_k=[\beta_{k+1}]$. وبما أن الكسر المتواصل للعدد α دوري ودورته m فيوجد j حيث $\alpha_{m+j}=\alpha_j$. ونرى أن $\beta_{m+j}=\beta_j$. الآن إذا كان $j>0$ فإن $\beta_j=a_{j-1}+\frac{1}{\beta_{j-1}}$ وأن $\beta_{m+j}=a_{m+j-1}+\frac{1}{\beta_{m+j-1}}$. وبما أن $a_{j-1}=[\beta_j]$ وأن $a_{m+j-1}=[\beta_{m+j}]$ فيكون $a_{j-1}=a_{m+j-1}$ و $\frac{1}{\beta_j}=\frac{1}{\beta_{m+j-1}}$. وبالقلب وأخذ المرافق نحصل على $\alpha_{j-1}=\alpha_{m+j-1}$. إذا كان $j-1>0$ فإننا نستمر على هذا المنوال إلى أن نحصل على $\alpha_0=\alpha_m$. وبالتالي فإن الكسر المتواصل للعدد α دوري تماماً.

لبرهان العكس نفرض أن $\alpha=\overline{[a_0; a_1, a_2, \dots, a_{m-1}]}$. إذا كان $m=1$ فمن الواضح أن α مختزل. لنفرض أن $m>1$. بما أن $\alpha_0=\alpha_m>1$ فإن $a_0\geq 1$. ولذا فإن $a_i>0$ لكل i. وبوضع $k=m-1$ في المعادلة $\beta_{k+1}=a_k+\frac{1}{\beta_k}$ نجد أن

$$\beta_0=\beta_m=a_{m-1}+\frac{1}{\beta_{m-1}}=[a_{m-1};\beta_{m-1}]$$

ولكن $\beta_{m-1}=a_{m-2}+\frac{1}{\beta_{m-2}}$. ويكون $\beta_0=[a_{m-1}; a_{m-2}, \beta_{m-2}]$. وبالاستمرار نحصل في النهاية على $\beta_0=[a_{m-1}; a_{m-2}, \dots, a_1, a_0, \beta_0]$. ونستنتج أن

$$-\frac{1}{\alpha'_0}=-\frac{1}{\alpha'}=\beta_0=\overline{[a_{m-1}; a_{m-2}, \dots, a_1, a_0, \beta_0]}$$

وأخيراً ، $-\frac{1}{\alpha'}>1$. ونخلص إلى أن α مختزل ◆

مثال (٦,١٢)

بين أن $\alpha=\frac{4+\sqrt{37}}{7}$ دوري تماماً وجد كسره المتواصل.

الحل

بما أن $\alpha>1$ وأن $-1<\alpha'=\frac{4-\sqrt{37}}{7}<0$ فإن α مختزل. ولذا فالكسر المتواصل الذي يمثله دوري تماماً. لاحظ أن $7\mid 37-4^2$. ولإيجاد الكسر المتواصل تستخدم المبرهنة (٦,١٩) لنحصل على:

k	r_k	s_k	a_k
0	4	7	1
1	3	4	2
2	5	3	3
3	4	7	

وبما أن $r_3=r_0$ و $s_3=s_0$ فإننا نخلص إلى أن $\frac{4-\sqrt{37}}{7}=\overline{[1;2,3]}$ □

(٦,٣,٢) الكسر المتواصل للعدد $\sqrt{d}$ (*Continued Fraction For* $\sqrt{d}$)

في البند القادم سندرس معادلة بيل وسنرى أن إيجاد حلول هذه المعادلة يكافيء إيجاد الكسر المتواصل للعدد $\sqrt{d}$ حيث $d\in\mathbb{Z}^+$ ليس مربعاً كاملاً. ولذا يكون من المهم معرفة كيفية إيجاد الكسر المتواصل لهذا العدد. لاحظ أولاً أن $\sqrt{d}$ ليس مختزلاً ولكن العدد غير الكسري التربيعي $\sqrt{d}+[\sqrt{d}]$ مختزلاً وهو ما نستخدمه لإيجاد الكسر المتواصل للعدد $\sqrt{d}$.

مبرهنة (٦,٢٤)

إذا كان $d \in \mathbb{Z}^+$ ليس مربعاً كاملاً فإن $\sqrt{d} = \overline{[a_0; a_1, a_2, \ldots, a_{m-1}, 2a_0]}$ حيث $a_0 = [\sqrt{d}]$ و $a_i = a_{m-i}$ لكل $1 \le i \le m-1$.

البرهان

لنفرض أن $a_0 = [\sqrt{d}]$ وأن $\alpha = [\sqrt{d}] + \sqrt{d}$. من الواضح أن الكسر المتواصل للعدد α دوري تماماً وأن $[\alpha] = 2[\sqrt{d}] = 2a_0$. وبهذا نجد أن

$$\alpha = [\sqrt{d}] + \sqrt{d} = \overline{[2a_0; a_1, a_2, \ldots, a_{m-1}]}$$
$$= [2a_0; a_1, a_2, \ldots, a_{m-1}, \overline{2a_0, a_1, a_2, \ldots, a_{m-1}}]$$

ونستنتج $\sqrt{d} = \alpha - [\sqrt{d}] = \alpha - a_0 = [a_0; \overline{a_1, a_2, \ldots, a_{m-1}, 2a_0}]$.

ولإكمال البرهان نثبت أن $a_i = a_{m-i}$ لكل $1 \le i \le m-1$. الآن باستخدام المبرهنة (٦,٢٣) لدينا:

$$-\frac{1}{\alpha'} = \frac{1}{\sqrt{d} - [\sqrt{d}]} = \overline{[a_{m-1}; a_{m-2}, \ldots, a_2, a_1, 2a_0]}$$

وبما أن $\sqrt{d} - [\sqrt{d}] = [0; \overline{a_1, a_2, \ldots, a_{m-1}, 2a_0}]$ فنخلص إلى أن

$$\overline{[a_1; a_2, \ldots, a_{m-1}, 2a_0]} = \overline{[a_{m-1}; a_{m-2}, \ldots, a_2, a_1, 2a_0]}$$

إذن، $a_i = a_{m-i}$ لكل $1 \le i \le m-1$ ◆

ملحوظات

(١) لاحظ أن دورة $\sqrt{d}$ تبدأ بعد الحد الأول.

(٢) الحد الوحيد في الكسر المتواصل للعدد $\sqrt{d}$ الذي يساوي $2a_0 = 2[\sqrt{d}]$ هو الحد الأخير في الدورة. ولذا عند حساب الكسر المتواصل فإننا نتوقف عند الحصول على $2[\sqrt{d}]$. على سبيل المثال لحساب الكسر المتواصل للعدد $\sqrt{23}$ فإننا نتوقف عند الحصول على الحد $2[\sqrt{d}] = 8$ فيكون $\sqrt{d} = [4; 1, 3, 1, 8]$.

(٣) الجدول (٤) يبين الكسر المتواصل للعدد $\sqrt{d}$ حيث $1 < d < 100$ وحيث أن d ليس مربعاً كاملاً.

مبرهنة (٦,٢٥)

ليكن $\frac{p_k}{q_k}$ هو المقارب ذو الرتبة k للعدد $\sqrt{d}$ وليكن r_k و s_k هي كما في المبرهنة (٦,١٩) . عندئذ ، $\frac{p_k+q_k\sqrt{d}}{p_{k-1}+q_{k-1}\sqrt{d}}=\frac{r_{k+1}+\sqrt{d}}{s_k}$ لكل $k\geq 0$.

البرهان

باستخدام الاستقراء الرياضي على k.

إذا كان $k=0$ فإن $r_0=0$ و $s_0=1$. وبما أن $\sqrt{d}=\frac{0+\sqrt{d}}{1}$ فإن $r_1=a_0s_0-r_0=a_0$. ولذا فإن الطرف الأيمن من المتطابقة هو $a_0+\sqrt{d}$. وأما الطرف الأيسر فهو $\frac{p_0+q_0\sqrt{d}}{p_{-1}+q_{-1}\sqrt{d}}$. وتكون العبارة صحيحة عند $k=0$.

لنفرض الآن أن العبارة صحيحة عند $k=m$. بما أن $p_{m+1}=a_{m+1}p_m+p_{m-1}$ وأن $q_{m+1}=a_{m+1}q_m+q_{m+1}$ فإن

$$p_{m+1}+q_{m+1}\sqrt{d}=a_{m+1}(p_m+q_m\sqrt{d})+p_{m-1}+q_{m-1}\sqrt{d}.$$

ونجد:

$$\begin{aligned}\frac{p_{m+1}+q_{m+1}\sqrt{d}}{p_m+q_m\sqrt{d}}&=a_{m+1}+\frac{p_{m-1}+q_{m-1}\sqrt{d}}{p_m+q_m\sqrt{d}}\\&=a_{m+1}+s_m\frac{\sqrt{d}-r_{m+1}}{d-r_{m+1}^2}\\&=a_{m+1}+\frac{\sqrt{d}-r_{m+1}}{s_{m+1}}\\&=a_{m+1}+\frac{\sqrt{d}-r_{m+1}}{s_{m+1}}\end{aligned}$$

$$= \frac{a_{m+1}s_{m+1} - r_{m+1} + \sqrt{d}}{s_{m+1}}$$

$$= \frac{r_{m+2} + \sqrt{d}}{s_{m+1}}$$

وبالتالي فإن العبارة صحيحة عند $k = m+1$ ◆

مبرهنة (٦,٢٦)

إذا كانت دورة الكسر المتواصل للعدد $\sqrt{d}$ هي m وكان $\frac{p_k}{q_k}$ المقارب من الرتبة k وكان كل من r_k و s_k كما في المبرهنة (٦,١٩) فإن:

(١) $p_{k-1}^2 - dq_{k-1}^2 = (-1)^k s_k$.

(٢) $s_k > 0$ لكل $k \geq 0$.

(٣) $s_k > 1$ إذا وفقط إذا كان $k \mid m$.

البرهان

(١) باستخدام المبرهنة (٦,٢٥) وأخذ المرافق نحصل على:

$$\frac{p_j + q_j\sqrt{d}}{p_{j-1} + q_{j-1}\sqrt{d}} = \frac{r_{j+1} + \sqrt{d}}{s_j} \quad \text{و} \quad \frac{p_j - q_j\sqrt{d}}{p_{j-1} - q_{j-1}\sqrt{d}} = \frac{r_{j+1} - \sqrt{d}}{s_j}$$ لكل $j \geq 0$. وبضرب المعادلتين أعلاه واستخدام المتطابقة $d - r_{j+1}^2 = s_j s_{j+1}$ نحصل على:

$$\frac{p_j^2 - dq_j^2}{p_{j-1}^2 - dq_{j-1}^2} = -\frac{s_{j+1}}{s_j}.$$

ويكون:

$$\prod_{j=0}^{k-1} \frac{p_j^2 - dq_j^2}{p_{j-1}^2 - dq_{j-1}^2} = \prod_{j=0}^{k-1} -\frac{s_{j+1}}{s_j}.$$

إذن ،

$$\frac{p_{k-1}^2 - dq_{k-1}^2}{p_{-1}^2 - dq_{-1}^2} = (-1)^k \frac{s_k}{s_0}.$$

وبما أن $p_{-1}=1$ ، $q_{-1}=0$ و $s_0=1$ فإننا نخلص إلى أن $p_{k-1}^2-dq_{k-1}^2=(-1)^k s_k$.

(٢) باستخدام المبرهنة (٦,٧) نعلم أن $c_{2i}<\sqrt{d}<c_{2j+1}$ لكل $i\geq 0$ وكل $j\geq 0$. ولذا فإن $\frac{p_j^2-dq_j^2}{p_{j-1}^2-dq_j^2}>0$ لكل $j\geq 0$. أي أن $\frac{sj+1}{s_j}>0$ لكل $j\geq 0$. وبما أن $s_0=1$ فإن $s_k>0$ لكل $k\geq 0$.

(٣) سنثبت أن $s_{jm}=1$ لكل $j\geq 1$. باستخدام المبرهنة (٦,٢٤) نعلم أن $\sqrt{d}=[a_0;\overline{a_1,a_2,\ldots,a_{m-1},2a_0}]$. وإذا كانت α_k كما في التعريف (٦,٥) فإننا نجد أن: $\ldots=\alpha_{3m}=\alpha_{2m}=\alpha_m=[\sqrt{d}]+\sqrt{d}$ ولكن باستخدام المبرهنة (٦,١٩) نعلم أن $\alpha_k=\frac{r_k+\sqrt{d}}{s_k}$. ولذا فإن $s_{jm}=1$ لكل $j\geq 1$. وعلى وجه الخصوص إذا كان $m\mid k$ فإن $s_k=1$.

لنفرض الآن أن $s_k=1$ حيث $k\geq 1$. بما أن للعدد α_k كسر متواصل دوري تماماً فإن α_k مختزل. ولذا فإن $0<\alpha_k'<1$. ولكن $\alpha_k'=\frac{r_k-\sqrt{d}}{s_k}=r_k-\sqrt{d}$. ومنه فإن $0<\sqrt{d}-r_k<1$. أي أن $r_k=[\sqrt{d}]$. إذن، $\alpha_k=[\sqrt{d}]+\sqrt{d}$. وبهذا فإن k يجب أن يكون مضاعفاً لدورة $[\sqrt{d}]+\sqrt{d}$ وهي m. إذن، $m\mid k$ ◆

(٦,٣,٣) استخدام الكسور المتواصلة في التحليل

(Factoring Using Continued Fraction)

قدمنا في الفصل الأول طريقة فيرما لتحليل الأعداد الفردية حيث اعتمدنا على أن العدد الفردي n مؤلف إذا وفقط إذا كان $n=x^2-y^2$. وفي هذه الحالة نستطيع تحليل العدد $n=(x+y)(x-y)$. اعتمدت طريقة فيرما على البحث عن مربع كامل من بين حدود المتتالية

$$t^2-n,(t+1)^2-n,(t+2)^2-n,\ldots$$

حيث t هو أصغر عدد صحيح أكبر من $\sqrt{n}$. ومن المعلوم أنه إذا كان $n=ab$ فإن طريقة فيرما مناسبة عندما يكون القاسمان a و b قريبين من بعض. من الممكن استبدال الشرط $n=x^2-y^2$ بشرط أضعف وهو وجود أعداد صحيحة غير صفرية x,y,z حيث $nz=x^2-y^2$. أي أن $x^2-y^2\equiv 0(\bmod n)$. وبهذا تكون قواسم العدد n هي قواسم للعدد x^2-y^2 . وفي هذه الحالة لا بد من وجود قاسم d للعدد n حيث d يقسم $x+y$ أو $x-y$. وإذا كان $d\neq 1$ و $d\neq n$ فإننا نكون قد وجدنا قاسماً فعلياً للعدد n ونجحنا في اجتياز الخطوة الأولى لتحليل n. إن جوهر المسألة هو أنه بمجرد الحصول على عددين صحيحين x و y يحققان $n\mid x^2-y^2$ فنستطيع وبسهولة معرفة ما إذا كان $(x+y,n)>1$ أو $(x-y,n)>1$ وذلك باستخدام خوارزمية إقليدس. ولذا إذا وجد حل موجب للمعادلة $nz=x^2-y^2$ فنقوم بحساب كل من $(x+y,n)=d_1$ و $(x-y,n)=d_2$. وبما أن $d_1\mid n$ و $d_2\mid n$ فنكون قد حللنا n جزئياً إذا كان d_1 أو d_2 قاسماً فعلياً. وبالطبع إذا كان n أولياً فإن d_1 و d_2 هي 1 و n .

لضمان نجاح طريقة فيرما المعدلة نحتاج إلى إيجاد فرق بين مربعين يقبل القسمة على n وهنا نلجأ إلى الكسور المتواصلة لأنه إذا كان $n>0$ ليس مربعاً كاملاً فنعلم استناداً إلى المبرهنة (٦,٢٦) أن $p_k^2-nq_k^2=(-1)^{k+1}s_{k+1}$ لكل $k\geq 0$ حيث $\frac{p_k}{q_k}$ هو المقارب ذو الرتبة k لكسر $\sqrt{n}$ المتواصل وأن s_{k+1} هي كما في المبرهنة (٦,١٩).

إذا كان k فردياً وكان s_{k+1} مربعاً كاملاً وليكن $s_{k+1}=y^2$ فتأخذ المعادلة أعلاه الشكل المطلوب: $p_k^2-y^2=nq_k^2$

إن هذه الطريقة قابلة للتطبيق لأن لدينا خوارزميات فعالة لحساب s_{k+1} و p_k وحساب الكسر المتواصل $\sqrt{n}$. لاحظ أننا لسنا بحاجة لحساب q_k. وعند حصولنا على p_k و $y=\sqrt{s_{k+1}}$ نلجأ إلى خوارزمية إقليدس لحساب كل من (p_k+y,n) و (p_k-y,n).

مثال (٦,١٣)

حلل العدد $n = 22223$ باستخدام الكسور المتواصلة.

الحل

باستخدام المبرهنة (٦,١٩) لإيجاد الكسر المتواصل للعدد $\sqrt{22223}$ نجد أن $\sqrt{22223} = [149; 13, 1, 1, 4, 1, 1, 1, 1, 4, 1, 1, 13, 298]$. نقوم الآن بانشاء الجدول التالي مع اختزال p_k قياس 22223 لتصغير الأعداد.

k	r_k	s_k	a_k	p_k
0	0	1	149	149
1	149	22	13	1938
2	137	157	1	2087
3	20	139	1	4025
4	119	58	4	18187
5	113	163	1	22212
6	50	121	1	18176
7	71	142	1	18165
8	71	121	1	

لاحظ أن أول قيمة تجعل s_k مربعاً كاملاً هي $s_6 = 121$. ولذا فإن $x^2 - y^2 \equiv 0 (\text{mod } n)$ حيث $x = p_5 = 22212$ و $y = \sqrt{s_6} = 11$. الآن باستخدام خوارزمية إقليدس نجد أن:

$$(x + y, n) = (22223, 22223) = 22223$$

$$(x - y, n) = (22201, 22223) = 1$$

وهذا يقودنا إلى التحليل التافه $n = n \times 1$. بأخذ القيمة التالية التي تجعل s_k مربعاً كاملاً وهي $s_8 = 121$. نجد أن $x = p_7 = 18165$ و $y = \sqrt{s_8} = 11$. الآن :

$$(x + y, n) = (18176, 22223) = 71$$

$$(x - y, n) = (18154, 22223) = 313$$

وبهذا نحصل على التحليل $22223 = 71 \times 313$. لاحظ أن كل من 71 و 313 عدداً أولياً □

(٦,٣,٤) تمارين محلولة (*Solved Exercises*)

تمرين (١)

جد الكسر المتواصل لكل من $\sqrt{n^2+1}$ و $\sqrt{n^2+1}+n^2$ حيث $n \in \mathbb{Z}^+$.

الحل

باستخدام المبرهنة (٦,١٩) لدينا

k	r_k	s_k	a_k
0	0	1	n
1	n	1	$2n$
2	n	1	

بما أن $r_2 = r_1$ و $s_2 = s_1$ فإن $\sqrt{n^2+1}$ دوري وأن $\sqrt{n^2+1} = [n;\overline{2n}]$. الآن

$$\sqrt{n^2+1}+n^2 = n^2+[n;\overline{2n}] = n^2+n+\frac{1}{[\overline{2n}]} = [n^2+n;\overline{2n}] \quad \triangle$$

تمرين (٢)

إذا كان $a,b \in \mathbb{Z}^+$ حيث $b = ac$ فأثبت أن $[\overline{b;a}] = \dfrac{b+\sqrt{b^2+4c}}{2}$. ومن ثم جد $[\overline{n}]$.

الحل

لنفرض أن $\alpha = [\overline{b;a}]$. عندئذ، $\alpha = b+\dfrac{1}{a+\dfrac{1}{\alpha}} = \dfrac{(ab+1)\alpha+b}{a\alpha+1}$.

ومنه فإن $a\alpha^2 - ab\alpha - b = 0$. ويكون

$$\alpha=\frac{ab+\sqrt{a^2b^2+4ab}}{2a}=\frac{ab+\sqrt{a^2b^2+4a^2c}}{2a}=\frac{b+\sqrt{b^2+4c}}{2}$$

لنفرض الآن أن $\alpha=[\overline{n;n}]$. وبوضع $a=b=n$ و $c=1$ نحصل على

$$\triangle \quad \alpha=[\overline{n}]=\frac{n+\sqrt{n^2+4}}{2}$$

تمرين (٣)

إذا كان $\alpha=\sqrt{d}$ حيث d ليس مربعاً كاملاً وكانت α_k ، r_k و s_k هي كما في المبرهنة (٦,١٩) فأثبت أن $0<r_k<\sqrt{d}$ وأن $0<s_k<2\sqrt{d}$ لكل $k\geq 1$.

الحل

باستخدام المبرهنة (٦,٢٦) نعلم أن $s_k>0$ لكل k. ونرى أن $0<s_k=\frac{d-r_k^2}{2_{k-1}}$. ومنه فإن $r_k<\sqrt{d}$. لنفرض الآن أن $r_k\leq 0$. بما أن $r_k=a_{k-1}s_{k-1}-r_{k-1}$ فإن $s_{k-1}\leq a_{k-1}s_{k-1}\leq r_{k-1}<\sqrt{d}$. ولكن:

$$1<\frac{1}{\alpha_{k-1}-a_{k-1}}=\alpha_k=\frac{r_k+\sqrt{d}}{s_k}$$. وبهذا نجد:

$$1>\alpha_{k-1}-a_{k-1}=\frac{1}{\alpha_k}=\frac{s_k}{r_k+\sqrt{d}}=\frac{d-r_k^2}{s_{k-1}(r_k+\sqrt{d})}=\frac{\sqrt{d}-r_k}{s_{k-1}}>\frac{\sqrt{d}}{s_{k-1}}>1$$

وهذا مستحيل. إذن، $r_k>0$. وأخيراً، بما أن $r_{k+1}=a_ks_k-r_k$ فإن :

$$\triangle \quad s_k=\frac{r_k+r_{k+1}}{a_k}\leq r_k+r_{k+1}<2\sqrt{d}$$

تمرين (٤)

أثبت أن طول دورة الكسر المتواصل للعدد $\sqrt{d}$ تساوي1 إذا وفقط إذا كان $d=a_0^2+1$.

الحل

لنفرض أن طول الدورة هو1. عندئذ، $\sqrt{d}=[a_0,\overline{2a_0}]$. لنفرض أن $\alpha=[\overline{2a_0}]$. ولذا فإن $\alpha=2a_0+\frac{1}{\alpha}$. ومنه فإن $\alpha^2-2a_0\alpha-1=0$. أي أن $\alpha=a_0+\sqrt{a_0^2+1}$. ويكون $\sqrt{d}=a_0+\frac{1}{\alpha}=a_0+\frac{1}{a_0+\sqrt{a_0^2+1}}=\sqrt{a_0^2+1}$.

وبالعكس، إذا كان $d=a_0^2+1$ فنجد باستخدام التمرين المحلول (١) أن $\sqrt{d}=[a_0;\overline{2a_0}]$. ويكون طول الدورة يساوي1 △

تمارين (٦,٣)

(١) جد الكسر المتواصل لكل من الأعداد التالية:

(أ) $\sqrt{31}$ (ب) 46 (ج) $\sqrt{76}$

(د) $\sqrt{47}$ (هـ) $\sqrt{130}$ (و) $\frac{7+\sqrt{130}}{9}$ (ز) $\frac{2+\sqrt{10}}{2}$

(٢) جد العدد الذي له الكسر المتواصل التالي:

(أ) $[2;1,\overline{5}]$ (ب) $[2;\overline{1,5}]$ (ج) $[\overline{2;1,5}]$ (د) $[2;3,\overline{1,}]$

(هـ) $[\overline{1;2}]$ (و) $[1;3,\overline{1,2}]$ (ز) $[\overline{3;1,7}]$ (ح) $[3;\overline{1,7}]$ (ط) $[5;\overline{2,1,3}]$

(٣) (أ) أثبت أن $\sqrt{n^2+2}=[n;\overline{n,2n}]$ لكل $n\geq 1$.

(ب) استخدم الفقرة (أ) لإيجاد الكسر المتواصل لكل من الأعداد $\sqrt{9803}$ ، $\sqrt{291}$ ، $\sqrt{11666}$.

(٤) (أ) أثبت أن $\sqrt{n^2-1}=[n-1;\overline{1,2n-2}]$ لكل $n\geq 2$.

(ب) استخدم الفقرة (أ) لإيجاد الكسر المتواصل لكل من الأعداد $\sqrt{9800}$ ، $\sqrt{288}$ ، $\sqrt{11663}$.

(٥) (أ) أثبت أن $\sqrt{n^2-2}=[n-1;\overline{1,n-2,1,2n-2}]$ لكل $n\geq 3$.

(ب) استخدم الفقرة (أ) لإيجاد الكسر المتواصل لكل من الأعداد $\sqrt{9799}$ ، $\sqrt{287}$ ، $\sqrt{11662}$.

(٦) (أ) أثبت أن $\sqrt{n^2-n}=[n-1;\overline{2,2n-2}]$ لكل $n\geq 2$.

(ب) استخدم الفقرة (أ) لإيجاد الكسر المتواصل لكل من الأعداد $\sqrt{9702}$ ، $\sqrt{272}$ ، $\sqrt{11556}$.

(٧) (أ) إذا كان $n>1$ عدداً فردياً فأثبت أن

$$\sqrt{n^2+4}=[n;\overline{\frac{n-1}{2},1,1,\frac{n-1}{2},2n}]$$

(ب) استخدم الفقرة (أ) لايجاد الكسر المتواصل لكل من $\sqrt{9805}$ و $\sqrt{293}$.

(٨) (أ) إذا كان $n>3$ عدداً فردياً فأثبت أن

$$\sqrt{n^2-4}=[n-1;\overline{1,\frac{n-3}{2},2,\frac{n-3}{2},1,2n-2}]$$

(ب) استخدم الفقرة (أ) لايجاد الكسر المتواصل لكل من $\sqrt{9797}$ و $\sqrt{285}$.

(٩) بين أياً من الأعداد غير الكسرية التربيعية التالية له كسراً متواصلاً دورياً تماماً.

(أ) $\frac{11-\sqrt{10}}{9}$ (ب) $\frac{3+\sqrt{23}}{2}$ (ج) $2+\sqrt{8}$

(د) $4+\sqrt{17}$ (هـ) $\frac{1+\sqrt{3}}{2}$ (و) $\frac{3+\sqrt{13}}{2}$

(ز) $5+\sqrt{32}$ (ح) $\frac{7-\sqrt{11}}{5}$

(١٠) إذا كان d عدداً صحيحاً موجباً ليس مربعاً كاملاً وكان $\frac{a+\sqrt{d}}{b}=\frac{r+\sqrt{d}}{s}$ حيث $b\neq 0$ و $s\neq 0$ فأثبت أن $a=r$ و $b=s$.

(١١) إذا كان $\alpha=[a_0;\overline{a_1,a_2,\ldots a_{m-1},2a_0}]$ حيث $a_i=a_{m-i}$ لكل $1\le i\le m-1$ فأثبت أن $\alpha=\sqrt{r}$ حيث r عدداً كسرياً.

(١٢) إذا كان $\sqrt{d}=[a_0;\overline{a_1,\ldots,a_{m-1},2a_0}]$ وكان r_k و s_k كما في المبرهنة (٦,١٩) فأثبت أن $s_i=s_{m-i}$ و $r_{i+1}=r_{m-i}$ لكل $0\le i\le m$.

(١٣) إذا كان $\sqrt{d}=[a_0;\overline{a_1,\ldots,a_{m-1},2a_0}]$ فأثبت أن $a_k\le a_0$ حيث $1\le k\le m-1$.

(١٤) استخدم الكسور المتواصلة لتحليل كل من الأعداد التالية:

(أ) 1000009 (ب) 76183 (ج) 893 (د) 17819

(٦,٤) معادلة بيل
Pell's Equation

إذا كان d عدداً صحيحاً موجباً ليس مربعاً كاملاً فإن مسألة إيجاد تقريب كسري (أي كسر متواصل) للعدد $\sqrt{d}$ تؤدي إلى إيجاد حل للمعادلة الديوفنتية $x^2-dy^2=1$. لأنه إذا كان (x,y) حلاً للمعادلة حيث $y\neq 0$ فإن

$(x/y)^2 = d + \frac{1}{y^2}$. وعندما يكون y كبيراً جداً فإن x/y تقريب جيد للعدد $\sqrt{d}$.

نسب أويلر المعادلة $x^2 - dy^2 = 1$ إلى الرياضي الانجليزي جون بيل (١٦٦١ – ١٦٨٥م) على الرغم من أن الكثير من الرياضيين حاولوا إيجاد حل للمعادلة قبل بيل بقرون حيث عالج الرياضي الهندي باسكارا *(Bhaskara)* المعادلة في شيء من التفصيل في القرن الثاني عشر للميلاد.

إن أول رياضي أوروبي اهتم بمعادلة بيل هو الرياضي الفرنسي المشهور فيرما *(Fermat)* ، عندما تحدى فيرما في العام ١٦٥٧م الرفيقين جون ولسن *(John Wallis)* ووليام برونكر *(William Brouncker)* لحل المعادلتين $x^2 - 61y^2 = 1$ و $x^2 - 109y^2 = 1$ ، استطاع برونكر حل معادلة بيل بخوارزمية مكافئة للخوارزمية المستخدمة في إيجاد الكسر المتواصل للعدد $\sqrt{d}$ ، واستخدم أويلر الكسر المتواصل للعدد $\sqrt{d}$ لإيجاد أصغر حل موجب للمعادلة وبين إمكانية إيجاد حلول أخرى بمعرفة أحد الحلول مستخدماً علاقات إرتدادية. وعلى الرغم من اعتقاد كل من فيرما وولسن وجود عدد غير منته من الحلول لمعادلة بيل، إلا أن أول من قدم برهاناً لذلك هو الرياضي لاجرانج *(Lagrange)* في العام ١٧٦٨م، وبين أنه يمكن الحصول على هذه الحلول من الكسر المتواصل للعدد $\sqrt{d}$ وسنقدم برهان لاجرانج في هذا البند حيث نبرهن وجود عدد غير منته من الحلول لكل d وأنه يمكن الحصول على الحلول الموجبة من مقاربات $\sqrt{d}$ ، كما سنبرهن أن الحلول الموجبة يمكن توليدها من أصغر حل موجب للمعادلة.

تعريف (٦,١٠)

نقول إن الحل (x_0,y_0) للمعادلة $x^2-dy^2=1$ موجباً إذا كان $x_0>0$ و $y_0>0$. ونسمي أصغر حل موجب للمعادلة، الحل الأساسي (*fundamental soltuion*).

ملحوظات

(١) إذا كان d صغيراً نسبياً فإن الطريقة المناسبة لإيجاد الحل الأساسي للمعادلة $x^2-dy^2=1$ تكون بتجريب قيم متتالية موجبة لـ y ونأخذ أول قيمة تجعل dy^2+1 مربعاً كاملاً.

(٢) من الواضح أنه لإيجاد جميع حلول المعادلة $x^2-dy^2=1$. فإنه يكفي أن نجد جميع الحلول الموجبة.

مبرهنة(٦,٢٧)

إذا كان (p,q) حلاً موجباً للمعادلة $x^2-dy^2=1$ فإن $\frac{p}{q}$ أحد مقاربات $\sqrt{d}$.

البرهان

بما أن $p^2-dq^2=(p-q\sqrt{d})(p+q\sqrt{d})=1$ فإن $p-q\sqrt{d}=\frac{1}{p+q\sqrt{d}}$، ونرى أن $\frac{p}{q}-\sqrt{d}=\frac{1}{q(p+q\sqrt{d})}$. وبما أن $p>q\sqrt{d}$ فإن $p+q\sqrt{d}>2q\sqrt{d}$. ومنه فإن $0<\frac{p}{q}-\sqrt{d}<\frac{1}{2q^2\sqrt{d}}<\frac{1}{2q^2}$. واستناداً إلى المبرهنة (٦,١٧) نجد أن $\frac{p}{q}$ هو أحد مقاربات $\sqrt{d}$ ◆

ملحوظة

إذا كان (p,q) حلاً موجباً للمعادلة $x^2-dy^2=1$ فإن $\frac{p}{q}>\sqrt{d}$. وتكون رتبة المقارب $\frac{p}{q}$ فردية. وعليه فليست جميع مقاربات $\sqrt{d}$ تضمن لنا حلول للمعادلة. سنبين فيما يلي أن المقاربات التي تزودنا بحلول نحصل عليها من معرفتنا لطول دورة $\sqrt{d}$.

مبرهنة (٦,٢٨)

ليكن طول دورة الكسر المتواصل للعدد $\sqrt{d}$ هو m.

(١) إذا كان m زوجياً فإن جميع الحلول الموجبة للمعادلة $x^2-dy^2=1$ هي $x=p_{jm-1}$ و $y=q_{jm-1}$ لكل $j\geq 1$.

(٢) إذا كان m فردياً فإن جميع الحلول الموجبة للمعادلة $x^2-dy^2=1$ هي $x=p_{2jm-1}$ و $y=q_{2jm-1}$ لكل $j\geq 1$.

البرهان

باستخدام المبرهنة (٦,٢٧) نعلم أن الحلول الموجبة للمعادلة $x^2-dy^2=1$ نحصل عليها من مقاربات للعدد $\sqrt{d}$. لنفرض الآن أن (p_k,q_k) حل موجب للمعادلة. ولذا فإن $p_k^2-dq_k^2=1$. ولكن باستخدام المبرهنة (٦,٢٦) لدينا $p_k^2-dq_k^2=(-1)^{k+1}s_{k+1}$. ويكون $s_{k+1}=1$ و k فردي. كذلك $m\mid(k+1)$. أي أن $k+1=jm$ حيث $j\geq 1$. ولذا فإن $p_{jm-1}^2-dq_{jm-1}^2=(-1)^{jm}$. إذا كان m زوجياً فإن p_{jm-1} و q_{jm-1} حل للمعادلة. وإذا كان m فردياً فلكي يكون هناك حل للمعادلة $x^2-dy^2=1$ يجب أن يكون j زوجياً. ونستنتج أن p_{2jm-1} و q_{2jm-1} حل للمعادلة ◆

من المبرهنة (٦,٢٨) نحصل مباشرة على النتيجة التالية:

نتيجة (٦,٢٩)

ليكن m طول دورة الكسر المتواصل للعدد $\sqrt{d}$. عندئذ يوجد عدد غير منته من الحلول الموجبة للمعادلة $x^2 - dy^2 = 1$. وإذا كان m زوجياً فإن الحل الأساسي هو (p_{m-1}, q_{m-1}). وأما إذا كان m فردياً فإن الحل الأساسي هو (p_{2m-1}, q_{2m-1}) ◆

مثال (٦,١٤)

جد الحل الأساسي للمعادلة $x^2 - 23y^2 = 1$.

الحل

نعلم أن $\sqrt{23} = [4; \overline{1, 3, 1, 8}]$. حينئذ، $m = 4$ ويكون الحل الأساسي هو (p_3, q_3). الآن

k	a_k	p_k	q_k
0	4	4	1
1	1	5	1
2	3	19	4
3	1	24	5

وبالتالي فإن $(p_3, q_3) = (24, 5)$ هو الحل الأساسي للمعادلة □

إذا أردنا أن نجد حلولاً أخرى للمعادلة في المثال (٦,١٤) فإن الحل الذي يلي الحل الأساسي هو (p_7, q_7) ولإيجاده يلزمنا أن نكمل انشاء الجدول إلى أن نصل إلى الحل المطلوب، وعوضاً عن ذلك فإنه توجد طريقة أسهل لحساب حلول المعادلة من الحل الأساسي تقدمها لنا المبرهنة التالية:

مبرهنة (٦,٣٠)

إذا كان (x_1,y_1) هو الحل الأساسي للمعادلة $x^2-dy^2=1$ فإن جميع الحلول الموجبة (x_n,y_n) للمعادلة تحقق $x_n+y_n\sqrt{d}=(x_1+y_1\sqrt{d})^n$ لكل $n\geq 1$.

البرهان

سنبرهن أولاً أن (x_n,y_n) حل للمعادلة لكل $n\geq 1$.

$$\begin{aligned}x_n^2-dy_n^2&=(x_n+y_n\sqrt{d})(x_n-y_n\sqrt{d})\\&=(x_1+y_1\sqrt{d})^n(x_1-y_1\sqrt{d})^n\\&=(x_1^2-dy_1^2)^n=1\end{aligned}$$

ولذا فإن (x_n,y_n) حل للمعادلة لكل $n\geq 1$. لنفرض لغرض التناقض أن (a,b) حل موجب للمعادلة مختلفاً عن الحلول (x_n,y_n) لكل $n\geq 1$. عندئذ يوجد عدد صحيح k يحقق $(x_1+y_1\sqrt{d})^k<a+b\sqrt{d}<(x_1+y_1\sqrt{d})^{k+1}$. وبضرب المتباينة بالعدد $(x_1+y_1\sqrt{d})^{-k}=(x_1-y_1\sqrt{d})^k$ نحصل على:

$$1<(a+b\sqrt{d})(x_1-y_1\sqrt{d})^k<x_1+y_1\sqrt{d}.$$

لاحظ أن $x_1^2-dy_1^2=1$. ولذا فإن $\dfrac{1}{x_1+y_1\sqrt{d}}=x_1-y_1\sqrt{d}$. وبوضع $r+s\sqrt{d}=(x_1-y_1\sqrt{d})^k(a+b\sqrt{d})$ نجد أن $1<r+s\sqrt{d}<x_1+y_1\sqrt{d}$ وأن:

$$\begin{aligned}r^2-ds^2&=(r-s\sqrt{d})(r+s\sqrt{d})\\&=(x_1+y_1\sqrt{d})^k(a-b\sqrt{d})(x_1-y_1\sqrt{d})^k(a+b\sqrt{d})\\&=(x_1^2-dy_1^2)^k(a^2-dy^2)=1\end{aligned}$$

ومن ثم فإن (r,s) حل للمعادلة $x^2-dy^2=1$. وبملاحظة أن $1<r+s\sqrt{d}<x_1+y_1\sqrt{d}$ وأن $r+s\sqrt{d}>1$ نجد أن $0<(r+s\sqrt{d})^{-1}=r-s\sqrt{d}<1$. بهذا نرى

$$r=\frac{1}{2}[(r+s\sqrt{d})+(r-s\sqrt{d})]>0$$

$$.s=\frac{1}{2\sqrt{d}}[(r+\sqrt{d})-(r-s\sqrt{d})]>0$$

إذن، فإن (r,s) حل موجب للمعادلة. وبما أن (x_1,y_1) هو أصغر حل موجب للمعادلة فنرى $x_1\le r$ وأن $y_1\le s$. وبهذا نجد أن $x_1+y_1\sqrt{d}<r+s\sqrt{d}$ وهذا تناقض. ونخلص إلى وجود $n\ge 1$ يحقق $(a,b)=(x_n,y_n)$ ◆

نتيجة (٦,٣١)

إذا كان $n\in\mathbb{Z}^+$ وكان (x_n, y_n) كما في المبرهنة (٦,٣٠) فإن جميع حلول المعادلة $x^2-dy^2=1$ هي إما على الصورة (x_n, y_n) أو على الصورة $(-x_n,-y_n)$.

البرهان

إذا كان $n=0$ فإن $x_0+y_0\sqrt{d}=1$. ومنه فإن $x_0=1$ و $y_0=0$. ويكون لدينا الحلان التافهان $(x_0, y_0)=(1,0)$ و $(-x_0,-y_0)=(-1,0)$.

لنفرض الآن أن (a,b) حل موجب للمعادلة. حينئذ، يوجد $n\in\mathbb{Z}^+$ حيث $(a,b)=(x_n,y_n)$. ويكون الحل الآخر $(-a,-b)=(-x_n,-y_n)$. وأخيراً بما أن $x_n-y_n\sqrt{d}=(x_1+y_1\sqrt{d})^{-n}=(x_{-n},y_{-n})$ فإن الحل $(a,-b)$ هو (x_{-n},y_{-n}) والحل $(-a,b)$ هو $(-x_{-n},-y_{-n})$ ◆

نتيجة (٦,٣٢)

إذا كان (x_n,y_n) كما في المبرهنة (٦,٣٠) فإن $x_{n+1}=x_1x_n+y_1y_nd$ وأن $y_{n+1}=x_1y_n+y_1x_n$.

البرهان

$$\begin{aligned} x_{n+1}+y_{n+1}\sqrt{d} &= (x_1+y_1\sqrt{d})(x_1+y_1\sqrt{d})^n \\ &= (x_1+y_1\sqrt{d})(x_n+y_n\sqrt{d}) \\ &= (x_1x_n+y_1y_nd)+(x_1y_n+y_1x_n)\sqrt{d} \end{aligned}$$

ولذا فإن $x_{n+1}=x_1x_n+y_1y_nd$ وأن $y_{n+1}=x_1y_n+y_1x_n$ ◆

باستخدام المبرهنة (٦,٢٨) والمبرهنة (٦,٣٠) نحصل مباشرة على النتيجة التالية.

نتيجة (٦,٣٣)

ليكن (x_n,y_n) حل موجب للمعادلة $x^2-dy^2=1$ وليكن m هو طول دورة $\sqrt{d}$. عندئذ:

$$(x_n,y_n)=\begin{cases}(p_{nm-1},q_{nm-1}), & m \text{ زوجي} \\ (p_{2nm-1},q_{2nm-1}), & m \text{ فردي}\end{cases} \quad ◆$$

مثال (٦,١٥)

جد جميع الحلول الموجبة للمعادلة $x^2-23y^2=1$.

الحل

لقد وجدنا في المثال (٦,١٤) أن الحل الأساسي للمعادلة هو $(x_1,y_1)=(24,5)$. ولذا فإن الحلول الموجبة هي (x_n,y_n) حيث $x_n+y_n\sqrt{23}=(24+5\sqrt{23})^n$ لكل $n\geq 1$ □

(٦,٤,١) المعادلة $x^2-dy^2=-1$ $(\textit{The Equation } x^2-dy^2=-1)$

بعد أن قمنا بإيجاد جميع حلول معادلة بيل ننتقل إلى المعادلة المرادفة $x^2-dy^2=-1$. بطريقة مشابهة تماماً لبرهان المبرهنة (٦,٢٧) نستطيع الحصول على:

مبرهنة (٦,٣٤)

إذا كان (p,q) حلاً موجباً للمعادلة $x^2-dy^2=-1$ فإن $\frac{p}{q}$ أحد مقاربات $\sqrt{d}$.

البرهان

يترك كتمرين للقارئ ◆

مبرهنة (٦,٣٥)

ليكن طول دورة الكسر المتواصل للعدد $\sqrt{d}$ هو m.

(١) إذا كان m زوجياً فإنه لا يوجد حل للمعادلة $x^2-dy^2=-1$.

(٢) إذا كان m فردياً فإن جميع الحلول الموجبة للمعادلة $x^2-dy^2=-1$ هي $x=p_{jm-1}$ و $y=p_{jm-1}$ لكل $j=1,3,5,7,\ldots$ ويكون (p_{m-1},q_{m-1}) هو الحل الأساسي.

(٣) إذا كان m فردياً فإن جميع الحلول الموجبة للمعادلة $x^2-dy^2=1$ هي $x=p_{jm-1}$ و $y=q_{jm-1}$ لكل $j=2,4,6,\ldots$ ويكون الحل الأساسي هو (p_{2m-1},p_{2m-1}).

البرهان

(١) لنفرض أن m زوجي وأن (x,y) حل للمعادلة $x^2-dy^2=-1$. عندئذ، باستخدام المبرهنة (٦,٣٥) نجد أن $\frac{x}{y}=\frac{p_k}{q_k}$ حيث $\frac{p_k}{q_k}$ مقارباً للعدد $\sqrt{d}$. وباستخدام المبرهنة (٦,٢٦)، نجد أن $p_k^2-dq_k^2=(-1)^{k+1}s_{k+1}=-1$. ولذا فإن k زوجي وأن $s_{k+1}=1$. ومنه فإن $m \mid (k+1)$. أي أن $k+1=jm$ فردياً. ويكون m فردياً وهذا تناقض.

(٢) لنفرض أن m فردي. لقد بينا في برهان المبرهنة (٦,٢٨) أن $p_{jm-1}^2 - dq_{jm-1}^2 = (-1)^{jm}$. عندئذ، لوجود حل للمعادلة $x^2 - dy^2 = -1$ يجب أن يكون j فردياً. وبالتالي فإن حلول المعادلة p_{jm-1} و q_{jm-1} حيث $j = 1, 3, 5, 7, \ldots$.

(٣) مماثل للفقرة (٢) ◆

كما هو الحال في المعادلة $x^2 - dy^2 = 1$ فإننا نستطيع الحصول على جميع الحلول الموجبة للمعادلة $x^2 - dy^2 = -1$ من الحل الأساسي وهذا هو فحوى المبرهنة التالية:

مبرهنة (٦,٣٦)

إذا كان (a,b) حلاً أساسياً للمعادلة $x^2 - dy^2 = -1$ وكان $x_n + y_n\sqrt{d} = (a+b\sqrt{d})$ لكل $n \geq 1$ فإن:

(١) (x_2, y_2) الحل الأساسي للمعادلة $x^2 - dy^2 = 1$.

(٢) جميع الحلول الموجبة للمعادلة $x^2 - dy^2 = 1$ تكون على الصورة (x_n, y_n) حيث n زوجي.

(٣) جميع الحلول الموجبة للمعادلة $x^2 - dy^2 = -1$ تكون على الصورة (x_n, y_n) حيث n فردي.

البرهان

(١) لاحظ أولاً أن (x_2, y_2) حل للمعادلة $x^2 - dy^2 = 1$، لأن:

$$\begin{aligned} x_2^2 - dy_2^2 &= (x_2 + y_2\sqrt{d})(x_2 - y_2\sqrt{d}) \\ &= (a+b\sqrt{d})^2(a-b\sqrt{d})^2 \\ &= (a^2 - b^2 d)^2 = (-1)^2 = 1 \end{aligned}$$

ولـــــذا فـــــإن (x_2,y_2) حـــــل للمعادلـــــة $x^2-dy^2=1$.

ويكون $x_2+y_2\sqrt{d}=(r+s\sqrt{d})^n$ حيث $n\geq 1$ و (r,s) هو الحل الأساسي للمعادلة $x^2-dy^2=1$. إذا كان $n=2k$ زوجياً فإن :

$$x_2+y_2\sqrt{d}=(a+b\sqrt{d})^2=(r+s\sqrt{d})^{2k}.$$

وبهذا يكون $a+b\sqrt{d}=(r+s\sqrt{d})^k$.

وبما أن $a+b\sqrt{d}<r+s\sqrt{d}$ فإن $k=0$. ونرى أن $a+b\sqrt{d}=1$ وهـــذا مستحيل. إذن، $n=2k+1$ فردياً. ومنه فإن $(a+b\sqrt{d})^2=(r+s\sqrt{d})^{2k+1}$.

ونجد أن $(r+s\sqrt{d})^{2k}<a+b\sqrt{d}<r+s\sqrt{d}$. وعليه فإن $k=0$. وبالتالي $x_2+y_2\sqrt{d}=(a+b\sqrt{d})^2=r+s\sqrt{d}$. أي ، $x_2=r$ و $y_2=s$. ومن ثم فإن (x_2,y_2) هو الحل الأساسي للمعادلة $x^2-dy^2=1$.

(٢) باستخدام المبرهنة (٦,٣٠) نجد أن جميع الحلول الموجبـــة (x_n,y_n) للمعادلـــة $x^2-dy^2=1$ يجب أن تحقق $x_n+y_n\sqrt{d}=(x_2+y_2\sqrt{d})^n(a+b\sqrt{d})^2$.

(٣) لنفرض أن n فردي. لاحظ أن $(x_n,\ y_n)$ حل للمعادلة $x^2-dy^2=-1$ لأن:

$$\begin{aligned}x_n^2-dy_n^2&=(x_n+y_n\sqrt{d})(x_n-y_n\sqrt{d})\\&=(a+b\sqrt{d})^n(a-b\sqrt{d})^n\\&=(a^2-b^2d)^n=(-1)^n=-1\end{aligned}$$

وذلك لأن n فردي.

لنفـــرض الآن أن (u,v) حـــل آخـــر للمعادلـــة $x^2-dy^2=-1$. إذا كـــان $r+s\sqrt{d}=(a+b\sqrt{d})(u+v\sqrt{d})$ فمن الواضـــح أن (r,s) حـــل للمعادلـــة $x^2-dy^2=1$. ونرى أن $r+s\sqrt{d}=(a+b\sqrt{d})^k$ حيث k زوجياً. ومنه فإن $u+v\sqrt{d}=(a+b\sqrt{d})^{k-1}=x_{k-1}+y_{k-1}\sqrt{d}$ حيـــث $k-1$ فـــردي.

وبالتالي فإن $(u,v)=(x_{k-1},y_{k-1})$ ◆

مثال (٦,١٦)

لقد بينا في المثال (٦,١٤) أن $\sqrt{23}=[4;\overline{1,3,18}]$. ولذا فإن $m=4$ عدداً زوجياً. ومن ثم فإنه لا يوجد حلول موجبة للمعادلة $x^2-23y^2=-1$ □

مثال(٦,١٧)

بما أن $\sqrt{29}=[5;\overline{2,1,1,2,10}]$ فإن $m=5$ فردياً. عندئذ، يوجد حل لكل من المعادلتين $x^2-29y^2=1$ و $x^2-29y^2=-1$. ويكون الحل الأساسي للمعادلة $x^2-29y^2=-1$ هو $(a,b)=(p_4,q_4)=(70,13)$. وعليه فإن جميع الحلول الموجبة للمعادلة $x^2-29y^2=-1$ هي (x_n,y_n) حيث n فردي و $x_n+y_n\sqrt{29}=(70+13\sqrt{29})^n$. وجميع الحلول الموجبة للمعادلة $x^2-29y^2=1$ هي على الصورة أعلاه حيث n زوجي. الحل الأساسي للمعادلة $x^2-29y^2=1$ هو $(x_2,y_2)=(9801,1820)$ □

(٦,٤,٢) المعادلة $x^2-dy^2=N$ *(The Equation $x^2-dy^2=N$)*

ليكن $d,N\in\mathbb{Z}^*$. لدينا الحالات التالية:

(١) إذا كان $d<0$ و $N<0$ فمن الواضح عدم وجود حلول للمعادلة $x^2-dy^2=N$.

(٢) إذا كان $d<0$ و $N>0$ فمن الممكن أن يكون للمعادلة $x^2-dy^2=N$ عدداً منتهياً من الحلول لأن $|x|\le\sqrt{d}$ وأن $|y|\le\sqrt{N/|d|}$.

(٣) إذا كان $d=n^2$ مربعاً كاملاً فـإن $x^2-dy^2=(x-ny)(x+ny)=N$.

وبمـا أن عـدد طـرق تحليـل N منتـه فـإن عـدد الحلـول الممكنـة للمعادلة $x^2-dy^2=N$ يجب أن يكون منتهياً.

ولذا فإننا سندرس إمكانية حل المعادلة $x^2-dy^2=N$ في الحالة التي يكون فيها $d>0$ ليس مربعاً كاملاً.

سنبرهن الآن أن وجود حل للمعادلة يؤدي إلى وجود عدد غير منتـه مـن الحلول.

مبرهنة (٦,٣٧)

إذا كان للمعادلة $x^2-dy^2=N$ حلاً موجباً فإنه يوجد عدد غير منته مـن الحلول.

البرهان

لنفرض أن (a,b) حل موجب للمعادلة $x^2-dy^2=1$. وأن (r,s) حـل موجب للمعادلة $x^2-dy^2=N$. عندئذ:

$$N=1\times N=(a^2-db^2)(r^2-ds^2)$$
$$=(ar\pm dbs)^2-d(as\pm br)^2$$

ولذا فإن $(ar\pm dbs, as\pm br)$ حل للمعادلة $x^2-dy^2=N$. وبمـا أن عـدد الحلول الموجبة للمعادلة $x^2-dy^2=1$ غير منته فنخلص إلى وجود عدد غير منته من الحلول للمعادلة $x^2-dy^2=N$ ◆

إذا كان $|N|\geq\sqrt{d}$ فهـذا لا يعـني الحـصول علـى حلـول المعادلـة $x^2-dy^2=N$ من مقاربات $\sqrt{d}$، ولكن في الحالة التي يكون فيهـا $|N|<\sqrt{d}$ فإن المقاربات تلعب دوراً مهماً في إيجاد الحلول وهذا ما تبنيه لنا المبرهنة التالية:

مبرهنة (٦,٣٨)

إذا كان $|N| < \sqrt{d}$ وكان (a,b) حلاً موجباً للمعادلة $x^2 - dy^2 = N$

فإن $\frac{a}{b}$ أحد مقاربات الكسر المتواصل للعدد $\sqrt{d}$.

البرهان

لنفرض أولاً أن $N > 0$. بما أن $a^2 - db^2 = (a - b\sqrt{d})(a + b\sqrt{d}) = N$

فإن $\frac{a}{b} - \sqrt{d} = \frac{N}{b(a + b\sqrt{d})} < \frac{\sqrt{d}}{b(a + b\sqrt{d})}$. وبما أن $N > 0$ فإن $\frac{a}{b} - \sqrt{d} > 0$.

ونرى أن $a > b\sqrt{d}$. ويكون $0 < \frac{a}{b} - \sqrt{d} < \frac{\sqrt{d}}{b(2b\sqrt{d})} = \frac{1}{2b^2}$. وعليه استناداً

إلى المبرهنة (٦,١٧) نجد أن $\frac{a}{b}$ أحد مقاربات $\sqrt{d}$.

لنفرض الآن أن $N < 0$. بما أن $a^2 - db^2 = N$ فإن $b^2 - \frac{1}{d}a^2 = \frac{-N}{d}$

حيث $\frac{-N}{d} > 0$. وبطريقة مماثلة لما سبق نجد:

$\frac{b}{a - \sqrt{1/d}} = \frac{-N}{da(b + a\sqrt{1/d})}$. وبما أن $b > a\sqrt{1/d}$ فنحصل على

$0 < \frac{b}{a} - \sqrt{1/d} < \frac{1}{2a^2}$. ويكون $\frac{b}{a}$ أحد مقاربات $\frac{1}{\sqrt{d}}$. وبالتالي نستنتج أن $\frac{a}{b}$

هو أحد مقاربات $\sqrt{d}$ ◆

ملحوظات

(١) العددين a و b في المبرهنة (٦,٣٨) ليس بالضرورة أن يكونا أوليين نسبياً ولكننا نستطيع دائماً أن نستبدلهما بعددين $r = \frac{a}{m}$ و $s = \frac{b}{m}$ حيث m القاسم المشترك الأعظم للعددين a و b بحيث يكون $\frac{r}{s}$ مقارباً للعدد $\sqrt{d}$. على سبيل

المثال، $a=10$ و $b=2$ حل للمعادلة $x^2-24y^2=4$ وأن $(a,b)=2$.

ومن السهل أن نرى أن $\frac{r}{s}=\frac{5}{1}=\frac{p_1}{q_1}$.

(٢) من الممكن إيجاد $|N|>\sqrt{d}$ بحيث تبقى المبرهنة (٦,٣٨) صحيحة، على سبيل المثال ، (19,4) حل للمعادلة $x^2-23y^2=-7$ حيث $\frac{19}{4}=\frac{p_2}{q_2}$ مقارباً للعدد $\sqrt{23}$.

(٣) إذا كان (x_1,y_1) الحل الأساسي للمعادلة $x^2-dy^2=N$ وكان $(u+v\sqrt{d})^n=u_n+v_n\sqrt{d}=(x_1+y_1\sqrt{d})^n$ فمن السهل التحقق من أن (u_n,v_n) حل موجب للمعادلة $x^2-dy^2=N$. ولكن ليس بالضرورة الحصول على جميع الحلول الموجبة للمعادلة $x^2-dy^2=N$ بهذه الطريقة، على سبيل المثال، لاحظ أن $(p_0,q_0)=(4,1)$ ، $(p_2,q_2)=(19,4)$ و $(p_4,q_4)=(221,44)$ حلولاً للمعادلة $x^2-23y^2=1$ وأن الحل الأساسي لها هو (24,5) . ولكن $(24+5\sqrt{23})(4+\sqrt{23})=211+44\sqrt{23}$. وبهذا لا يمكن الحصول على الحل (19,4) بهذه الطريقة.

(٦,٤,٣) تمارين محلولة *(Solved Exercises)*

تمرين (١)

(أ) إذا كان k عدداً صحيحاً موجباً فأثبت وجود عدد غير منته من الحلول للمعادلة $x^2-dy^2=1$ بحيث يكون y مضاعفاً للعدد k.

(ب) إذا كانت (x_n, y_n) جميع الحلول الموجبة للمعادلة $x^2 - dy^2 = 1$ حيث $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ و (x_1, y_1) الحل الأساسي فأثبت وجود عدد غير منته من الأعداد الأولية p حيث كل p يقسم عدد غير منته من الأعداد x_n.

الحل

(أ) لنفرض أن $D = k^2 d$. عندئذ، للمعادلة $x^2 - Dy^2 = 1$ عدد غير منته من الحلول. ومنه إذا كان (a,b) حلاً للمعادلة $x^2 - Dy^2 = 1$ فإن (a, kb) حل للمعادلة $x^2 - dy^2 = 1$.

(ب) سنثبت أولاً أن لأي مجموعة منتهية $A = \{p_1, p_2, \dots, p_s\}$ من الأعداد الأولية يوجد عدد أولي $p \notin A$ ويوجد $m \in \mathbb{Z}$ حيث $p \mid x_m$. ولهذا الغرض نفرض أن $P = p_1 p_2 \dots p_s$ وأن $D = dP^2$. باستخدام الفقرة (أ) يوجد y_m حيث $P \mid y_m$. وبما أن $(x_m, y_m) = 1$ فإن p_i لا يقسم x_m لكل $1 \le i \le s$. ولذا فإنه يوجد $p \notin A$ حيث $p \mid x_m$.

لنفرض الآن أن $p \mid x_m$. باستخدام الفقرة (أ) يوجد عدد غير منته من الأعداد n حيث $p \mid y_n$. ولكن $(x_m + y_m\sqrt{d})(x_n + y_n\sqrt{d}) = x_{m+n} + y_{m+n}\sqrt{d}$ حيث $x_{m+n} = x_m x_n + y_m y_n d$. وبما أن $p \mid y_n$ و $p \mid x_m$ فإن $p \mid x_{m+n}$ △

تمرين (٢)

إذا كان (a,b) الحل الأساسي للمعادلة $x^2 - dy^2 = 1$ وكان m طول دورة الكسر المتواصل للعدد $\sqrt{d}$ فأثبت أن :

(أ) $0 < a - b\sqrt{d} < \sqrt{2} - 1$.

(ب) $0<a-b\sqrt{d}<\frac{1}{m}$ إذا كان m زوجياً وأن $0<a-b\sqrt{d}<\frac{1}{2m}$ إذا كان m فردياً.

الحل

(أ) بما أن $a>b$ فإن $a+b\sqrt{d}>1+\sqrt{d}\geq 1+\sqrt{2}$. ولذا فإن

$$0<a-b\sqrt{d}=\frac{1}{a+b\sqrt{d}}<\frac{1}{1+\sqrt{2}}=\sqrt{2}-1$$

(ب) إذا كان m زوجياً فإن $a=p_{m-1}$ و $b=q_{m-1}$. ولكن باستخدام المبرهنة (٥,١٣) نجد أن:

$$0<a-b\sqrt{d}=b\,|\sqrt{d}-\frac{a}{b}|<q_{m-1}\frac{1}{q_{m-1}q_m}=\frac{1}{q_m}\leq\frac{1}{m}$$

وأما إذا كان m فردياً فإن $a=p_{2m-1}$ و $b=q_{2m-1}$ ويكون :

$$\triangle\quad 0<a-b\sqrt{d}<q_{2m-1}\frac{1}{q_{2m-1}\,q_{2m}}=\frac{1}{q_{2m}}\leq\frac{1}{2m}$$

تمرين (٣)

ليكن (a,b) الحل الأساسي للمعادلة $x^2-dy^2=-1$ (إن وجد) وإلا ليكن (a,b) الحل الأساسي للمعادلة $x^2-dy^2=1$. وليكن (x_n,y_n) حيث $x_n+y_n\sqrt{d}=(a+b\sqrt{d})^n$ لكل $n\geq 1$. أثبت أن x_n هو أقرب عدد صحيح للعدد $\frac{(a+b\sqrt{d})^n}{2}$ وأن y_n هو أقرب عدد صحيح للعدد $\frac{x_n}{\sqrt{d}}$.

الحل

لاحظ أن $|a^2-db^2|=|a+b\sqrt{d}\;|\;|a-b\sqrt{d}\;|$. وبما أن $|a^2-db^2|=1$.

$a+b\sqrt{d}>2$ فإن $|a-b\sqrt{d}|=\frac{1}{a+b\sqrt{d}}<\frac{1}{2}$. ولكن من السهولة أن نرى أن $|x_n-(a+b\sqrt{d})^n/2|=|a-b\sqrt{d}|^n/2<(1/2)^n$.

وبهذا يكون x_n أقرب عدد صحيح للعدد $\frac{(a+b\sqrt{d})^n}{2}$.

وأخيراً بما أن $|x_n-y_n\sqrt{d}|=|a-b\sqrt{d}|^n<\frac{1}{2}$ فإن $|y_n-\frac{x_n}{\sqrt{d}}|<\frac{1}{2\sqrt{2}}<\frac{1}{2}$. ومنه فإن y_n أقرب عدد صحيح للعدد $\frac{x_n}{\sqrt{d}}$ △

تمرين (٤)

(أ) استخدم التمرين المحلول (٣) لإيجاد أصغر حلين موجبين لكل من $x^2-41y^2=1$ و $x^2-41y^2=-1$.

(ب) استخدم الفقرة (أ) لإيجاد k حيث $q_k=1311360$.

(ج) جد $\frac{p_{14}}{q_{14}}$ دون اللجوء للحساب المباشر للمقاربات.

الحل

(أ) لاحظ أولاً أن $\sqrt{41}=[6;\overline{2,2,12}]$. وبهذا فإن دورة $\sqrt{41}$ هي $m=3$. ونرى أن أصغر حل موجب للمعادلة $x^2-41y^2=-1$ هو $(p_2,q_2)=(32,5)=(x_1,y_1)$. الآن إذا كان (x_n,y_n) حيث $x_n+y_n\sqrt{41}=(32+5\sqrt{41})^n$ فإننا نحصل على الحلول الموجبة للمعادلة $x^2-41y^2=-1$ عندما يكون n فردياً ونحصل على الحلول الموجبة للمعادلة $x^2-41y^2=1$ عندما يكون n زوجياً. وباستخدام التمرين المحلول (٣) نجد أن الحل الموجب الثاني للمعادلة $x^2-41y^2=-1$ هو

$(x_3, y_3) = (131168, 20485)$ لأن 131168 هو أقرب عدد صحيح للعدد $\frac{(32+5\sqrt{41})^3}{2}$ وأن 20485 هو أقرب عدد صحيح للعدد $\frac{131168}{\sqrt{41}}$.

أما الحل الأساسي للمعادلة $x^2 - 41y^2 = 1$ فهو $(x_2, y_2) = (2049, 320)$ لأن 2049 هو أقرب عدد صحيح للعدد $\frac{(32+5\sqrt{41})^2}{2}$ وأن 320 أقرب عدد صحيح للعدد $\frac{2049}{\sqrt{41}}$. وبالمثل أقرب عدد صحيح للعدد $\frac{(32+5\sqrt{41})^4}{2}$ هو 8396801 وأقرب عدد صحيح للعدد $\frac{8396801}{\sqrt{41}}$ هو 1311360. وبالتالي فإن الحل الموجب الثاني للمعادلة $x^2 - 41y^2 = 1$ هو $(x_4, y_4) = (8396801, 1311360)$.

(ب) باستخدام المبرهنة (٦,٣٥) نجد أن الحل الثاني الموجب للمعادلة $x^2 - 41y^2 = 1$ هو (p_{11}, q_{11}). ومن الفقرة (أ) نجد أن $q_{11} = 1311360$.

(ج) باستخدام المبرهنة (٦,٣٥) نجد أن (p_{14}, q_{14}) هو ثالث حل موجب للمعادلة $x^2 - 41y^2 = 1$ وباستخدام المبرهنة (٦,٣٦) . نجد أن هذا الحل هو (x_5, y_5) . وباستخدام التمرين (٣) نجد أن $x_5 = 537526432$ وأن $y_5 = 83947525$.

وبالتالي فإن $\frac{p_{14}}{q_{14}} = \frac{537526432}{83947525}$ △

تمرين (٥)

إذا كان p عدداً أولياً فأثبت أن للمعادلة $x^2 - py^2 = -1$ حلول موجبة إذا وفقط إذا كان $p \equiv 1 \pmod 4$ أو $p = 2$.

الحل

لنفرض أولاً أن $p \equiv 1 \pmod 4$. ولنفرض أن (a,b) الحل الأساسي للمعادلة $x^2 - py^2 = 1$. بما أن $p \equiv 1 \pmod 4$ وأن $a^2 - pb^2 = 1$ فإن $a^2 - b^2 \equiv 1 \pmod 4$. ولذا فإن a فردي و b زوجي. الآن $a^2 - pb^2 = 1$ إذا وفقط إذا كان $(a+1)(a-1) = pb^2$ وأن كل من $a+1$ و $a-1$ زوجياً والفرق بينهما يساوي 2. ومن ثم فإن $(a+1, a-1) = 2$. لنفرض أن $b = 2w$ وأن $a+1 = 2t$. حينئذ، $t(t-1) = pw^2$. ومنه فإن $t = r^2$ أو أن $t - 1 = ps^2$

$t = ps^2$ و $t - 1 = r^2$.

في الحالة الأولى لدينا: $r^2 - ps^2 = t - (t-1) = 1$ وهذا مستحيل لأن $r < a$ وأن (a,b) الحل الأساسي للمعادلة $x^2 - py^2 = 1$. ونرى أن $t = ps^2$ و $t - 1 = r^2$. ومنه فإن $r^2 - ps^2 = (t-1) - t = -1$ ويكون (r,s) حل للمعادلة $x^2 - py^2 = -1$ إذا كان $p \equiv 1 \pmod 4$.

أما إذا كان $p = 2$ فإن $\sqrt{2} = [1; \overline{2}]$ ونرى أن $m = 1$ فردي. ولذا فإن للمعادلة $x^2 - 2y^2 = -1$ حلول موجبة.

ولبرهان العكس، نفرض أن $p \equiv 3 \pmod 4$. إذا كان $x^2 - py^2 = -1$ فإن $x^2 \equiv -1 \pmod p$. وهذه المعادلة ليست قابلة للحل △

تمارين (٤, ٦)

(١) جد جميع الحلول الصحيحة لكل من المعادلات التالية:

(أ) $x^2 + 3y^2 = 4$ (ب) $x^2 + 5y^2 = 7$ (ج) $2x^2 + 7y^2 = 30$

(٢) جد جميع الحلول الصحيحة الموجبة لكل مما يلي:

(أ) $x^2-y^2=8$ (ب) $x^2-4y^2=8$

(ج) $x^2-9y^2=25$ (د) $x^2-9y^2=12$

(٣) جد ثلاث حلول موجبة للمعادلة $x^2-13y^2=12$.

(٤) جد الحل الأساسي لكل من المعادلتين $x^2-82y^2=-1$ و $x^2-82y^2=1$.

(٥) جد جميع الحلول الموجبة لكل من المعادلتين $x^2-7y^2=-1$ و $x^2-7y^2=1$

(٦) جد الحل الأساسي لكل من $x^2-30y^2=1$ و $x^2-30y^2=-1$.

(٧) أثبت أن المعادلة $x^2-9943y^2=-1$ غير قابلة للحل دون إيجاد الكسر المتواصل للعدد $\sqrt{9943}$.

(٨) جد الحل الأساسي لكل من المعادلتين $x^2-73y^2=-1$ و $x^2-73y^2=1$.

(٩) إذا علمت أن $\sqrt{61}=[7;\overline{1,4,3,1,2,2,1,3,4,1,14}]$ فجد الحل الأساسي لكل من $x^2-61y^2=-1$ و $x^2-61y^2=1$.

(١٠) جد جميع الحلول الموجبة لكل من $x^2-99y^2=1$ و $x^2-99y^2=-1$.

(١١) إذا كان طول دورة $\sqrt{d}$ عدداً فردياً فأثبت وجود عدد غير منته من الأعداد k حيث طول دورة $\sqrt{k^2d}$ يساوي 1 [إرشاد: $\sqrt{n^2+1}=[n;\overline{2n}]$].

(١٢) إذا كان d ليس مربعاً كاملاً فأثبت وجود عدد غير منته من الأعداد k حيث طول دورة $\sqrt{k^2d}$ يساوي 2 [إرشاد: $\sqrt{n^2-1}=[n-1;\overline{1,2n-2}]$]

(١٣) إذا كان (x_1,y_1) الحل الأساسي للمعادلة $x^2-dy^2=1$ وكان (x_n,y_n) الحل العام للمعادلة فأثبت أن $y_n \mid y_{kn}$ لكل $k\in\mathbb{Z}^+$.

(١٤) ليكن (a,b) حلاً للمعادلة $x^2-dy^2=1$. أثبت أن (a,b) حلاً موجباً إذا وفقط إذا كان $a+b\sqrt{d}>1$.

(١٥) هل يوجد حلول موجبة للمعادلة $x^2-23y^2=1$ حيث $24<x<1151$؟

(١٦) أثبت وجود عدد غير منته من الأعداد n حيث كل من $n-1$، n، $n+1$ مجموع مربعين.

(١٧) استخدم النتيجة (٢) للمبرهنة (٦,٣٠) لإيجاد أول ثلاثة حلول موجبة لكل من $x^2-10y^2=-1$ و $x^2-10y^2=1$.

(١٨) إذا كان $k\geq 2$ فأثبت أن $x^2-(k^2-1)y^2=-1$ غير قابلة للحل.

(١٩) إذا كان $(89,3)$ حلاً للمعادلة $x^2-880y^2=1$ فبين ما إذا كان طول دورة $\sqrt{880}$ فردياً أم زوجياً؟

(٢٠) إذا كان (r,s) الحل الأساسي للمعادلة $x^2-dy^2=-1$ فأثبت أن الحل الأساسي للمعادلة $x^2-dy^2=1$ هو $(2r^2+1,2rs)$.

(٢١) إذا كان p عدداً أولياً فأثبت عدم وجود حلول موجبة للمعادلة $x^4-361y^4=-p$.

(٢٢) إذا كان (r,s) حلاً موجباً للمعادلة $x^2-dy^2=M$ وكان (u,v) حلاً موجباً للمعادلة $x^2-dy^2=N$ فأثبت أن (a,b) حل موجب للمعادلة $x^2-dy^2=MN$ حيث $a+b\sqrt{d}=(r+s\sqrt{d})(u+v\sqrt{d})$.

(٢٣) استخدم التمرين (٢٢) لإيجاد ثلاث حلول موجبة للمعادلة $x^2-10y^2=31$.

(٢٤) إذا علمت أن $(13,2)$ حل للمعادلة $x^2-41y^2=5$ فجد حلاً آخر ثم جد حلين للمعادلة $x^2-41y^2=-5$.

(٢٥) جد ثلاث حلول للمعادلة $x^2-29y^2=5$ بحيث يكون $y<40000$ لكل منها.

نبذة عن حياة باسكارا *Biography of Bhaskara*

ولد : عام ١١١٤م في الهند .

توفي: عام ١١٨٥م في الهند



يمثل باسكارا ذروة المعرفة الرياضية والفلكية في القرن الثاني عشر، ولقد سبق رياضي أوروبا في معرفته الدقيقة وفهمه العميق لأنظمة الأعداد وحلول المعادلات بعدة قرون وكان على علم بوجود الصفر والأعداد السالبة. من أشهر مؤلفاته كتابي الجميلة *(Lelivati Lelivati)* وأصول العد *(Bijaganita)*.

يحتوي كتابه "الجميلة" (الذي يعتقد أنه كتبه ليسري عن ابنته الحزينة على موت زوجها) على مسائل حسابية أساسية مكتوبة على صيغة ألغاز بلغة خيالية جميلة، بالإضافة إلى مسائل هندسية. وأفرد الفصل الأخير من الكتاب للمعادلات الديوفنتية الخطية.

أما كتابه أصول العد فيتضمن رياضيات أعمق مما يحتويه كتاب الجميلة، حيث كان اهتمام باسكارا في هذا الكتاب منصباً على حل معادلة بيل $x^2 - dy^2 = 1$ ومعادلات ديوفنتية أخرى لها علاقة بمعادلة بيل وقدم خوارزمية فعالة لحل معادلة بيل

للأعداد 67 ، 61 ، 32 ، 11 ، 8 = d وبين أن أحد الحلول في الحالة 61 = d هـو $x = 1776319049$ و $y = 22615390$.

نبذة عن حياة بيل *Biography of Pell*



ولد : ١٦١١/٣/١م في سسكس (بريطانيا)
توفي: ١٦٨٥/١٢/١٢م في لندن (بريطانيا).

على الرغم من أن اسم الرياضي الانجليزي جون بيل اقترن بالمعادلة $x^2 - dy^2 = 1$ إلا أنه من المعتقد أن أويلر نسب أعمال الرياضي برونكر خطأ إلى بيل حيث ظهرت هذه المعادلة بكتاب كتبه كل من ران *(Rahn)* وبيل، ومن المحتمل أن يكون أويلر على علم بأبحاث بيل ولذا نسب المعادلة إليه.

حصل بيل في العام ١٦٢٨م على درجة الماجستير من كلية ترينتي بجامعة كامبريج وعمل بعد ذلك مديراً لمدرسة ثم درَّس الرياضيات في لندن لمدة خمس سنوات قبل أن يغادها لتقلد منصب استاذاً للرياضيات في جامعة امستردام مع بداية العام ١٦٤٣م. ورجع في العام ١٦٥٢م إلى بريطانيا وأصبح راهباً في الكنيسة إلى أن غيبه الموت عام ١٦٨٥م . لقد كانت معظم اسهامات بيل في الجبر ونظرية الأعداد وعمل جدولاً لقواسم الأعداد الصحيحة التي لا تزيد عن 100000.

للأعداد 67 ، 61 ، 32 ، 11 ، 8 = d وبين أن أحد الحلول في الحالة 61 = d هـو $x = 1776319049$ و $y = 22615390$.

نبذة عن حياة بيل *Biography of Pell*



ولد : ١٦١١/٣/١م في سسكس (بريطانيا)
توفي: ١٦٨٥/١٢/١٢م في لندن (بريطانيا).

على الرغم من أن اسم الرياضي الانجليزي جون بيل اقترن بالمعادلة $x^2 - dy^2 = 1$ إلا أنه من المعتقد أن أويلر نسب أعمال الرياضي برونكر خطأ إلى بيل حيث ظهرت هذه المعادلة بكتاب كتبه كل من ران *(Rahn)* وبيل، ومن المحتمل أن يكون أويلر على علم بأبحاث بيل ولذا نسب المعادلة إليه.

حصل بيل في العام ١٦٢٨م على درجة الماجستير من كلية ترينتي بجامعة كامبريج وعمل بعد ذلك مديراً لمدرسة ثم درَّس الرياضيات في لندن لمدة خمس سنوات قبل أن يغادها لتقلد منصب استاذاً للرياضيات في جامعة امستردام مع بداية العام ١٦٤٣م. ورجع في العام ١٦٥٢م إلى بريطانيا وأصبح راهباً في الكنيسة إلى أن غيبه الموت عام ١٦٨٥م . لقد كانت معظم اسهامات بيل في الجبر ونظرية الأعداد وعمل جدولاً لقواسم الأعداد الصحيحة التي لا تزيد عن 100000.

الفصل السابع

الجذور البدائية
PRIMITIVE ROOT

(٧,١) الجذور البدائية
Primitive Roots

لنفرض أن $(a,n)=1$. بينا في البند (٣,٥) على وجود عدد صحيح موجب أصغري k يحقق $a^k \equiv 1 \pmod{n}$ وهو رتبة العدد a قياس n، ونعلم أيضاً استناداً إلى مبرهنة أويلر أن $a^{\varphi(n)} \equiv 1 \pmod{n}$. إن هاتين الحقيقتين تقترحان علينا التعريف التالي:

تعريف (٧,١)

ليكن $n \in \mathbb{Z}^+$ وليكن $a \in \mathbb{Z}$ حيث $(a,n)=1$. إذا كان $ord_n(a)=\varphi(n)$ فنقول إن a جذراً بدائياً قياس n *(primitive root modulo n)*.

مثال (٧,١)

إذا كان $n=14$ فإن 3 جذر بدائي قياس 14 وذلك لأن $\varphi(14)=6$ وأن:

$3^1 \equiv 3 \pmod{14}$ ، $3^2 \equiv 9 \pmod{14}$ ، $3^3 \equiv 13 \pmod{14}$

$3^4 \equiv 11 \pmod{14}$ ، $3^5 \equiv 5 \pmod{14}$ ، $3^6 \equiv 1 \pmod{14}$.

وبالتالي فإن $ord_{14}(3)=6=\varphi(14)$ □

من المهم أن نلاحظ أنه ليس بالضرورة أن يكون لجميع الأعداد n جذوراً بدائية وهذا ما يوضحه المثال التالي:

مثال (٧,٢)

لا يوجد جذراً بدائياً قياس العدد 8.

الحل

بما أن $a^2 \equiv 1 \pmod 8$ لكل عدد أولي فردي a (أي لكل a أولي نسبياً مع 8) فإن $ord_8(a) \le 2$. ولكن $\varphi(8) = 4$. وبالتالي فإنه لا يوجد جذراً بدائياً قياس العدد 8 □

من المهم أيضاً أن نلفت نظر القارئ إلى أن مسألة حساب جذر بدائي a قياس عدد n (إن وجد) ليست بالمسألة السهلة. ولكن المبرهنة التالية تساعدنا في كثير من الأحيان على إثبات فيما إذا كان العدد a الأولي نسبياً مع n جذراً بدائياً قياس n.

مبرهنة (٧,١)

ليكن $(a,n) = 1$. عندئذ، a جذر بدائي قياس n إذا وفقط إذا كان $a^{\varphi(n)/q} \not\equiv 1 \pmod n$ لكل قاسم أولي q للعدد $\varphi(n)$.

البرهان

إذا كان a جذراً بدائياً قياس n فإن $ord_n(a) = \varphi(n)$. ولذا فإن $a^{\varphi(n)/q} \not\equiv 1 \pmod n$ لكل قاسم أولي q للعدد $\varphi(n)$.

لبرهان العكس، نفرض أن $a^{\varphi(n)/q} \not\equiv 1 \pmod n$ لكل قاسم أولي q للعدد $\varphi(n)$. لنفرض لغرض التناقض أن a ليس جذراً بدائياً قياس n. عندئذ، $ord_n(a) = d < \varphi(n)$. ولكن باستخدام المبرهنة (٣,٤٠) نعلم أن $d \mid \varphi(n)$. أي

أن $\varphi(n)=dk$ حيث $k\in\mathbb{Z}$. ليكن q قاسم أولي للعدد k (ومن ثم للعدد $\varphi(n)$). الآن:

$$a^{\frac{\varphi(n)}{q}}=a^{\frac{dk}{q}}=(a^d)^{\frac{k}{q}}\equiv(1)^{\frac{k}{q}}\equiv 1(\bmod n)$$

وهذا يناقض الفرض. إذن، a جذر بدائي قياس n ◆

ملحوظة

إذا كان n عدداً صحيحاً وكان من السهل تحليل العدد $\varphi(n)$ فإن المبرهنة (٧,١) تقدم لنا طريقة فعالة لاختبار ما إذا كان العدد a جذراً بدائياً قياس n.

مثال(٧,٣)

أثبت أن العدد 3 جذر بدائي قياس العدد 31.

الحل

لاحظ أن $\varphi(31)=30=2\times3\times5$ وأن

$$3^6\equiv(3^3)^2\equiv(-4)^2\equiv16\not\equiv1(\bmod 31)$$

$$3^{10}\equiv3^6\,3^4\equiv16\times(-4)\times3\equiv25\not\equiv1(\bmod 31)$$

$$3^{15}\equiv3^{10}\,3^5\equiv25\times26\equiv30\not\equiv1(\bmod 31)$$

وبهذا نرى أن 3 جذر بدائي قياس 31 □

مثال (٧,٤)

أثبت أن 5 جذر بدائي قياس العدد 18.

الحل

لاحظ أن $\varphi(18)=6=2\times3$ وأن:

$5^2\equiv7(\bmod 18)$ ، $5^3\equiv17(\bmod 18)$.

ولذا فإن 5 جذر بدائي قياس العدد 18 □

المثال التالي يبين لنا أن العدد 7 جذر بدائي قياس عدد ميرسين الأولي $M_{31}=2^{31}-1$ والذي سيكون له أهمية خاصة في البند (٧,٣)

مثال (٧,٥)

أثبت أن العدد 7 جذر بدائي قياس عدد ميرسين الأولي M_{31}.

الحل

لاحظ أولاً أن $M_{31}=2147483647$ وأن:

$$\begin{aligned}M_{31}-1&=2^{31}-2=2(2^{30}-1)=2(2^{15}-1)(2^{15}+1)\\&=2(2^5-1)(2^{10}+2^5+1)(2^5+1)(2^{10}-2^5+1)\\&=2\times3^2\times7\times11\times31\times151\times331\end{aligned}$$

ولذا فباستخدام المبرهنة (٧,١) يكفي إثبات أن $7^{M_{31}-1/q}\not\equiv1(\text{mod } M_{31})$ لكل $q=2,3,7,11,31,151,331$. وباستخدام خوارزمية التربيع والضرب نجد أن:

$$7^{\frac{M_{31}-1}{331}}\equiv1761885083\not\equiv1(\text{mod } M_{31})$$

$$7^{\frac{M_{31}-1}{151}}\equiv535044134\not\equiv1(\text{mod } M_{31})$$

$$7^{\frac{M_{31}-1}{31}}\equiv512\not\equiv1(\text{mod } M_{31})$$

$$7^{\frac{M_{31}-1}{11}}\equiv1969212174\not\equiv1(\text{mod } M_{31})$$

$$7^{\frac{M_{31}-1}{7}}\equiv120536285\not\equiv1(\text{mod } M_{31})$$

$$7^{\frac{M_{31}-1}{3}}\equiv1513477735\not\equiv1(\text{mod } M_{31})$$

$$7^{\frac{M_{31}-1}{2}}\equiv2147483646\not\equiv1(\text{mod } M_{31})$$

من ذلك نرى أن 7 جذر بدائي قياس M_{31} □

سنبين فيما يلي أنه إذا وجد جذر بدائي قياس العدد n فإن عدد الجذور البدائية قياس n يساوي $\varphi(\varphi(n))$ ولكننا نحتاج أولاً إلى الحقيقة التالية:

مبرهنة (٧,٢)

إذا كان a جذراً بدائياً قياس العدد n فإن $\{a,a^2,\ldots,a^{\varphi(n)}\}$ نظام رواسب مختزل قياس n .

البرهان

بما أن $(a,n)=1$ فإن $(a^k,n)=1$ لكل $k\in\mathbb{Z}^+$. ولاثبات أن المجموعة $\{a,a^2,\ldots,a^{\varphi(n)}\}$ نظام رواسب مختزل قياس n يكفي اثبات أن $a^r\not\equiv a^s \pmod n$ لكل $r\neq s$. ولكن هذا يتبع من المبرهنة (٣,٤٠). وبالتالي تكون المجموعة نظام رواسب مختزل قياس n ◆

مبرهنة (٧,٣)

إذا وجد جذر بدائي a قياس العدد n فإن عدد الجذور البدائية قياس n يساوي $\varphi(\varphi(n))$ وهي الأعداد a^k ، $1\le k\le\varphi(n)$ حيث $(k,\varphi(n))=1$.

البرهان

باستخدام المبرهنة (٧,٢) نعلم أن $a,a^2,\ldots,a^{\varphi(n)}$ نظام رواسب مختزل قياس n . الآن:

$$ord_n(a^k)=\frac{ord_n(a)}{(k,ord_n(a))}=\frac{\varphi(n)}{(k,\varphi(n))}$$

وهذا يكون a^k جذراً بدائياً قياس n إذا وفقط إذا كان $\frac{\varphi(n)}{(k,\varphi(n))}=\varphi(n)$. أي أن a^k جذر بدائي قياس n إذا وفقط إذا كان $(k,\varphi(n))=1$. ولكن عدد الأعداد k التي لا تزيد عن $\varphi(n)$ وتحقق $(k,\varphi(n))=1$ يساوي $\varphi(\varphi(n))$. وبهذا نستنتج أن عدد الجذور البدائية قياس n يساوي $\varphi(\varphi(n))$ ◆

مثال (٧,٦)

لقد بينا في المثال (٧,١) أن 3 جذر بدائي قياس العدد 14 . ولذا فإن عدد الجذور البدائية قياس العدد 14 يساوي $\varphi(\varphi(14))=\varphi(6)=2$ وهذان الجذران هما $3^k \pmod{14}$ حيث $1\le k\le 6$ ، $(k,6)=1$. أي أنهما العددان 3 و 9 □

ننتقل الآن إلى مسألة وجود الجذور البدائية قياس العدد n حيث سنبرهن في هذا البند وجود جذر بدائي قياس n إذا وفقط إذا كان $n=2,4,p^k,2p^k$ لكل $k\ge 1$ ولكل عدد أولي فردي p.

(٧,١,١) الجذور البدائية قياس 2^k (Primitive Roots Mod 2^k)

من الواضح أن 1 جذر بدائي قياس العدد 2. وبما أن $3^2\equiv 1(\text{mod } 4)$ فإن $ord_4(3)=\varphi(4)=2$. ولذا فإن 3 جذر بدائي قياس العدد $4=2^2$. سنبرهن الآن عدم وجود جذور بدائية قياس العدد 2^k لكل $k\ge 3$.

مبرهنة (٧,٤)

إذا كان a عدداً فردياً وكان $n\ge 3$ فإن $a^{2^{n-2}}\equiv 1(\text{mod } 2^n)$.

البرهان

بالاستقراء الرياضي على n. بما أن a فردي فإن $a^2\equiv 1(\text{mod } 8)$. وتكون العبارة صحيحة عندما $n=3$.

لنفرض الآن أن $a^{2^{k-2}}\equiv 1(\text{mod } 2^k)$ حيث $k\ge 3$. عندئذ، $2^k \mid (a^{2^{k-2}}-1)$. وبما أن a فردي فإن $a^{2^{k-2}}\equiv 1(\text{mod } 2)$ ونرى أن $2 \mid (a^{2^{k-2}}+1)$. ولذا فإن $(a^{2^{k-2}}+1)(a^{2^{k-2}}-1)$ | 2×2^k . أي أن $2^{k+1} \mid (a^{2^{k-1}}-1)$ ويكون

$a^{2^{k-1}} \equiv 1 (\text{mod } 2^{k+1})$. وعليه فإن العبارة صحيحة عندما $n = k+1$ ◆

نتيجة (٧,٥)

إذا كان $n = 2^k$ حيث $k \geq 3$ فلا توجد جذور بدائية قياس n.

البرهان

لنفرض أن $k \geq 3$ وأن $(a, 2^k) = 1$. استناداً إلى المبرهنة (٧,٤) نجد أن $a^{2^{k-2}} \equiv 1 (\text{mod } 2^k)$. وعليه فإن $ord_{2^k}(a) \mid 2^{k-2}$. ومنه فإن $ord_{2^k}(a) \leq 2^{k-2}$. ولكن $\varphi(2^k) = 2^{k-1}$. إذن، $ord_{2^k}(a) \neq \varphi(2^k)$. ونخلص إلى أن a ليس جذر بدائي قياس 2^k ◆

(٧,١,٢) الجذور البدائية قياس p^k (Primitive Roots Mod p^k)

إذا كان p عدداً أولياً فردياً فسنبرهن في هذا البند الجزئي وجود جذور بدائية قياس p^k لكل $k \geq 1$.

لقد بينا في المبرهنة (٣,٤٨) أنه إذا كان p عدداً أولياً فردياً فإن عدد الحلول غير المتطابقة قياس p للتطابق $f(x) \equiv 0 (\text{mod } p)$ هو على الأكثر n حيث $f(x) = \sum_{i=0}^{n} a_i x^i$، $a_i \in \mathbb{Z}$، $(a_n, p) = 1$. نوظف هذه المبرهنة لنحصل على:

مبرهنة (٧,٦)

إذا كان p عدداً أولياً فردياً فإن عدد حلول التطابق $x^{p-1} - 1 \equiv 0 (\text{mod } p)$ يساوي $p-1$.

البرهان

باستخدام مبرهنة فيرما نجد أن $a^{p-1} - 1 \equiv 0 (\text{mod } p)$ لكل a حيث $(a, p) = 1$. ولذا فإن الأعداد $a = 1, 2, 3, \ldots, p-1$ جميعها حلول للتطابق. ولكن

استناداً إلى المبرهنة (٣،٤٨) نعلم أن عدد حلول التطابق هو على الأكثر $p-1$. وبهذا يكون عدد هذه الحلول يساوي $p-1$ ◆

مبرهنة (٧,٧)

إذا كان p عدداً أولياً وكان $d \mid (p-1)$ فإن عدد حلول التطابق $x^d - 1 \equiv 0 \pmod{p}$ يساوي d.

البرهان

إذا كان $d = p-1$ فإننا نحصل على المطلوب باستخدام المبرهنة (٧,٦)، ولذا نفرض أن $d \neq p-1$. عندئذ، $p-1 = hd$ حيث $1 < h < p$. لنفرض أن $f(x) = x^d - 1$ وأن

$$g(x) = \frac{x^{p-1}-1}{f(x)} = x^{(h-1)d} + x^{(h-2)d} + \ldots + x^d + 1 .$$

ولنفرض أن عدد حلول التطابق :

$$f(x) \equiv 0 \pmod{p} \qquad (١)$$

يساوي j وأن عدد حلول التطابق :

$$g(x) \equiv 0 \pmod{p} \qquad (٢)$$

يساوي k. سنبرهن أن $j = d$.

لاحظ أنه إذا كان a حلاً للتطابق (١) فإن $a^d \equiv 1 \pmod{p}$. ومن ثم فإن

$$g(a) \equiv 1+1+\ldots+1+1 \equiv h \not\equiv 0 \pmod{p}$$

أي أنه لا توجد حلول مشتركة بين التطابقين (١) و (٢).

الآن : بما أن $x^{p-1} - 1 = f(x)g(x)$ فإن:

$x^{p-1} - 1 \equiv 0 \pmod{p}$ إذا وفقط إذا كان $f(x) \equiv 0 \pmod{p}$ أو $g(x) \equiv 0 \pmod{p}$. وعليه فإن عدد حلول التطابق $x^{p-1} - 1 \equiv 0 \pmod{p}$ يساوي مجموع عدد حلول التطابقين (١) و (٢). أي أن $p-1 = j+k$. ولكن: $\deg(g(x)) = (h-1)d = hd - d = p-1-d$. إذن، $k \leq p-1-d$. ومنه

فإن $k \le p-1-d = j+k-d$. أي أن $j \ge d$. ولكن باستخدام المبرهنة (٣,٤٨) نعلم أن $j \le d$. وبهذا يكون $j = d$ ◆

مثال (٧,٧)

للتطابق $x^5 - 1 \equiv 0 \pmod{11}$ خمسة حلول مختلفة وذلك لأن $5 \mid 10$. ومن السهل أن نرى أن هذه الحلول هي: $1, 3, 4, 5, 9$ □

مبرهنة (٧,٨)

ليكن p عدداً أولياً وليكن $d \mid (p-1)$. عندئذ، عدد الأعداد a التي تحقق $1 \le a \le p-1$ و $ord_p(a) = d$ يساوي $\varphi(d)$.

البرهان

لنفرض أن $f(d)$ هو عدد الأعداد a التي تحقق $1 \le a \le p-1$ و $ord_p(a) = d$. سنبرهن أولاً أن $0 \le f(d) \le \varphi(d)$ لكل قاسم d للعدد $p-1$. لاحظ أولاً أن a حل للتطابق:

$$x^d - 1 \equiv 0 \pmod{p} \qquad (١)$$

الآن، باستخدام المبرهنة (٧,٣) نعلم أن a^j حل للتطابق (١) لكل $1 \le j \le d$. ولكن استناداً إلى المبرهنة (٧,٧) نجد أن عدد حلول التطابق (١) يساوي d. إذن، كل حل من حلول التطابق (١) يجب أن يكون على الصورة a^j حيث $1 \le j \le d$. وبما أن $(a,p) = 1$ فإن $ord_p(a^j) = d$ إذا وفقط إذا كان $(j,d) = 1$. ولكن عدد مثل هذه الأعداد j يساوي $\varphi(d)$. ونستنتج أن $0 \le f(d) \le \varphi(d)$ لكل قاسم d للعدد $p-1$.

الآن، استناداً إلى المبرهنة (٣,٤٠) نعلم أن:

$$\sum_{d \mid (p-1)} f(d) = p-1$$

واستناداً إلى المبرهنة (٥,١٨) نعلم أن:

$$\sum_{d|(p-1)} \varphi(d) = p-1$$

من ذلك نجد أن $\sum_{d|(p-1)} f(d) = \sum_{d|(p-1)} \varphi(d) = p-1$.

وبما أن $0 \le f(d) \le \varphi(d)$ لكل قاسم $d \mid (p-1)$ فهذا يؤدي إلى أن $f(d) = \varphi(d)$ لكل d ◆

المثال التالي يوضح المبرهنة (٧,٨) :

مثال (٧,٨)

إذا كان $p = 11$ فإن $p-1 = 10$ وقواسم العدد 10 هي: $d = 1, 2, 5, 10$.

إذا كان $d = 1$ فإنه يوجد عدد وحيد $\varphi(1) = 1$ رتبته 1 قياس 11 وهو 1.

إذا كان $d = 2$ فإنه يوجد عدد وحيد $\varphi(1) = 1$ رتبته 2 قياس 11 وهو العدد 10.

إذا كان $d = 5$ فإنه يوجد $\varphi(5) = 4$ عدداً رتبة كل منها 5 قياس 11 وهي: $3, 4, 5, 9$.

وأخيراً إذا كان $d = 10$ فإنه يوجد $\varphi(10) = 4$ عدداً رتبة كل منها 10 قياس 11 وهي: $2, 6, 7, 8$ □

النتيجة التالية تبين لنا وجود جذور بدائية قياس العدد الأولي الفردي p.

نتيجة (٧,٩)

إذا كان p عدداً أولياً فردياً فإنه يوجد جذر بدائي قياس p وعدد الجذور البدائية قياس p يساوي $\varphi(p-1)$.

البرهان

بما أن $(p-1) \mid (p-1)$ فإنه استناداً إلى المبرهنة (٧,٨) يوجد $\varphi(p-1)$ عدداً رتبة كل منها قياس p يساوي $\varphi(p) = p-1$. وبما أن كل من هذه

الأعداد هو جذراً بدائياً قياس p فإننا نخلص إلى وجود $\varphi(p-1)$ من الجذور البدائية قياس p ◆

مثال (٧,٩)

إذا كان $p=13$ فإن $\varphi(p-1)=\varphi(12)=4$. ولذا فإنه يوجد 4 جذور بدائية قياس العدد 13. وبالتجريب نجد أن العدد 2 هو جذر بدائي قياس العدد 13. أما الجذور الثلاثة الأخرى فهي على الصورة 2^k حيث $k=(12,1)$. وهذه هي:

$2^5\equiv 6(\text{mod } 13)$ ، $2^7\equiv 11(\text{mod } 13)$ ، $2^{11}\equiv 7(\text{mod } 13)$ □

ملحوظات

(١) سنقدم في الجدول (٥) أصغر جذر بدائي g قياس العدد الأولي p حيث $p<1000$. في الحقيقة لا توجد خوارزمية فعالة لإيجاد الجذور البدائية قياس العدد الأولي p. إحدى الطرق المتبعة لحساب أصغر جذر بدائي a قياس العدد الأولي p تتم على النحو التالي:

(أ) ضع $a=2$ إذا كان $ord_p(a)=p-1$ نتوقف ويكون a جذر بدائي قياس p.

(ب) إذا كان $ord_p(a)<p-1$ فإننا نستبدل a بالعدد $a+1$ وننفذ الخطوة (أ).

لاحظ أنه من الممكن تسريع هذه الطريقة وذلك بتجاهل الأعداد التي تكون مربعات كاملة. كما يمكننا الاستعانة بالمبرهنة (٧,١) .

(٢) من الجدول (٥) ، نلاحظ أن العدد 2 جذر بدائي لحوالي نصف الأعداد الأولية التي أصغر من 1000 ، ولقد طرح الرياضي الألماني أرتين (Artin) الذي عاش في الفترة ١٨٩٨م — ١٩٦٢م. السؤال التالي:

"هل يوجد عدد غير منته من الأعداد الأولية p بحيث يكون 2 جذراً بدائياً قياس p؟ هذه المسألة لا زالت مفتوحة وننتظر الحل.

مثال (٧,١٠)

جد أصغر جذر بدائي قياس 109.

الحل

لاحظ أن $\varphi(109)=108=2^2\times 3^3$ ونرى أن قواسم $\varphi(109)$ الأولية هي 2 و 3. لإيجاد أصغر جذر بدائي قياس العدد 109 نجرب أولاً العدد 2. بما أن $2^{108/3}=2^{36}\equiv 1 \pmod{109}$ فنجد استناداً إلى المبرهنة (٧,١) أن 2 ليس جذراً بدائياً قياس 109. نجرب الآن العدد 3 فنجد أن $3^{108/2}=3^{54}\equiv 1 \pmod{109}$ ومن ثم فإن 3 ليس جذراً بدائياً قياس العدد 109. وبتجريب العدد 5 نجد أن $5^{108/2}=5^{54}\equiv 1(109)$ ومن ثم فالعدد 5 ليس جذراً بدائياً قياس العدد 109. الآن، بتجريب العدد 6 نجد أن

$$6^{108/3}=6^{36}\equiv 63\neq 1 \pmod{109}$$

$$6^{108/2}=6^{54}\equiv 108\neq 1 \pmod{109}$$

وبهذا يكون 6 أصغر جذر بدائي قياس العدد 109 □

إذا كان a جذراً بدائياً قياس العدد الأولي p فإنه غالباً ما يكون a جذراً بدائياً قياس العدد p^2. على سبيل المثال، 2 جذر بدائي قياس 13 وقياس 13^2. ولكن يوجد استثناءات لذلك، على سبيل المثال ، 14 جذر بدائي قياس 29 ولكن 14 ليس جذراً بدائياً قياس 29^2. سنبين الآن كيفية الحصول على جذر بدائي قياس p^2 باستخدام جذر بدائي قياس p.

مبرهنة (٧,١٠)

ليكن p عدداً أولياً فردياً وليكن a جذراً بدائياً قياس العدد p. عندئذ، إما أن a أو أن $a+p$ جذر بدائي قياس p^2.

البرهان

لنفرض أن $ord_{p^2}(a)=n$. عندئذ، $a^n \equiv 1 (\mathrm{mod}\ p^2)$. ومنه فإن $a^n \equiv 1 (\mathrm{mod}\ p)$. ولكن a جذراً بدائياً قياس p. أي أن $a^{\varphi(p)}=a^{p-1} \equiv 1 (\mathrm{mod}\ p)$. ولذا فإن $ord_p(a)=(p-1) \mid n$. وبما أن $a^n \equiv 1 (\mathrm{mod}\ p^2)$ فنجد باستخدام المبرهنة (٣,٤٠) أن $n \mid \varphi(p^2)=p(p-1)$. ولكن $(p-1) \mid n$. إذن،

$$n=p-1 \text{ أو أن } n=p(p-1).$$

إذا كان $n=p(p-1)$ فإن a جذر بدائي قياس p^2 ونكون قد انتهينا.

لنفرض إذن، أن $n=p-1$. عندئذ، $a^{p-1} \equiv 1 (\mathrm{mod}\ p^2)$. سنبرهن الآن أن $b=a+p$ جذر بدائي قياس p^2.

بما أن $b \equiv a (\mathrm{mod}\ p)$ وأن a جذر بدائي قياس p فإن b جذر بدائي قياس p. ولذا كما بينا في البرهان أعلاه فإن $ord_{p^2}(b)$ يساوي $p-1$ أو $p(p-1)$. سنثبت الآن أن $ord_{p^2}(b) \neq p-1$. باستخدام مبرهنة ذات الحدين لدينا:

$$b^{p-1}=(a+p)^{p-1}=a^{p-1}+(p-1)a^{p-2}p+\binom{p-1}{2}a^{p-3}p^2+\ldots+p^{p-1}$$

$$\equiv a^{p-1}+(p-1)pa^{p-2} (\mathrm{mod}\ p^2)$$

وبما أن $a^{p-1} \equiv 1 (\mathrm{mod}\ p^2)$. فإن:

$$b^{p-1} \equiv 1+(p-1)pa^{p-2} \equiv 1-pa^{p-2} (\mathrm{mod}\ p^2)$$

سنبرهن الآن أن $b^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$. ولهذا الغرض، نفرض أن $b^{p-1} \equiv 1 (\mathrm{mod}\ p^2)$. عندئذ، $pa^{p-2} \equiv 0 (\mathrm{mod}\ p^2)$. ومنه فإن $a^{p-2} \equiv 0 (\mathrm{mod}\ p)$ وهذا مستحيل لأن $p \nmid a$. إذن، $b^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$ ومن ثم فإن $ord_{p^2}(b) \neq p-1$. وبالتالي فإن $ord_{p^2}(b)=p(p-1)$. أي أن $b=a+p$ جذر بدائي قياس p^2 ◆

ملحوظة

ليكن a جذراً بدائياً قياس العدد الأولي الفردي p. لقد بينا في المبرهنة (٧,١٠) التالي:

إذا كان $a^{p-1} \not\equiv 1 \pmod{p^2}$ فإن a جذر بدائي قياس p^2. أما إذا كان $a^{p-1} \equiv 1 \pmod{p^2}$ فإن $a+p$ جذر بدائي قياس p^2. ومن المهم ملاحظة أن التطابق الأخير نادر الحدوث (انظر التمرين المحلول (٤) في نهاية البند). كما أنه من الممكن الحصول على جذور بدائية قياس p^2 بطرق أخرى منها:

(١) إذا كان $a^{p-1} \not\equiv 1 \pmod{p^2}$ فإن a جذر بدائي قياس p^2. أما إذا كان $a^{p-1} \equiv 1 \pmod{p^2}$ فإن a^{p-2} جذر بدائي قياس p^2.

(٢) $a^p - p$ جذر بدائي قياس p^2.

(٣) $a^p - ap$ جذر بدائي قياس p^2.

وللتفاصيل انظر [131].

مثال (٧,١١)

لاحظ أن 2 جذر بدائي قياس 13 لأن $2^{12} \equiv 1 \pmod{13}$. وبما أن $2^{12} \equiv 40 \not\equiv 1 \pmod{13^2}$ فإن 2 جذر بدائي أيضاً قياس العدد $13^2 = 169$

□

مثال (٧,١٢)

باستخدام خوارزمية التربيع نجد أن: $14^{28} \equiv 1 \pmod{29}$.

ولذا فإن 14 جذر بدائي قياس 29. أيضاً: $14^{28} \equiv 1 \pmod{29^2}$

ولذا فإن $14 + 29 = 43$ جذر بدائي قياس $29^2 = 841$ وذلك استناداً إلى المبرهنة (٧,١٠). كما أن الأعداد:

$$14^{27} \equiv 781 \pmod{841}$$

$$14^{29} - 29 \equiv 826 \pmod{841}$$

$$14^{29}-14\times 29\equiv 449(\text{mod } 841)$$

جميعها جذور بدائية قياس 841 وذلك استناداً إلى الملحوظة المقدمة أعلاه □

المبرهنة التالية تبين لنا كيفية الحصول على جذور بدائية قياس p^k لكل $k\geq 1$.

مبرهنة (٧,١١)

إذا كان a جذراً بدائياً قياس p^2 حيث p عدد أولي فردي فإن a جذر بدائي قياس العدد p^k لكل $k\geq 2$.

البرهان

بالاستقراء الرياضي على k . من الواضح أن العبارة صحيحة عندما $k=2$.

لنفرض الآن أن a جذر بدائي قياس p^n حيث $n\geq 2$. سنبرهن أن a جذر بدائي قياس p^{n+1} . ولهذا الغرض ، نفرض أن $ord_{p^{n+1}}(a)=m$. عندئذ، $m\mid \varphi(p^{n+1})=p\varphi(p^n)$. الآن:

$$a^m\equiv 1(\text{mod } p^{n+1})\Rightarrow a^m\equiv 1(\text{mod } p^n)$$

وبما أن $ord_{p^n}(a)=\varphi(p^n)$ (لأن a جذر بدائي قياس p^n) فإن $\varphi(p^n)\mid m$. وعليه فإن $m=p$ أو $m=\varphi(p^{n+1})$. سنبرهن أن $m=\varphi(p^{n+1})$ استناداً إلى مبرهنة أويلر لدينا:

$$a^{\varphi(p^{n-1})}\equiv 1(\text{mod } p^{n-1})$$

ومنه فإن:

$$a^{\varphi(p^{n-1})}=1+rp^{n-1}\text{ حيث } r\in\mathbb{Z}\ .$$

وبما أن a جذر بدائي قياس p^n فإن:

$$a^{\varphi(p^{n-1})} \not\equiv 1 (\text{mod } p^n)$$

ومن ثم فإن $p \nmid r$. الآن:

$$a^{\varphi(p^n)} = (a^{\varphi(p^{n-1})})^p = (1 + r\ p^{n-1})^p$$
$$= 1 + r\, p^n + \sum_{i=1}^{p} \binom{p}{i} (r\ p^{n-1})^i$$
$$\not\equiv 1 (\text{mod } p^{n+1})$$

وبالتالي فإن $m = \varphi(p^{n+1})$ ونخلص إلى أن a جذر بدائي قياس p^{n+1} ◆

مثال (٧,١٣)

لقد بينا أن في المثال (٧,١٢) أن 43 جذر بدائي قياس 13^2 . ولذا فإن 43 جذر بدائي قياس 13^k لكل $k \geq 2$ □

ننتقل الآن إلى إيجاد الجذور البدائية قياس $2p^k$ حيث p عدد أولي فردي و $k \in \mathbb{Z}^+$.

(٧,١,٣) الجذور البدائية قياس $2p^k$ (Primitive Roots Modulo $2p^k$)

سنبرهن الآن على وجود جذور بدائية قياس العدد $2p^k$ لكل $k \geq 1$ حيث p عدداً أولياً فردياً.

مبرهنة (٧,١٢)

ليكن p عدداً أولياً فردياً وليكن $k \in \mathbb{Z}^+$. وليكن a جذراً بدائياً قياس العدد p^k.

(١) إذا كان a عدداً فردياً فإن a جذر بدائي قياس $2p^k$.

(٢) إذا كان a عدداً زوجياً فإن $a + p^k$ جذر بدائي قياس $2p^k$.

البرهان

بما أن a جذر بدائي قياس العدد p^k فإن $a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$. ولكن $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$. ولذا فإن $a^{\varphi(2p^k)} \equiv 1 \pmod{p^k}$.

(١) لنفرض أن a فردي. عندئذ، $a^{\varphi(2p^k)} \equiv 1 \pmod{2}$. ونرى أن $a^{\varphi(2p^k)} \equiv 1 \pmod{2p^k}$. وبهذا يكون a جذراً بدائياً قياس العدد $2p^k$ في هذه الحالة.

(٢) لنفرض أن a زوجي. عندئذ، $a+p^k$ فردي.

ولذا فإن $(a+p^k)^{\varphi(2p^k)} \equiv 1 \pmod{2}$. كما أن $a+p^k \equiv a \pmod{p^k}$. ومنه فإن $(a+p^k)^{\varphi(2p^k)} \equiv a^{\varphi(2p^k)} \equiv 1 \pmod{p^k}$. إذن،

$(a+p^k)^{\varphi(2p^k)} \equiv 1 \pmod{2p^k}$. وبالتالي فإن $a+p^k$ جذر بدائي قياس العدد $2p^k$ ◆

مثال (٧,١٤)

(أ) أثبت أن 3 جذر بدائي قياس العدد 2×7^k لكل $k \geq 1$.

(ب) أثبت أن $6+109^k$ جذر بدائي قياس العدد 2×109^k لكل $k \geq 1$.

الحل

(أ) لاحظ أولاً أن $\varphi(7) = 6$ وأن $3^2 \equiv 2 \not\equiv 1 \pmod{7}$ وأن $3^3 \equiv 6 \not\equiv 1 \pmod{7}$ ولذا نرى أن 3 جذر بدائي قياس العدد 7 . وبهذا فهو جذر بدائي قياس العدد 7^2 لأن $3^6 \equiv 43 \not\equiv 1 \pmod{49}$. إذن، 3 جذر بدائي قياس العدد 7^k لكل $k \geq 1$. وبما أن 3 فردي فيكون جذراً بدائياً قياس العدد 2×7^k لكل $k \geq 1$.

(ب) لاحظ أولاً أن $\varphi(109) = 108 = 2^2\times3^3$ وأن $6^{36} \equiv 87 \not\equiv 1 \pmod{109}$ وأن $6^{54} \equiv 9 \not\equiv 1 \pmod{109}$. ولذا نرى أن 6 جذر بدائي قياس العدد 109.

وبما أن $6^{108} \equiv 1 \pmod{109^2}$ فإن $155 = 109 + 6$ جذر بدائي قياس العدد $(109)^2$ وبهذا فهو جذراً بدائياً قياس العدد $(109)^k$ لكل $k \geq 1$. وبما أن 115 عدد فردي فهو جذراً بدائياً قياس العدد $2 \times (109)^k$ لكل $k \geq 1$ □

(٧,١,٤) الجذور البدائية قياس n
(Primitive Roots Modulo n)

سنصف الآن جميع الأعداد الصحيحة n التي يكون لها جذور بدائية. سنحتاج أولاً إلى التمهيدية التالية:

تمهيدية (٧,١٣)

إذا كان $n = rs$ حيث $r > 2$ ، $s > 2$ و $(r,s) = 1$ توجد جذور بدائية قياس n.

البرهان

بما أن $(r,s) = 1$ فإن $\varphi(n) = \varphi(r)\varphi(s)$. وبما أن $r > 2$ و $s > 2$ فإن كل من $\varphi(r)$ و $\varphi(s)$ عدد زوجي. ولذا فإن $4 \mid \varphi(n)$. ومنه فإن $\frac{\varphi(n)}{2}$ يقبل القسمة على كل من $\varphi(r)$ و $\varphi(s)$. لنفرض الآن أن $a \in \mathbb{Z}$ حيث $(a,n) = 1$. عندئذ، $(a,r) = (a,s) = 1$. وباستخدام مبرهنة أويلر نجد أن $a^{\varphi(r)} \equiv 1 \pmod{r}$ وأن $a^{\varphi(s)} \equiv 1 \pmod{s}$. ونرى أن $a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{r}$ وأن $a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{s}$. وبما أن $(r,s) = 1$ وأن $n = rs$ فإن $a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n}$. وبالتالي فإن a ليس جذراً بدائياً قياس n ◆

المبرهنة التالية تصنف لنا جميع الأعداد n التي لها جذور بدائية.

مبرهنة (٧,١٤)

توجد جذور بدائية قياس العدد n إذا وفقط إذا كان $n=1,2,4,p^k,2p^k$ حيث p عدد أولي فردي و $k\geq 1$.

البرهان

إذا كان $n=1,2,4$ فمن الواضح أنه يوجد جذر بدائي قياس العدد n.

وإذا كان $n=p^k$ فنحصل على الجذر البدائي قياس العدد n باستخدام النتيجة (٧,٩) والمبرهنتين (٧,١٠) و (٧,١١).

أما إذا كان $n=2p^k$ فإننا نحصل على الجذر البدائي قياس العدد n باستخدام المبرهنة (٦,١٢).

لبرهان العكس، نفرض أن $n\neq 1,2,4,p^k,2p^k$. عندئذ، يكون لدينا الحالات التالية:

(١) $n=2^k$ حيث $k\geq 3$. أو

(٢) $n=2^k p^t$ حيث $k\geq 2$ ، $t\geq 1$ و p أولي فردي. أو

(٣) يوجد على الأقل قاسمان أوليان فرديان للعدد n.

لقد بينا في النتيجة (٧,٥) عدم وجود جذور بدائية قياس العدد n في الحالة (١).

أما إذا كان n كما هو في الحالة (٢) فإننا نستخدم التمهيدية (٧,١٣) بوضع $r=2^k$ و $s=p^t$.

وأخيراً إذا كان n كما هو في الحالة (٣) فإننا نستخدم التمهيدية (٧,١٣) بوضع $r=p^k$ حيث $p^k \| n$ و $s=\frac{n}{r}$ ◆

(٧,١,٥) تمارين محلولة *(Solved Exercises)*

تمرين (١)

إذا كان عدد فيرما F_n أولياً حيث $n>1$ فأثبت أن العدد 2 لا يمكن أن يكون جذراً بدائياً قياس F_n.

الحل

بما أن $2^{2^{n+1}}-1=(2^{2^n}-1)(2^{2^n}+1)=(2^{2^n}-1)F_n\equiv 0(\text{mod } F_n)$

فإن $2^{2^{n+1}}\equiv 1(\text{mod } F_n)$. ولذا فإن $ord_{F_n}(2)\mid 2^{n+1}$. وبما أن F_n أولياً فإن $\varphi(F_n)=F_n-1=2^{2^n}$. ولكن من السهل أن نرى بإستخدام الاستقراء الرياضي على n أن $2^{2^n}>2^{n+1}$ لكل $n>1$. وبهذا نرى أن

$\varphi(F_n)>2^{n+1}>ord_{F_n}(2)$. وبالتالي فإن 2 لا يمكن أن يكون جذراً بدائياً قياس F_n △

تمرين (٢)

لنفرض أنه يوجد جذر بدائي قياس العدد n . ولـيكن $a_r,\ldots,a_2,a_1$ نظام رواسب مختزل قياس n. أثبت أن $a_r^k,\ldots,a_2^k,a_1^k$ نظام رواسب مختزل قياس n إذا وفقط إذا كان $(k,\varphi(n))=1$.

الحل

لنفرض أن b جذر بدائي قياس n. عندئذ، استناداً إلى المبرهنة (٧,٢) نجد أن $b,b^2,\ldots,b^{\varphi(n)}$ نظام رواسب مختزل قياس n. ولذا فإنه لكل $1\le i\le r$ يوجد عدد وحيد $1\le j\le\varphi(n)$ بحيث يكون $a_i\equiv(b^k)^j(\text{mod } n)$. ولكننا نعلم أن b^k جذر بدائي قياس n إذا وفقط إذا كان $(k,\varphi(n))=1$. وبهذا يكون $a_r^k,\ldots,a_2^k,a_1^k$ نظام رواسب مختزل قياس n إذا وفقط إذا كان $(k,\varphi(n))=1$ △

تمرين (٣)

ليكن p عدداً أولياً فردياً وليكن $k \geq 2$. أثبت أن الجذور البدائية قياس p^{k+1} (غير المتطابقة) هي على الصورة $a+jp^k$ حيث a جذر بدائي قياس p^k ، $1 \leq a < p^k$ و $0 \leq j \leq p-1$.

الحل

لنفرض أن b جذر بدائي قياس العدد p^{k+1} حيث $1 < b < p^{k+1}$. باستخدام خوارزمية القسمة نجد أن $b = a + jp^k$ حيث $1 \leq a < p^k$ و $0 \leq j \leq p-1$.
بما أن b جذر بدائي قياس p^{k+1} فإنه من الواضح أن b جذر بدائي قياس p^k ومن ثم فإن a جذر بدائي قياس p^k (لأن $b \equiv a \pmod{p^k}$) .

ومن ناحية أخرى ، إذا كان $a+jp^k$ عدداً حيث a جذر بدائي قياس p^k فإن $a+jp^k \equiv a \pmod{p^k}$. ومن ثم فإن $a+jp^k$ جذر بدائي قياس p^k. وبالتالي فهو جذراً بدائياً قياس p^{k+1} △

تمرين (٤)

ليكن p عدداً أولياً فردياً. أثبت أنه يوجد بالضبط $\varphi(p-1)$ جذراً بدائياً قياس العدد p وغير متطابقة قياس العدد p^2 وليست جذوراً بدائية قياس العدد p^2.

الحل

لنفرض أن a جذر بدائي قياس p. عندئذ، $a, a+p, a+2p, \ldots, (p-1)p$ جميعها جذور بدائية قياس p وغير متطابقة قياس p^2 (لاحظ أن عددها يساوي p).
وبما أنه يوجد $\varphi(p-1)$ جذراً بدائياً قياس p فإنه يوجد $p\varphi(p-1)$ جذراً بدائياً قياس p وغير متطابقة قياس p^2. ولكن عدد الجذور البدائية قياس p^2 هو:

$$\varphi(\varphi(p^2)) = \varphi(p(p-1)) = \varphi(p)\varphi(p-1) = (p-1)\varphi(p-1).$$

ولهذا نرى أن عدد الجذور البدائية فياس p غير المتطابقة قياس p^2 وليست جذور بدائية قياس p^2 هو:

$\triangle\ p\varphi(p-1)-(p-1)\varphi(p-1)=\varphi(p-1)$

تمرين (٥)

إذا كان $n=3^k$ حيث $k\geq 1$ فأثبت أن $3n\mid(2^n+1)$.

الحل

بما أن $2^{\varphi(9)}=2^6\equiv 1(\mathrm{mod}\ 3^2)$ فإن 2 جذر بدائي قياس العدد 3^2. ويكون العدد 2 جذر بدائي قياس العدد $3^{k+1}=3n$ لكل $k\geq 1$. ومنه فإن:

$2^{2n}\equiv 1(\mathrm{mod}\ 3n)$. ولذا فـإن $ord_{3n}(2)=\varphi(3n)=\varphi(3^{k+1})=2\times 3^k=2n$.

ومن ثم فإن 2^n حل للمعادلـة $x^2\equiv 1(\mathrm{mod}\ 3n)$. أي أن $2^n\equiv\pm 1(\mathrm{mod}\ 3n)$.

ولكن $2^n\not\equiv 1(\mathrm{mod}\ 3n)$ لأن $ord_{3n}(2)>n$. وبالتالي فإن $2^n\equiv -1(\mathrm{mod}\ 3n)$ $\triangle$

تمارين (١, ٧)

(١) أثبت أن 3 جذر بدائي قياس العدد 17 ثم عين الجذور البدائية غـير المتطابقـة قياس 17 الواقعة بين 1 و 16.

(٢) عين جميع الجذور البدائية غير المتطابقة قياس العدد 29 الواقعة بين 1 و 28.

(٣) عين جميع الجذور البدائية غير المتطابقة قياس العدد 18 الواقعة بين 1 و $\varphi(18)$.

(٤) عين جميع الجذور البدائية غير المتطابقة قياس العدد 23 الواقعة بين 1 و 22.

(٥) عين جميع الجذور البدائية قياس العدد 27 الواقعة بين 1 و $\varphi(27)$.

(٦) عين جميع الجذور البدائية قياس العدد 31 الواقعة بين 1 و 30.

(٧) عين جذراً بدائياً قياس العدد 7^k لكل $k\geq 1$.

(٨) عين جذراً بدائياً قياس العدد 2×7^k لكل $k\geq 1$.

(٩) هل 2 جذراً بدائياً قياس 19؟ هل هو جذر بدائي قياس 17؟

(١٠) احسب عدد الجذور البدائية قياس العدد p حيث:

(أ) $p=47$ (ب) $p=103$ (ج) $p=223$

(١١) احسب عدد الجذور البدائية قياس العدد p غير المتطابقة قياس p^2 والتي ليست جذوراً بدائية قياس العدد p^2 حيث p هو كما في التمرين (١٠).

(١٢) جد جذراً بدائياً قياس p^k لكل $k \geq 1$ حيث:

(أ) $p=13$ (ب) $p=11$ (ج) $p=17$

(١٣) جد جذراً بدائياً قياس العدد 338.

(١٤) عين الأعداد التي لها جذور بدائية من بين الأعداد:

198 ، 199 ، 200 ، 201 ، 202 ، 203.

(١٥) أثبت أن 6 جذر بدائي قياس العدد 41 ثم استخدم ذلك لإيجاد جميع العناصر التي رتبة كل منها 8 قياس 41.

(١٦) عين جميع الأعداد $n>1$ التي يكون لها جذراً بدائياً واحداً فقط.

(١٧) لنفرض أنه لا توجد جذور بدائية قياس العدد n. أثبت أن $a^{\frac{\varphi(n)}{2}} \equiv 1 (\mathrm{mod}\, n)$ لكل a أولي نسبياً مع n.

(١٨) إذا كان a^k جذراً بدائياً قياس n فأثبت أن a جذر بدائي قياس n.

(١٩) ليكن $p>3$ عدداً أولياً. أثبت أن حاصل ضرب جميع الجذور البدائية الواقعة بين 1 و $p-1$ قياس العدد p يجب أن يطابق 1 قياس p.

(٢٠) أثبت التعميم التالي لمبرهنة ويلسن: إذا وجد جذراً بدائياً قياس العدد n وكان $a_1, a_2, \ldots, a_{\varphi(n)}$ نظام رواسب مختزل قياس n فأثبت أن

$$a_1 a_2 \ldots a_{\varphi(n)} \equiv -1 (\mathrm{mod}\, n).$$

(٢١) إذا كان p عدداً أولياً وكان $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$ فهل من الضروري أن يكون a جذراً بدائياً قياس p؟

(٢٢) إذا كان p عدداً أولياً فردياً فأثبت وجود جذر بدائي للعددين p^k و $2p^k$ معاً لكل $k \geq 1$.

(٢٣) إذا كان p عدداً أولياً فردياً وكان $k \geq 1$ وكان a جذراً بدائياً قياس p^{k+1} فأثبت أن a جذر بدائي قياس p^k.

(٢٤) إذا كان p عدداً أولياً فردياً وكان $k \geq 2$ فأثبت وجود جذر بدائي قياس p^k غير المتطابقة قياس p^2 يساوي $(p-1)\varphi(p-1)$.

(٢٥) أثبت أن $ord_{2^k}(5) = 2^{k-2}$ لكل $k \geq 3$.

(٢٦) إذا كان $1 \leq a \leq \varphi(2^k)$ وكان $ord_{2^k}(a) = 2$ حيث $k \geq 3$ فأثبت أن $a = 2^k - 1$ أو أن $a = 2^{k-1} \pm 1$.

(٢٧) إذا كان $M_n = 2^n - 1 \geq 3$ عدداً أولياً فأثبت أن 2 ليس جذراً بدائياً قياس M_n.

(٧,٢) اللوغاريتمات المنفصلة
The Discrete Logarithms

بعد أن درسنا مفهوم الجذور البدائية في البند السابق نقوم بتوظيف هذا المفهوم لدراسة مسألة يعتمد عليها الكثير من أنظمة التعمية ذات المفتاح المعلن في علم التعمية وأمن المعلومات، تعرف هذه المسألة بمسألة اللوغاريتم المنفصل.

إذا كان r جذراً بدائياً قياس العدد n فقد بينا في البند السابق أن $r, r^2, \ldots, r^{\varphi(n)}$ نظام رواسب مختزل قياس n. وبهذا نرى أنه لكل عدد أولي نسبي a مع n يوجد عدد وحيد x، $1 \leq x \leq \varphi(n)$ يحقق $r^x \equiv a \pmod{n}$. إن هذا يقودنا إلى التعريف التالي:

تعريف (٧,٢)

الجذور البدائية

ليكن r جذراً بدائياً قياس العدد n وليكن $a \in \mathbb{Z}^+$ حيث $(a,n)=1$. يسمى العدد الوحيد x، $1 \le x \le \varphi(n)$ الذي يحقق $r^x \equiv a \pmod n$ اللوغاريتم المنفصل للعدد a للأساس r قياس n *(the discrete logarithm of a to the base r n modulo n)*

ويرمز له بالرمز $x = \log_r(a)$.

ملحوظات

(١) لاحظ أن $a \equiv r^{\log_r(a)} \pmod n$.

(٢) لاحظ أن $x = \log_r(a)$ تعني أن $x \equiv \log_r(a) \pmod n$ ولكننا نتجاهل القياس على اعتبار أنه واضح من السياق.

(٣) يسمى اللوغاريتم المنفصل أحياناً دليل a للأساس r *(index of a to the base r)* ويرمز له بالرمز $ind_r(a)$.

(٤) من الواضح أنه إذا كان $(a,n)=(b,n)=1$ فإن :

$a \equiv b \pmod n$ إذا وفقط إذا كان $\log_r(a) \equiv \log_r(b) \pmod{\varphi(n)}$.

(٥) لاحظ أيضاً أن $x = \log_r(a)$ إذا وفقط إذا كان $r^x = a$.

مثال (٧,١٥)

إذا كان $n=13$ فمن السهل أن نرى أن $r=6$ جذر بدائي قياس 13. وبما أن $(a,13)=1$ لكل $1 \le a \le 12$ فإنه يوجد $x = \log_6(a)$ لكل $1 \le a \le 12$.

وبما أن $x \equiv \log_6(a) \pmod{13}$ إذا وفقط إذا كان $6^x \equiv a \pmod{13}$ فإننا نستطيع إيجاد اللوغارتيمات المنفصلة بحساب قوى الجذر البدائي قياس 13 كما هو موضح في الجدول التالي:

x	1	2	3	4	5	6	7	8	9	10	11	12
6^x	6	10	8	9	2	12	7	3	5	4	11	1

وتكون اللوغاريتمات المنفصلة للأعداد a حيث $1 \le a \le 12$ هي كما هو موضح في الجدول التالي:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\log_6(a)$	12	5	8	10	9	1	7	3	4	2	11	6

□

مثال (٧,١٦)

إذا كان $n = 18$ فمن السهل أن نرى أن $r = 5$ جذر بدائي قياس 18. كما أن الأعداد $a = 1,5,7,11,13,17$ أولية نسبياً مع 18. ولذا فإن $x = \log(a)$ موجوداً لكل a أولي نسبياً مع 18. الجدول التالي يبين لنا القيم $5^x \pmod{18}$ $1 \le x \le \varphi(18) = 6$.

x	1	2	3	4	5	6
5^x	5	7	17	13	11	1

ولذا فإن $\log_5(a)$ هي كما مبينة في الجدول التالي:

a	1	5	7	11	13	17
$\log_5(a)$	6	1	2	5	4	3

□

المبرهنة التالية تزودنا بالخصائص الأساسية للوغاريتمات المنفصلة.

مبرهنة (٧,١٥)

إذا كان r جذراً بدائياً قياس العدد n وكان $(a,n) = (b,n) = 1$ فإن:

(١) $\log_r(1) = \varphi(n)$ ومن ثم فإن $\log_r(1) \equiv 0 \pmod{\varphi(n)}$.

(٢) $\log_r(ab) \equiv \log_r(a) + \log_r(b) \pmod{\varphi(n)}$.

(٣) $\log_r(a^k) \equiv k \log_r(a) \pmod{\varphi(n)}$ لكل $k \in \mathbb{Z}^+$.

(٤) $\log_r(r) = 1$ ومن ثم فإن $\log_r(r) \equiv 1 \pmod{\varphi(n)}$.

البرهان

(١) بما أن r جذر بدائي قياس n فإن $r^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$. وبالتالي فإن $\log_r(1) = \varphi(n) \equiv 0 (\mathrm{mod}\ \varphi(n))$.

(٢) باستخدام تعريف اللوغاريتم المنفصل لدينا:

$$r^{\log_r(ab)} \equiv ab (\mathrm{mod}\ n)$$

$$r^{\log_r(a)+\log_r(b)} \equiv r^{\log_r(a)} r^{\log_r(b)} \equiv ab (\mathrm{mod}\ n)$$

ومن ثم فإن $r^{\log_r(ab)} \equiv r^{\log_r(a)+\log_r(b)} (\mathrm{mod}\ n)$. وبهذا يكون

$$\log_r(ab) \equiv \log_r(a) + \log_r(b) (\mathrm{mod}\ \varphi(n))$$

(٣) باستخدام تعريف اللوغاريتم المنفصل لدينا:

$$r^{\log_r(a^k)} \equiv a^k (\mathrm{mod}\ n)$$

$$r^{k \log_r(a)} \equiv \left(r^{\log_r(a)}\right)^k \equiv a^k (\mathrm{mod}\ n)$$

ولذا فإن $r^{\log_r(a^k)} \equiv r^{k \log_r(a)} (\mathrm{mod}\ n)$. ونجد أن

$$\log_r(a^k) \equiv k \log_r(a) (\mathrm{mod}\ \varphi(n))$$

(٤) بما أن $r^1 = r$ فإن $\log_r(r) = 1 \equiv 1 (\mathrm{mod}\ \varphi(n))$ ◆

مثال (٧,١٧)

من المثال (٧,١٥) لدينا $\log_6(4) = 10$ و $\log_6(8) = 3$. ونرى باستخدام المبرهنة (٧,١٥) أن :

$$\log_6(32) \equiv \log_6(4) + \log_6(18) \equiv 10 + 3 \equiv 13 (\mathrm{mod}\ 12)$$

$$\log_6(64) = \log_6(4^3) \equiv 3\log_6(4) \equiv 3 \times 10 \equiv 30 \equiv 6 (\mathrm{mod}\ 12)$$ □

إن أحد تطبيقات اللوغاريتمات المنفصلة هو استخدامها لحل المعادلات التطابقية $bx^k \equiv c (\mathrm{mod}\ n)$ حيث $(bc, n) = 1$. لاحظ أنه بضرب طرفي المعادلة

بنظير b قياس n فإن المعادلة التطابقية تكافيء معادلة على الصورة $x^k \equiv a \pmod{n}$. إن هذا يقودنا إلى التعريف التالي:

تعريف (٧,٣)

ليكن $n \in \mathbb{Z}^+$ وليكن $a \in \mathbb{Z}$ حيث $(a,n)=1$. نقول إن a راسب من الدرجة k للعدد n *(residue of degree k of n)* إذا كان التطابق $x^k \equiv a \pmod{n}$ قابلاً للحل.

تزودنا المبرهنة التالية بالشرط اللازم والكافي لوجود حل للتطابق $x^k \equiv a \pmod{n}$.

مبرهنة (٧,١٦)

لنفرض أن للعدد $n \in \mathbb{Z}^+$ جذراً بدائياً وليكن $(a,n)=1$. عندئذ، يكون التطابق $x^k \equiv a \pmod{n}$ قابلاً للحل إذا وفقط إذا كان $a^{\frac{\varphi(n)}{(k,\varphi(n))}} \equiv 1 \pmod{n}$ (١)

إضافة إلى ذلك إذا كان $x^k \equiv a \pmod{n}$ قابلاً للحل فإن عدد حلوله غير المتطابقة يساوي $(k,\varphi(n))$.

البرهان

لنفرض أن r جذر بدائي قياس n ولنفرض أن $d=(k,\varphi(n))$. لاحظ أن $x^k \equiv a \pmod{n}$ إذا وفقط إذا كان $k\log_r(x) \equiv \log_r(a) \pmod{\varphi(n)}$. ولكننا نعلم أن التطابق الخطي الأخير قابل للحل إذا وفقط إذا كان $d=(k,\varphi(n)) \mid \log_r(a)$. وعندما يكون قابلاً للحل فإن عدد حلوله غير المتطابقة هو $d=(k,\varphi(n))$. لإكمال البرهان فيكفي إثبات أن التطابق (١) صحيحاً إذا وفقط إذا كان $d \mid \log_r(a)$. ولكن، $a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{n}$ إذا وفقط إذا كان

$\frac{\varphi(n)}{d}\log_r(a)\equiv 0(\bmod \varphi(n))$ إذا وفقط إذا كان $d \mid \log_r(a)$. وبهذا يتم البرهان ◆

نحصل على النتيجة التالية مباشرة من المبرهنة (٧,١٦) وذلك لوجود جذور بدائية قياس العدد الأولي p.

نتيجة (٧,١٧)

إذا كان p عدداً أولياً وكان $(a,p)=1$ فإن:

◆ $x^k \equiv a(\bmod p)$ قابل للحل إذا وفقط إذا كان $a^{\frac{p-1}{(k,p-1)}} \equiv 1(\bmod p)$

النتيجة التالية تقدم لنا تعميماً للمبرهنة (٧,٧).

نتيجة (٧,١٨)

إذا وجد جذراً بدائياً قياس العدد n وكان $k \mid \varphi(n)$. فإن عدد حلول التطابق $x^k - 1 \equiv 0(\bmod n)$ يساوي k.

البرهان

من الواضح أن التطابق $x^k \equiv 1(\bmod n)$ قابل للحل. وبما أن $k \mid \varphi(n)$ فإن $k=(k,\varphi(n))$. باستخدام المبرهنة (٧,١٦) نجد أن عدد حلول التطابق يساوي k ◆

ملحوظات

(١) على الرغم من أن النتيجة (٧,١٧) تقدم لنا طريقة فاعلة لمعرفة ما إذا كان a راسباً من الدرجة k للعدد الأولي p إلا أنه في معظم الأحيان يكون من الصعب إيجاد x الذي يحقق التطابق $x^k \equiv a(\bmod p)$. ولكن في الحالة الخاصة التي يكون فيها $(k,p-1)=1$ فالأمر سهل حيث نقوم باستخدام خوارزمية إقليدس لإيجاد $s,t \in \mathbb{Z}$ بحيث يكون $sk+t(p-1)=1$. ولذا فإن: $a^{sk}(a^{p-1})^t \equiv a(\bmod p)$ ومنه فإن $(a^s)^k \equiv a(\bmod p)$. ويكون a^s حلاً للتطابق.

(٢) إذا كان $x^k \equiv a \pmod{n}$ قابلاً للحل فمن الممكن الاستعانة باللوغاريتمات المنفصلة لإيجاد الحلول.

مثال (٧,١٨)

جد جميع حلول التطابق $7x^{10} \equiv 5 \pmod{13}$.

الحل

لاحظ أولاً أن $x^{10} \equiv 7^{-1} \times 5 \equiv 2 \times 5 \equiv 10 \pmod{13}$. وبما أن:

$10^{\frac{12}{(10,12)}} = 10^6 \equiv 3^6 = 27^2 \equiv 1 \pmod{13}$ فإن التطابق قابل للحل. لقد رأينا في المثال (٧,١٥) أن 6 جذر بدائي قياس 13 ووجدنا كذلك جدولاً لجميع $\log_6(a)$ حيث $1 \le a \le 12$.

لنفرض الآن أن $y = \log_6(x)$. عندئذ ، $x \equiv 6^y \pmod{13}$. الآن ، بأخذ لوغاريتم طرفي التطابق $7x^{10} \equiv 5 \pmod{13}$ نجد أن:

$$\log_6(7x^{10}) \equiv \log_6(7) + 10\log_6(x) \equiv \log_6(5) \pmod{12}$$

وباستخدام جدول اللوغاريتمات المبين في المثال (٧,١٥) نجد أن $10y \equiv 2 \pmod{12}$. أي أن: $7 + 10y \equiv 9 \pmod{12}$. وبما أن $(10,12) = 2$ فإنه يوجد حلان للتطابق هما $y \equiv 5,11 \pmod{12}$. وبهذا يكون $x \equiv 6^5 \equiv 2 \pmod{13}$ أو $x \equiv 6^{11} \equiv 11 \pmod{13}$ □

ملحوظة

لاحظ أنه لو استخدمنا جذراً بدائياً مختلفاً فإن قيم اللوغاريتمات تكون مختلفة ولكننا نحصل على الحلول نفسها.

مثال (٧,١٩)

جد جميع حلول التطابق $5^{2x+1} \equiv 7^{5x+2} \pmod{13}$.

الحل

سنستخدم الجذر البدائي 6 قياس 13. بأخذ لوغاريتم لطرفي التطابق نجد أن $(2x+1)\log_6(5) \equiv (5x+2)\log_6(7) \pmod{12}$. ونرى أن $(2x+1)\times 9 \equiv (5x+2)\times 7 \pmod{12}$. أي أن $7x \equiv 5 \pmod{12}$. وبما أن $(12,7)=1$ فإنه يوجد حل وحيد للتطابق الخطي هو $x \equiv 11 \pmod{12}$ □

(٧,٢,١) تمارين محلولة *(Solved Exercises)*

تمرين (١)

أثبت أن التطابق $x^4 \equiv -1 \pmod{p}$ قابل للحل إذا وفقط إذا كان $p \equiv 1 \pmod{8}$ حيث p عدد أولي فردي.

الحل

باستخدام النتيجة (٧,١٧) يوجد حل للتطابق $x^4 \equiv -1 \pmod{p}$ إذا وفقط إذا كان $(-1)^{\frac{p-1}{(4,p-1)}} \equiv 1 \pmod{p}$. أي إذا كان $\frac{p-1}{(4,p-1)}$ عدداً زوجياً. وبما أن $p = 8k+r$ حيث $r = 1,3,5,7$. فإن $\frac{p-1}{(4,p-1)} = 2k, 4k+1, 2k+1, 4k+3$ على التوالي. وبالتالي فإن $\frac{p-1}{(4,p-1)}$ زوجي إذا وفقط إذا كان $r=1$. أي أن $p \equiv 1 \pmod{8}$ △

تمرين (٢)

استخدم التمرين (١) للبرهان على وجود عدد غير منته من الأعداد الأولية التي على الصورة $8k+1$.

الحل

لنفرض أن $p_1 < p_2 < \ldots < p_n$ هي جميع الأعداد الأولية التي على الصورة $8k+1$. وليكن $N = (2p_1p_2 \ldots p_n)^4 + 1$. إذا كان p قاسماً أولياً للعدد N فإن $N \equiv 0 \pmod{p}$. ونرى أن $(2p_1p_2 \ldots p_n)^4 \equiv -1 \pmod{p}$. ولذا فإن التطابق

$x^4 \equiv -1 \pmod{p}$ قابل للحل. وباستخدام تمرين (١) نجد أن $p \equiv 1 \pmod 8$.
ومنه فإن $p = p_i$. وبهذا نجد أن $p \mid 1$ وهذا مستحيل △

تمارين (٧,٢)

(١) جد جدولاً للوغاريتمات المنفصلة مستخدماً الجذر البدائي 2 قياس 13 ثم استخدمه لحل كل من التطابقات التالية:

(أ) $7x^{10} \equiv 5 \pmod{13}$ (ب) $3^{5x} \equiv 11^{3x+1} \pmod{13}$

(ج) $3^{4x} \equiv 11^{x+3} \pmod{13}$ (د) $9^x \equiv 2 \pmod{13}$

(٢) جد جدولاً للوغاريتمات المنفصلة مستخدماً الجذر البدائي 3 قياس 17 ثم استخدمه لحل كل من التطابقات التالية:

(أ) $x^{12} \equiv 13 \pmod{17}$ (ب) $8x^5 \equiv 10 \pmod{17}$

(ج) $9x^8 \equiv 8 \pmod{17}$ (د) $7^x \equiv 7 \pmod{17}$

(٣) جد جدولاً للوغاريتمات المنفصلة مستخدماً الجذر البدائي 2 قياس 19 ثم استخدمه لحل كل من التطابقات التالية:

(أ) $8x^4 \equiv 3 \pmod{19}$ (ب) $5x^2 \equiv 2 \pmod{19}$

(ج) $x^7 \equiv 1 \pmod{19}$ (د) $x^8 \equiv 5 \pmod{19}$

(٤) جد جدولاً للوغاريتمات المنفصلة مستخدماً الجذر البدائي 5 قياس 23 ثم استخدمه لحل كل من التطابقات التالية:

(أ) $3x^5 \equiv 1 \pmod{23}$ (ب) $3x^{14} \equiv 2 \pmod{23}$

(ج) $3^x \equiv 2 \pmod{23}$ (د) $13^x \equiv 5 \pmod{23}$

(٥) حل التطابق $x^5 \equiv 2 \pmod{73}$.

(٦) أثبت أن 2 جذر بدائي قياس 29 ثم استخدمه لحل التطابق $4x^{12} \equiv -23 \pmod{29}$.

(٧) أثبت أن 2 جذ بدائي قياس 101 ثم استخدمه لحل التطابق $x^5 \equiv 6 \pmod{101}$.

(٨) أثبت أن 2 جذر بدائي قياس 59 ثم استخدمه لحل التطابق $5x^5 \equiv -16 \pmod{59}$.

(٩) أثبت أن 7 جذر بدائي قياس 71 ثم استخدمه لحل التطابق $x^5 \equiv 26 \pmod{71}$.

(١٠) استخدم اللوغاريتمات المنفصلة لحساب $5^{4^3} \pmod{19}$.

(١١) استخدم اللوغاريتمات المنفصلة لحساب $3^{3^3} \pmod{17}$.

(١٢) إذا كان كل من r و s جذراً بدائياً قياس العدد الأولي الفردي p وكان $(a,p)=1$ فأثبت أن $\log_s(a) \equiv (\log_r(a))(\log_r(r)) \pmod{p-1}$.

(١٣) إذا كان r جذراً بدائياً قياس العدد الأولي p فأثبت أن:

$$\log_r(-1) = \log_r(p-1) = \frac{1}{2}(p-1)$$

(١٤) إذا كان $p \equiv 2 \pmod 3$ عدداً أولياً فأثبت أن التطابق $x^3 \equiv a \pmod p$ قابل للحل لكل عدد صحيح $a < p$.

(١٥) ليكن $p \geq 5$ عدداً أولياً و $a \in \mathbb{Z}$ حيث $(a,p)=1$ وليكن $x^3 \equiv a \pmod p$.

(أ) إذا كان $p \equiv 1 \pmod 6$ فأثبت أنه إما أن يكون التطابق غير قابل للحل أو أن له ثلاثة حلول غير متطابقة قياس p.

(ب) إذا كان $p \equiv 5 \pmod 6$ فأثبت أن للتطابق حل وحيد قياس p.

(١٦) استخدم التمرين (١٥) لاثبات أن التطابق $x^3 \equiv 3 \pmod{19}$ غير قابل للحل وأن للتطابق $x^3 \equiv 11 \pmod{19}$ ثلاثة حلول غير متطابقة.

(١٧) بين ما إذا كان التطابق $x^{13} \equiv 10 \pmod{1323}$ قابلاً للحل؟

(١٨) إذا كان كل من p و q عدداً أولياً حيث $p = 2q+1$ فأثبت أنه إما أن يكون للتطابق $x^{2k} \equiv 1 \pmod p$ حلين أو يوجد له $p-1$ من الحلول لكل $k \in \mathbb{Z}^+$.

(١٩) ليكن p عدداً أولياً فردياً وليكن $n \in \mathbb{Z}^+$.

(أ) أثبت أن التطابق $x^{2^{n-1}} \equiv -1 \pmod{p}$ قابل للحل إذا وفقط إذا كان $p \equiv 1 \pmod{2^n}$.

(ب) استخدم الفقرة (أ) لإثبات وجود عدد غير منته من الأعداد الأولية التي على الصورة $2^n k + 1$.

(٧,٣) القوى الشاملة
Universal Exponents

ندرس في هذا البند مفهوم القوى الشاملة ونوظفه لبرهان عكس المبرهنة (٣,٤٤) ، كما أننا سنستخدم هذا المفهوم في بعض التطبيقات التي سنناقشها في الفصل العاشر من هذا الكتاب.

تعريف (٧,٤)

نقول إن عدد صحيح موجب U قوة شاملة (universal exponent) للعدد الصحيح الموجب n إذا تحقق:

$$a^U \equiv 1 \pmod{n}$$

لكل عدد صحيح a أولي نسبياً مع n.

لاحظ أولاً أنه استناداً إلى مبرهنة أويلر يكون $\varphi(n)$ قوة شاملة للعدد n . ولإيجاد قوة شاملة أخرى، نفرض أن

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$$

هو تحليل n إلى قوى عوامله الأولية. عندئذ، نجد استناداً إلى مبرهنة أويلر مرة أخرى. يكون $a^{\varphi(p_i^{\alpha_i})} \equiv 1 \pmod{p_{p_i}^{\alpha_i}}$ لكل i ، $1 \le i \le t$. فعندئذ ، إذا كان

$$U = [\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \dots, \varphi(p_t^{\alpha_t})]$$

فإن $\varphi(p_i^{\alpha_i}) \mid U$ لكل $i = 1, \dots, t$. وبهذا نجد أن $a^U \equiv 1 \pmod{p_i^{\alpha_i}})$ لكل $i = 1, \dots, t$ ويكون $a^U \equiv 1 \pmod{n}$. إذن، المضاعف المشترك الأصغر للأعداد $\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \dots, \varphi(p_t^{\alpha_t})$ هو قوة شاملة أخرى للعدد n.

مثال (٧,٢٠)

إذا كان $n = 720 = 2^4 \times 3^2 \times 5$ فإن $\varphi(720) = 192$ قوة شاملة للعدد 720 وإن $U = [\varphi(2^4), \varphi(3^2), \varphi(5)] = [8,6,4] = 24$ قوة شاملة أخرى للعدد 720 □

سنبين الآن كيفية الاستعانة بالجذور البدائية لإيجاد أصغر قوة شاملة U .

تعريف (٧,٥)

تسمى أصغر قوة شاملة للعدد الصحيح الموجب n ، القوة الشاملة الصغرى للعدد n ونرمز لها بالرمز $\lambda(n)$.

إذا وجد جذر بدائي قياس العدد n فإنه من الواضح أن $\lambda(n) = \varphi(n)$. وبما أن الأعداد التي لها جذور بدائية هي $n = 1,2,4,p^\alpha,2p^\alpha$ حيث p عدد أولي فردي نجد أن

$$\lambda(2) = \varphi(2) = 1$$
$$\lambda(4) = \varphi(4) = 2$$
$$\lambda(p^\alpha) = \varphi(p^\alpha)$$
$$\lambda(2p^\alpha) = \varphi(2p^\alpha) = \varphi(p^\alpha)$$

ومن المبرهنة (٧,٤) نعلم أن إذا كان a عددا فرديا فإن $a^{\varphi(2^k)/2} = a^{2^{k-2}} \equiv 1 (\mathrm{mod}\ 2^k)$ حيث $k \geq 3$ وإن $ord_{2^k}(a) = 2^{k-2}$ وبهذا يكون $\lambda(2^k) = 2^{k-2}$ لكل $k \geq 3$.

أما الحالة العامة فتقدمها لنا المبرهنة التالية :

مبرهنة (٧,١٩)

ليكن $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ هو تحليل n إلى قوى عوامله الأولية. عندئذ $\lambda(n) = [\lambda(2^{\alpha_0}), \varphi(p_1^{\alpha_1}), \dots, \varphi(p_t^{\alpha_t})]$. إضافة إلى ذلك، يوجد عدد صحيح a يحقق $ord_n(a) = \lambda(n)$.

البرهان

لنفرض أن $a \in \mathbb{Z}$ حيث $(a,n)=1$. ولنفرض أن $S=[\lambda(2^{\alpha_0}), \varphi(p_1^{\alpha_1}), \dots, \varphi(p_t^{\alpha_t})]$. سنبرهن الآن أن $S=\lambda(n)$.

بما أن كل من الأعداد $\lambda(2^{\alpha_0})$ ، $\varphi(p_1^{\alpha_1})$، ... ، $\varphi(p_t^{\alpha_t})$ يقسم S وأن $\varphi(p_i^{\alpha_i})=\lambda(p_i^{\alpha_i})$ لكل $i=1,2,\dots,t$ وأن $a^{\lambda(p_i^{\alpha_i})} \equiv 1 (\text{mod } p_i^{\alpha_i})$ فنجد أن $a^S \equiv 1 (\text{mod } p_i^{\alpha_i})$ لكل $i=1,2,\dots,t$ ونرى أن $a^S \equiv 1 (\text{mod } n)$ ويكون S قوة شاملة للعدد n.

سنبرهن الآن أن S هي بالفعل أصغر قوة شاملة للعدد n. لنفرض لهذا الغرض أن g_i جذراً بدائياً للعدد $p_i^{\alpha_i}$ لكل $i=1,2,\dots,t$. عندئذ، استناداً إلى مبرهنة الباقي الصينية يوجد حل وحيد a قياس n للنظام

$$\begin{aligned} x &\equiv 3 (\text{mod } 2^{\alpha_0}) \\ x &\equiv g_1 (\text{mod } p_1^{\alpha_1}) \\ x &\equiv g_2 (\text{mod } p_2^{\alpha_2}) \\ &\vdots \\ x &\equiv g_t (\text{mod } p_t^{\alpha_t}) \end{aligned}$$

سنبرهن الآن أن $ord_n(a)=S$. ولهذا الغرض نفرض أن $a^T \equiv 1 (\text{mod } n)$ حيث $T \in \mathbb{Z}^+$. عندئذ ، $a^T \equiv 1 (\text{mod } p_i^{\alpha_i})$ لكل $i=1,2,\dots,t$ وأن $a^T \equiv 1 (\text{mod } 2^{\alpha_0})$. ومن ذلك نرى $ord_{p_i^{\alpha_i}}(a) \mid T$ و $ord_{2^{\alpha_0}}(a) \mid T$. ولكن a يحقق كل من تطابقات النظام، وبهذا يكون $ord_{p_i^{\alpha_i}}(a)=\lambda(p_i^{\alpha_i})$ و $ord_{2^{\alpha_0}}(a)=\lambda(2^{\alpha_0})$. وعليه فإن $\lambda(p_i^{\alpha_i}) \mid T$ وأن $\lambda(2^{\alpha_0}) \mid T$ ونستنتج أن $S=[\lambda(2^{\alpha_0}), \lambda(p_1^{\alpha_1}), \dots, \lambda(p_t^{\alpha_t}) \mid T$.

الآن، $a^S \equiv 1 (\text{mod } n)$ و $S \mid T$ كلما كان $a^T \equiv 1 (\text{mod } n)$ يؤدي إلى أن $ord_n(a)=S$. إذن، $S=\lambda(n)$ و $ord_n(a)=\lambda(n)$ ◆

مثال (٧,٢١)

بما أن $720 = 2^4 \times 3^2 \times 5$ فإن :

$$\lambda(720) = [\lambda(2^4), \varphi(3^2), \varphi(5)] = [2^2, 6, 4] = 12$$

ولإيجاد a الذي يحقق $ord_{720}(a) = 12$ نبحث عن جذرين بدائيين للعددين 3^2 و 5. على سبيل المثال، 2 جذر بدائي للعدد 9 و 2 جذر بدائي للعدد 5.

الآن نستخدم مبرهنة الباقي الصينية لحل النظام

$$a \equiv 3 \pmod{16}$$
$$a \equiv 2 \pmod{9}$$
$$a \equiv 2 \pmod{5}$$

فنجد أن $a \equiv 227 \pmod{720}$. وبهذا يكون $ord_{720}(227) = 12$ □

(٧,٣,١) تمارين محلولة *(Solved Exercises)*

تمرين (١)

إذا كان $n > 2$ عدداً لكارمايكل فأثبت أن $n = p_1 p_2 \dots p_k$ حيث p_i أعداد أولية مختلفة تحقق $(p_i - 1) \mid (n-1)$ لكل $i = 1, 2, \dots, n$ [هذا التمرين هو عكس المبرهنة (٣,٤٤)].

الحل

بما أن n عدد كارمايكل فإن $b^{n-1} \equiv 1 \pmod{n}$ لكل عدد b أولي نسبياً مع n.

الآن ، استناداً إلى المبرهنة (٧,١٩) نستطيع إيجاد عدد a أولي نسبياً مع n ويحقق $ord_n(a) = \lambda(n)$. وبما أن n عدد كارمايكل فإن $a^{n-1} \equiv 1 \pmod{n}$. إذن، $\lambda(n) \mid (n-1)$. لاحظ أن n يجب أن يكون فردياً، لأنه لو كان زوجياً فإن $n-1$ فردي وهذا يناقض كون $\lambda(n)$ زوجي ويقسم $n-1$.

لنفرض الآن أن $n = p_1^{k_1} p_1^{k_2} \dots p_t^{k_t}$ هو تحليل n إلى قوى عواملة الأولية. سنبرهن أن $k_1 = k_2 = \dots = k_t = 1$. لنفرض أنه يوجد i حيث $k_i \geq 2$. عندئذ،

$$\lambda(p_i^{k_i}) = \varphi(p_i^{k_i}) = p_i^{k_i - 1}(p_i - 1)$$

وبما أن $\lambda(n)\mid(n-1)$ و $\varphi(p_i^{k_i})\mid\lambda(n)$ فإن $p_i^{k_i-1}(p_i-1)\mid(n-1)$ ويكون $p_i\mid(n-1)$ وهذا مستحيل لأن $p_i\mid n$. إذن، $k_i=1$ لكل $i=1,2,\ldots,t$ ويكون $n=p_1p_2\ldots p_t$.

ولإنهاء الاثبات لاحظ أن $\lambda(p_i)=\varphi(p_i)=p_i-1$. وبما أن $\lambda(p_i)\mid(n-1)$ فإن $(p_i-1)\mid(n-1)$ △

تمرين (٢)

إذا كان $n=p_1p_2\ldots p_t$ عدداً لكارمايكل فأثبت أن $t\geq 3$.

الحل

لنفرض أن $t=2$. عندئذ ، $n=p_1p_2$ حيث $p_1>p_2$. عندئذ ،

$$n-1=p_1p_2-1=(p_1-1)p_2+(p_2-1)$$
$$\equiv p_2-1\not\equiv 0(\text{mod } p_1-1)$$

ولذا فإن p_1-1 لا يقسم $n-1$ وهذا مستحيل إذن، $t\geq 3$ △

تمارين (٣,٧)

(١) عين القوة الشاملة الصغرى $\lambda(n)$ لكل من الأعداد التالية:

(أ) 120 (ب) 180 (ج) 288 (د) 600

(هـ) $2^6\times3^2\times5\times7\times13\times37$ (و) 20!

(٢) جد عدد صحيح a بحيث تكون رتبته قياس $n=36$ أكبر ما يمكن .

(٣) أعد التمرين (٢) إذا كان $n=63$.

(٤) إذا كان a أولياً نسبياً مع كل من 2, 3, 5, 7, 13 فأثبت أن $a^{12}\equiv 1(\text{mod } 65520)$.

(٥) إذا كان $n\in\mathbb{Z}^+$ فأثبت أن $\lambda(n)$ يقسم $\varphi(n)$.

(٦) إذا كان $(m,n)=1$ فأثبت أن $\lambda(mn)=[\lambda(m),\lambda(n)]$.

(٧) ليكن $n=p_1p_2\ldots p_t$ حيث p_i أعداد أولية مختلفة. أثبت أن $\frac{\lambda(n)}{\varphi(n)}\leq\frac{1}{2^{t-1}}$

نبذة عن حياة لاجرانج *Biography of Lagrange*

ولد: ١٧٣٦/١/٢٥م في تورين (إيطاليا)

توفي: ١٨١٣/٤/١٥م في باريس (فرنسا).





إن الشائع لدى معظم الرياضيين أن جوزيف لويس لاجرانج *(Joseph Louis Lagrange)* رياضي فرنسي، إلا أنه في الحقيقة ولد في إيطاليا لأبوين إيطاليين وهيئه والده لدراسة القانون في جامعة تورين.

في البداية لم يظهر لاجرانج أي اهتمام للرياضيات، وعلى العكس من ذلك فإنه كان يعتبر الهندسة الإقليدية موضوعاً مملاً ، إلا أن هذا لم يدم طويلاً حيث بدأ يحول إهتمامه إلى الرياضيات بعد دراسته لكتاب هالي *(Halley)* الذي يشرح فيه استخدامات الجبر في علم البصريات.

ولا شك في أن الرياضيات مدينة لفقر والد لاجرانج حيث اعترف لاجرانج إنه لو كان غنياً لما كرس حياته للرياضيات ، وهذا ما حصل بالفعل حيث اعتمد كلياً على نفسه لتعلم الرياضيات و لم يحظى بإشراف أحد من مشاهير الرياضيين في عصره.

لقد كان للبحث الذي أرسله لأويلر عام ١٧٥٥م في حساب تفاضل وتكامل التغيرات الفضل الكبير في شهرة لاجرانج حيث كان واضحاً لأويلر الأصالة والعمق الرياضي الذي يتمتع به هذا البحث، وعلى أثر ذلك عين وهو لم يتجاوز التاسعة عشر بعد أستاذاً للرياضيات في المدرسة الملكية لسلاح المدفعية في مدينة تورين وكان أحد الأعضاء المؤسسين للأكاديمية العلمية الملكية في مدينة تورين. وما إن تخلى أويلر في العام ١٧٦٦م عن منصبه في أكاديمية برلين العلمية لانتقاله إلى سانت بطرس بيرغ حتى رشح لاجرانج لهذا المنصب.

وبعد أن غيب الموت أويلر في العام ١٧٨٣ أصبح لاجرانج أهم الرياضيين في أوروبا. انضم لاجرانج في العام ١٧٨٧م إلى الأكاديمية الفرنسية تلبية للدعوة التي وجهت له من قبل الملك لويس السادس عشر وبقي في فرنسا حتى وافاه الأجل عام ١٨١٣م .

كان للاجرانج اسهامات مهمة في الكثير من فروع الرياضيات كالميكانيكا والجبر ونظرية الأعداد. من أهم اسهاماته في نظرية الأعداد تقديمه أول برهان منشور لمبرهنة ويلسن وإثباته إمكانية تمثيل أي عدد صحيح موجب كمجموع لأربعة مربعات. كما كانت له اليد الطولى في تطوير الكسور المتواصلة وإثبات قابلية الحل لمعادلة بيل، وله بعض النتائج المهمة في تطابقات كثيرات الحلول. أما إسهاماته في الجبر تتضمن نظرية المعادلات ونظرية الزمر حيث يعتبر إثباته أن رتبة أي زمرة جزئية من زمرة منتهية يجب أن تقسم رتبة الزمرة ألف باء نظرية الزمر.

الفصل الثامن

الرواسب التربيعية
QUADRATIC RESIDUES

قدمنا في الفصل الثالث التطابقات الخطية ودرسنا الشرط اللازم والكافي لوجود حل لمثل هذه التطابقات ومن ثم وجدنا جميع الحلول غير المتطابقة لها. كمنا درسنا أيضاً تطابقات كثيرات الحدود. في هذا الفصل سنركز اهتمامنا على تطابقات الدرجة الثانية لما لها من أهمية سواء من الناحية النظرية أو الناحية التطبيقية.

(٨,١) التطابقات التربيعية
Quadratic Congruences

التطابق التربيعي هو التطابق الذي يأخذ الصورة:

$$ax^2 + bx + c \equiv 0 (\text{mod } n)$$

ولقد بينا في الفصل الثالث أنه لإيجاد حلول مثل هذه فإننا نقوم بتحليل العدد n إلى عوامله الأولية

$$n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$$

ثم نجد حلول التطابق قياس $p_i^{k_i}$. ولذا فإننا سنبدأ بالحالة التي يكون فيها القياس عدداً أولياً ، وفي هذه الحالة يأخذ التطابق الصورة :

$$ax^2 + bx + c \equiv 0 \pmod{p} \qquad (1)$$

حيث p عدد أولي لا يقسم a .

باستخدام مبرهنة لاجرانج نعلم أن لهذا التطابق على الأكثر حلين غير متطابقين قياس p. إذا كان $p = 2$ فإن التطابق (١) يأخذ إحدى الصور التالية:

$$x^2 \equiv 0 \pmod 2,\ x^2 + 1 \equiv 0 \pmod 2,\ x^2 + x \equiv 0 \pmod 2,\ x^2 + x + 1 \equiv 0 \pmod 2 .$$

ومن السهل أن نرى أن $x \equiv 0 \pmod 2$ هو الحل الوحيد للتطابق $x^2 \equiv 0 \pmod 2$ ، $x \equiv 1 \pmod 2$ هو الحل الوحيد للتطابق $x^2 + 1 \equiv 0 \pmod 2$ ، $x \equiv 0,1 \pmod 2$ هما الحلان للتطابق $x^2 + x \equiv 0 \pmod 2$. وأما التطابق $x^2 + x + 1 \equiv 0 \pmod 2$ فإنه غير قابل للحل.

ولذا فإننا نقصر دراستنا على الحالة التي يكون فيها p عدداً أولياً فردياً.

مبرهنة (٨,١)

ليكن p عدداً أولياً فردياً لا يقسم العدد a. عندئذ، يكون x_0 حلاً للتطابق $ax^2 + bx + c \equiv 0 \pmod p$ إذا وفقط إذا كان $y_0 = 2ax_0 + b$ حلاً للتطابق $y^2 \equiv d \pmod p$ حيث $d = b^2 - 4ac$.

البرهان

لنفرض أن x_0 حل للتطابق $ax^2 + bx + c \equiv 0 \pmod p$. بما أن p لا يقسم a فإن p لا يقسم $4a$. ولذا فإن:

$$4a^2x_0^2 + 4abx_0 + 4ac \equiv 0 \pmod p$$

ومنه فإن $(2ax_0 + b)^2 \equiv b^2 - 4ac \pmod p$. وبهذا نرى أن $y_0 \equiv 2ax_0 + b \pmod p$ حل للتطابق $y^2 \equiv d \pmod p$ حيث $d = b^2 - 4ac$.

لبرهان العكس، نفرض أن $y_0 \equiv 2ax_0 + b \pmod p$ حل للتطابق $y^2 \equiv d \pmod p$. عندئذ، $(2ax_0+b)^2 \equiv b^2 - 4ac \pmod p$. ومنه فإن $ax_0^2 + bx_0 + c \equiv 0 \pmod p$. وبالتالي فإن x_0 حل للتطابق $ax^2 + bx + c \equiv 0 \pmod p$ ◆

مثال (٨,١)

لإيجاد حلول التطابق $11x^2 + 5x + 18 \equiv 0 \pmod{29}$ نقوم بإكمال المربع فنحصل على: $(22x+5)^2 \equiv 16 \pmod{29}$. ولذا فإن $22x + 5 \equiv \pm 4 \pmod{29}$. وبحل التطابق $22x + 5 \equiv 4 \pmod{29}$ نجد أن $x \equiv 25 \pmod{29}$. وأما حل التطابق $22x + 5 \equiv -4 \pmod{29}$ فهو $x \equiv 22 \pmod{29}$. وعليه نجد أن $x = 22, 25$ هما الحلان للتطابق $11x^2 + 5x + 18 \equiv 0 \pmod{29}$ □

مما سبق نجد أنه لحل التطابق (١) يكفي أن نقوم بحل التطابق:

$$x^2 \equiv a \pmod p \qquad (٢)$$

حيث p عدد أولي فردي و $1 \le a \le p-1$. ولكن استناداً إلى المبرهنة (٣,٤٨) فإن للتطابق (٢) على الأكثر حلان غير متطابقين. ومن الواضح أنه إذا كان $x \equiv x_0 \pmod p$ حلاً للتطابق فإن $x \equiv -x_0 \pmod p$ حلاً آخر وأن $x_0 \not\equiv -x_0 \pmod p$. وبالتالي فإنه إما أن يكون التطابق (٢) غير قابل للحل أو أن يكون له حلين غير متطابقين.

تعريف (٨,١)

(أ) إذا وجد حل للتطابق (٢) فنقول إن a راسب تربيعي قياس p (a *quadratic residue modulo* p) .

(ب) إذا لم يوجد حل للتطابق (٢) فنقول إن a راسب غير تربيعي قياس p (a *quadratic nonresidue modulo* p) .

ملحوظات

(١) سنرمز لمجموعة الرواسب التربيعية قياس العدد الأولي الفردي p بالرمز Q_p .

(٢) إذا كان p عدداً صغيراً فإنه من الممكن إيجاد عناصر Q_p بتربيع العناصر $1,2,3,\ldots,p$.

(٣) لاحظ أن الرواسب التربيعية قياس p ما هي إلا الرواسب من الدرجة k حيث $k=2$ التي قدمناها في الفصل السابع.

مثال (٨,٢)

إذا كان $p=2$ فإن:

$$1^2 \equiv 10^2 \equiv 1 (\text{mod } 11)$$
$$5^2 \equiv 6^2 \equiv 3 (\text{mod } 11)$$
$$2^2 \equiv 9^2 \equiv 4 (\text{mod } 11)$$
$$4^2 \equiv 7^2 \equiv 5 (\text{mod } 11)$$
$$3^2 \equiv 8^2 \equiv 9 (\text{mod } 11)$$

وعليه فإن $Q_{11}=\{1,3,4,5,9\}$ □

المبرهنة التالية تبين لنا أن عدد الرواسب التربيعية قياس العدد الأولي الفردي p يساوي عدد الرواسب غير التربيعية قياس p ولكننا نحتاج أولاً إلى التمهيدية التالية:

تمهيدية (٨,٢)

إذا كان p عدداً أولياً فردياً وكان $a^2 \equiv b^2 \pmod p$ حيث $1 \le a \le b \le \frac{1}{2}(p-1)$ فإن $a = b$.

البرهان

بما أن $a^2 \equiv b^2 \pmod p$ فإن $a \equiv \pm b \pmod p$. وبما أن $2 \le a+b \le p-1$ فإن $a+b \not\equiv 0 \pmod p$. ولذا فإن $a \equiv b \pmod p$. أي أن $b-a \equiv 0 \pmod p$ حيث $0 \le b-a \le \frac{p-3}{2}$. وعليه فإن $b-a=0$ ويكون $a=b$ ◆

مبرهنة (٨,٣)

إذا كان p عدداً أولياً فردياً فإن $|Q_p| = \varphi(p) = \frac{1}{2}(p-1)$ وإن عدد الرواسب غير التربيعية قياس p يساوي أيضاً $\frac{\varphi(p)}{2}$.

البرهان

نعتبر نظام الرواسب المختزل التالي قياس p :

$$1, 2, \ldots, \frac{1}{2}(p-1), -1, -2, \ldots, -\frac{1}{2}(p-1)$$

إذا كان $x \in \mathbb{Z}^+$ حيث $(x,p)=1$ فيوجد عدد وحيد i، $1 \le i \le \frac{1}{2}(p-1)$ حيث $x \equiv i \pmod p$ أو $x \equiv -i \pmod p$. وعليه فإن $x^2 \equiv i^2 \pmod p$. الآن ، إذا كان $a \in Q_p$ فإن $a \equiv i^2 \pmod p$ حيث $1 \le i \le \frac{1}{2}(p-1)$. ويكون $|Q_p| \le \frac{1}{2}(p-1)$. وبما أن $i^2 \pmod p$ ، $1 \le i \le \frac{1}{2}(p-1)$ جميعها أعداداً مختلفة استناداً إلى التمهيدية (٨,٢) فنرى أن $|Q_p| = \frac{1}{2}(p-1)$.

وأخيراً إذا كان m هو عدد الرواسب غير التربيعية قياس p فإن:

◆ $m = p - 1 - \frac{1}{2}(p-1) = \frac{1}{2}(p-1)$

ملحوظة

لاحظ أنه إذا كان p عدداً أولياً فردياً فإنه استناداً إلى المبرهنة (٨,٣) نجد أن الرواسب التربيعية قياس p هي المربعات $1^2, 2^2, \ldots, (\frac{1}{2}(p-1))^2$. على سبيل المثال، إذا كان $p = 11$ فإن الرواسب التربيعية هي: $1^2, 2^2, 3^2, 4^2, 5^2$. أي 1,4,9,5,3 قياس العدد11 وهذا يتفق مع ما وجدناه في المثال (٨,٢).

(٨,١,١) تمارين محلولة *(Solved Exercises)*

تمرين (١)

إذا كان كل من a و b راسباً تربيعياً قياس العدد الأولي p فأثبت أن كل من ab و a^{-1} راسب تربيعي قياس p .

الحل

بما أن a و b راسبان تربيعيان قياس p فإنه يوجد i و j أوليان نسبياً مع p بحيث يكون $i^2 \equiv a \pmod p$ و $j^2 \equiv a \pmod p$. وعليه فإن:

$$(ij)^2 = i^2 j^2 \equiv ab \pmod p$$

ويكون ab راسباً تربيعياً قياس p . أيضاً:

$$(i^{-1})^2 \equiv (i^2)^{-1} \equiv a^{-1} \pmod p$$

ولذا فإن a^{-1} راسب تربيعي قياس p △

تمرين (٢)

إذا كان p عدداً أولياً فردياً وكان $a,b \in \mathbb{Z}$ حيث $a \equiv b \pmod p$ و $|a| = |b| = 1$ فأثبت أن $a = b$.

الحل

بما أن $|a|=|b|$ فإن $a=\pm b$. إذا كان $a=-b$ فإن

$$|a-b|=|2a|=2|a|=2\times1=2$$

وبما أن $a\equiv b(\text{mod } p)$ فإن $p|(a-b)$. ومنه فإن $p|(|a-b|)$. أي أن $p|2$ وهذا مستحيل لأن p فردي. إذن، $a=b$ △

تمرين (٣)

(أ) إذا كان $p\equiv 4k+3$ عدداً أولياً وكان a راسباً تربيعياً قياس p فأثبت أن حلي التطابق $x^2\equiv a(\text{mod } p)$ هما $\pm a^{k+1}(\text{mod } p)$.

(ب) استخدم الفقرة (أ) لحل التطابق $x^2\equiv 46(\text{mod } 59)$.

الحل

(أ) بما أن a راسب تربيعي قياس p فإن التطابق $x^2\equiv a(\text{mod } p)$ قابل للحل. ولذا نجد من معيار أويلر أن $a^{\frac{p-1}{2}}\equiv 1(\text{mod } p)$. أي أن $a^{2k+1}\equiv 1(\text{mod } p)$. ونرى أن

$$\left(\pm a^{k+1}\right)^2\equiv aa^{2k+1}\equiv a(\text{mod } p)$$

وبهذا فإن $\pm a^{k+1}(\text{mod } p)$ هما حلا التطابق $x^2\equiv a(\text{mod } p)$.

(ب) بما أن $59=4\times14+3$ فإن حلي التطابق هما

$$\pm(46)^{14+1}=\pm(46)^{15}\equiv\pm39(\text{mod } 59)$$

أي أن الحلين هما $20,39(\text{mod } 59)$ △

تمارين (١, ٨)

(١) حل التطابق $3x^2+2x+3\equiv 0(\text{mod } 11)$.

(٢) حل التطابق $2x^2+x+3\equiv 0(\text{mod } 5)$.

(٣) جد جميع الرواسب التربيعية قياس العدد 7.

(٤) جد جميع الرواسب التربيعية قياس العدد 13.

(٥) جد جميع الرواسب التربيعية قياس العدد 17.

(٦) جد جميع الرواسب التربيعية قياس العدد 19.

(٧) إذا كان a راسباً تربيعياً قياس العدد الأولي p وكان $a \equiv b \pmod{p}$ فأثبت أن b راسب تربيعي قياس p.

(٨) ليكن p عدداً أولياً فردياً وليكن $ax^2+bx+c \equiv 0 \pmod{p}$ حيث $p \nmid a$ وليكن $d = b^2 - 4ac$.

(أ) إذا كان d ليس راسباً تربيعياً قياس p فأثبت أنه لا يوجد حل للتطابق.

(ب) إذا كان $p \mid d$ فإنه يوجد حل وحيد للتطابق.

(ج) إذا كان d راسباً تربيعياً قياس p فأثبت أنه يوجد حلان للتطابق.

(٩) استخدم التمرين المحلول (٣) لايجاد حلول كل من التطابقات التالية:

(أ) $x^2 \equiv 49 \pmod{59}$ (ب) $x^2 \equiv 6 \pmod{43}$

(ج) $x^2 \equiv 36 \pmod{103}$ (د) $x^2 \equiv 4 \pmod{107}$

(١٠) إذا كان a ليس راسباً تربيعياً قياس كل من العددين الأوليين p و q فهل يمكن أن يكون a راسباً تربيعياً قياس pq؟

(١١) جد جميع حلول التطابق $x^2 \equiv 860 \pmod{11021}$.

(٨,٢) رمز ليجندر
Legendre Symbol

نقدم في هذا البند رمز ليجندر والذي يُسهِّل علينا معرفة فيما إذا كان العدد a الأولي نسبياً مع العدد الأولي الفردي p راسباً تربيعياً قياس p.

تعريف (٨,٢)

إذا كان p عدداً أولياً فردياً وكان $(p,a)=1$ فإننا نكتب $\left(\frac{a}{p}\right)$ لرمز ليجندر ونعرفه على النحو التالي:

$$\left(\frac{a}{p}\right)=\begin{cases}1, & a\in Q_p\\ -1, & a\notin Q_p\end{cases}$$

مثال (٨,٣)

استناداً إلى المثال (٨,٢) يكون:

$$\left(\frac{1}{11}\right)=\left(\frac{3}{11}\right)=\left(\frac{4}{11}\right)=\left(\frac{5}{11}\right)=\left(\frac{9}{11}\right)=1$$

$$\left(\frac{2}{11}\right)=\left(\frac{6}{11}\right)=\left(\frac{7}{11}\right)=\left(\frac{8}{11}\right)=\left(\frac{10}{11}\right)=-1 \quad \square$$

ملحوظات

(١) لاحظ أن إيجاد قيمة رمز ليجندر $\left(\frac{a}{p}\right)$ يكافيء معرفة فيما إذا كان التطابق $x^2\equiv a(\text{mod } p)$ قابلاً للحل.

(٢) من الممكن الآن استخدام رمز ليجندر لتقديم نصاً مكافئاً لمعيار أويلر فيكون هذا النص : إذا كان p عدداً أولياً فردياً وكان $(a,p)=1$ فإن:

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}(\text{mod } p)$$

المبرهنة التالية تزودنا بالخواص الأساسية لرمز ليجندر :

مبرهنة (٨,٤)

إذا كان p عدداً أولياً فردياً وكان $a,b\in\mathbb{Z}^+$ حيث $(a,p)=(b,p)=1$ فإن:

(١) إذا كان $a \equiv b \pmod p$ فإن $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(٢) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(٣) $\left(\frac{a^2}{p}\right) = 1$.

البرهان

(١) إذا كان $a \equiv b \pmod p$ فمن الواضح أن التطابق $x^2 \equiv a \pmod p$ قابل للحل إذا وفقط إذا كان التطابق $x^2 \equiv b \pmod p$ قابلاً للحل. وبهذا نرى أن $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(٢) باستخدام معيار أويلر لدينا:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

وبما أن $\left|\left(\frac{ab}{p}\right)\right| = \left|\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right| = 1$ فنجد باستخدام التمرين (٢) من التمارين المحلولة (٨,١,١) أن $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(٣) باستخدام الفقرة (٢) نجد أن $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)^2 = 1$ ◆

ملحوظات

(١) لاحظ أننا نستطيع أن نستنتج من الفقرة (٢) للمبرهنة (٨,٤) أن حاصل ضرب راسبان تربيعيان (أو غير تربيعيان) هو راسب تربيعي وأن حاصل ضرب راسب تربيعي مع راسب غير تربيعي هو راسب غير تربيعي قياس العدد الأولي p.

(٢) باستخدام المبرهنة (٨,٤) ، نجد أنه لحساب قيمة $\left(\frac{a}{p}\right)$ يكفي أن نقوم بحساب القيم $\left(\frac{q_1}{p}\right), \ldots, \left(\frac{q_k}{p}\right)$ حيث $a = q_1 q_2 \ldots q_k$ و q_i أعداد أولية.

المبرهنة التالية تبين لنا متى يكون العدد -1 راسباً تربيعياً قياس العدد الأولي p.

مبرهنة (٨,٥)

إذا كان p عدداً أولياً فردياً فإن:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \ , & p \equiv 1 \pmod 4 \\ -1 \ , & p = -1 \pmod 4 \end{cases}$$

أي أن : $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

البرهان

باستخدام معيار أويلر لدينا: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \pmod p$.

إذا كان $p \equiv 1 \pmod 4$ فإن $\frac{p-1}{2} = 2k$ حيث $k \in \mathbb{Z}$. ومنه فإن $(-1)^{\frac{p-1}{2}} = 1$.

أي أن $\left(\frac{-1}{p}\right) = 1$.

أما إذا كان $p \equiv -1 \pmod 4$ فإن $\frac{p-1}{2} = 2k+1$ حيث $k \in \mathbb{Z}$. ومنه فإن

$(-1)^{\frac{p-1}{2}} = -1$. وبالتالي فإن $\left(\frac{-1}{p}\right) = -1$ ◆

تبين لنا المبرهنة التالية متى يكون العدد 2 راسباً تربيعياً قياس العدد الأولي الفردي p.

مبرهنة (٨,٦)

إذا كان p عدداً أولياً فردياً فإن:

$$\left(\frac{2}{p}\right)=\begin{cases}1, & p\equiv\pm1(\text{mod }8)\\ -1, & p\equiv\pm3(\text{mod }8)\end{cases}.$$

أي أن $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

البرهان

إذا كان $p\equiv1(\text{mod }8)$ أو $p\equiv5(\text{mod }8)$ فنجد :

$$2^{(p-1)/2}\left(\frac{p-1}{2}\right)!=2\times4\times6\times\ \dots\ \times(p-1)$$

$$\equiv2\times4\times6\times\ \dots\ \times\left(\frac{p-1}{2}\right)\times\left(\frac{-p-3}{2}\right)\times\ \dots\ \times(-5)\times(-3)\times(-1)$$

$$\equiv(-1)^{(p-1)/4}\left(\frac{p-1}{2}\right)!\ (\text{mod }p)$$

ولذا فإن $2^{(p-1)/2}\equiv(-1)^{(p-1)/4}(\text{mod }p)$. ولكن استناداً إلى معيار أويلر لدينا :

$$\left(\frac{2}{p}\right)\equiv2^{(p-1)/2}(\text{mod }p)$$

إذن ،
$$\left(\frac{2}{p}\right)=(-1)^{(p-1)/4}=\begin{cases}1, & p\equiv1(\text{mod }8)\\ -1, & p\equiv5(\text{mod }8)\end{cases}$$

وبالمثل ، إذا كان $p\equiv3(\text{mod }8)$ أو $p\equiv7(\text{mod }8)$ فإن :

$$2^{(p-1)/2}\left(\frac{p-1}{2}\right)!\equiv2\times4\times6\times\ \dots\ \times\left(\frac{p-3}{2}\right)\times\left(-\frac{p-1}{2}\right)\times\ \dots\ \times(-5)\times(-3)\times(-1)$$

$$\equiv(-1)^{(p+1)/4}\left(\frac{P-1}{2}\right)!\ (\text{mod }p)$$

ولذا فإن :

$$\left(\frac{2}{p}\right)=(-1)^{(p+1)/4}=\begin{cases}1, & p\equiv7(\text{mod }8)\\ -1, & p\equiv3(\text{mod }8)\end{cases}$$

وأخيراً، لاحظ أن $\frac{p^2-1}{8}$ زوجياً إذا كان $p \equiv \pm 1 \pmod 8$ وفردياً إذا كان $p \equiv \pm 3 \pmod 8$. ولذا فإن $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$ ◆

نتيجة (٨,٧)

إذا كان p عدداً أولياً فردياً فإن :

$$\left(\frac{-2}{p}\right)=\begin{cases}1, & p \equiv 1 \text{ أو } 3 \pmod 8 \\ -1, & p \equiv 5 \text{ أو } 7 \pmod 8\end{cases}$$

البرهان

بما أن $\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ فإن:

$\left(\frac{-2}{p}\right)=1$ إذا وفقط إذا كان $\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=1$ أو $\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=-1$

الآن، باستخدام المبرهنتين (٨,٥) و (٨,٦) نجد أن:

$\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=1$ إذا وفقط إذا كان $p \equiv 1 \pmod 4$ و $p \equiv \pm 1 \pmod 8$. وعليه نستنتج أن $p \equiv 1 \pmod 8$ في هذه الحالة.

كما أن $\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=-1$ إذا وفقط إذا كان $p \equiv 3 \pmod 4$ و $p \equiv \pm 3 \pmod 8$. ولذا فإن $p \equiv 3 \pmod 8$ في هذه الحالة . وبهذا يكون

وبالتالي فإننا نخلص إلى أن: $\left(\frac{-2}{p}\right)=\begin{cases}1, & p \equiv 1,3 \pmod 8 \\ -1, & p \equiv 5,7 \pmod 8\end{cases}$ ◆

(٨,٢,١) تمارين محلولة (Solved Exercises)

تمرين (١)

ليكن q عدداً أولياً فردياً حيث $p=4q+1$ عدداً أولياً.

(أ) أثبت أن $\left(\frac{2}{p}\right)=-1$ (ب) أثبت أن p يقسم 4^q+1 .

الحل

(أ) بما أن q عدد فردي فإن $q=2k+1$. ومن ثم فإن $p=4q+1=8k+5$.

إذن، $\left(\frac{2}{p}\right)=-1$.

(ب) باستخدام معيار أويلر لدينا: $\left(\frac{2}{p}\right)\equiv 2^{(p-1)/2}=2^{2q}=4^q \pmod p$.$-1=$

وعليه فإن p يقسم 4^q+1 △

تمرين (٢)

إذا كان a جذراً بدائياً قياس العدد الأولي الفردي p فأثبت أن $\left(\frac{a}{p}\right)=-1$.

الحل

بما أن a جذر بدائي قياس p فإن $ord_p(a)=p-1$. ومن ثم فإن $a^{p-1}\equiv 1 \pmod p$ وأن $a^k\not\equiv 1 \pmod p$ لكل $k<p-1$. الآن، باستخدام معيار أويلر نجد أن $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\not\equiv 1 \pmod p$. وبهذا يكون $\left(\frac{a}{p}\right)=-1$ △

تمرين (٣)

أثبت أن أي راسب غير تربيعي قياس العدد الأولي الفردي p يجب أن يكون جذراً بدائياً قياس p إذا وفقط إذا كان $p=F_k$ حيث $k\in\mathbb{Z}$.

الحل

لاحظ أولاً أن عدد الرواسب غير التربيعية قياس p يساوي $\frac{1}{2}(p-1)$ وأن عدد الجذور البدائية قياس p يساوي $\varphi(p-1)$. وعليه فإن أي راسب غير تربيعي هو جذر بدائي قياس p إذا وفقط إذا كان $\varphi(p-1)=\frac{1}{2}(p-1)$. ولكننا نعلم استناداً إلى تمرين (١٠) من التمارين (٥,٤) أن $\varphi(n)=\frac{n}{2}$ إذاً وفقط إذا كان $n=2^m$ حيث $m\in\mathbb{Z}$. عندئذ، أي راسب غير تربيعي هو جذراً بدائياً قياس p إذا وفقط إذا كان $p-1=2^m$ حيث $m\in\mathbb{Z}$. وبما أن $p=2^m+1$ أولي فنجد استناداً المبرهنة (٢,١٥) إلى أن $m=2^k$ حيث $k\in\mathbb{Z}$. أي أن $p=F_k$ △

تمارين (٨,٢)

(١) استخدم معيار أويلر لايجاد قيمة رمز ليجندر لكل مما يلي:

(أ) $\left(\frac{5}{23}\right)$ (ب) $\left(\frac{3}{29}\right)$ (ج) $\left(\frac{2}{19}\right)$ (د) $\left(\frac{2}{23}\right)$

(٢) إذا كان a راسباً تربيعياً قياس العدد الأولي الفردي p فأثبت أن $-a$ راسب تربيعي قياس p إذا وفقط إذا كان $p\equiv 1 \pmod 4$.

(٣) إذا كان p عدداً أولياً فردياً فأثبت أن:

$$\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)+\ldots+\left(\frac{p-1}{p}\right)=0$$

(٤) إذا كان p عدداً أولياً فردياً وكان $(a,p)=1$ فأثبت أن

$$\left(\frac{a(a+1)}{p}\right)=\left(\frac{a^{-1}+1}{p}\right)$$

حيث a^{-1} هو النظير الضربي للعدد a قياس p.

(٥) إذا كان p عدداً أولياً فردياً فأثبت أن:

$$\left(\frac{1\times 2}{p}\right)+\left(\frac{2\times 3}{p}\right)+\ldots+\left(\frac{(p-2)(p-1)}{p}\right)=-1$$

(٦) إذا كان $p>5$ عدداً أولياً فأثبت أنه يوجد راسبان تربيعيان متتاليان قياس p.

(٧) إذا كان $ab\equiv 1(\text{mod } p)$ حيث p عدد أولي فردي فأثبت أن $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

(٨) ليكن p عدداً أولياً فردياً ولتكن $a_1,a_2,\ldots,a_{\frac{p-1}{2}}$ جميع الرواسب التربيعية قياس p ولنفرض أن $m=a_1a_2\ldots a_{\frac{p-1}{2}}$.

(أ) إذا كان $p\equiv 1(\text{mod } 4)$ فأثبت أن $m\equiv -1(\text{mod } p)$.

(ب) إذا كان $p\equiv 3(\text{mod } 4)$ فأثبت أن $m\equiv 1(\text{mod } p)$.

(٩) إذا كان $p>3$ عدداً أولياً فردياً فأثبت أن مجموع الرواسب التربيعية قياس p يقبل القسمة على p.

(١٠) استخدم معيار أويلر لاثبات أن 83 لا يقسم $2^{41}-1$.

(١١) استخدم معيار أويلر لإثبات أن 1999 يقسم $2^{999}-1$.

(١٢) إذا كان $n=4k+3$ عدداً صحيحاً موجباً حيث $p=2n+1$ عدد أولي فأثبت أن $2^n\equiv 1(\text{mod } p)$.

(١٣) إذا كان p عدداً أولياً فردياً ويقسم a^2+b^2 حيث $(a,p)=(b,p)=1$ فأثبت أن $p\equiv 1(\text{mod } 4)$

(٨,٣) قانون التعاكس التربيعي
The Law of Quadratic Reciprocity

إذا كان p عدداً أولياً فردياً وكان $a>1$ حيث $(a,p)=1$ فلحساب قيمة $\left(\frac{a}{p}\right)$ يكفي حساب القيم $\left(\frac{q}{p}\right)$ لكل قاسم أولي q للعدد a وذلك بالاستعانة

بخواص رمز ليجندر. سنقدم في هذا البند قانون التعاكس التربيعي الذي يساعدنا على حساب قيمة $\left(\frac{q}{p}\right)$ حيث p و q عددان أوليان فرديان.

يوجد العديد من البراهين المختلفة لقانون التعاكس التربيعي والبرهان الـذي سنقدمه في هذا البند يعتمد على تمهيدية لجاوس قدمها في العام ١٨٠٨م.

مبرهنة (٨,٨) [تمهيدية جاوس]

ليكن p عدداً أولياً فردياً وليكن $a \in \mathbb{Z}^+$ حيث $(a,p)=1$.

ولتكن $A=\left\{a,2a,3a,\ldots,\left(\frac{p-1}{2}\right)a\right\}$

ولتكن $B=\{b(\bmod p): b\in A\ ,\ 0\le b<p\}$

ولتكن $R=\{r_1,r_2,\ldots,r_n\}$ حيث $r_i\in B$ و $r_i>\frac{p}{2}$

ولتكن $S=\{s_1,s_2,\ldots,s_m\}$ حيث $s_j\in B$ و $s_i\le\frac{p}{2}$.

عندئذ ، $\left(\frac{a}{p}\right)=(-1)^n$.

البرهان

سنبرهن أولاً أن عناصر A غير متطابقة قياس p . لنفـرض أن $ia\equiv ja(\bmod p)$ حيث $1\le i\le j\le\frac{p-1}{2}$. عندئذ، $i\equiv j(\bmod p)$ لأن $(a,p)=1$. ونرى أن $j-i\equiv 0(\bmod p)$ ، $0\le j-i\le\frac{p-3}{2}$. ولـذا فـإن $j-i=0$. ويكون $i=j$.

الآن ، بما أن عناصر A غير متطابقة قياس p فإن جميع عناصر R وجميع عناصر S غير متطابقة قياس p. سنبرهن الآن أن جميع العناصر $p-r_i$ حيث $r_i\in R$ مختلفة عن عناصر S . لنفرض أن $p-r_i=s_j$. عندئذ، $r_i+s_j\equiv 0(\bmod p)$. الآن، $r_i\equiv ga(\bmod p)$ ، $s_j=ha(\bmod p)$ حيث $1\le g,h\le\frac{p-1}{2}$. ويكون

$$(g+h)a \equiv ga+ha \equiv r_i + s_j \equiv 0 \pmod{p}$$

ومنه فإن $g+h \equiv 0 \pmod{p}$ وهذا مستحيل الآن $2 \le g+h \le p-1$. إذن، $p-r_i \neq s_j$ لكل i و j. مما سبق نخلص إلى أن مجموعة العناصر :

$$\{p-r_1, p-r_2, \dots, p-r_n, s_1, s_2, \dots, s_m\}$$

جميعها عناصر مختلفة عددها $\frac{p-1}{2}$ وكل منها يقع بين 1 و $\frac{p-1}{2}$. ولذا فإنها تبديلاً للمجموعة $\left\{1,2,3,\dots,\frac{p-1}{2}\right\}$. وبهذا نرى أن

$$\prod_{i=1}^{n}(p-r_i)\prod_{j=1}^{m}s_j \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$$

أي أن :

$$(-1)^n \prod_{i=1}^{n} r_i \prod_{j=1}^{m} s_j \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$$

ولكن :

$$(-1)^n \prod_{i=1}^{n} r_i \prod_{j=1}^{m} s_j \equiv (-1)^n \prod_{k=1}^{\frac{p-1}{2}} ka \equiv (-1)^n a^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} k$$

$$\equiv (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}$$

ومنه فإن:

$$(-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$$

ونخلص إلى أن:

$$a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$$

وبالتالي، استناداً إلى معيار أويلر نجد أن: $\left(\frac{a}{p}\right) = (-1)^n$ ◆

مثال (٨,٤)

استخدم تمهيدية جاوس لإثبات أن $\left(\frac{3}{19}\right) = -1$.

الحل

بما أن $\frac{1}{2}(19-1) = 9$ فإن $A = \{3, 6, 9, 12, 15, 18, 21, 24, 27\}$.

وبحساب هذه الأعداد قياس 19 نجد أن: $B=\{3, 6, 9, 12, 15, 18, 2, 5, 8\}$.

الآن، مجموعة أعداد B التي أكبر من $\frac{19}{2}$ هي $R=\{12,15,18\}$. وبما أن $|R|=3$ فنجد باستخدام تمهيدية جاوس أن $\left(\frac{3}{19}\right)=(-1)^3=-1$ □

لقد بينا في المبرهنة (٨,٦) كيفية حساب $\left(\frac{2}{p}\right)$ حيث p عدداً أولياً فردياً.

والآن نقوم بحساب قيمة $\left(\frac{a}{p}\right)$ في الحالة التي يكون فيها $p\equiv a\equiv 1(\text{mod } 2)$.

تمهيدية (٨,٩)

إذا كان p عدداً أولياً وكان $p\equiv a\equiv 1(\text{mod } 2)$ حيث $(a,p)=1$ فإن:

$$\left(\frac{a}{p}\right)=(-1)^t \quad \text{حيث} \quad t=\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]$$

البرهان

نستخدم الترميز الذي قدمناه في تمهيدية جاوس. نعلم من تمهيدية جاوس أن $\left(\frac{a}{p}\right)=(-1)^n$. ولذا فإننا سنبرهن أن $(-1)^n=(-1)^t$.

باستخدام خوارزمية القسمة لدينا:

$$ka=p\left[\frac{ka}{p}\right]+g_k \quad \text{حيث} \quad g_k=r_i \quad \text{أو} \quad g_k=s_j .$$

الآن :

$$a\sum_{k=1}^{\frac{p-1}{2}}k=\sum_{k=1}^{\frac{p-1}{2}}ka=\sum_{k=1}^{\frac{p-1}{2}}\left(p\left[\frac{ka}{p}\right]+g_k\right)$$

$$=p\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]+\sum_{k=1}^{\frac{p-1}{2}}g_k=pt+\sum_{i=1}^{n}r_i+\sum_{j=1}^{m}s_j$$

ويكون :

$$a\sum_{k=1}^{\frac{p-1}{2}} k = pt + \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j \qquad (1)$$

ولكن من ناحية أخرى لدينا:

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{n} (p - r_i) + \sum_{j=1}^{m} s_j = np - \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j \qquad (2)$$

وبطرح المعادلة (٢) من المعادلة (١) نحصل على :

$$(a-1)\sum_{k=1}^{\frac{p-1}{2}} k = p(t-n) + 2\sum_{i=1}^{n} r_i$$

وبالحساب قياس العدد 2 نجد أن $t - n \equiv 0 \pmod 2$. أي أن $t \equiv n \pmod 2$.

وبهذا يكون $(-1)^t = (-1)^n$ ◆

مثال (٨,٥)

استخدم التمهيدية (٨,٩) لحساب قيمة $\left(\frac{3}{19}\right)$.

الحل

بما أن $p = 19$ فإن $\frac{p-1}{2} = 9$ ولذا نرى أن

$$t = \sum_{k=1}^{9} \left[\frac{3k}{19}\right]$$

$$= \left[\frac{3}{19}\right] + \left[\frac{6}{19}\right] + \left[\frac{9}{19}\right] + \left[\frac{12}{19}\right] + \left[\frac{15}{19}\right] + \left[\frac{18}{19}\right] + \left[\frac{21}{19}\right] + \left[\frac{24}{19}\right] + \left[\frac{27}{19}\right]$$

$$= 0+0+0+0+0+1+1+1 = 3$$

وبالتالي فإن $\left(\frac{3}{19}\right) = (-1)^3 = -1$ □

التمهيدية التالية هي التمهيدية الأخيرة التي نحتاجها لبرهان قانون التعاكس التربيعي.

تمهيدية (٨,١٠)

إذا كان كل من p و q عدداً أولياً فردياً حيث $p \neq q$ فإن:

$$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right] = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$$

البرهان

نعتبر مجموعة النقاط :

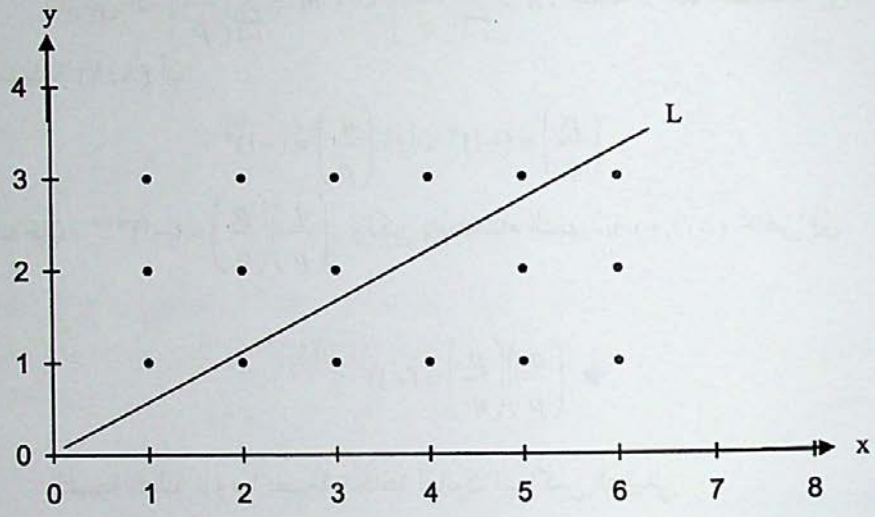
$$S = \left\{(i,j) : 1 \le i \le \frac{p-1}{2}, 1 \le j \le \frac{q-1}{2}, i,j \in \mathbb{Z}\right\}$$

وليكن L هو المستقيم الذي معادلته $py = qx$ (انظر الشكل التوضيحي بعد البرهان للحالة $13y = 7x$). سنبرهن الآن أن جميع نقاط S لا تقع على المستقيم L.

لنفرض أن $(i,j) \in S$ تقع على المستقيم L. عندئذ، $pj = qi$. ومن ثم فإن $p \mid qi$. وبما أن $(p,q) = 1$ فإن $p \mid i$ وهذا مستحيل لأن $1 \le i \le \frac{p-1}{2}$. إذن ، كل من نقاط S إما أنها تقع أعلى المستقيم L أو أسفل المستقيم L. كما أن عددها وهو $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ يساوي مجموع عدد النقاط أعلى المستقيم وعدد النقاط أسفل المستقيم. أي أنه إذا كان m عدد النقاط التي أسفل المستقيم وكان n عدد النقاط التي أعلى المستقيم فإن $m + n = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$.

لنفرض الآن أن $(i,j) \in S$ أسفل المستقيم L. عندئذ، $pj < qi$. ومنه فإن $j < \frac{qi}{p}$. ولذا فإنه لكل i حيث (i,j) أسفل L يكون $1 \le j \le \left[\frac{qi}{p}\right]$. إن هذا يؤدي إلى $m = \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right]$. وبالمثل ، لكل j حيث (i,j) أعلى L يكون $1 \le i \le \left[\frac{pj}{q}\right]$. وهذا بدوره يؤدي إلى أن $n = \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right]$. مما سبق نستنتج أن

◆ $\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right] = m + n = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$



المستقيم $13y = 7x$

لاحظ أن $\frac{q-1}{2} = 3$ ، $\frac{p-1}{2} = 6$ ، $q = 7$ ، $p = 13$.

$m = \sum_{i=1}^{6} \left[\frac{7i}{13}\right] = 9$ ، $n = \sum_{j=1}^{3} \left[\frac{13j}{7}\right] = 9$.

مبرهنة (٨,١١) [قانون التعاكس التربيعي]

إذا كان كل من p و q عدداً أولياً فردياً حيث $p \neq q$ فإن:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

البرهان

لنفرض أن $m=\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{qi}{p}\right]$ وأن $n=\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{pj}{q}\right]$. عندئذ، نجد استناداً إلى التمهيدية (٨,٩) أن:

$$\left(\frac{q}{p}\right)=(-1)^m \quad \text{وأن} \quad \left(\frac{p}{q}\right)=(-1)^n$$

ومنه فإن $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{m+n}$. ولكن باستخدام التمهيدية (٨,١٠) نخلص إلى أن :

$$\blacklozenge \quad \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

النتيجة التالية تزودنا بصيغة مكافئة لقانون التعاكس التربيعي:

نتيجة (٨,١٢) [صيغة مكافئة لقانون التعاكس التربيعي]

إذا كان p و q عددين أوليين فرديين مختلفين فإن:

$$\left(\frac{p}{q}\right)=\begin{cases}\left(\frac{q}{p}\right) & , \ p\equiv 1 \pmod 4 \text{ أو } q\equiv 1 \pmod 4\\ -\left(\frac{q}{p}\right) & , \ p\equiv q\equiv 3 \pmod 4\end{cases}$$

البرهان

لاحظ أن $\frac{p-1}{2}$ زوجي إذا كان $p\equiv 1 \pmod 4$ وأن $\frac{p-1}{2}$ فردي إذا كان $p\equiv 3 \pmod 4$. وبهذا نرى أن $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ زوجي إذا كان $p\equiv 1 \pmod 4$ أو $q\equiv 1 \pmod 4$ وأن $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ فردي إذا كان $p\equiv q\equiv 3 \pmod 4$.

ونستنتج:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\begin{cases}1\ , & q\equiv 1(\text{mod } 4) \text{ أو } q\equiv 1(\text{mod } 4)\\ -1\ , & p\equiv q\equiv 3(\text{mod } 4)\end{cases}$$

وبالتالي فإن:

$$\blacklozenge\ \left(\frac{p}{q}\right)=\begin{cases}\left(\frac{q}{p}\right), & p\equiv 1(\text{mod } 4) \text{ أو } q\equiv 1(\text{mod } 4)\\ -\left(\frac{q}{p}\right), & p\equiv q\equiv 3(\text{mod } 4)\end{cases}$$

نقدم الآن مثالاً يوضح كيفية توظيف قانون التعاكس التربيعي وخواص رمز ليجندر لمعرفة فيما إذا كان العدد a الأولي نسبياً مع العدد الأولي p راسباً تربيعياً قياس p.

مثال (٨,٦)

بين ما إذا كان $83\in Q_{103}$.

الحل

بما أن كل من 83 و 103 عدداً أولياً فإن:

$$\left(\frac{83}{103}\right)=-\left(\frac{103}{83}\right)$$

لأن $83\equiv 103\equiv (\text{mod } 4)$

$$=-\left(\frac{20}{83}\right)$$

لأن $103\equiv 20(\text{mod } 83)$

$$=-\left(\frac{2}{83}\right)^2\left(\frac{5}{83}\right)$$

$$=-\left(\frac{5}{83}\right)$$

$$=-\left(\frac{83}{5}\right)$$

لأن $5\equiv 1(\text{mod } 4)$

$$=-\left(\frac{3}{5}\right)$$

لأن $83\equiv 3(\text{mod } 5)$

$$=-\left(\frac{5}{3}\right)$$ لأن $5\equiv 1(\text{mod } 4)$

$$=-\left(\frac{2}{3}\right)$$ لأن $5\equiv 2(\text{mod } 3)$

$$=(-1)(-1)=1$$ لأن $3\equiv 3(\text{mod } 8)$

وبهذا نستنتج أن $83\in Q_{103}$ □

ملحوظة

يبين لنا قانون التعاكس التربيعي العلاقة بين حلول التطابق $x^2\equiv q(\text{mod } p)$ وحلول التطابق $x^2\equiv p(\text{mod } q)$ حيث $p\neq q$ أوليان فرديان. فإذا كان $p\equiv q\equiv 3(\text{mod } 4)$ فإن واحداً فقط من هذين التطابقين قابلاً للحل. أما إذا كان $p\equiv 1(\text{mod } 4)$ أو $q\equiv 1(\text{mod } 4)$ فإنه إما أن يكون التطابقان قابلان للحل معاً أو يكونا غير قابلين للحل معاً.

إن لقانون التعاكس التربيعي العديد من التطبيقات. إحدى هذه التطبيقات الاختبار التالي الذي قدمه *(Pepin)* لاختبار أولية أعداد فيرما.

مبرهنة (٨,١٣) [اختبار بن]

ليكن $F_n=2^{2^n}+1$ عدد فيرما. عندئذ، F_n أولياً إذا وفقط إذا كان $3^{\frac{F_n-1}{2}}\equiv -1(\text{mod } F_n)$.

البرهان

لنفرض أولاً أن $F_n=2^{2^n}+1$ عدد أولي. باستخدام قانون المقلوب التربيعي. لدينا:

$$\left(\frac{3}{F_n}\right)=\left(\frac{F_n}{3}\right)=\left(\frac{2}{3}\right)=-1$$

وذلك لأن $F_n \equiv 1(\text{mod } 4)$ وأن $F_n \equiv 2(\text{mod } 3)$. ولكن باستخدام معيار أويلر نعلم أن $\left(\frac{3}{F_n}\right) \equiv 3^{\frac{F_n-1}{2}} (\text{mod } F_n)$. وبهذا يكون $3^{\frac{F_n-1}{2}} = -1(\text{mod } F_n)$.

لبرهان العكس، نفرض أن $3^{\frac{F_n-1}{2}} \equiv -1(\text{mod } F_n)$. ولنفرض أن p قاسم أولي للعدد F_n. عندئذ، $3^{F_n-1} = \left(3^{\frac{F_n-1}{2}}\right)^2 \equiv 1(\text{mod } F_n)$. ولذا فإن $3^{F_n-1} \equiv 1(\text{mod } p)$. ومنه فإن $ord_p(3) \mid (F_n - 1) = 2^{2^n}$. أي أن $ord_p(3) = 2^k$ حيث $k \in \mathbb{Z}^+$. وبما أن $3^{\frac{F_n-1}{2}} \equiv -1(\text{mod } F_n)$ فإن $ord_p(3) \nmid \left(\frac{F_n-1}{2}\right) = 2^{2^n-2}$.

وعليه يكون $ord_p(3) = 2^{2^n} = F_n - 1$. ولكن $ord_p(3) \le p - 1$. ولذا فإن $F_n - 1 \le p - 1$. أي أن $F_n \le p$. وبما أن $p \mid F_n$ فنخلص إلى أن $F_n = p$ عدد أولي ◆

ملحوظة

لقد استخدمنا الأساس 3 في اختبار بين لأن 3 راسب غير تربيعي قياس F_n لكل $n \ge 1$.

(٨,٣,١) تمارين محلولة (Solved Exercises)

تمرين (١)

استخدم تمهيدية جاوس لإثبات أن: $\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1(\text{mod } 8) \\ -1, & p \equiv \pm 3(\text{mod } 8) \end{cases}$.

الحل

باستخدام تمهيدية جاوس نعتبر المجموعة :

$$S=\left\{2a:1\le a\le\frac{p-1}{2}\right\}=\{2,4,6,\dots,p-1\}$$

لنفرض الآن أن $S_p=\left\{b\in S:b>\frac{p}{2}\right\}$.

إذا كان $p=8k+1$ فإن $\frac{p}{2}=4k+\frac{1}{2}$ ويكون

$$S_p=\{4k+2,4k+4,\dots,8k\}$$

وإذا كان $p=8k-1$ فإن $\frac{p}{2}=4k-\frac{1}{2}$ ويكون

$$S_p=\{4k,4k+2,\dots,8k-2\}$$

وفي كلتا الحالتين فإن عدد عناصر S_p يساوي $2k$. وبهذا نرى أن $\left(\frac{2}{p}\right)=(-1)^{2k}=1$.

إذا كان $p=8k+3$ فإن $\frac{p}{2}=4k+\frac{3}{2}$. ومن ثم فإن

$$S_p=\{4k+2,4k+4,\dots 8k+2\}$$

أما إذا كان $p=8k+5$ فإن $\frac{p}{2}=4k+\frac{5}{2}$. ومن ثم فإن

$$S_p=\{4k+4,4k+6,\dots 8k+4\}$$

وفي كلتا الحالتين نجد أن عدد عناصر S_p يساوي $2k+1$ وبهذا يكون

$$\left(\frac{2}{p}\right)=(-1)^{2k+1}=-1 \quad \triangle$$

تمرين (٢)

إذا كان $p>3$ عدداً أولياً فردياً حيث $p\equiv 3(\text{mod }4)$ وكان $q=2p+1$ أولياً فأثبت أن $M_p=2^p-1$ عدد مؤلف.

الحل

لاحظ أن $q\equiv 7(\text{mod }8)$. ولذا فإن $\left(\frac{2}{q}\right)=1$. وباستخدام معيار أويلر نجد أن

$$2^p=2^{\frac{q-1}{2}}\equiv 1(\text{mod } q)$$

ولذا فإن $q \mid (2^p - 1)$. وبما أن $p > 3$ فإن $q > 2^p - 1$. وينتج عن ذلك أن $M_p = 2^p - 1$ مؤلف △

تمرين (٣)

إذا كان $p = 4k + 3$ عدداً أولياً حيث $k \geq 1$ وكان N عدد الرواسب غير التربيعية قياس p الواقعة بين العددين 1 و $\frac{p}{2}$ فأثبت أن

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^N \pmod{p}.$$

الحل

لنفرض أن $m = \frac{p-1}{2}$. الآن: $\left(\frac{m!}{p}\right) = \left(\frac{1}{p}\right)\left(\frac{2}{p}\right)\ldots\left(\frac{m}{p}\right) = (-1)^N$.

وباستخدام مبرهنة ويلسن لدينا:

$$\begin{aligned} -1 &\equiv (p-1)! = 1\times 2\times \ldots \times m \times (m+1)\times \ldots \times (p-2)\times (p-1) \\ &\equiv 1\times 2\times \ldots \times m \times (-m)\times \ldots \times (-2)\times (-1) \\ &\equiv (-1)^m (m!)^2 \equiv -(m!)^2 \pmod{p} \end{aligned}$$

ولذا فإن $(m!)^2 \equiv 1 \pmod{p}$. ونرى أن $m! \equiv \pm 1 \pmod{p}$.

إذا كان $m! \equiv 1 \pmod{p}$ فإن $\left(\frac{m!}{p}\right) = \left(\frac{1}{p}\right) = 1$.

وإذا كان $m! \equiv -1 \pmod{p}$ فإن $\left(\frac{m!}{p}\right) = \left(\frac{-1}{p}\right) = -1$. وفي الحالتين يكون $\left(\frac{m!}{p}\right) \equiv m! \pmod{p}$. إذن، $m! \equiv (-1)^N \pmod{p}$ △

تمرين (٤)

ليكن $p = 4k + 1$ عدداً أولياً. إذا كان d قاسماً فردياً للعدد k فأثبت أن $d \in Q_p$.

الحل

لنفرض أن q قاسماً أولياً للعدد d . بما أن $p \equiv 1 \pmod 4$ فإن

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)=\left(\frac{4k+1}{q}\right)=\left(\frac{1}{q}\right) .$$

ولذا فإن $q \in Q_p$ لكل قاسم أولي q للعدد d . وبالتالي فإن $d \in Q_p$ △

تمرين (٥)

إذا كان p عدداً أولياً فردياً فأثبت أن:

$$\left(\frac{3}{p}\right)=\begin{cases}1 & , p \equiv \pm 1 \pmod{12} \\ -1 & , p \equiv \pm 5 \pmod{12}\end{cases} .$$

الحل

لنفرض أولاً أن $p \equiv 1 \pmod 4$. باستخدام قانون التعاكس التربيعي نجد أن:

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)=\begin{cases}1 & , p \equiv 1 \pmod 3 \\ -1 & , p \equiv 2 \pmod 3\end{cases}$$

$$=\begin{cases}1 & , p \equiv 1 \pmod{12} \\ -1 & , p \equiv 5 \pmod{12}\end{cases}$$

لنفرض الآن أن $p \equiv 3 \pmod 4$. عندئذ، باستخدام قانون التعاكس التربيعي نجد أن:

$$\left(\frac{3}{p}\right)=-\left(\frac{p}{3}\right)=\begin{cases}-1 & , p \equiv 1 \pmod 3 \\ 1 & , p \equiv 2 \pmod 3\end{cases}$$

$$=\begin{cases}-1 & , p \equiv 7 \pmod{12} \\ 1 & , p \equiv 11 \pmod{12}\end{cases}$$

وبالتالي فإن:

$$\triangle \quad \left(\frac{3}{p}\right)=\begin{cases}1 & , p \equiv \pm 1 \pmod{12} \\ -1 & , p \equiv \pm 5 \pmod{12}\end{cases}$$

تمرين (٦)

حل التطابق $x^4-6x^2+35\equiv 0 \pmod{37}$.

الحل

بإكمال المربع نجد أن $(2x^2-6)^2\equiv 44\equiv 81 \pmod{37}$. ومنه فإن $2x^2-6\equiv \pm 9 \pmod{37}$.

أي أن $2x^2\equiv 15 \pmod{37}$ أو أن $2x^2\equiv -3 \pmod{37}$.

ونجد أن $x^2\equiv 26 \pmod{37}$ أو $x^2\equiv 17 \pmod{37}$.

الآن: $1=-\left(\frac{2}{11}\right)=-\left(\frac{13}{11}\right)=-\left(\frac{11}{13}\right)=-\left(\frac{37}{13}\right)=-\left(\frac{13}{37}\right)\left(\frac{2}{37}\right)=\left(\frac{26}{37}\right)$.

أيضاً: $-1=\left(\frac{2}{3}\right)=\left(\frac{17}{3}\right)=\left(\frac{3}{17}\right)=\left(\frac{37}{17}\right)=\left(\frac{17}{37}\right)$.

ولذا فإن $x^2\equiv 17 \pmod{37}$ غير قابل للحل. وأما التطابق $x^2\equiv 26\equiv 100 \pmod{37}$ فهو قابل للحل وله الحلان $x\equiv \pm 10 \pmod{37}$ △

تمرين (٧)

إذا كان $n>1$ وكان p قاسماً أولياً لعدد فيرما $F_n=2^{2^n}+1$ فأثبت أن $p=2^{n+2}k+1$.

الحل

بما أن $p\mid F_n$ فإن $2^{2^n}\equiv -1 \pmod{p}$. وبما أن $4\mid 2^n$ فإن التطابق $x^4=-1 \pmod{p}$ قابل للحل. باستخدام المبرهنة (٧,١٦) نجد أن $(-1)^{\frac{p-1}{(4,p-1)}}\equiv 1 \pmod{p}$. ولذا فإن $\frac{p-1}{(4,p-1)}$ زوجي. أي أن $p=8k+1$. وبهذا نرى 2 راسب تربيعي قياس p. ومن ثم فيوجد s حيث $s^2\equiv 2 \pmod{p}$. وبهذا يكون s حل للتطابق $x^{2^{n+2}}\equiv -1 \pmod{p}$. وباستخدام المبرهنة (٧,١٦) مرة

أخرى نجد أن $\frac{p-1}{(2^{n+1},p-1)}$ عدد زوجي. وبالتالي فإن 2^{n+2} يقسم $p-1$. أي أن

$p=2^{n+2}k+1$ حيث $k\in\mathbb{Z}$ $\triangle$

تمارين (٨,٣)

(١) هل $219\in Q_{383}$؟

(٢) هل $147\in Q_{29}$؟

(٣) هل $19\in Q_{457}$؟

(٤) احسب $\left(\frac{713}{1009}\right)$.

(٥) احسب $\left(\frac{105}{1009}\right)$.

(٦) احسب $\left(\frac{196}{1357}\right)$.

(٧) احسب $\left(\frac{1234}{4567}\right)$.

(٨) احسب $\left(\frac{461}{773}\right)$.

(٩) احسب $\left(\frac{3658}{12703}\right)$.

(١٠) احسب $\left(\frac{219}{419}\right)$.

(١١) إذا كان p عدداً أولياً فردياً فأثبت أن $-3\in Q_p$ إذا وفقط إذا كان $p\equiv 1 \pmod 6$.

(١٢) صنف الأعداد الأولية الفردية p التي تحقق $5\in Q_p$.

(١٣) صنف الأعداد الأولية الفردية p التي تحقق $6\in Q_p$.

(١٤) صنف الأعداد الأولية الفردية p التي تحقق $7\in Q_p$.

(١٥) صنف الأعداد الأولية الفردية p التي تحقق $10\in Q_p$.

(١٦) صنف الأعداد الأولية الفردية p التي تحقق $169\in Q_p$.

(١٧) إذا كان p عدداً أولياً فردياً وكان a أصغر راسب غير تربيعي موجب قياس p فأثبت أن a عدد أولي.

(١٨) إذا كان p عدداً أولياً فردياً وكان a أصغر راسب غير تربيعي موجب قياس p فأثبت أن $a<\sqrt{p}+1$.

(١٩) بين أياً من التطابقات التالية قابلاً للحل:

(أ) $x^2 \equiv -2 \pmod{263}$ (ب) $x^2 \equiv 38 \pmod{79}$

(ج) $3x^2 + 6x + 5 \equiv 0 \pmod{89}$ (د) $2x^2 + 5x - 9 \equiv 0 \pmod{101}$

(٢٠) حل التطابق $5x^2 + 9x + 11 \equiv 0 \pmod{13}$.

(٢١) حل كلاً من التطابقين التاليين:

(أ) $x^2 \equiv 46 \pmod{59}$ (ب) $9x^2 - 24x + 13 \equiv 0 \pmod{59}$

(٢٢) إذا كان $p = 4^n + 1$ عدداً أولياً فأثبت أن $3 \notin Q_p$.

(٢٣) إذا كان $n > 3$ فأثبت أن $n! + \ldots + 2! + 1!$ لا يمكن أن يكون مربعاً كاملاً.

(٢٤) أثبت وجود عدد غير منته من الأعداد الأولية التي على الصورة $10k - 1$.

(٢٥) أثبت وجود عدد غير منته من الأعداد الأولية التي على الصورة:

(أ) $8k + 3$ (ب) $8k + 5$ (ج) $8k + 7$

(٢٦) صنف القواسم الأولية الفردية لكل من الأعداد التالية:

(أ) $n^2 + 1$ (ب) $n^2 + 2$ (ج) $n^2 + 3$

(د) $9n^2 - 6n + 4$ (هـ) $n^2 + 4n + 6$ (و) $n^2 - 2n - 4$

(٢٧) إذا كان $p \equiv q \pmod{26}$ حيث p و q عددان أوليان فرديان فأثبت أن $\left(\frac{13}{p}\right) = \left(\frac{13}{q}\right)$.

(٢٨) إذا كان r جذراً بدائياً قياس العدد الأولي $p \equiv 3 \pmod{4}$ فأثبت أن رتبة $-r$ قياس p هي $\frac{p-1}{2}$.

(٢٩) ليكن p و q عددين أوليين فرديين حيث $p = 2q + 1$.

(أ) إذا كان $q \equiv 1 \pmod{4}$ فأثبت أن 2 جذر بدائي قياس p.

(ب) إذا كان $q \equiv 3 \pmod{4}$ فأثبت أن -2 جذر بدائي قياس p.

(٣٠) إذا كان p عدداً أولياً فردياً وكان q قاسماً أولياً للعدد $M_p = 2^p - 1$ فأثبت أن $q \equiv \pm 1 \pmod{8}$.

(٣١) استخدم التمرين (٣٠) لإثبات أن كل من M_{11} ، M_{23} و M_{251} عدداً مؤلفاً.

(٣٢) استخدم اختبار بين لإثبات أن كل من أعداد فيرما F_n ، $1 \le n \le 4$ أولياً.

(٣٣) استخدم اختبار بين لإثبات أن 3 جذر بدائي قياس أي عدد فيرما أولي.

(٨,٤) الجذور التربيعية قياس عدد أولي
Square Roots Module A Prime

إن استخدام رمز ليجندر يبين لنا فيما إذا كان التطابق $x^2 \equiv a \pmod p$ قابلاً للحل حيث p عدد أولي فردي و $(a,p)=1$. فإذا كان $a \in Q_p$ فإن التطابق قابل للحل، وفي هذه الحالة يوجد له حلان غير متطابقين قياس p، يسميان، الجذران التربيعيان للعدد a قياس p. لنفرض إذن أن $a \in Q_p$.

إذا كان $p \equiv 3 \pmod 4$ فقد وجدنا في التمرين (٣) من التمارين المحلولة (٨,١,١) أن الجذران التربيعيان للعدد a قياس p هما $\pm a^{(p+1)/4} \pmod p$.

أما إذا كان $p \equiv 1 \pmod 4$ فتحتاج مسألة إيجاد الجذران التربيعيان للعدد a قياس p لبذل مزيد من الجهد، وفي هذا البند نقدم خوارزمية برهنها الرياضي شانكس *(Shanks)* لحساب الجذران التربيعيان للعدد a قياس عدد أولي فردي p.

خوارزمية شانكس [*Shanks Algorithm*]

ليكن p عدداً أولياً فردياً وليكن $a \in Q_p$ حيث $0 < a < p$. الخطوات التالية تجد لنا الجذران التربيعيان للعدد a قياس p (حلا التطابق $x^2 \equiv a \pmod p$):

(١) استخدم خوارزمية القسمة لكتابة $p-1 = 2^k m$ حيث $k \ge 1$ ، m عدد فردي.

(٢) استخدم قانون التعاكس التربيعي لإيجاد راسب غير تربيعي q قياس العدد p.

(٣) استخدم خوارزمية التربيع لحساب $b \equiv q^m \pmod p$.

(٤) ضع $r \equiv a^{\frac{m+1}{2}} \pmod p$.

(٥) ضع $n \equiv a^m \pmod p$.

(٦) استخدم خوارزمية التربيع لإيجاد أصغر عدد $j \geq 0$ يحقق $n^{2^j} \equiv 1 \pmod p$.

(٧) إذا كان $j = 0$ توقف ويكون الحلان هما $x \equiv \pm r \equiv \pm a^{\frac{m+1}{2}} \pmod p$.

(٨) إذا كان $j > 0$ ضع $c \equiv b^{2^{k-j-1}} \pmod p$ ثم استبدل r بالعدد rc واستبدل n بالعدد nc^2 ونفذ الخطوة (٦).

ملحوظات

نبرر الآن صواب خوارزمية شانكس:

(١) لاحظ أولاً أن : $r^2 \equiv a^{m+1} \equiv aa^m \equiv an \pmod p$. فإذا كان $n \equiv 1 \pmod p$ فإن $r^2 \equiv a \pmod p$ ويكون الحلان هما:

$$x \equiv \pm r \equiv \pm a^{\frac{m+1}{2}} \pmod p$$

أما إذا كان $n \not\equiv 1 \pmod p$ فبملاحظة أن $a \in Q_p$ واستخدام معيار أويلر نرى:

$$n^{2^{k-1}} \equiv (a^m)^{2^{k-1}} \equiv a^{2^{k-1}m} \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1 \pmod p$$

ولذا فإن $ord_p(n) \mid 2^{k-1}$. أي أنه يوجد j ، $1 \leq j \leq k-1$ حيث $ord_p(n) = 2^j$. وعليه يكون باستطاعتنا إيجاد j يحقق الخطوة (٦).

(٢) لاحظ أيضاً أن رتبة $t = b^{2^{k-j}}$ تساوي 2^j . لأن:

$$t^{2^{j-1}} \equiv b^{2^{k-1}} \equiv q^{2^{k-1}m} \equiv q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \equiv -1 \pmod p$$

وذلك لأن q راسب غير تربيعي قياس p . كما أن:

$$t^{2^j} \equiv b^{2^k} \equiv q^{2^k m} \equiv q^{p-1} \equiv 1 \pmod p$$

وذلك بتوظيف مبرهنة فيرما الصغرى . وبالتالي فإن $ord_p(t) = 2^j$.

(٣) لاحظ أن $t \equiv c^2 \pmod p$ حيث $c \equiv b^{2^{k-j-1}} \pmod p$.

(٤) لاحظ أيضاً أن j يقل بمقدار 1 على الأقل في كل خطوة من خطوات تنفيذ الخوارزمية. وعليه فإننا نحتاج إلى $k-1$ خطوة على الأكثر للحصول على الجذرين.

(٥) إذا كان $p \equiv 3 \pmod 4$ فإن $k=1$ وإن $m=\frac{1}{2}(p-1)$. ومنه $\frac{m+1}{2}=\frac{p+1}{4}$. وفي هذه الحالة يكون $j=0$ ونحصل على الجذرين

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod p .$$

مثال (٨,٧)

استخدم خوارزمية شانكس لحل التطابق $x^2 \equiv 38 \pmod{79}$.

الحل

بما أن $\left(\frac{38}{79}\right)=\left(\frac{2}{79}\right)\left(\frac{19}{79}\right)=-\left(\frac{79}{19}\right)=-\left(\frac{3}{79}\right)=1$ فإن $38 \in Q_{79}$. وبما أن $p \equiv 3 \pmod 4$ فنجد استناداً إلى الملحوظة (٥) المقدمة أعلاه أن:

$$\square \quad x \equiv \pm a^{\frac{p+1}{4}} \equiv \pm 38^{20} \equiv 65 \pmod{79}$$

مثال (٨,٨)

استخدم خوارزمية شانكس لحل التطابق $x^2 \equiv 33 \pmod{37}$.

الحل

بما أن $\left(\frac{33}{37}\right)=\left(\frac{-4}{37}\right)=\left(\frac{-1}{37}\right)\left(\frac{4}{37}\right)=\left(\frac{-1}{37}\right)=1$ فإن $33 \in Q_{37}$. الآن : $p-1=37-1=2^2 \times 9$. ولذا فإن $a=33$ ، $k=2$ ، $m=9$. وبأخذ $q=2 \notin Q_{37}$ نجد أن:

$$b \equiv q^m \equiv 2^9 \equiv 31 \pmod{37}$$
$$r \equiv a^{\frac{m+1}{2}} \equiv 33^5 \equiv 12 \pmod{37}$$
$$n \equiv a^m \equiv 33^9 \equiv 1 \pmod{37}$$

ولذا فإن $j=0$ ونتوقف ويكون $x \equiv \pm a^{\frac{m+1}{2}} \equiv \pm 12 \pmod{37}$ □

مثال (٨,٩)

استخدم خوارزمية شانكس لحل التطابق:

$$x^2 \equiv 14 \pmod{113}$$

الحل

بما أن $\left(\frac{14}{113}\right)=\left(\frac{2}{113}\right)\left(\frac{7}{113}\right)=\left(\frac{113}{7}\right)=\left(\frac{1}{7}\right)=1$ فإن $14 \in Q_{113}$.

الآن : $p-1=112=2^4\times 7$. ولذا فإن $a=14$ ، $k=4$ ، $m=7$. وبأخذ $q=3 \notin Q_{113}$ نجد أن:

$$b \equiv q^m \equiv 3^7 \equiv 40 \pmod{113}$$

$$r \equiv a^{\frac{m+1}{2}} \equiv 14^4 \equiv 109 \pmod{113}$$

$$n \equiv a^m \equiv 14^7 \equiv 98 \pmod{m}$$

$$n^2 \equiv 98^2 \equiv 112 \equiv -1 \pmod{113}$$

$$n^4 \equiv (-1)^2 \equiv 1 \pmod{113}$$

إذن، $j=2$. ننفذ الآن الخطوة (٨) من خوارزمية شانكس فنجد:

$$c \equiv b^{2^{k-j-1}} \equiv 40^2 \equiv 18$$

$$c^2 \equiv 18^2 \equiv 98$$

$$rc \equiv 109\times 18 \equiv 41 \rightarrow r$$

$$nc^2 \equiv 98\times 98 \equiv 112 \equiv -1 \rightarrow n$$

الآن ننفذ الخطوة (٦) من الخوارزمية:

$$n \equiv -1$$

$$n^2 \equiv 1$$

إذن، $j=1$ ونعود إلى الخطوة (٨) :

$$c \equiv b^{2^{k-j-1}} \equiv b^4 \equiv 40^4 \equiv 98$$

$$c^2 \equiv 98^2 \equiv -1$$

$$rc \equiv 41 \times 98 \equiv 63 \to r$$

$$nc^2 \equiv (-1)(-1) \equiv 1 \to n$$

إذن، $j = 0$ ونتوقف ليكون:

□ $x \equiv \pm 63 \pmod{113}$

تمارين (٨,٤)

جد حلول كل من التطابقات التالية (إن وجدت) :

(١) $x^2 \equiv 6 \pmod{43}$.
(٢) $x^2 \equiv 2 \pmod{97}$.
(٣) $x^2 \equiv 8 \pmod{41}$.
(٤) $x^2 \equiv 30 \pmod{311}$.
(٥) $x^2 \equiv 263 \pmod{331}$.
(٦) $x^2 \equiv 41 \pmod{103}$.
(٧) $x^2 \equiv 461 \pmod{773}$.
(٨) $x^2 \equiv 6 \pmod{97}$.
(٩) $x^2 \equiv 87 \pmod{397}$.
(١٠) $x^2 \equiv 39 \pmod{401}$.

(٨,٥) الجذور التربيعية قياس عدد مؤلف
Square Roots Modulo A composite

لقد درسنا في البند الرابع من هذا الفصل كيفية إيجاد الجذور التربيعية لراسب تربيعي قياس عدد أولي p. في هذا البند سنبين كيفية ايجاد الجذور التربيعية قياس عدد مؤلف.

بينا في الفصل الثالث (انظر التمرين (٢) من التمارين المحلولة (٣,٧,١)) أنه إذا كان a عدداً فردياً فإن:

(١) التطابق $x^2 \equiv a \pmod{2}$ قابل للحل وله حل وحيد.

(٢) التطابق $x^2 \equiv a \pmod 4$ قابل للحل إذا وفقط إذا كان $a \equiv 1 \pmod 4$. وفي حالة وجود حل فإن له حلان غير متطابقين.

(٣) التطابق $x^2 \equiv a \pmod{2^k}$ حيث $k \geq 3$ قابل للحل إذا وفقط إذا كان $a \equiv 1 \pmod 8$. وفي حالة وجود حل له فإن له أربعة حلول غير متطابقة هي $\pm x_0, \pm x_0 + 2^{k-1}$ حيث x_0 أحد الحلول.

ندرس الآن التطابق $x^2 \equiv a \pmod{p^k}$ حيث p عدد أولي فردي.

مبرهنة (٨,١٤)

ليكن p عدداً أولياً فردياً وليكن $(a,p)=1$ و $k \in \mathbb{Z}^+$. عندئذ:

(١) إذا كان $a \notin Q_p$ فإن $x^2 \equiv a \pmod{p^k}$ غير قابل للحل.

(٢) إذا كان $a \in Q_p$ فيوجد حلان فقط غير متطابقين للتطابق $x^2 \equiv a \pmod{p^k}$ وهما على الصورة $x \equiv \pm b_k \pmod{p^k}$ حيث $(b_k, p)=1$.

البرهان

(١) بما أن $a \notin Q_p$ فإن التطابق $x^2 \equiv a \pmod p$ غير قابل للحل ومن ثم فإنه لا يمكن أن يكون التطابق $x^2 \equiv a \pmod{p^k}$ قابل للحل.

(٢) لنفرض أن $a \in Q_p$. نستخدم الاستقراء الرياضي على k . من الواضح أن للتطابق $x^2 \equiv a \pmod p$ حلان هما $x \equiv \pm b_1 \pmod p$ حيث $(b_1, p)=1$ وذلك لأن $a \in Q_p$. إذن العبارة صحيحة عندما $k=1$.

لنفرض الآن أن العبارة صحيحة عندما $k = n-1$. أي أن للتطابق $x^2 \equiv a \pmod{p^{n-1}}$ حلان هما $x \equiv \pm b_{n-1} \pmod{p^{n-1}}$ حيث $(b_{n-1}, p)=1$.

ولنفرض أن $f(x) = x^2 - a$. عندئذ ، $f'(x) = 2x$. ولذا باستخدام المبرهنة (٣,٥) نحصل على حلول التطابق $x^2 \equiv a \pmod{p^n}$ بحل التطابق الخطي:

$$sf'(b_{n-1}) \equiv -\frac{f(b_{n-1})}{p^{n-1}} \pmod p$$

للمجهول s . أي حل التطابق الخطي:

$$2b_{n-1}s \equiv -\frac{(b_{n-1}^2 - a)}{p^{n-1}} \pmod{p}$$

وبما أن $(b_{n-1}, p) = 1$ فللتطابق حل وحيد هـو $s \equiv s_n \pmod{p}$. الآن، بوضع $b_n = b_{n-1} + s_n p^{n-1}$ نجد أن حلا التطابق $x^2 \equiv a \pmod{p^n}$ هما:

$$x \equiv \pm b_n \pmod{p^n}.$$

وأخيراً $(b_n, p) = 1$ لأن $(b_{n-1}, p) = 1$ ◆

مثال (٨,١٠)

حل التطابق $x^2 \equiv 3 \pmod{13^3}$.

الحل

بما أن $\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$ فإن $3 \in Q_{13}$ ومن ثم فإن للتطابق $x^2 \equiv 3 \pmod{13}$ حلان هما: $x \equiv \pm 9 \pmod{13}$.

إذن، $b_1 = 9$. استناداً إلى المبرهنة (٨,١٤) نجد أن حلي التطابق $x^2 \equiv 3 \pmod{13^2}$ هما $x \equiv \pm b_2 \pmod{13^2}$.

حيث $b_2 \equiv b_1 + 13s_1 \pmod{13^2}$ و s_1 هو حل التطابق الخطي:

$2b_1 s_1 \equiv -\frac{(b_1^2 - 3)}{13} \pmod{13}$. أي $18s_1 \equiv -6 \pmod{13}$.

ومن ثم فإن $s_1 \equiv 4 \pmod{13}$ ويكون $b_2 \equiv 9 + 13 \times 4 \equiv 16 \pmod{13^2}$.

الآن، للتطابق $x^2 \equiv 3 \pmod{13^3}$ حلان هما: $x \equiv \pm b_3 \pmod{13^2}$ حيث $b_3 \equiv b_2 + 169s_2 \pmod{13^3}$ وحيث s_2 هو حل التطابق الخطي:

$2b_2 s_2 \equiv -\frac{(b_2^2 - 3)}{13^2} \pmod{13}$. أي التطابق $122s_2 \equiv -22 \pmod{13}$. أي التطابق $5s_2 \equiv 4 \pmod{13}$. من هذا نرى أن $s_2 \equiv 6 \pmod{13}$. ومن ثم فإن $b_3 \equiv 61 + 169 \times 6 \equiv 1075 \pmod{13^3}$. ويكون حلا التطابق هما:

□ $x \equiv \pm 1075 \pmod{13^3}$

ننتقل الآن إلى إيجاد الجذور التربيعية (الحلول) للتطـــابق $x^2 \equiv a \pmod m$ حيث m عدد فردي.

بكتابة $m = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ حيث p_i أعداد أولية فردية مختلفة نجـــد أن التطابق

$$x^2 \equiv a \pmod m \qquad (١)$$

قابل للحل إذا فقط إذا كان النظام :

$$\begin{aligned} x^2 &\equiv a \pmod{p_1^{k_1}} \\ x^2 &\equiv a \pmod{p_2^{k_2}} \\ &\vdots \\ x^2 &\equiv a \pmod{p_t^{k_t}} \end{aligned} \qquad (٢)$$

قابلاً للحل.

لنفرض الآن أن $a \in Q_{p_i}$ لكل i . عندئذ $x^2 \equiv a \pmod{p_i^{k_i}}$ قابل للحل لكل i . ليكن $x \equiv c_i \pmod{p_i^{k_i}}$ حل للتطابق $x^2 \equiv a \pmod{p_i^{k_i}}$. عندئـــذ، استناداً إلى مبرهنة الباقي الصينية يوجد حل وحيد قياس m للنظام:

$$\begin{aligned} x &\equiv c_1 \pmod{p_1^{k_1}} \\ x &\equiv c_2 \pmod{p_2^{k_2}} \\ &\vdots \\ x &\equiv c_t \pmod{p_t^{k_t}} \end{aligned}$$

وأخيراً لاحظ أن لكل من تطابقات النظام (٢) حلين، لذا فإن عدد مجموعات قيم c_i يساوي 2^t ، ومن ثم نحصل على حلول عددها 2^t للنظام (٣) وهي عدد حلـــول التطابق (١) .

مثال (٨,١١)

جد جميع حلول التطابق $x^2 \equiv 5 \pmod{2299}$.

الحل

التطابق $x^2 \equiv 5 \pmod{2299} \equiv 5 \pmod{11^2 \times 19}$ يكافيء النظام:

$$x^2 \equiv 5 (\mathrm{mod}\ 19)$$

$$x^2 \equiv 5 (\mathrm{mod}\ 121)$$

وبما أن $\left(\frac{5}{19}\right)=\left(\frac{5}{11}\right)=1$ فإن $5 \in Q_{19}$ و $5 \in Q_{11}$ ومن ثم فإن كل من التطابقين قابلاً للحل.

لحل التطابق $x^2 \equiv 5 (\mathrm{mod}\ 19)$ لاحظ أن $19 \equiv 3 (\mathrm{mod}\ 4)$. ولذا فإن حلا التطابق $x^2 \equiv 5 (\mathrm{mod}\ 19)$ هما:

$$x \equiv \pm 5^{\frac{19+1}{4}} \equiv \pm 5^5 \equiv \pm 9 (\mathrm{mod}\ 19)$$

كما أن $11 \equiv 3 (\mathrm{mod}\ 4)$ ونرى أن حلا التطابق $x^2 \equiv 5 (\mathrm{mod}\ 11)$ هما:

$$x \equiv \pm 5^{\frac{11+1}{4}} \equiv 5^3 \equiv \pm 4 (\mathrm{mod}\ 11)$$

ولذا فإن $b_1 = 4$ ويكون حلا التطابق $x^2 \equiv 5 (\mathrm{mod}\ 11^2)$ هما:

$$x \equiv \pm b_2 \equiv \pm (b_1 + 11 s_1) (\mathrm{mod}\ 11^2)$$

حيث s_1 هو حل التطابق الخطي:

$$2 b_1 s_1 \equiv -\frac{(b_1^2 - 5)}{11} (\mathrm{mod}\ 11)$$

أي: $8 s_1 \equiv -1 (\mathrm{mod}\ 11)$. ومنه فإن $s_1 \equiv 4 (\mathrm{mod}\ 11)$. وبالتالي فإن حلا التطابق $x^2 \equiv 5 (\mathrm{mod}\ 11^2)$ هما:

$$x \equiv \pm (4 + 11 \times 4) \equiv \pm 48 (\mathrm{mod}\ 11^2)$$

الآن، لدينا أنظمة التطابقات الخطية التالية:

(١) $x \equiv 9 (\mathrm{mod}\ 19)$ $\quad$ $x \equiv 48 (\mathrm{mod}\ 121)$

(٢) $x \equiv 9 (\mathrm{mod}\ 19)$ $\quad$ $x \equiv -48 (\mathrm{mod}\ 121)$

(٣) $x \equiv -9 (\mathrm{mod}\ 19)$ $\quad$ $x \equiv 48 (\mathrm{mod}\ 121)$

(٤) $x \equiv -9 (\mathrm{mod}\ 19)$ $\quad$ $x \equiv -48 (\mathrm{mod}\ 121)$

بتوظيف مبرهنة الباقي الصينية لحل كل من أنظمة التطابقات الخطية نحصل على الجذور التربيعية للعدد 5 قياس 2299 وهي:

□ ±48 ، ±1016

(٨,٥,١) تمارين محلولة (Solved Exercises)

تمرين (١)

إذا كان $n=pq$ حيث p و q عددان أوليان فرديان مختلفان وكان $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=1$ فأثبت أن الجذور التربيعية للعدد a قياس n هي:

$$x_1 \equiv qy_1x_p + py_2x_q \pmod{n}$$
$$x_2 \equiv qy_1x_p + py_2(-x_q) \pmod{n}$$
$$x_3 \equiv qy_1(-x_p) + py_2x_q \pmod{n}$$
$$x_4 \equiv qy_1(-x_p) + py_2(-x_q) \pmod{n}$$

حيث $\pm x_p$ هما الجذران التربيعيان للعدد a قياس p ، $\pm x_q$ هما الجذران التربيعيان للعدد a قياس q ، $qy_1 \equiv 1 \pmod{p}$ ، $py_2 \equiv 1 \pmod{q}$.

الحل

بما أن $x \equiv \pm x_p \pmod{p}$ هما حلا التطابق $x^2 \equiv a \pmod{p}$ وأن $x \equiv \pm x_q \pmod{q}$ هما حلا التطابق $x^2 \equiv a \pmod{q}$ فإننا نحصل على الأنظمة الخطية الأربعة التالية:

(١) $x \equiv x_p \pmod{p}$ ، $x \equiv x_q \pmod{q}$

(٢) $x \equiv x_p \pmod{p}$ ، $x \equiv -x_q \pmod{q}$

(٣) $x \equiv -x_p \pmod{p}$ ، $x \equiv x_q \pmod{q}$

(٤) $x \equiv -x_p \pmod{p}$ ، $x \equiv -x_q \pmod{q}$

وبحل كل هذه الأنظمة باستخدام مبرهنة الباقي الصينية نحصل على الحلول $\triangle$ x_1, x_2, x_3, x_4

تمرين (٢)

باستخدام ترميز التمرين (١) أثبت أن $x_1+x_4=x_2+x_3=n$.

الحل

من التمرين (١) لدينا : $x_1+x_4\equiv 0(\text{mod } n)$.

وبما أن $0<x_1+x_4<2n$ فنستنتج أن أن $x_1+x_4=n$. وبالمثل $x_2+x_3=n$ △

تمرين (٣)

باستخدام ترميز التمرين (١) أثبت أن :

$$(x_1+x_2,n)=(x_3+x_4,n)=q$$
$$(x_1+x_3,n)=(x_2+x_4,n)=p$$

الحل

باستخدام التمرين (١) لدينا:

$$x_1+x_2\equiv 2qy_1x_p(\text{mod } n)\equiv 2qy_1x_p(\text{mod } p)$$
$$\equiv 2x_p(\text{mod } p)\not\equiv 0(\text{mod } p)$$

أيضاً $x_1+x_2\equiv 0(\text{mod } q)$. أي أن x_1+x_2 مضاعف غير صفري للعدد q ولكنه ليس مضاعفاً للعدد p . ولهذا نرى أن $(x_1+x_2,n)=q$. والحالات الأخرى مشابهة △

تمارين (٥,٨)

جد جميع حلول التطابقات التالية (إن وجدت) :

(١) $x^2\equiv 2(\text{mod } 7\times 17)$ (٢) $x^2\equiv 3(\text{mod } 55)$

(٣) $x^2\equiv 3(\text{mod } 11^2\times 13^3)$ (٤) $x^2\equiv 860(\text{mod } 103\times 107)$

(٥) $x^2\equiv 1(\text{mod } 15)$ (٦) $x^2\equiv 3(\text{mod } 143)$

(٧) $x^2 \equiv 207 (\mathrm{mod}\ 1001)$ (٨) $x^2 \equiv 7 (\mathrm{mod}\ 33)$

(٩) $x^2 \equiv 7 (\mathrm{mod}\ 57)$ (١٠) $x^2 \equiv 1 (\mathrm{mod}\ 56)$

(٨,٦) رمز جاكوبي
Jacobi Symbol

إذا كان $m = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ هو تحليل m إلى قوى عوامله الأولية فلقد بينا في البند السابق أن التطابق $x^2 \equiv a (\mathrm{mod}\ m)$ قابل للحل إذا وفقط إذا كان $\left(\frac{a}{p_i}\right) = 1$ لكل i ، $1 \le i \le t$. سنقدم الآن رمز جاكوبي الذي يمكننا من حساب $\left(\frac{a}{m}\right)$ دون أن يشترط بأن يكون m عدداً أولياً ودون الحاجة إلى تحليل a إلى عوامله الأولية.

تعريف (٨,٣)

ليكن m عدداً فردياً وليكن $m = p_1 p_2 p_3 \dots p_t$ هو تحليل m إلى عوامله الأولية (ليس بالضرورة أن تكون الأعداد الأولية p_i مختلفة) وليكن $a \in \mathbb{Z}$ حيث $(a,m) = 1$. يعرف رمز جاكوبي $\left(\frac{a}{m}\right)$ على النحو التالي:

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_t}\right).$$

ملحوظات

(١) لاحظ أن $\left(\frac{a}{m}\right) = \pm 1$.

(٢) لاحظ أيضاً أن $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{k_1}\left(\frac{a}{p_2}\right)^{k_2} \dots \left(\frac{a}{p_t}\right)^{k_t}$

حيث $m = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ هو تحليل m إلى قوى عوامل أولية مختلفة.

(٣) لقد بينا أن التطابق $x^2 \equiv a \pmod{p}$ قابل للحل إذا وفقط إذا كان $\left(\frac{a}{p}\right) = 1$ حيث p عدد أولي. إن ذلك ليس صحيحاً في حالة رمز جاكوبي. على سبيل المثال ، التطابق $x^2 \equiv -1 \pmod{21}$ غير قابل للحل، على الرغم من أن $\left(\frac{-1}{21}\right) = 1$ كما سنرى بعد قليل. ولكن ما يبقى صحيحاً هو أنه إذا كان $\left(\frac{a}{m}\right) = -1$ فإن التطابق $x^2 \equiv a \pmod{m}$ غير قابل للحل وذلك لأن أحد رموز ليجندر $\left(\frac{a}{p_i}\right) = -1$.

(٤) كان من الممكن تعريف رمز جاكوبي على النحو التالي: $\left(\frac{a}{m}\right) = 1$ إذا وفقط إذا كان التطابق $x^2 \equiv a \pmod{m}$ قابلاً للحل، ولكننا في هذه الحالة نخسر قانون التعاكس التربيعي لرمز جاكوبي وهو ثمن باهظ.

(٥) سنبين فيما يلي أن رمز جاكوبي يتمتع بمعظم خواص رمز ليجندر بما في ذلك قانون التعاكس التربيعي.

مبرهنة (٨,١٥)

ليكن كل من $m > 1$ و $n > 1$ عدداً فردياً وليكن $a, b \in \mathbb{Z}$ حيث $(ab, mn) = 1$. عندئذ :

(١) إذا كان $a \equiv b \pmod{m}$ فإن $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.

(٢) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$

(٣) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

(٤) $\left(\frac{a^2}{m}\right) = \left(\frac{a}{m^2}\right) = 1$

(٥) $\left(\frac{1}{m}\right) = 1$

البرهان

لنفـــرض أن $m = p_1 p_2 \dots p_t$ ، $n = q_1 q_2 \dots q_s$ هـمـــا تحلـــيلا m و n إلى عواملهما الأولية. لاحظ أن $(ab, mn) = 1$ يؤدي إلى أن :

$$(a,m) = (a,n) = (b,m) = (b,n) = 1$$

(١) إذا كان $a \equiv b \pmod{m}$ فإن $a \equiv b \pmod{p_i}$ لكل i، $1 \le i \le t$. ولذا فإن $\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$. الآن :

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_t}\right) = \left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\dots\left(\frac{b}{p_t}\right) = \left(\frac{b}{m}\right).$$

(٢)
$$\begin{aligned}\left(\frac{ab}{m}\right) &= \left(\frac{ab}{p_1}\right)\left(\frac{ab}{p_2}\right)\dots\left(\frac{ab}{p_t}\right)\\ &= \left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{b}{p_2}\right)\dots\left(\frac{a}{p_t}\right)\left(\frac{b}{p_t}\right)\\ &= \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_t}\right)\left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\dots\left(\frac{b}{p_t}\right)\\ &= \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)\end{aligned}$$

حيث استخدمنا المبرهنة (٨,٤) .

(٣)
$$\begin{aligned}\left(\frac{a}{mn}\right) &= \left(\frac{a}{p_1 p_2 \dots p_t q_1 q_2 \dots q_s}\right)\\ &= \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_t}\right)\left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right)\dots\left(\frac{a}{q_s}\right)\\ &= \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)\end{aligned}$$

(٤)
$$\left(\frac{a^2}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{m}\right) = \left(\frac{a}{m}\right)^2 = 1$$

وذلك باستخدام الفقرة (٢). وباستخدام الفقرة (٣) نجد أن :

$$\left(\frac{a^2}{m}\right)=\left(\frac{a}{m^2}\right)=1 \text{، إذن } \left(\frac{a}{m^2}\right)=\left(\frac{a}{m}\right)\left(\frac{a}{m}\right)=\left(\frac{a}{m}\right)^2=1 .$$

(٥) يتبع مباشرة من الفقرة (٣) والمبرهنة (٨,٤) ◆

مبرهنة (٨,١٦)

ليكن $m>1$ عدداً فردياً وليكن $m=p_1^{k_1}p_2^{k_2}\dots p_t^{k_t}$ تحليل m إلى قوى عوامله الأولية المختلفة. عندئذ :

$$m-1\equiv\sum_{i=1}^{t}k_i(p_i-1)\pmod 4 \qquad (١)$$

$$\frac{m-1}{2}\equiv\sum_{i=1}^{t}k_i\left(\frac{p_i-1}{2}\right)\pmod 2 \qquad (٢)$$

$$m^2-1\equiv\sum_{i=1}^{t}k_i(p_i^2-1)\pmod{64} \qquad (٣)$$

$$\frac{m^2-1}{8}\equiv\sum_{i=1}^{t}k_i\left(\frac{p_i^2-1}{8}\right)\pmod 8 \qquad (٤)$$

البرهان

(١) باستخدام الاستقراء الرياضي على t.

لاحظ أولاً أن p_i-1 عدد زوجي ومن ثم فإن $(p_i-1)^k\equiv 0\pmod 4$ لكل $k\geq 2$. أيضاً $(p_i-1)(p_j-1)\equiv 0\pmod 4$ لكل $i\neq j$.

لنفرض الآن أن $t=1$. عندئذ :

$$\begin{aligned} m=p_1^{k_1}&=[1+(p_1-1)]^{k_1}\\ &=1+k_1(p_1-1)+\binom{k_1}{2}(p_1-1)^2+\dots+(p_1-1)^{k_1}\\ &\equiv 1+k_1(p_1-1)\pmod 4 \end{aligned}$$

ولذا فإن العبارة صحيحة عندما $t=1$.

لنفرض الآن أن العبارة صحيحة عندما $r=t-1$. عندئذ:

$$m = p_1^{k_1} p_2^{k_2} \dots p_{t-1}^{k_{t-1}} p_t^{k_t}$$
$$\equiv \left[1+\sum_{i=1}^{t-1} k_i (p_i - 1)\right]\left[1+k_t (p_t - 1)\right] (\text{mod } 4)$$

وذلك باستخدام فرضية الاستقراء عندما $t=1$ و $r=t-1$. وبما أن $(p_i-1)(p_t-1) \equiv 0 (\text{mod } 4)$ لكل i فإننا نجد :

$$m \equiv 1+\sum_{i=1}^{t} k_i (p_i - 1) (\text{mod } 4)$$

ومن ثم فإن العبارة صحيحة عندما $r=t$.

(٢) برهان هذه الفقرة يتبع مباشرة من الفقرة (١) .

(٣) لاحظ أولاً أن $m^2 = \left(p_1^2\right)^{k_1} \left(p_2^2\right)^{k_2} \dots \left(p_t^2\right)^{k_t}$. وبما أن p_i عدد فردي فإن $p_i^2 \equiv 1 (\text{mod } 8)$. نستخدم الآن الاستقراء الرياضي على t.

عندما $t=1$ لدينا:

$$m^2 = \left(p_1^2\right)^{k_1} \left[1+\left(p_1^2-1\right)\right]^{k_1}$$
$$= 1+k_1\left(p_1^2-1\right)+\binom{k_1}{2}\left(p_1^2-1\right)^2 + \dots + \left(p_1^2-1\right)^{k_1}$$
$$\equiv 1+k_1\left(p_1^2-1\right) (\text{mod } 64)$$

ومنه فإن العبارة صحيحة عندما $t=1$.

لنفرض الآن أن العبارة صحيحة عندما $r=t-1$. عندئذ :

$$m^2 = \left(p_1^2\right)^{k_1} \left(p_2^2\right)^{k_2} \dots \left(p_{t-1}^2\right)^{k_{t-1}} \left(p_t^2\right)^{k_t}$$
$$\equiv \left[1+\sum_{i=1}^{t-1} k_i \left(p_i^2-1\right)\right]\left[1+k_t\left(p_t^2-1\right)\right]$$
$$\equiv 1+\sum_{i=1}^{t} k_i \left(p_i^2-1\right) (\text{mod } 64)$$

وذلك باستخدام صواب العبارة عند $t=1$ وعند $r=t-1$. وبالتالي نتوصل إلى أن العبارة صحيحة عندما $r=t$.

(٤) يتبع مباشرة من الفقرة (٣) ◆

مبرهنة (٨,١٧)

إذا كان $m>1$ عدداً فردياً فإن:

(١) $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$ (٢) $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$.

البرهان

لنفرض أن $m=p_1^{k_1}p_2^{k_2}\dots p_t^{k_t}$ هو تحليل m إلى عوامله الأولية المختلفة.

(١) استناداً إلى المبرهنة (٨,٥) نعلم أن :

$\left(\frac{-1}{p_i}\right)=(-1)^{\frac{p_i-1}{2}}$ لكل i ، $1\le i\le t$. وبهذا نرى أن

$$\left(\frac{-1}{m}\right)=\left(\frac{-1}{p_1}\right)^{k_1}\left(\frac{-1}{p_2}\right)^{k_2}\dots\left(\frac{-1}{p_t}\right)^{k_t}$$

$$=(-1)^{k_1\frac{(p_1-1)}{2}+k_2\left(\frac{p_2-1}{2}\right)+\dots+k_t\left(\frac{p_t-1}{2}\right)}\equiv(-1)^{\frac{m-1}{2}}\pmod 2$$

وذلك استناداً إلى الفقرة (٢) من المبرهنة (٨,١٦). ونستنتج أن

$\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$.

(٢) استناداً إلى المبرهنة (٨,٦) نعلم أن $\left(\frac{2}{p_i}\right)=(-1)^{\left(\frac{p_i^2-1}{8}\right)}$ لكل i ، $1\le i\le t$

وعليه فإن :

$$\left(\frac{2}{m}\right)=\left(\frac{2}{p_1}\right)^{k_1}\left(\frac{2}{p_2}\right)^{k_2}\dots\left(\frac{2}{p_t}\right)^{k_t}$$

$$=(-1)^{k_1\left(\frac{p_1^2-1}{8}\right)+k_2\left(\frac{p_2^2-1}{8}\right)+\dots+k_t\left(\frac{p_t^2-1}{8}\right)}\equiv(-1)^{\frac{m^2-1}{8}}\pmod 8$$

وبالتالي فإن $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$ ◆

المبرهنة التالية هي قانون التعاكس التربيعي لرمز جاكوبي.

مبرهنة (٨,١٨) [قانون التعاكس التربيعي ليرمز جاكوبي]

إذا كان كل من m و n عدداً فردياً حيث $(m,n)=1$ فإن:

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=(-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)}$$

البرهان

لنفرض أن $m=p_1^{\alpha_1}p_2^{\alpha_1}\ldots p_t^{\alpha_t}$ وأن $n=q_1^{\beta_1}q_2^{\beta_2}\ldots q_s^{\beta_s}$ هما تحليلا m و n إلى قوى عواملهما الأولية المختلفة. عندئذ :

$$\left(\frac{n}{m}\right)=\prod_{i=1}^{t}\left(\frac{n}{p_i}\right)^{\alpha_i}=\prod_{i=1}^{t}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)^{\alpha_i\beta_j}$$

$$\left(\frac{m}{n}\right)=\prod_{j=1}^{s}\left(\frac{m}{q_j}\right)^{\beta_j}=\prod_{j=1}^{s}\prod_{i=1}^{t}\left(\frac{p_i}{q_j}\right)^{\beta_j\alpha_i}$$

ولذا فإن:

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=\prod_{i=1}^{t}\prod_{j=1}^{s}\left[\left(\frac{q_i}{p_i}\right)\left(\frac{p_i}{q_i}\right)\right]^{\alpha_i\beta_j}$$

ولكننا نعلم استناداً إلى قانون التعاكس التربيعي لرمز ليجندر :

$$\left(\frac{q_i}{p_i}\right)\left(\frac{p_i}{q_j}\right)=(-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q_i-1}{2}\right)}$$

ولذا فإن :

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=\prod_{i=1}^{t}\prod_{j=1}^{s}(-1)^{\alpha_i\left(\frac{p_i-1}{2}\right)\beta_j\left(\frac{q_j-1}{2}\right)}$$

$$=(-1)^{\sum_{i=1}^{t}\sum_{j=1}^{s}\alpha_i\left(\frac{p_i-1}{2}\right)\beta_j\left(\frac{q_i-1}{2}\right)}$$

$$=(-1)^{\sum_{j=1}^{s}\alpha_i\left(\frac{p_i-1}{2}\right)\sum_{j=1}^{s}\beta_j\left(\frac{q_i-1}{2}\right)}$$

ولكن باستخدام المبرهنة (٨,١٦) نعلم أن:

$$\frac{m-1}{2}\equiv\sum_{i=1}^{t}\alpha_i\left(\frac{p_i-1}{2}\right)\pmod 2$$

$$\frac{n-1}{2} \equiv \sum_{j=1}^{t} \beta_j \left(\frac{p_j - 1}{2} \right) \pmod 2$$

وعليه فإن:

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) \equiv (-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)} \pmod 2$$

وبالتالي فإن:

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)} \quad \blacklozenge$$

النتيجة التالية تزودنا بصيغة مكافئة لقانون التعاكس التربيعي لرمز جاكوبي.

نتيجة (٨,١٩)

إذا كان m و n عددين فردين حيث $(m,n)=1$ فإن:

$$\left(\frac{m}{n}\right) = \begin{cases} \left(\frac{n}{m}\right), & m \equiv 1 \pmod 4 \text{ أو } n \equiv 1 \pmod 4 \\ -\left(\frac{n}{m}\right), & m \equiv n \equiv 3 \pmod 4 \end{cases}$$

البرهان

يشبه برهان النتيجة (٨,١٢) ونترك التفاصيل للقارئ ◆

مثال (٨,١٢)

احسب قيمة $\left(\frac{117}{1925}\right)$.

الحل

$$\left(\frac{117}{1925}\right) = \left(\frac{117}{25}\right)\left(\frac{117}{7}\right)\left(\frac{117}{11}\right)$$

$$=(1)\left(\frac{5}{7}\right)\left(\frac{7}{11}\right)$$
$$=\left(\frac{7}{5}\right)(-1)\left(\frac{11}{7}\right)$$
$$=-\left(\frac{2}{5}\right)\left(\frac{4}{7}\right)$$
$$=(-1)(-1)(1)=1$$

أو من الممكن استخدام قانون التعاكس التربيعي لرمز جاكوبي فيكون:

$$\left(\frac{117}{1925}\right)=\left(\frac{1925}{117}\right)=\left(\frac{53}{117}\right)=\left(\frac{117}{53}\right)=\left(\frac{11}{53}\right)=\left(\frac{53}{11}\right)=\left(\frac{9}{11}\right)=1.$$

وهذا يتفق مع ما وجدنا أعلاه □

ملحوظة

لنفرض أننا نود إيجاد أصغر راسب غير تربيعي p قياس العدد $m \geq 3$ ولكننا لا نعلم فيما إذا كان العدد m أولياً أم مؤلفاً أو أننا نعلم أن m مؤلف ولكننا لا نعلم عوامله الأولية. في كلتا الحالتين نقوم بحساب رمز جاكوبي $\left(\frac{p}{m}\right)$ فإذا كان $\left(\frac{p}{m}\right)=-1$ فإن p راسب غير تربيعي وأما إذا كان $\left(\frac{p}{m}\right)=1$ فإننا نقوم باستبدال p بالعدد الأولي الذي يليه وهكذا، والمثال التالي يوضح ذلك.

مثال (٨,١٣)

جد أصغر راسب غير تربيعي قياس العدد 3503 .

الحل

نقوم بتجريب الأعداد $p=2,3,5,7,...$ وحساب $\left(\frac{p}{3503}\right)$ فنجد:

$$\left(\frac{2}{3503}\right)=(-1)^{\frac{3503^2-1}{8}}=(-1)^{1533876}=1$$

$$\left(\frac{3}{3503}\right)=-\left(\frac{3503}{3}\right)=-\left(\frac{2}{3}\right)=-(-1)=1$$

$$\left(\frac{5}{3503}\right)=\left(\frac{3503}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1$$

أصغر $p=5$ أصغر راسب غير تربيعي قياس 3503 □

(٨,٦,١) تمارين محلولة *(Solved Exercises)*

تمرين (١)

افرض أن m عدداً فردياً حيث $(3,m)=1$.

(أ) جد جميع قيم m بحيث يكون $\left(\frac{3}{m}\right)=-1$.

(ب) جد جميع قيم m بحيث يكون $\left(\frac{3}{m}\right)=1$.

الحل

لنفرض أن $m=p_1^{k_1}p_2^{k_2}\ldots p_t^{k_t}$ هو تحليل m إلى قوى عواملـــه الأوليـــة المختلفة (p_i فردي لكل i).

(أ) لنفرض أن $\left(\frac{3}{m}\right)=-1$. عندئذ :

$$\left(\frac{3}{p_1}\right)^{k_1}\left(\frac{3}{p_2}\right)^{k_2}\ldots\left(\frac{3}{p_t}\right)^{k_t}=-1$$

ولكننا نعلم أن $\left(\frac{3}{p_i}\right)=-1$ إذا وفقط إذا كان $p_i \equiv \pm 5 \pmod{12}$. وبما أن $3 \nmid m$ و $4 \nmid m$ فإن $\left(\frac{3}{m}\right)=1$ إذا وفقط إذا وجدت على الأقل قيمة واحدة i بحيث يكون $p_i \equiv \pm 5 \pmod{12}$.

(ب) لاحظ أن قيمة $\left(\frac{3}{p_i}\right)$ لا تؤثر على قيمة $\left(\frac{3}{m}\right)$ إذا كان k_i زوجي. ولذا فإن:

$\left(\frac{3}{m}\right)=1$ إذا وفقط إذا كان $\left(\frac{3}{p_i}\right)=-1$ لعدد زوجي من الأعداد الأولية p_i التي يكون فيها k_i فردياً. أي أن $\left(\frac{3}{m}\right)=1$ إذا وفقط إذا كان $p_i \equiv \pm 5 \pmod{12}$ لعدد زوجي من الأعداد p_i التي يكون فيها k_i فردياً △

تمرين (٢)

ليكن $n=pq$ حيث $p \equiv q \equiv 3 \pmod 4$ عددان أوليان مختلفان.

(١) إذا كان $(a,n)=1$ حيث $\left(\frac{a}{n}\right)=1$ فأثبت أن $a \in Q_n$ و $b \in Q_n$ حيث $b \equiv -a \pmod n$.

(٢) إذا كان $a \in Q_n$ وكانت $\pm x, \pm y \pmod n$ هي الجذور التربيعية الأربعة للعدد a قياس n فأثبت أن:

(أ) $\left(\frac{x}{p}\right)=\left(\frac{x}{q}\right)=1$. أي أن $x \in Q_n$.

(ب) $\left(\frac{-x}{p}\right)=\left(\frac{-x}{q}\right)=-1$. أي أن $-x \notin Q_n$.

(ج) $\left(\frac{y}{p}\right)=-1$ و $\left(\frac{y}{q}\right)=1$.

(د) $\left(\frac{-y}{p}\right)=1$ و $\left(\frac{-y}{q}\right)=-1$.

الحل

(١) بما أن $\left(\frac{a}{n}\right)=1$ فإن $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=1$ أو أن $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$.

في الحالة الأولى يكون $a\in Q_p$ و $a\in Q_q$ ومن ثم فإن $a\in Q_n$.

أما إذا كانت الحالة الثانية هي المحققة فإن:

$$\left(\frac{-a}{p}\right)=\left(-\frac{1}{p}\right)\left(\frac{a}{p}\right)=(-1)(-1)=1$$

$$\left(-\frac{a}{q}\right)=\left(-\frac{1}{q}\right)\left(\frac{a}{q}\right)=(-1)(-1)=1$$

ومن ثم فإن $-a\in Q_p$ و $-a\in Q_q$. وبالتالي فإن $-a\in Q_n$.

(٢) بما أن $x^2\equiv y^2 \pmod n$ فإن $x^2\equiv y^2 \pmod p$. ومن ثم فإن $x\equiv \pm y \pmod p$. وبالمثل $x\equiv \pm y \pmod q$.

ولكن $x\not\equiv \pm y \pmod n$ وبالتالي يكون لدينا الحالتين التاليتين:

$$x\equiv y \pmod p \quad \text{و} \quad x\equiv -y \pmod q$$

أو

$$x\equiv -y \pmod p \quad \text{و} \quad x\equiv y \pmod q$$.

الآن، إذا كان $x\equiv y \pmod p$ و $x\equiv -y \pmod q$ فإن:

$$\left(\frac{x}{n}\right)=\left(\frac{x}{p}\right)\left(\frac{x}{q}\right)=\left(\frac{y}{p}\right)\left(\frac{-y}{q}\right)=\left(\frac{y}{p}\right)\left(\frac{-1}{q}\right)\left(\frac{y}{q}\right)=-\left(\frac{y}{n}\right)$$

وبالمثل، إذا كان $x\equiv -y \pmod p$ و $x\equiv y \pmod q$ فإننا نحصل على $\left(\frac{x}{n}\right)=-\left(\frac{y}{n}\right)$.

أخيراً نحصل على الفقرات من (أ) إلى (د) باستخدام الخواص الضربية لرمزي ليجندر وجاكوبي △

تمارين (٦, ٨)

(١) احسب قيمة رمز جاكوبي لكل مما يلي:

(أ) $\left(\frac{384}{443}\right)$ (ب) $\left(\frac{3828}{2539}\right)$ (ج) $\left(\frac{693}{1993}\right)$ (د) $\left(\frac{109}{1925}\right)$

(٢) احسب قيمة رمز جاكوبي لكل مما يلي دون استخدام خواص رمز ليجندر:

(أ) $\left(\frac{102}{1001}\right)$ (ب) $\left(\frac{-70}{709}\right)$ (ج) $\left(\frac{401}{425}\right)$ (د) $\left(\frac{105}{307}\right)$

(٣) أثبت أن كل من التطابقات التالية غير قابل للحل:

(أ) $x^2 \equiv 30 (\mathrm{mod}\ 1001)$ (ب) $x^2 \equiv 91 (\mathrm{mod}\ 561)$

(ج) $x^2 \equiv 330 (\mathrm{mod}\ 997)$ (د) $x^2 \equiv 2663 (\mathrm{mod}\ 3299)$

(٤) استخدم رمز جاكوبي لإيجاد أصغر راسب غير تربيعي قياس كل من الأعداد التالية دون محاولة تحليل العدد:

(أ) 11111 (ب) 1111111 (ج) 6641 (د) 7003

(٥) جد جميع الأعداد الصحيحة الموجبة m الأولية نسبياً مع 15 بحيث يكون $\left(\frac{15}{m}\right)=1$.

(٦) إذا كان $n = p_1 p_2 \dots p_t$ حيث p_i أعداد أولية فردية مختلفة فأثبت وجود عدد a يحقق $(a,n)=1$ و $\left(\frac{a}{n}\right)=-1$.

(٧) ليكن $n = p_1 p_2 \dots p_n$ حيث p_i أعداد أولية فردية مختلفة. وليكن $\{k_1, k_2, \dots k_{\varphi(n)}\}$ نظام رواسب مختزل قياس n . أثبت أن $\sum_{i=1}^{\varphi(n)} \left(\frac{k_i}{n}\right)=0$.

نبذة عن حياة ليجندر
Biography of Legendre



ولد : ١٧٥٢/٩/١٨م في باريس فرنسا
توفي: ١٨٣٣/١/١٠م في باريس فرنسا

ولد أدريان ليجندر لعائلة فرنسية ثرية مما أتاح له المجال لدراسة الرياضيات والفيزياء في كلية مازارين (College Mazarin) في باريس، حيث حصل على شهادة الدكتوراة في الرياضيات والفيزياء في العام ١٧٧٠م. عين ليجندر أستاذاً في المدرسة الحربية في العام ١٧٧٥م ، بناء على توصية من آلمبرت (d'Alembert) .

أدى حصول ليجندر على جائزة أكاديمية برلين في العام ١٧٨٢م إلى لفت نظر الرياضيين إليه، حيث كتب لاجرانج الذي كان يرأس قسم الرياضيات في أكاديمية برلين إلى لابلاس لتزويده بمعلومات عن الرياضي الشاب الذي فاز بالجائزة.

عين ليجندر في العام ١٧٨٣م في أكاديمية باريس للعلوم مباشرة بعد كتابته لبحث حول مجسمات القطوع الناقصة الذي قدم فيه دوال تعرف اليوم بدوال ليجندر.

وفي العام ١٧٨٥م قدم ليجندر محاولات لبرهان قانون التعاكس التربيعي (الذي برهنه فيما بعد جاوس) ومحاولات لبرهان وجود عدد غير منته من الأوليات على الصورة $am+b$ حيث $(a,b)=1$ (الذي برهنه فيما بعد دريشليه).

انتخب ليجندر في العام ١٧٨٧م كعضو في جمعية لندن الملكية . عمل ليجندر مع آخرين على توحيد الأوزان والقياسات وعمل جداول للوغاريتمات

والدوال المثلثية. في العام ١٧٩٤م نشر كتابه المشهور مبادئ الهندسة حيث قدم فيه براهين مبسطة وإعادة ترتيب للعديد من مبرهنات كتاب العناصر لإقليدس، كما قدم فيه برهاناً بسيطاً على أن العدد π غير كسري وبرهن لأول مرة أن العدد π^2 غير كسري. واعتبر كتابه المرجع الرئيسي في الهندسة لفترة تزيد عن مائة عام.

وفي العام ١٨٠٣م نشر كتاب عن مدارات المذنبات قدم فيه طريقة المربعات الصغرى لرسم المنحنيات من بيانات معطاة (تنسب هذه الطريقة الآن إلى جاوس الذي قدم وصفاً آخر لها في العام ١٨٠٩م).

وفي العام ١٨٠٨م نشر ليجندر الطبعة الثانية من كتابه نظرية الأعداد (الطبعة الأولى نشرها في العام ١٧٩٨م) حيث قدم فيه برهان جاوس لقانون التعاكس التربيعي وقدم أيضاً حداً أعلى لعدد الأعداد الأولية التي لا تزيد عن n.

وفي الأعوام ١٨١١م ، ١٨١٧م ، ١٨١٩م نشر الأجزاء الثلاثة لأبحاثه عن الدوال الناقصية حيث قدم دالتا بيتا وجاما.

في العام ١٨٢٤م رفض ليجندر التصويت لصالح مرشح الحكومة في المعهد الوطني مما تسبب في قطع راتب التقاعد عنه ومات معدماً في العام ١٨٣٣م.

نبذة عن حياة جاكوبي
Biography of Jacobi



ولد : ١٨٠٤/١٢/١٩م في ألمانيا
توفي: ١٨٥١/٢/١٨م في ألمانيا

ولد كارل جاكوبي لأب مصرفي حيث كان ترتيبه الثاني من بين أربع أبناء أحدهم أصبح فيزيائي مشهور هو مورتس جاكوبي (Moritz Jacobi) .

تتلمذ جاكوبي في البداية على يد خاله ثم دخل المدرسة في العام ١٨١٦م وعمره لا يتجاوز الثانية عشرة ، ونظراً لما أظهره من نبوغ فإنه وضع في السنة النهائية ومع نهاية العام الدراسي ١٨١٦ – ١٨١٧م كان مؤهلاً لدخول الجامعة ولكنه لم يستطع لأن جامعة برلين لا تقبل طلاباً سنهم أقل من ١٦ عاماً، فاضطر جاكوبي للبقاء في السنة النهائية لمدة أربع سنوات حتى بلغ السادسة عشرة .

وأثناء تلك الفترة تمكن جاكوبي من أن ينمي معرفته في الرياضيات وقبل مغادرته المدرسة كان ملماً بكتاب أويلر "مقدمة في التحليل اللانهائي" وبدأ بمحاولة حل معادلات الدرجة الخامسة بطريقة استخلاص الجذور.

بعد مرور سنتين على دخوله جامعة برلين قرر جاكوبي أنه يريد التخصص في الرياضيات ولكنه لم يستطيع التسجيل في مقررات رياضيات متقدمة في الجامعة وذلك لعدم وجود مثل هذه المقررات في الجامعات الألمانية في تلك الحقبة الزمنية، ولذا فإنه بدأ بتعليم نفسه بدراسة أبحاث لاجرانج وغيره من مشاهير علماء الرياضيات، ومع نهاية العام الدراسي ١٨٢٣ – ١٨٢٤م اجتاز جاكوبي الاختبارات التي مكنته من تدريس الرياضيات، واللغتين الاغريقية واللاتينية في المدارس الثانوية وحصل على وظيفة مدرس في العام ١٨٢٥م في واحدة من أفضل

المدارس الثانوية في برلين وأثناء ذلك قدم مشروع رسالة الدكتوراة لجامعة برلين، ثم حصل على وظيفة مدرس في جامعة برلين ولكنه لم يستمر طويلاً وانتقل إلى جامعة كونجسبيرغ حيث التقى هناك نيومان وبسل، أثناء تلك الفترة اكتشف بعض النتائج عن الرواسب التربيعية، ولكن الاسهامات الرئيسة كانت في مجال الدوال الناقصة التي أدت إلى ترقيته إلى أستاذ مشارك في العام ١٨٢٧م بناء على توصية من ليجندر الذي اعتبره أفضل الذين اشتغلوا في التحليل في تلك الحقبة الزمنية.

حصل جاكوبي على درجة الأستاذية في العام ١٨٣٢م. واشتغل جاكوبي في الفترة من ١٨٣٣م إلى ١٨٣٤م في المعادلات التفاضلية العادية والجزئية، كما كان له بعض الاسهامات في المحددات حيث اكتشف ما يطلق عليه اليوم دالة محدد جاكوبي.

أدى الركود الاقتصادي في أوربا في تلك الحقبة إلى إفلاس جاكوبي ومرضه بالسكري ولاحظ دريشليه علامات الفقر والمرض على جاكوبي عند زيارته له في العام ١٨٤٢م وكتب رسالة إلى الملك فردريك الرابع طالباً منه المساعده المالية لجاكوبي . ومع بداية العام ١٨٥١م مرض جاكوبي بالانفلونزا ثم الجدري مما أدى إلى وفاته في فبراير من العام ١٨٥١م.

الفصل التاسع

علم التعمية
CRYPTOLOGY

(٩,١) أنظمة التعمية التقليدية
Classical Cryptosystems

كتم الأسرار وإخفاء المعلومات من طبيعة البشر، ولذا فإن علم التعمية نشأ منذ أكثر من ألفي عام، حيث كان هذا العلم يقتصر على إخفاء الأسرار وحجب المعلومات التي يود صاحبها عدم كشفها إلا لأشخاص منتقين.

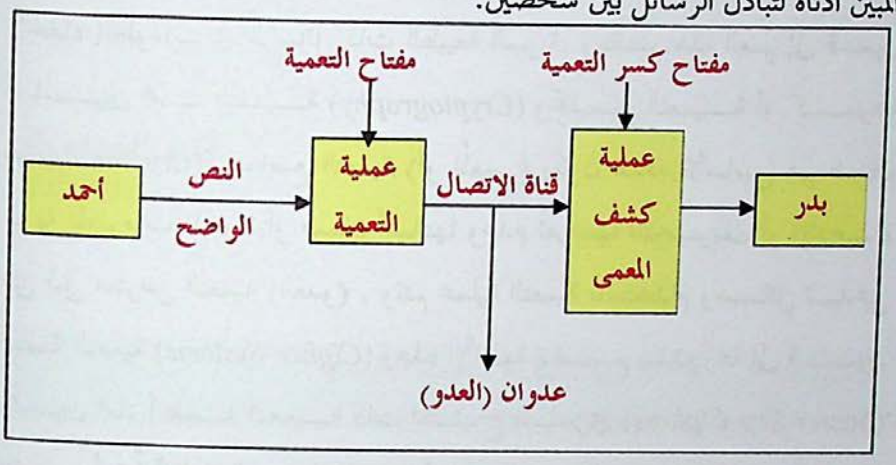
اقتصر استخدام علم التعمية في بداياته على الحفاظ على أمن المعلومات العسكرية والمراسلات الدبلوماسية وحماية الأمن الوطني للدول. ومع التقدم السريع للاتصالات (وسائل نقل المعلومات) والحاسبات الآلية (وسائل تخزين ومعالجة المعلومات) أصبحت الحاجة إلى إخفاء المعلومات المهمة أكثر إلحاحاً في العصر الحالي مما أدى إلى اهتمام أكبر في علم التعمية من أجل الحماية الأمنية و المالية والاقتصادية للمعلومات المنقولة عبر شبكات الاتصال التي يسهل اختراقها كالهاتف والبريد الإلكتروني وغيرها. ولهذه الأسباب فقد ادعى البعض أن الحرب العالمية

الثالثة ستكون حرب علماء الرياضيات على اعتبار أنها ستكون حرب معلومات وان الكثير من علماء الرياضيات سيتنافسون في حماية المعلومات وفي اختراقها.

يعرف علم التعمية (*Cryptology*) على أنه العلم الذي يهتم بالوسائل المثلى لإخفاء المعلومات في الرسائل ذات الطبيعة السرية. وينقسم هذا العلم إلى قسمين أساسيين هما التعمية (*Cryptography*) وتحليل التعمية أو كسرها (*Cryptanalysis*) . فواضع التعمية (أو المُعمي) يكون هدفه الأساسي هو ضمان سرية المعلومات المنقولة أو ضمان أصالتها وعدم تعرضها للتحريف أو الإدعاء من قبل معترض التعمية (العدو) . وتتم عملية التعمية باستخدام وسائل تدعى أنظمة التعمية (*Cipher Systems*) وهذه الأنظمة تنقسم بدورها إلى قسمين رئيسيين هما: أنظمة التعمية ذات المفتاح السري (*Secret Key Ciphers*) وتسمى أيضاً أنظمة التعمية التقليدية وأنظمة التعمية الحديثة ذات المفتاح المعلن (*Public Key Ciphers*) . وتلعب نظرية الأعداد دوراً رياديا في كلا قسمي التعمية. أما محلل التعمية فإنه يسعى إلى الهدف المضاد تماماً وهو كسر التعمية ومعرفة محتوى المعلومات المنقولة أو تحريفها بشكل يؤدي إلى قبولها على أنها المعلومات المرسلة. وبناء على ذلك فمن الممكن تعريف التعمية على أنها تحويل نص واضح ومقروء إلى نص غير مفهوم (معمى) باستخدام إحدى طرائق التعمية والتي قد تكون غير سرية ولكنها تستخدم مفتاحاً سرياً يمكن من يمتلكه من أن يعيد النص المعمى إلى النص الواضح (يستخرج التعمية) بينما يتعذر على أي شخص آخر لا يملك المفتاح السري أن يتوصل إلى النص الواضح على الرغم من معرفته لطريقة التعمية المستخدمة. في المقابل، يقوم محلل النظام (العدو) بدراسة الطرائق

التي تؤدي إلى معرفة المفتاح السري من معلومات متوفرة لديه ، ومن ثم الحصول على النص الواضح.

لإلقاء المزيد من الضوء على عملية التعمية وتحليلها، نفترض أن لدينا الوضع المبين أدناه لتبادل الرسائل بين شخصين:



كما يوضح المخطط أعلاه، لدينا شخصان سميناهما، أحمد وبدر ، يودان التواصل فيما بينهما، وأما الشخص الثالث أعطيناه اسم عدوان فهو الشخص الذي يتنصت عليهما (العدو). تتم عملية التعمية على النحو التالي:

قبل إرسال أحمد الرسالة التي تسمى النص الواضح (*plaintext*) إلى بدر يقوم أحمد بتعميتها (*encrypt* أو *encipher*) مستخدماً مفتاحاً للتعمية متفق عليه مسبقاً مع بدر (في العادة تكون عملية التعمية معروفة لعدوان، ولكن مفتاح التعمية هو الذي يحافظ على سريتها). وعند استقبال بدر للرسالة المعماة والتي تدعى النص المعمى (*ciphertext*) ، يقوم بدر بتحويلها إلى النص الواضح (*decrypt* أو *decipher*) ومن ثم قراءتها مستخدماً مفتاح كشف المعمى.

إن الأهداف التي يسعى عدوان إلى تحقيقها هي:

(١) قراءة الرسالة ، أو

(٢) معرفة مفتاح التعمية ومن ثم قراءة جميع الرسائل المعماة التي تستخدم هذا المفتاح، أو

(٣) تغيير رسالة أحمد إلى رسالة أخرى بطريقة تجعل بدر يعتقد أن الرسالة المغيرة هي التي تم إرسالها من قبل أحمد، أو

(٤) انتحال شخصية أحمد ومن ثم يقوم عدوان بالاتصال ببدر بحيث يعتقد بدر أن الشخص الذي يتواصل معه هو أحمد.

يعرف نظام التعمية التقليدي على النحو التالي:

تعريف (٩,١)

يتكون نظام التعمية من الخماسي (P,C,K,E,D) حيث:

(١) P مجموعة منتهية من الرموز تسمى النص الواضح.

(٢) C مجموعة منتهية من الرموز تسمى النص المعمى.

(٣) K مجموعة منتهية من المفاتيح تسمى فضاء المفاتيح (*keyspace*) .

(٤) لكل $k \in K$ توجد دالة تعمية (*encryption function*) $e_k \in E$ تقابلها دالة كشف المعمى (*decryption function*) $d_k \in D$ بحيث يكون $e_k : P \to C$ و $d_k : C \to P$ و $d_k(e_k(x)) = x$ لكل $x \in P$.

عند تعمية الرسائل فإنه من الممكن أن يتم ذلك بأي لغة مخاطبة كالعربية أو الانجليزية أو الفرنسية أو غيرها من اللغات ولكننا نقصر التعمية في هذا الفصل على

اللغة الانجليزية، وعليه نقابل بين الهجائية الانجليزية وبين الأعداد قياس 26 كما هو مبين في الجدول التالي:

الحرف	العدد	الحرف	العدد	الحرف	العدد	الحرف	العدد
A	0	H	7	O	14	V	21
B	1	I	8	P	15	W	22
C	2	J	9	Q	16	X	23
D	3	K	10	R	17	Y	24
E	4	L	11	S	18	Z	25
F	5	M	12	T	19		
G	6	N	13	U	20		

جدول (٩,١)

نستخدم اللون الأحمر للدلالة على النص المعمى و اللون الأخضر للدلالة على النص الواضح، كما أننا نتجاهل عادة الفراغات بين الكلمات وعلامات الترقيم.

نقدم الآن بعض الأنظمة التقليدية للتعمية حيث تستخدم جميع هذه الأنظمة مفتاحاً سرياً ونفترض في جميع عمليات التعمية أن كل من أحمد و بدر على دراية بالمفتاح السري المستخدم في عملية كشف المعمى. ومن الممكن أيضاً استخدام مفتاح التعمية لحساب مفتاح كشف المعمى كما سنرى في بعض الأنظمة التي نقدمها في هذا البند. وفي حالات كثيرة يكون مفتاح التعمية ومفتاح كشف المعمى متساويين.

(٩,١,١) نظام الإزاحة (*Shift Cipher*)

يعد نظام الإزاحة من أقدم أنظمة التعمية التقليدية وقد استخدم القيصر حالة خاصة منه للاتصال بجنوده وإليك تعريفه.

تعريف (٩,٢) [نظام الإزاحة]

في نظام الإزاحة يكون $P=C=K=\mathbb{Z}_{26}$ حيث $\mathbb{Z}_{26}$ ترمز لنظام الرواسب التام $\{0,1,2,\ldots,25\}$ قياس 26. دالتا التعمية وكشف المعمى هما

$$e_k(x)\equiv x+k \pmod{26}$$

$d_k(x)\equiv x-k \pmod{26}$ لكل $x\in P$ و $k\in K$.

مثال (٩,١)

إذا كان $k=12$ والنص الواضح في نظام الإزاحة هو :

Please send me money

فيقوم المرسل باستخدام الجدول (٩,١) لتحويل الرسالة إلى الأعداد المقابلة ليحصل على :

15 11 4 0 18 4 18 4 13 3 12 14 13 4 24

وبإضافة 12 إلى كل من أعداد الرسالة يكون:

1 23 16 12 4 16 4 25 15 24 0 25 16 10

وباستخدام الجدول (٩,١) مرة أخرى لإيجاد الحروف المقابلة يكون النص المعمى للرسالة هو:

□ *BXQMEQEQZPYAZQK*

(٩,١,٢) نظام التعويض *(The Substitution Cipher)*

إن نظام التعويض للتعمية يشبه نظام الازاحة من حيث أن كل منهما يحافظ على موقع الحرف بعد التعمية ولكنه يعمل على استبداله بحرف آخر والفرق بينهما هو أن نظام الازاحة يستخدم 26 مفتاحاً بينما نظام التعويض يستخدم!26 من المفاتيح.

تعريف (٩,٣) [نظام التعويض للتعمية]

في هذا النظام يكون $P=C=\mathbb{Z}_{26}$ ، $K=S_{26}$ (أي زمرة تباديل المجموعة $\{0,1,2,\ldots,25\}$) بحيث يكون لكل $x\in\mathbb{Z}_{26}$ ولكل $\pi\in K$:

$$e_\pi(x)=\pi(x)$$
$$d_\pi(x)=\pi^{-1}(x)$$

مثال (٩,٢)

إذا كان مفتاح التعمية π هو التبديل:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
S	F	L	R	C	V	M	U	E	K	J	D	I	X	N	Y	A	H	P	O	G	Z

وإذا كان النص الواضح هو : *Substitution Cipher*

فنرى أن النص المعمى باستخدام نظام التعويض والتبديل π أعلاه هو:

PGFPOEOGENXLEYUCH

وإذا كان النص المعمى هو :

HCDSOEZCDBYHEICXGIFCHP

فنجد باستخدام π^{-1} أن النص الواضح هو :

□ *relatively prime numbers*

(٩,١,٣) النظام التآلفي *(The Affine Cipher)*

نظام التعمية التآلفي هو تعميم لنظام الإزاحة ولكنه يبقى حالة خاصة من نظام التعويض.

تعريف (٩,٤) [نظام التعمية التآلفي]

في النظام التآلفي يكون $P = C = \mathbb{Z}_{26}$،

$K = \{(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a,26) = 1\}$ حيث لكل $x \in \mathbb{Z}_{26}$ ولكل $k = (a,b) \in K$ تكون دلتا التعمية وكشف المعمى هما

$$e_k(x) \equiv ax + b \pmod{26}$$

$$d_k(x) \equiv a^{-1}(x - b) \pmod{26}$$

ملحوظة

عناصر $\mathbb{Z}_{26}$ التي لها نظير ضربي هي : $1,3,5,7,9,11,15,17,19,21,23,25$

والجدول التالي يبين هذه النظائر.

$a \in \mathbb{Z}_{26}$	1	3	5	7	11	17	25
$a^{-1} \in \mathbb{Z}_{26}$	1	9	21	15	19	23	25

لنفرض أن $k = (a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$ حيث $\gcd(a,26) = 1$. عندئذ،

$$d_k(e_k(x)) \equiv d_k(ax + b) \equiv a^{-1}(ax + b - b) \equiv a^{-1}ax \equiv x \pmod{m}$$

لكل $x \in \mathbb{Z}_{26}$. وبهذا يكون النظام التآلفي هو بالفعل نظام تعمية.

مثال (٩,٣)

استخدم نظام التعمية التآلفي لتحويل النص الواضح التالي إلى نص معمى مستخدماً المفتاح $k=(3,24)$: *phone home*

الحل

$$e_k(p)=e_k(15)\equiv 3\times 15+24\equiv 17 \pmod{26}$$
$$e_k(h)=e_k(7)\equiv 3\times 7+24\equiv 19 \pmod{26}$$
$$e_k(o)=e_k(14)\equiv 3\times 14+24\equiv 14 \pmod{26}$$
$$e_k(n)\equiv e_k(13)\equiv 3\times 13+24\equiv 11 \pmod{26}$$
$$e_k(e)\equiv e_k(4)\equiv 3\times 4+12\equiv 10 \pmod{26}$$
$$e_k(m)\equiv e_k(12)\equiv 3\times 12+24\equiv 8 \pmod{26}$$

ونرى أن النص المعمى هو:

17	19	14	11	10	19	14	8	10
R	*T*	*O*	*L*	*K*	*T*	*O*	*I*	*K*

أي ***RTOLKTOIK*** □

(٩,١,٤) نظام فيجينير (*Vigenere Cipher*)

في جميع أنظمة التعمية التي قدمناها حتى الآن نجد أنه عند معرفتنا للمفتاح فإن كل حرف من حروف الهجائية المستخدمة يقابله حرف وحيد في النص المعمى والعكس صحيح أيضاً. لهذا السبب تسمى هذه الأنظمة بالأنظمة الأحادية *(monoalphabetic)* . سنقدم في هذا البند الجزئي والذي يليه أنظمة تعددية *(polyalphabetic)* حيث يكون فضاء المفاتيح مكوناً من كلمات طول كل منها n وعند اختيارنا للمفتاح فمن الممكن لحرف من الهجائية المستخدمة أن يعمى إلى أكثر من حرف واحد من حروف الهجائية. وبالتالي يكون من الواضح أن كسر مثل هذه الأنظمة أصعب من كسر الأنظمة الأحادية.

إن نظام فيجينير للتعمية مثال على أنظمة التعمية التعددية ويمكن اعتباره تعميماً لنظام الإزاحة الأحادي. بدأت فكرة هذا النظام على يد كل من ألبرتي (*Alberti*) و بورتا (*Porta*) في القرن السادس عشر، إلا أن فيجينير هو الذي طور هذا النظام ولذا فهو يحمل اسمه . على الرغم من المحاولات العديدة لكسر هذا النظام ومنها المحاولات التي قام بها كل من باباج (*Babbage*) وكاسيسكي (*Kasiski*) في القرن التاسع عشر، إلا أن النظام استعصى على جميع هذه المحاولات واعتبر نظاماً آمناً إلى أن استطاع فريدمان (*Friedman*) اكتشاف طريقة لكسره في العام ١٩٢٠م.

إن الفكرة الأساسية التي يعمل بها النظام هي استخدام كلمة سر (*keyword*) طولها n كمفتاح للتعمية. ولذا يكون بمقدور واضع التعمية أن يعمى كلمات طولها n في آن واحد. التعريف التالي يقدم لنا وصفاً دقيقاً لهذا النظام.

تعريف (٩,٥) [نظام فيجينير للتعمية]

ليكن $n \in \mathbb{Z}^+$ وليكن $P = C = K = (\mathbb{Z}_{26})^n$. لكل $k = (k_1, k_2, \ldots, k_n) \in K$. تُعرف دالتي التعمية وكسر التعمية على النحو التالي:

$$e_k(x_1, x_2, \ldots, x_n) \equiv (x_1 + k_1 (\text{mod } 26), x_2 + k_2 (\text{mod } 26), \ldots, x_n + k_n (\text{mod } 26))$$
$$d_k(x_1, x_2, \ldots, x_n) \equiv (x_1 - k_1 (\text{mod } 26), x_2 - k_2 (\text{mod } 26), \ldots, x_n - k_n (\text{mod } 26))$$

مثال (٩,٤)

لنفرض أن $n = 5$ وأن $k = Arabs$. ولنفرض أن أحمد يريد تعمية الرسالة التالية :

"the arabs in fact invented cryptanalysis, the science of unscrambling a message without knowledge of the key"

الحل

يقوم أحمد بتقسيم حروف الرسالة إلى مجموعة من الكلمات طول كل منها 5 ثم يجد الأعداد المقابلة لهذه الحروف. بعد ذلك يضع الأعداد المقابلة لكلمة السر تحت أعداد الرسالة الواضحة ويجمع قياس 26 ليحصل على:

0	1	18	8	13
0	17	0	1	18
0	18	18	9	5

19	7	4	0	17
0	17	0	1	18
19	24	4	1	9

13	21	4	13	19
0	17	0	1	18
13	12	4	14	11

5	0	2	19	8
0	17	0	1	18
5	17	2	20	2

15	19	0	13	0
0	17	0	1	18
15	10	0	14	18

4	3	2	17	24
0	17	0	1	18
4	20	2	18	16

19	7	4	18	2
0	17	0	1	18
19	24	4	19	20

11	24	18	8	18
0	17	0	1	18
11	15	18	9	10

14	5	20	13	18
0	17	0	1	18
14	22	20	14	10

8	4	13	2	4
0	17	0	1	18
8	21	13	3	22

2	17	0	12	1
0	17	0	1	18
2	8	0	13	19

11	8	13	6	0
0	17	0	1	18
11	25	13	7	18

12	4	18	18	0
0	17	0	1	18
12	21	18	19	18

6	4	22	8	19
0	17	0	1	18
6	21	22	9	11

7	14	20	19	10
0	17	0	1	18
7	5	20	20	2

13	14	22	11	4
0	17	0	1	18
13	5	22	12	22

3	6	4	14	5
0	17	0	1	18
3	23	4	15	23

19	7	4	10	4
0	17	0	1	18
19	24	4	11	22

24
0
24

الآن يقوم أحمد بإيجاد الحروف المقابلة للمجاميع وتكون رسالته المعماة هي:

"TYEBJASSJFFRCUANMEOLEUCSQPKAOSLPSJKTYETUIVNDWO
WUOKCIANTLZNHSMVSTSGVWJLHFUUCNFWMWDXEPXTYELWY"

لاحظ على سبيل المثال أن كلا من الحروف E ، V ، W في النص المعمى يقابل الحرف e في النص الواضح وذلك لأن نظام فيجينير تعددي □

(٩,١,٥) نظام هيل (*Hill Cipher*)

نظام هيل هو مثال آخر على الأنظمة التعددية. اكتشف هيل نظام التعمية المرتبط باسمه عام ١٩٢٩م ويعتمد على المصفوفات القابلة للعكس (أو التحويلات الخطية القابلة للعكس) ومن الممكن وصفه على النحو التالي:

تعريف (٩,٦) [نظام هيل للتعمية]

ليكن $n \in \mathbb{Z}^+$. وليكن $P = C = (\mathbb{Z}_{26})^n$ وليكن

$K = \{A \in M_n(\mathbb{Z}_{26}) : \gcd(\det A, 26) = 1\}$. لكل $A \in K$ و $X \in (\mathbb{Z}_{26})^n$

دالتا التعمية وكشف المعمى تعرفان على النحو التالي:

$$e_A(x) \equiv AX \pmod{26}$$

$$d_A(X) \equiv A^{-1}X \pmod{26}$$

مثال (٩,٥)

استخدم نظام هيل للتعمية حيث $n = 2$ لتعمية النص الواضح: "*ignore this*"

مستخدماً المفتاح $A = \begin{bmatrix} 23 & 3 \\ 10 & 25 \end{bmatrix}$.

الحل

بما أن $\det A = 23 \times 25 - 3 \times 10 \equiv 25 \pmod{26}$ وأن $\gcd(25, 26) = 1$

فإن A مفتاح مقبول. نقوم الآن بتقسيم الحروف إلى ثنائيات (لأن $n = 2$) ونجد الأعداد المقابلة لها لنحصل على:

$$\begin{bmatrix} i \\ g \end{bmatrix} = \begin{bmatrix} 8 \\ 6 \end{bmatrix}, \begin{bmatrix} n \\ o \end{bmatrix} = \begin{bmatrix} 13 \\ 14 \end{bmatrix}, \begin{bmatrix} r \\ e \end{bmatrix} = \begin{bmatrix} 17 \\ 4 \end{bmatrix}, \begin{bmatrix} t \\ h \end{bmatrix} = \begin{bmatrix} 19 \\ 7 \end{bmatrix}, \begin{bmatrix} i \\ s \end{bmatrix} = \begin{bmatrix} 8 \\ 18 \end{bmatrix}$$

الآن:

$$e_A\begin{bmatrix}8\\6\end{bmatrix}\equiv A\begin{bmatrix}8\\6\end{bmatrix}\equiv\begin{bmatrix}20\\22\end{bmatrix}(\text{mod }26)$$

$$e_A\begin{bmatrix}13\\14\end{bmatrix}\equiv A\begin{bmatrix}13\\14\end{bmatrix}\equiv\begin{bmatrix}3\\12\end{bmatrix}(\text{mod }26)$$

$$e_A\begin{bmatrix}17\\4\end{bmatrix}\equiv A\begin{bmatrix}17\\4\end{bmatrix}\equiv\begin{bmatrix}13\\10\end{bmatrix}(\text{mod }26)$$

$$e_A\begin{bmatrix}19\\7\end{bmatrix}\equiv A\begin{bmatrix}19\\7\end{bmatrix}\equiv\begin{bmatrix}16\\1\end{bmatrix}(\text{mod }26)$$

$$e_A\begin{bmatrix}8\\18\end{bmatrix}\equiv A\begin{bmatrix}8\\18\end{bmatrix}\equiv\begin{bmatrix}4\\10\end{bmatrix}(\text{mod }26)$$

ولذا فإن النص المعمى هو: ***UWDMNKQBEK*** .

لاحظ أن الظهور الأول للحرف i في النص الواضح قابله الحرف ***U*** في النص المعمى وأما الظهور الثاني فقابله الحرف ***E***. وهذا يوضح المقصود بتعددية النظام □

من الممكن تعميم نظام هيل للتعمية إلى نظام تعمية يعتمد على التحـــويلات التآلفية على النحو التالي:

تعريف (٩,٧) [نظام هيل التآلفي]

ليكن $n\in\mathbb{Z}^+$. وليكن $P=C=(\mathbb{Z}_{26})^n$.

وليكن $K=\{A\in M_n(\mathbb{Z}_{26}),\ B\in M_{n1}(\mathbb{Z}_{26}):\gcd(A,26)=1\}$

لكل $(A,B)\in K$ و $X\in(\mathbb{Z}_{26})^n$ دالتا التعمية وكسر التعمية تعرفان كالتالي:

$$e_{(A,B)}(X)\equiv AX+B\,(\text{mod }26)$$

$$d_{(A,B)}(X)\equiv A^{-1}(X-B)\,(\text{mod }26)$$

مثال (٩,٦)

استخدم نظام هيل التآلفي لتعمية الرسالة : "*Hill*" علماً بأن:

$$e(X)\equiv\begin{bmatrix}5 & 2\\ 11 & 15\end{bmatrix}X+\begin{bmatrix}14\\ 3\end{bmatrix}(\text{mod } 26)$$

الحل

بما أن $\det A=\begin{vmatrix}5 & 2\\ 11 & 15\end{vmatrix}=53\equiv 1(\text{mod } 26)$ فإن $\gcd(\det A,26)=1$.

ومن ثم فإن A تصلح كمفتاح تعمية. الآن:

$$e\begin{bmatrix}h\\ i\end{bmatrix}=\begin{bmatrix}5 & 2\\ 11 & 15\end{bmatrix}\begin{bmatrix}7\\ 8\end{bmatrix}+\begin{bmatrix}14\\ 3\end{bmatrix}=\begin{bmatrix}13\\ 18\end{bmatrix}(\text{mod } 26)$$

$$e\begin{bmatrix}l\\ l\end{bmatrix}=\begin{bmatrix}5 & 2\\ 11 & 15\end{bmatrix}\begin{bmatrix}11\\ 11\end{bmatrix}+\begin{bmatrix}14\\ 3\end{bmatrix}=\begin{bmatrix}13\\ 3\end{bmatrix}(\text{mod } 26)$$

ويكون المعمى هو: *NSND* □

تمارين (٩,١)

(١) استخدم نظام الإزاحة لتعمية الرسالة: *the weather is bad* علماً بأن $k=7$.

(٢) جد النص الواضح للرسالة التالية المعماة بنظام القيصر (نظام إزاحة بمفتاح $k=3$) :

JDXOLVGLYLGHGLQWRWKUHHSDUWV

(٣) اقرأ الرسالة التالية المعمالة بنظام الازاحة حيث $k=11$.

HPHTWWXPPEXTOYTRSE

(٥) ليكن مفتاح التعمية في نظام التعويض هو:

0	1	2	3	4	5	6	7	8	9	10	11	12
21	12	25	17	24	23	19	15	22	13	18	3	9
13	14	15	16	17	18	19	20	21	22	23	24	25
5	10	2	8	16	11	14	7	1	4	20	0	6

(أ) جد النص المعمى للرسالة :

The shift cipher is a special case of the substitution cipher

(ب) اقرأ الرسالة: *CQKZYYRJYYOWFTVLVTQYYR* .

(٦) ليكن $(a,b)=(7,10)$ مفتاح التعمية في النظام التآلفي.

(أ) جد النص المعمى للرسالة : *do not reveal the secret*

(ب) اقرأ الرسالة: *LJMKGMGMXFQEXMW*

(٧) استخدم مفتاح التعمية ***Heisenberg*** لتعمية الرسالة التالية في نظام فيجينير:

It is logically impossible to measure simultaneously every facet of a given object with perfect precision. In other words even in principle we cannot know the present in all detail.

(٨) إذا علمت أن مفتاح التعمية لنظام هيل هو $A=\begin{bmatrix}5 & 17\\ 4 & 15\end{bmatrix}$ فاقرأ الرسالة المعماة: *QOUH* .

(٩) إذا علمت أن مفتاح التعمية لنظام هيل هو $A=\begin{bmatrix}11 & 2 & 19\\ 5 & 23 & 25\\ 20 & 7 & 1\end{bmatrix}$ فاقرأ الرسالة المعماة : *ITNNEPACWUL* .

(١٠) اقرأ الرسالة *HIAT* المعماة بنظام هيل علماً بأن مفتاح التعمية هو $A=\begin{bmatrix}3 & 3\\ 2 & 5\end{bmatrix}$.

(١١) جد النص المعمى للنص الواضح: *no answer* مستخدماً نظام هيل بمفتاح $A=\begin{bmatrix}2 & 3\\ 7 & 8\end{bmatrix}$. استخدم المفتاح A^{-1} لإيجاد النص الواضح للنص المعمى: *FWMDIQ* .

(١٢) إذا كان $A=\begin{bmatrix}4 & 3\\ 9 & 20\end{bmatrix}$ هو مفتاح التعمية في نظام هيل فاقرأ الرسالة المعماة: *APZH*

(٩,٢) تحليل التعمية
Cryptanalysis

إن الصراع الدائم بين مصمم نظام التعمية ومحلل التعمية لا يزال قائماً منذ أن استخدم الانسان أنظمة التعمية، حيث يكون الأمر الأهم للمصمم هو تطوير نظام يصعب على محلل التعمية اكتشاف مفتاحه السري. أما محلل التعمية فإنه يقوم بدراسة الطرق الممكنة التي تؤدي الى اكتشاف بعض الثغرات في النظام المستخدم ومن ثم معرفة مفتاحه وكسره، وبالتالي يصبح هذا النظام عديم الفائدة من الناحية الأمنية.

تنقسم جميع أنظمة (خوارزميات) التعمية إلى قسمين رئيسيين حسب نوع المفتاح المستخدم، وهما المفتاح السري والمفتاح المعلن. سندرس المفتاح المعلن البند القادم من هذا الفصل. أما بالنسبة للمفتاح السري فيفترض في جميع عمليات التعمية أن يكون كل من أحمد وبدر على دراية بمفتاح التعمية ومفتاح كشف المعمى. فمن الممكن أن يشترك كل من أحمد وبدر بمفتاح التعمية ومن ثم يستخدم مفتاح التعمية لحساب مفتاح كشف المعمى، وفي حالات كثيرة يكون مفتاح

التعمية هو مفتاح كشف المعمى نفسه. إن جميع أنظمة التعمية التقليدية هي أنظمة ذات مفتاح سري.

من الصعب جداً معرفة درجة أمان خوارزميات التعمية. إن لمعظم هذه الخوارزميات مفتاح تعمية وبالتالي فإن أمن النظام المستخدم يعتمد على مدى صعوبة اكتشاف هذا المفتاح من قبل العدو. إحدى الطرق المتوقعة لمحاولة معرفة هذا المفتاح هي طريقة الاستفاد (*exhaustion method*) وهي تجريب جميع المفاتيح الممكنة للحصول على إعادة تعمية ناجحة. وفي هذه الحالة يكون لطول المفتاح ارتباط مباشر مع طول الفترة الزمنية التي يحتاجها محلل التعمية (أو الحاسب) لاستنفاد فضاء المفاتيح (جميع المفاتيح) . على سبيل المثال، إذا كان النظام المستخدم هو نظام الازاحة ، فإن عدد المفاتيح يكون 26 وبالتالي فإن النظام غير آمن. أما إذا كان النظام المستخدم هو نظام التعويض فإن عدد عناصر فضاء المفاتيح هو !26 وهو عدد كبير جداً. ولذا فكلما كان طول المفتاح كبيراً كلما أصبحت مهمة محلل التعمية أكثر صعوبة ولكن هذا لا يضمن أن يكون النظام آمناً لأن لخوارزمية التعمية المستخدمة دور كبير في أمن النظام حيث توجد طرق أخرى لكسر التعمية. سندرس بعضها في هذا البند (مثل، استخدام تردد اللغة) لكسر أنظمة يكون فضاء مفاتيحها كبيراً جداً. على سبيل المثال ، عدد مفاتيح نظام التعويض يساوي $4\times10^{26}\approx 26!$ ولكن هذا النظام سهل الكسر كما سنرى في هذا البند. أما عدد مفاتيح نظام تعمية البيانات القياسي (*data encryption standard*) والذي يعرف بنظام *DES* فهو $7.2\times10^{16}\approx 2^{56}$ وباستخدام الحاسب المخصص لكسر نظام *DES* نحتاج عادة إلى يوم كامل لإيجاد

مفتاح النظام *DES* . ولذا فمحلل التعمية لا يلجأ عادة إلى استنفاد المفاتيح إلا إذا لم يكن في جعبته أي طريقة أخرى لكسر نظام التعمية.

نود التأكيد هنا على نقطة مهمة جداً، ألا وهي أن كَوْن نظام تعمية معين آمناً اليوم فهذا لا يضمن استمرار أمنه في المستقبل، ويرجع ذلك إلى ذكاء محللي التعمية الذين لا يألون جهداً في محاولة اكتشاف طرق جديدة لكسر النظام أو إلى التقدم السريع في صناعة التكنولوجيا. على سبيل المثال ، بعد أن صمد نظام *DES* في وجه أي محاولة لكسره عشرين عاماً. استطاعت حواسب متوازية كسره. وسنقدم في البند القادم نظام تعمية يعتمد كسره على صعوبة تحليل الأعداد الكبيرة (أعداد تتكون من 200 مرتبة) ، فإذا أردنا تحليل مثل هذا العدد باختبار جميع الأوليات التي أصغر من أو تساوي جذر هذا العدد فإننا نحتاج لاختبار 4×10^{97} عدداً أولياً وهي جميع الأعداد الأولية التي لا تزيد عن 10^{100} وهذا مستحيل . ولهذا فلا بد من استخدام خوارزميات أكثر فعالية لتحليل الأعداد، في الحقيقة مثل هذه الخوارزميات موجودة، فعند اكتشاف أول نظام تعمية ذي مفتاح معلن قبل ثلاثين عاماً والذي يعتمد أمنه على تحليل الأعداد، كان من المعتقد أن استخدام عدد مكون من 129 مرتبة كمفتاح لهذا النظام يجعل هذا النظام آمناً لفترة طويلة، ولكن مع اكتشاف خوارزميات جديدة لتحليل الأعداد ومع التقدم في الصناعة التكنولوجية أصبح تحليل مثل هذا العدد عملاً روتينياً. ولذا فالأعداد المستخدمة اليوم في هذا النظام لضمان أمنه تتكون من أكثر من 200 مرتبة.

توجد أربعة مستويات رئيسة في كسر التعمية مصنفة بناء على كمية المعلومات المتوافرة لمحلل التعمية (عدوان) لدى محاولته معرفة مفتاح التعمية، هذه المستويات هي:

(١) **معرفة النص المعمى فقط** (*known ciphertext only*) : يكون محلل التعمية على دراية بالنص المعمى فقط.

(٢) **معرفة النص الواضح** (*known plaintext*) : يكون محلل التعمية على دراية بجزء من الرسالة الواضحة وما يقابل هذا الجزء من الرسالة المعماة. على سبيل المثال ، لنفترض أن عدوان اعترض رسالة معماة ثم استطاع بعد ذلك الحصول على النص الواضح لهذه الرسالة، فإذا كان هذا الجزء من النص المعمى وما يقابله من النص الواضح كافياً لمعرفة مفتاح التعمية فيكون بإمكان عدوان قراءة جميع رسائل أحمد المعماة (على افتراض أن أحمد استمر في استخدام المفتاح نفسه في عمليات التعمية). أو لنفترض أن أحمد يستهل جميع رسائله بالبسملة (بسم الله الرحمن الرحيم) ، فيكون لدى عدوان جزء من النص المعمى وما يقابله من النص الواضح. إن هذا الجزء ولو أنه صغير إلا أنه كاف لمعرفة مفتاح العديد من الأنظمة التعموية.

(٣) **اختيار النص الواضح** (*chosen plaintext*) : في هذه الحالة يكون محلل التعمية (عدوان) قد حصل على مدخل مؤقت دون أن يكون باستطاعته معرفة مفتاح التعمية، ومن ثم يقوم عدوان باستغلال هذه الدخول المؤقت لتعمية عدد كبير من النصوص الواضحة المختارة بعناية ومن ثم استخدام ذلك لمحاولة معرفة مفتاح التعمية.

(٤) **اختيار النص المعمى** (*chosen ciphertext*) : في هذه الحالة يكون محلل التعمية قد حصل على مدخل مؤقت لعملية كشف المعمى. وعليه يقوم عدوان بكشف المعمى لعدد كبير من الرسائل المعماة للحصول على ما يقابلها من النص الواضح ومن ثم محاولة معرفة مفتاح التعمية.

ملحوظة

يفترض الباحثون في نظرية التعمية الحديثة مبدأ كرتشكوف (*Kerchkoff's principle*) والذي ينص على أن العدو على دراية بنظام التعمية المستخدم. وهذا ما سنفترضه هنا.

لقد استخدمت وسائل كثيرة لتحليل أنظمة التعمية باستخدام الخواص الاحصائية للغة المستخدمة ويعتبر أبو يوسف الكندي (*AL-Kindi*) والذي سمي فيلسوف العرب هو أول من استخدم خصائص اللغة العربية في كسر التعمية حيث عثر في العام ١٩٨٧م على بحث له في أرشيف الدولة العثمانية في اسطنبول يشرح فيه كيفية تحليل التعمية بطريقة النص المعمى فقط وفحواه:

"إذا علمنا لغة التعمية فإن احدى وسائل كسر التعمية هي القيام بعد حروف صفحة من أي مصدر مكتوب باللغة نفسها وترتيب هذه الحروف تنازلياً حسب تكرارها في تلك الصفحة. بعد ذلك تقوم باحصاء حروف النص المعمى المراد كسره ونقابل بين الحرف الأكثر تردداً في النص المعمى مع الحروف الأكثر تردداً في النص الواضح وهكذا".

قام العديد من المهتمين بحساب التردد النسبي لأحرف الهجائية الانجليزية من خلال احصاء الأحرف لبعض الروايات والمجلات والصحف اليومية، والجدول (٩,٢) يبين إحصائية قام بها كل من بيكر (*Beker*) وبيبر (*Piper*) للغة الانجليزية.

الحرف	الاحتمال p	p^2	الحرف	الاحتمال p	p^2	الحرف	الاحتمال p	p^2
A	.082	.00672	K	.008	.00006	U	.028	.00078
B	.015	.00023	L	.040	.00160	V	.010	.00010
C	.028	.00078	M	.024	.00058	W	.023	.00053
D	.043	.00185	N	.067	.00449	X	.001	.00001
E	.127	.01613	O	.075	.00563	Y	.020	.00040
F	.022	.00048	P	.019	.00036	Z	.001	.00001
G	.020	.00040	Q	.001	.00001			
H	.016	.00372	R	.060	.00360			
I	.070	.00490	S	.063	.00397			
J	.002	.00001	T	.091	.00828			

جدول (٩,٢)

لاحظ أن $\sum_{i=0}^{25} p_i^2 = 0.065$

من الجدول (٩,٢) نجد أن أحرف الهجائية الانجليزية تقسم إلى خمسة أقسام هي:

(١) الحرف E باحتمال 0.12 .

(٢) الحروف T ، A ، O ، I ، N ، S ، H ، R بإحتمالات واقعة بين 06. و 09.

(٣) الحرفان D و L واحتمال كل منهما 04.

(٤) الحروف C ، U ، M ، W ، F ، G ، Y ، P ، B بإحتمالات واقعة بين 015. و 023. .

(٥) الحروف V ، K ، J ، X ، Q و Z واحتمال كل منهما أقل من 01..

كما أن أكثر الثنائيات تردداً مرتبة تنازلياً فهي:

NT ، TO ، AT ، EN ، ST ، ES ،ON ، ED ، RE ، AN ، ER ، IN ، HE ، TH
، SE ، TE ، AR ، ET ،IS ، TI ، OR ، AS ، NG ، EA ، OU ، ND ، HA ،
. OF ، HI

أما أكثر الثلاثيات شيوعاً فهي:

ETH ،WAS ، NTH ،THA ،ENT ،ERE ، HER ،AND ،ING ، THE
. DTH ، FOR ،

(٩,٢,١) تحليل نظام الإزاحة *(Cryptanalysis of shift Cipher)*

إن عدد عناصر فضاء المفاتيح في نظام الازاحة يساوي 26 . ولذا فمن الممكن كسر هذا النظام بسهولة باستنفاد المفاتيح. كما أنه أيضاً نظام سهل الكسر باستخدام تحليل التردد كما هو موضح في المثال التالي:

مثال (٩,٧)

استخدم تحليل التردد لقراءة الرسالة المعمية التالية باستخدام نظام الإزاحة:

NYGUBHTUVGVFABGXABJAJUBSVE
FGERNYVFRQGUNGGURINEVNGVBAV
AGURSERDHRAPVRFBSYRGGREFPBHYQ
ORRKCYBVGRQVABEQREGBOERNXPVC
UREFGURRNEYVRFGXABJAQRFPEVC
GVBABSGURGRPUAVDHRVFOLGURA
VAGUPRAGHELFPVRAGVFGNOHLHFH
SLNDHONYXVAQVXABJANFGURCUVY
BFBCUREBSGURNENOF

الحل

الجدول التالي يوضح ترددات الحروف في النص المعمى :

الحرف	التردد	الحرف	التردد	الحرف	التردد	الحرف	التردد
A	18	*H*	9	*O*	6	*V*	22
B	17	*I*	1	*P*	7	*W*	0
C	5	*J*	4	*Q*	6	*X*	5
D	3	*K*	1	*R*	28	*Y*	8
E	14	*L*	4	*S*	6	*Z*	0
F	15	*M*	0	*T*	1		
G	25	*N*	13	*U*	16		

من الجدول يتضح لنا أن الحروف ***R*** هو الأكثر تردداً في النص المعمى. ولـــذا فعلى الأرجح يكون $e_k(e)=R$ (لأن الحرف e هو الحرف الأكثر تردداً في اللغـــة الانجليزية). ولذا فإن $4+k \equiv 17 \bmod(26)$. أي أن $k=13$. وبتحويل الـــنص المعمى إلى الأعداد المقابلة له ثم القيام بطرح 13 من كل منها وتحويـــل النـــاتج إلى الحروف المقابلة نحصل على النص الواضح:

althoughitisnotknownwhofirstrealizedthatthevariation the frequenciesoflette rscouldbeexploitedinordertobreakciphersttheearliest knowndescriptionofthetechniqueisbytheninthcenturyscientistabuyusuf yaqubalkindiknownasthephilosopherofthearabs

وبالتالي فإنه بالإمكان قراءة النص الواضح وهو:

Although it is not known who first realized that the variation in the frequencies of letters could be exploited in order to break ciphers, the earliest known description of the technique is by the ninth century scientist ABU Yusuf Yaqub Al Kindi. Known as the philosopher of the Arabs.

ملحوظات

(١) يتم كسر نظام الازاحة بمعرفة النص الواضح إذا كان محلل التعمية على دراية بحرف واحد من النص الواضح وما يقابله من النص المعمى. على سبيل المثال لـــو

علم محلل التعمية أن الحرف الواضح t يقابل الحرف المعمى G في المثـــال (١,٢٤) فبإمكانه حساب مفتاح التعمية كالتالي:

$$G = e(t) \equiv t + k \Rightarrow 6 \equiv 19 + k \Rightarrow k \equiv -13 \equiv 13 (\text{mod } 26)$$

(٢) كسر نظام الازاحة باختيار النص الواضح يتم كما يلي: إذا اختار محلل التعمية حرفاً من النص الواضح وعرف الحرف المقابل له من النص المعمى فإن هذا كاف لمعرفة مفتاح التعمية كما في المحلوظة (١).

(٣) كسر نظام الازاحة باختيار النص المعمى يتم بصورة مماثلة لما تقدم.

(٩,٢,٢) تحليل نظام التعويض (*Cryptanalysis of Substitution Cipher*)

إن عدد عناصر فضاء المفاتيح لنظام التعويض هو $26! \approx 4 \times 10^{26}$ لذا فـــإن هذا العدد كبير جداً ومن ثم فإن كسر النظام باستنفاد المفـــاتيح يكـــاد يكـــون مستحيلاً. إلا أنه ليس صعباً كسر النظام باستخدام تحليل التردد. سنوضح هـــذه الطريقة في المثال التالي وسنفترض للسهولة وجود فراغ بين كلمات النص.

مثال (٩,٨)

استخدم تحليل التردد لكسر الرسالة المعماة التالية علماً بأن نظـــام التعميـــة المستخدمة هو نظام التعويض:

CPO QXU CI OPAJUFLYPD SOKKXDOK
QCMRV ZO ICJ LBO KOPVOJ LC
OPAJUFL XRR LBO VXUK LJXIIYA
XAACJVYPD LC LBO VXU EOU LBYK
QCMRV SOXP LBXL ICJ X QBCRO
VXU XL LBO KLXJL CI OXAB SOKKXDO
XRR OPYDSX CFOJXLCJ QCMRV KOL
LBOYJ SXABYPOK XAACJVYPD LC LBO

VXU EOU LBOP OXAB LYSO XSOKKXDO
POOVOV LC ZO KOPL YL QCMRV ZO
IYJKL LUFOV YPLC LBO SXABYOP
LBO OPAYFBOJOV CMLFML QCMRV LBOP
ZO JOACJVOV XPV BXPVOV LC LBO
JXVYC CFOJXLCJ ICJ LJXPKSYKKYCP
LBO ACVO ZCCE ZU KYSCP KYPDB

الحل

سنقوم بتحليل الرسالة على خطوات وندعوا القارئ الذي يعتقد أن لديه القدرة على كسر الرسالة دون اتباع الخطوات المقدمة أن يفعل ذلك.

(١) إن أول خطوات كسر النص المعمى هي عمل جدول لترددات حروفه وهذا ما قمنا به في الجدول التالي:

الحرف	التردد	الحرف	التردد	الحرف	التردد	الحرف	التردد
A	15	*H*	0	*O*	50	*V*	23
B	21	*I*	8	*P*	23	*W*	0
C	32	*J*	21	*Q*	7	*X*	29
D	7	*K*	19	*R*	10	*Y*	18
E	3	*L*	38	*S*	9	*Z*	6
F	7	*M*	7	*T*	0		
G	0	*N*	0	*U*	11		

(٢) الحرف O هو أكثر الحروف ترددا في الجدول ولذا فإنه غالباً ما يكون $d_k(O)=e$.

(٣) حروف النص المعمى التي ترددها على الأقل 25 هي C ، L و X. ولذا فإنها يمكن أن تقابل أياً من الحروف t ، a ، i ، n ، s ، h ، r.

(٤) بما أن الكلمتان الوحيدتان باللغة الانجليزية المكونتان من حرف واحد فقط هما i و a وأن X هي إحدى كلمات النص المعمى فإن $d_k(X)=a$ أو $d_k(X)=i$. ولكن OX تكرر ثلاث مرات في النص المعمى وأن ea ثنائي أكثر تردداً من الثنائي e_i في اللغة الانجليزية. ولذا فإننا نخلص إلى أن $d_k(X)=a$.

(٥) بما أن C تجاور معظم حروف النص المعمى فإنها على الأغلب تقابل حرف علّة. ولذا فإن $d_k(C)=o$ أو $d_k(C)=i$. ولكن الثنائي CC ظهر في النص المعمى وأن تردد الثنائي oo أكثر من تردد الثنائي ii في اللغة الانجليزية. وبالتالي فإننا نخلص إلى أن $d_k(C)=o$.

(٦) في هذه المرحلة ينصح عادة بمحاولة إيجاد الحرف المقابل للحرف h لأن الثنائي he أكثر شيوعاً من الثنائي eh في اللغة الانجليزية. ولهذا الغرض نجد أن BO تكرر كثيراً في النص المعمى ولكن OB لم يتكرر أبداً. ولذا فإن $d_k(B)=h$.

(٧) بما أن الثنائي LC والثلاثي LBO تكررا كثيراً في النص المعمى وأن كل من الثنائي to والثلاثي the شائع في اللغة الانجليزية فإننا نخلص إلى أن $d_k(L)=t$.

(٨) الآن، الكلمة $XPCV$ تقابل aPV وأن أكثر الكلمات الثلاثية شيوعاً والتي تبدأ بالحرف a في اللغة الإنجليزية هي كلمة and فإنه لا بد وأن يكون $d_k(P)=n$ و $d_k(V)=d$.

(٩) بما أن أكثر الكلمات الثلاثية التي حرفها الأوسط هو o شيوعاً في اللغة هي كلمة for وأن الكلمة ICJ تكررت في النص المعمى فإننا نخلص إلى أن $d_k(I)=f$ و $d_k(J)=r$.

(١٠) يكون من المناسب الآن كتابة النص المعمى بعد القيام بإستبدال الحروف التي وجدناها لنحصل على:

One QaU of enArUFtYnD SekkaDek QoMRD Ze for the Kender to enArUFt aRR the daUk traIIYA aAAordYnD to the daU EeU thYK QoMRd Sean that for a QhoRe daU at the KtaJt of eaAh SekkaDe aRR enYDSa oFeratorK QoMRd Ket theYr SaAhynek aAAordYnD to the daU EuU then eaAh tYSe a SekkaDe needed to Ze Kent Yt QoMRd ze fyrkt tUFed Ynto the SaAhyne the enAYFnered oMtFMt QoMRd then Ze reAorded and handed to the radyo oFerator for tranKSYKKYon the Aode ZooE Zu KYSon KynDh

(١١) من الواضح الآن أن الكلمة ***Ze*** هي *be*. ولذا فإن $d_k(Z)=b$. كما أن الكلمة ***ZU*** لا بد وأن تكون *by*. ومن ثم فإن $d_k(U)=y$. أما الكلمة ***QaU*** هي *way*. ومنه فإن $d_k(U)=y$. ولذا فإن الكلمة *QaU* هي *way*. ومنه فإن $d_k(Q)=w$. ولذا فإن الكلمة ***daUK*** لا بد وأن تكون *days*. أي أن $d_k(K)=s$. من الواضح أيضاً أن الكلمة ***theYr*** هي *their*. ومنه فإن $d_k(Y)=i$. والكلمة ***eaAh*** لا بد وأن تكون *each*. أي أن $d_k(A)=c$. الآن، الثلاثي ***YnD*** هو ***inD*** ولقد تكرر في النص المعمى. وبما أن *ing* ثلاثي شائع في اللغة الانجليزية فإننا نخلص إلى أن $d_k(D)=g$. وبما أن ***OM*** تردد كثيراً في النص المعمى وأن *ou* ثنائي شائع فإن $d_k(M)=u$. من الواضح الآن أن *wouRd* هي *would*. ولذا فإن $d_k(R)=l$.

(١٢) باستبدال الحروف التي حصلنا عليها في الخطوة (١١) في نص الخطوة (١٠) نستطيع الآن وبسهولة أن نخمن باقي الحروف ومن ثم نقرأ النص وهو:

one way of encrypting messages would be for the sender to encrypt all the day's traffic according to the day key. This would mean that for a whole day at the start of each message all Enigma operators would set their machines according to the day key. Then, each time a message needed to be sent, it would be first typed into the machine; the enciphered output would then be recorded, and handed to the radio operator for transmission.

The code book by Simon Singh

ويكون التبديل المستخدم هو:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
X	Z	A	V	O	I	D	B	Y	G	E	R	S	P	C	F	H	J	K	L	M	N	Q	T	U	W

(٩,٢,٣) تحليل النظام التآلفي (*Cryptanalysis of Affine Cipher*)

إن عدد عناصر فضاء المفاتيح لنظام التعمية التآلفي هو $26\varphi(26) = 312$ ولذا فهو لا يعتبر آمناً. كما أنه من الممكن كسر التعمية باستخدام تحليل التردد وسنوضح ذلك في المثال التالي:

مثال (٩,٩)

إذا استقبلت الرسالة المعماة التالية وعلمت أن النظام المستخدم هو التآلفي فجد النص الواضح للرسالة.

USLJPDLGPLRWJLPYLPXWYRVTGPDL GULHXCUURNF TGUF VPYXCURHYTCSX

الحل

الجدول التالي يبين ترددات حروف النص المعمى

Y	X	W	V	U	T	S	R	P	N	L	J	H	G	F	D	C	الحرف
4	4	2	2	6	3	2	4	6	1	7	2	2	4	2	2	3	التردد

من الجدول أعلاه يتضح لنا أن الحروف الأكثر تردداً في النص المعمى هي على التوالي مرتبة تنازلياً: L وعدد ترددات 7، P و U وتردد كل منهما 6 و G ، R ، X ، Y وتردد كل منها 4.

ولذا فإن التخمين الأول يكون $e_k(e)=L$ و $e_k(t)=P$. ونجد

$$4a+b\equiv 11 \pmod{26}$$
$$19a+b\equiv 15 \pmod{26}$$

بحل هذا النظام نجد أن $(a,b)=(2,3)$ وهو مفتاح غير مقبول لأن $\gcd(2,26)=2\neq 1$. ولذا فإننا ننتقل إلى التخمين الثاني ونجعل $e_k(e)=L$ و $e_k(t)=U$. ويكون

$$4a+b\equiv 11 \pmod{26}$$
$$19a+b\equiv 20 \pmod{26}$$

بحل هذا النظام نجد أن $(a,b)=(11,19)$ وهو مفتاح مقبول لأن $\gcd(11,26)=1$.

حينئذ تكون دالة كشف المعمى.

$$d_k(x)\equiv 11^{-1}(x-19)\equiv 19(x-19)\equiv 19x+3 \pmod{26}.$$

الآن، نستخدم الدالة d_k لإيجاد النص الواضح فإذا حصلنا على نص مقروء نكون قد انتهينا ويكون المفتاح (11,19) هو بالفعل المفتاح المستخدم في عملية التعمية وأما إذا حصلنا على نص ليس له معنى فنقوم بإعادة التخمين حتى نحصل على نص مقروء.

باستخدام المفتاح (11,19) نحصل على النص التالي:

thescienceofsecrecyfromancientegypttoquantumcryptography.

أي

the science of secrecy from ancient Egypt to quantum cryptography.

وبهذا نخلص إلى أن المفتاح (11,19) هو بالفعل المفتاح المستخدم □

ملحوظة

عند محاولة كسر النظام التآلفي بمعرفة النص الواضح فإن معرفة حرفين من النص الواضح وما يقابلهما من النص المعمى يكون في العادة كافياً لكسر النظام أو على الأقل يختزل المفاتيح الممكنة إلى عدد مقبول وبالتالي تكون معرفتنا لبعض الحروف الإضافية كافية لمعرفة المفتاح والمثالان التاليان يوضحان ذلك.

مثال (٩,١٠)

إذا علمت أن النص الواضح في النظام التآلفي يبدأ بالحرفين gr والنص المعمى يبدأ بالحرفين PQ فعين مفتاح التعمية.

الحل

بما أن $e(6)=15$ و $e(17)=16$ فإننا نحصل على التطابقين:

$$6a+b \equiv 15 \pmod{26}$$

$$17a+b \equiv 16 \pmod{26}$$

ومنه $11a \equiv 1 \pmod{26}$. ولذا فإن $a=19$. ونرى أن

$b \equiv -6\times 19+15 \equiv 5 \pmod{26}$ ويكون مفتاح التعمية هو $(a,b)=(19,5)$ □

مثال (٩,١١)

إذا علمت أن النص الواضح في النظام التآلفي يبدأ بالحرفين go والنص المعمى يبدأ بالحرفين PR فعين مفتاح التعمية.

الحل

بما أن $e(6)=15$ و $e(14)=17$ فإننا نحصل على التطابقين:

$$6a+b \equiv 15 \pmod{26}$$

$$14a+b \equiv 17 \pmod{26}$$

وبطرح التطابقين نجد أن $8a \equiv 2 \pmod{26}$. وبما أن $\gcd(8,26) = 2$ يقسم 26 فيوجد حلان لهذا التطابق هما 10 و 23 . وبالتعويض في أحد تطابقي النظام نجد أن $b = 7$ في كلتا الحالتين. ولذا فإن $(a,b) = (23,7)$ هو المفتاح الممكن لأن $\gcd(10,26) \neq 1$ □

(٩,٢,٤) تحليل نظام فيجينير (*Cryptanalysis of Vigenere Cipher*)

إن عدد عناصر فضاء المفاتيح في نظام فيجينير هو "26" وهذا العدد كبير جداً حتى لو كان n صغيراً نسبياً. ولذا فإن النظام يعد آمناً ضد طريقة استنفاد المفاتيح. ولكن من الممكن كسره بمستويات التحليل المختلفة.

(١) معرفة النص الواضح

يسهل كسر النظام بهذه الطريقة خاصة إذا استخدم محلل التعمية نصاً واضحاً طوله كبير نسبياً (على الأقل بطول المفتاح) فإذا كان النص الواضح هو $(x_1, x_2, \dots, x_n)$ والنص المعمى المقابل هو $(y_1, y_2, \dots, y_n)$ فيكون مفتاح التعمية.

$$k = (y_1 - x_1, y_2 - x_2, \dots, y_n - x_n)$$

(٢) اختيار النص الواضح

من السهل كسر النظام بهذه الطريقة أيضاً حيث يقوم محلل التعمية بتعمية العديد $(0,0,0,\dots)$ فيكون النص المعمى الناتج هو مفتاح التعمية. والمشكلة الوحيدة تكمن في الحالة التي يكون طول الرسالة الواضحة أقل من طول المفتاح وبهذه الطريقة يقوم محلل التعمية باختيار عديد طويل نسبياً إلى أن يحصل على نص معمى مكرر وبذلك يستخلص مفتاح التعمية.

(٣) اختيار النص المعمى

يتم كسر التعمية بطريقة مشابهة تماماً لطريقة المعرفة المؤقتة للنص الواضح غير أن العديد (0,0,0,...) يكون في هذه الحالة هو النص المعمى.

(٤) معرفة النص المعمى فقط

إن كسر نظام فيجينير بمعرفة النص المعمى فقط يحتاج إلى مزيد من الحنكة ويتم على مرحلتين: في المرحلة الأولى يقوم محلل التعمية بمحاولة تحديد طول كلمة السر وفي المرحلة الثانية يحاول محلل التعمية معرفة كلمة السر نفسها لكسر النظام . والقارئ المهتم يمكنه الرجوع إلى [1] لمزيد من التفاصيل.

(٩,٢,٥) تحليل نظام هيل (*Cryptanalysis of Hill Cipher*)

(١) كسر النظام باستنفاد المفاتيح

لكسر نظام هيل للتعمية باستنفاد المفاتيح يلزمنا معرفة عدد هذه المفاتيح. أي عدد المصفوفات من الدرجة n القابلة للعكس قياس 26 وهذا العدد يساوي 16×10^{11} عندما $n=3$. (انظر [1]) وهو كبير جداً. ولذا فنظام هيل يعد آمناً باستنفاد المفاتيح.

(٢) كسر النظام بمعرفة النص المعمى فقط

من السهل أن نرى أن تغيير حرف واحد من النص الواضح يتبعه تغيير n من حروف النص المعمى. فإذا استبدلنا الحرف الأول i من النص الواضح المقدم في المثال (٩,٥) بالحرف e يكون لدينا :

$$\begin{bmatrix}23 & 3\\ 10 & 25\end{bmatrix}\begin{bmatrix}4\\ 6\end{bmatrix}\equiv\begin{bmatrix}6\\ 8\end{bmatrix}(\text{mod } 26)$$

أي أن بداية النص المعمى تصبح FH بدلاً من UW . وهذا بدوره يجعل تحليل تردد اللغة الانجليزية بمعرفة النص المعمى فقط صعب جداً (خاصة إذا كان n عدداً كبيراً).

(٣) كسر النظام بمعرفة النص الواضح

من السهل على محلل التعمية كسر نظام هيل بهذه الطريقة. فإذا كان محلل التعمية لا يعرف قيمة n فإنه يجرب قيماً مختلفة حتى يحصل على العدد المستخدم. لنفرض إذن أن محلل التعمية على دراية بقيمة العدد n . عندئذ، يقوم محلل التعمية بتقسيم النص الواضح إلى عديدات من النوع n ثم يختار n من هذه العديدات ولتكن:

$$1 \le j \le n, x_{1j}, x_{2j}, \dots, x_{nj}$$

ثم يجد ما يقابلها من النص المعمى ولتكن:

$$1 \le j \le n \quad Y_{1j}, Y_{2j}, \dots, Y_{nj}$$

عندئذ، يكون:

$$A \begin{bmatrix} x_{1j} \\ x_{2j} \\ \vdots \\ x_{nj} \end{bmatrix} \equiv \begin{bmatrix} Y_{1j} \\ Y_{2j} \\ \vdots \\ Y_{nj} \end{bmatrix} \pmod{26} \quad \text{حيث} \quad 1 \le j \le n$$

أي أن $AX \equiv Y \pmod{26}$ حيث $X = [x_{ij}]$ و $Y = [Y_{ij}]$ مصفوفتان من الدرجة n . فإذا كانت X مصفوفة قابلة للعكس قياس 26 فإن $A \equiv YX^{-1} \pmod{26}$. ومن ثم يكون محلل التعمية قد نجح في إيجاد مفتاح مناسب. أما إذا كانت X غير قابلة للعكس قياس 26 أو أن المفتاح A غير قابل

للعكس قياس 26 فيقوم بتغيير عديدات النص الواضح حتى يحصل على مفتاح مقبول، ومن ثم يستخدمه لقراءة النص.

(٤) كسر النظام باختيار النص الواضح

في هذه الحالة يقوم محلل التعمية باختيار n من عديدات النص الواضح هي:

$$\begin{bmatrix}1\\0\\0\\\vdots\\0\end{bmatrix},\begin{bmatrix}0\\1\\0\\\vdots\\0\end{bmatrix},\begin{bmatrix}0\\0\\1\\\vdots\\0\end{bmatrix},\cdots,\begin{bmatrix}0\\0\\\vdots\\0\\1\end{bmatrix}$$

ويجد ما يقابلها من النص المعمى ولتكن:

$$\begin{bmatrix}a_{11}\\a_{21}\\\vdots\\a_{n1}\end{bmatrix},\begin{bmatrix}a_{12}\\a_{2n}\\\vdots\\a_{n2}\end{bmatrix},\cdots,\begin{bmatrix}a_{1n}\\a_{2n}\\\vdots\\a_{nn}\end{bmatrix}$$

فيكون مفتاح التعمية هو : $A=\begin{bmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\a_{21} & a_{22} & \cdots & a_{2n}\\ & \vdots & & \\a_{n1} & a_{n2} & \cdots & a_{nn}\end{bmatrix}$

(٥) كسر النظام باختيار النص المعمى

يقوم محلل التعمية باختبار العديدات

$$\begin{bmatrix}1\\0\\0\\\vdots\\0\end{bmatrix},\begin{bmatrix}0\\1\\0\\\vdots\\0\end{bmatrix},\cdots,\begin{bmatrix}0\\0\\\vdots\\0\\1\end{bmatrix}$$

من النص المعمى ويجد ما يقابلها من النص الواضح فتكون هذه العديدات هي صفوف مفتاح كسر التعمية.

مثال (٩,١٢)

لنفرض أنك اعترضت رسالة معماة بنظام هيل للتعمية ووجدت أن $n=2$ وأن الثنائيين الأكثر تردداً في النص المعمى هما RH و NI وخمنت أنهما يجب أن يقابلا الثنائيين الأكثر تردداً في اللغة الانجليزية وهما th و he على التوالي. احسب مصفوفة التعمية.

الحل

في هذه الحالة يكون $AX \equiv Y \pmod{26}$ حيث

$$Y=\begin{bmatrix} R & N \\ H & I \end{bmatrix}=\begin{bmatrix} 17 & 13 \\ 7 & 8 \end{bmatrix} \text{ و } X=\begin{bmatrix} t & h \\ h & e \end{bmatrix}=\begin{bmatrix} 19 & 7 \\ 7 & 4 \end{bmatrix}$$

بما أن $\gcd(\det X,26)=\gcd(1,26)=1$ فإن X قابلة للعكس قياس 26 . وبإيجاد معكوس X نجد أن:

$X^{-1}\equiv\begin{bmatrix} 4 & 19 \\ 19 & 19 \end{bmatrix}\pmod{26}$. وبالتالي فإن $A=YX^{-1}\equiv\begin{bmatrix} 3 & 24 \\ 24 & 25 \end{bmatrix}\pmod{26}$

. وبما أن $\gcd(\det A.26)=\det(19,26)=1$ فإن A قابلة للعكس قياس 26 ومن ثم فهي تصلح كمفتاح تعمية □

تمارين (٩,٢)

(١) اقرأ الرسالة التالية المعماة بنظام الإزاحة : *KDKKMU*

(٢) أعد التمرين (١) للرسالة المعماة : *HPHTWWXPPEXTOYTRSE*

(٣) أقرأ الرسالة التالية المعماة بنظام التعويض:

JXRFB	*KXYV*	*BORRSXP*	*RYEO*	*MK*
QXK	*QYRRYPD*	*LC*	*ZO*	*X*
ICCR	*XPV*	*LBO*	*QXU*	*LC*
DOL	*LC*	*LBO*	*JOKOXJAB*	*YK*
LC	*ZO*	*X*	*ICCR*	*ZOAXMKO*
CPRU	*ICCRK*	*EOOF*	*LJUYPD*	*UCM*
BXNO	*YVOX*	*PMSZOJ*	*CPO*	*UCM*
DOL	*OTAYLOV*	*XPV*	*YL*	*IRCFK*
UCM	*DOL*	*YVOX*	*PMSZOJ*	*PYPLU*
PYPO	*UCM*	*DOL*	*OTAYLOV*	*XPV*
YL	*IRCFK*	*CPRU*	*X*	*ICCR*
QCMRV	*ZO*	*OTAYLOV*	*ZU*	*LBO*
YVOX	*PMSZOJ*	*BMPVJOV*	*ZML*	*DCV*
JOQXJVK	*ICCRK*			

(٤) إذا حصلنا على النص المعمى التالي باستخدام النظم التآلفي فعين المفتاح k ودالة كشف المعمى d_k واقرأ الرسالة :

YFXMPCESPZCJTDFDPQFWQZCPYNTASPCTYRXPDDLRPD

(٥) إذا اعترضت الرسالة التالية وكنت على علم مسبق بأنها عُميَّت باستخدام النظام التآلفي فعين المفتاح k ودالة كشف المعمى واقرأ الرسالة :

USLELJUTCCYRTPSURKLTYGGFVELYUSLRYXDJURTUULVCUU
RJRKQLLQLYXSRVLBRYZCYREKLVEXBRYZDGHRGUSLJLIMLYP
DJLJTJUFALGUPTGVTJULYUSLDALTJRWUSLJFEOLPU

(٦) جد النص الواضح للرسالة المعماة التالية علماً بأن النظام المستخدم هو التآلفي:

IEXXKFZKXCUUKZCSTKJW

(٧) جد النص الواضح للرسالة المعماة التالية علماً بأن النظام المستخدم هو النظام التآلفي:

JTUQFUMCTMGXAJ

(٨) عند اعتراضك لرسالة طويلة معماة باستخدام النظام التآلفي لاحظت أن أكثر حرفين تردداً هما Y و V على التوالي. وبفرض أن هذين الحرفين يقابلان الحرفين e و t على التوالي باللغة الانجليزية فجد المفتاح k ودالة كسر التعمية d_k ثم اقرأ الرسالة المعماة :

QAOOYQQEVHEQV

(٩) أثناء اعتراضك المرسالة المعماة: *OFJDFOHFXOL* استخدمت الهجائية الانجليزية مضافاً إليها فراغ (يقابل العدد 26) والنظام التآلفي وعلمت أن أول كلمات الرسالة هي "i –" . عين المفتاح k واقرأ الرسالة.

(١٠) إذا كانت $d_k(x)\equiv 9x+20 \pmod{26}$ هي دالة كشف المعمى للنظام التآلفي فعين دالة التعمية ثم استخدمها لتعمية : *the idea is wonderful* .

(١١) إذا كانت دالة التعمية للنظام التآلفي تحقق $e_k(b)=N$ و $e_k(e)=S$ فعين قاعدة تعريف دالة التعمية ثم استخدمها لتعمية الرسالة: *king Saud university* .

(١٢) إذا اعترض عدوان الرسالة *CVVWPM* المعماة بالنظام التآلفي وعلم أن الرسالة الواضحة تنتهي بالحرفين *ne* فجد مفتاح التعمية والنص الواضح.

(١٣) اقرأ الرسالة التالية المعماة بالنظام التآلفي: *INZKRMRLVPHAFERH*

(١٤) عند اعتراض عدوان لرسالة معماة بالنظام التآلفي وجد أن حرفي النص الواضح nz يقابلان حرفي النص المعمى UA. هل يستطيع عدوان إيجاد مفتاح التعمية؟

(١٥) اقرأ الرسالة التالية المعماة بالنظام التآلفي:

CBCUUILLKBSTYKBVAWCLTCUFXSWCLOHNSEBVALSNBVYLTB VAFCNTUYNAUCLOCLO

(١٦) اقرأ الرسالة التالية المعماة بالنظام التآلفي:

GPWRXERFWYMQQEEXGPFZGYBGLEOWMZCTEFWAWRUTER OZCRXCPXREYDEQFQWIDEFGFGWP

(١٧) إذا علمت أن الحرف الواضح g يقابل الحرف المعمى T في النظام التآلفي فما هي القيم الممكنة لمفتاح التعمية؟

(١٨) هل يمكن تصميم نظام تعمية بدالة تعمية $e(x) \equiv ax^2 + b \pmod{26}$ حيث $\gcd(a,26) = 1$ ؟

(١٩) ليكن $k = (5,18)$ هو المفتاح المستخدم في النظام التآلفي

(أ) جد عدد الحروف التي يثبتها هذا المفتاح.

(ب)إذا علمت أن النص التالي قد عُمي بهذا المفتاح فجد النص الواضح:

EOAAMZGECKAGFW

(٢٠) جد جميع الأزواج (a,b) بحيث تكون دالتا التعمية وكشف المعمى في النظام التآلفي متساويتين.

(٢١) هل تستطيع إيجاد مفتاح k في نظام تآلفي بحيث يكون $e_k(e) = D$ و $e_k(s) = T$؟

(٢٢) إذا اعترضت رسالة معماة بنظام هيل حيث $n=2$ ووجدت أن الثنائيين في النص المعمى KX و VZ يقابلان الثنائيين الأكثر شيوعاً في اللغة الانجليزية وهما th و he على التوالي فاحسب مفتاح التعمية.

(٢٣) إذا اعترضت الرسالة المعماة بنظام هيل حيث $n=2$:

$$RLOQNZOFXMCQKGQIVDAZ$$

وعلمت أن بداية الرسالة الواضحة هو $beware$ فهل يكفي ذلك لقراءة هذه الرسالة؟

(٢٤) اعترض عدوان الرسالة التالية المعماة بنظام هيل :

$$QAIXPXDAFGIDYQJS$$

وعلم أن $n=2$ وأن PX و DA يقابلان الثنائيين ut و te على التوالي. هل يستطيع كسر الرسالة؟

(٢٥) هل يمكن إيجاد مصفوفة من الدرجة 2 تصلح مفتاحاً لنظام هيل بحيث يكون النص المعمى للرسالة الواضحة $stop$ هو $BABW$ ؟

(٢٦) هل يمكن إيجاد مصفوفة من الدرجة 2 تصلح مفتاحاً لنظام هيل بحيث يكون النص المعمى للرسالة الواضحة $hill$ هو $DPLW$ ؟

(٢٧) اعترض عدوان الرسالة التالية المعماة بنظام هيل حيث $n=3$:

$$FBRTLWUGAJQINZHHXTEPHBNXSW$$

واستطاع عدوان أن يعرف أن الرسالة تنتهي بتوقيع المرسل وهو $jamesbond$. هل يستطيع عدوان كسر الرسالة؟

(٢٨) إذا كانت مصفوفة التعمية في نظام هيل حيث $n=2$ تحقق $A^2 \equiv I \pmod{26}$ فأثبت أن A تصلح لأن تكون مصفوفة كشف المعمى.

(٢٩) جد جميع أزواج الحروف التي تبقى ثابتة في نظام هيل حيث مصفوفة التعمية هي $A=\begin{bmatrix}7 & 17\\ 1 & 6\end{bmatrix}$.

(٣٠) أعد التمرين (٢٩) إذا كانت مصفوفة التعمية هي $A=\begin{bmatrix}4 & 5\\ 3 & 1\end{bmatrix}$.

(٣١) أعد التمرين (٢٩) إذا كانت مصفوفة التعمية هي $A=\begin{bmatrix}3 & 5\\ 6 & 3\end{bmatrix}$.

(٩,٣) أنظمة التعمية الحديثة
Contemporary Cryptosystems

إن جميع أنظمة التعمية التقليدية التي درسناها في البند الأول من هذا الفصل هي أنظمة ذات مفاتيح سرية. أي أن كلاً من مفتاح التعمية ومفتاح كشف المعمى يجب أن يكون معلوماً لكل من المرسل (أحمد) والمستقبل (بدر) . على سبيل المثال، من الممكن أن يشتركا في مفتاح التعمية ومن ثم يُستخدم هذا المفتاح لحساب مفتاح كشف المعمى، وفي كثير من الحالات يكون مفتاح التعمية هو مفتاح كشف المعمى نفسه.

إن العقبة الأساسية في أنظمة التعمية التقليدية تكمن في عملية توزيع المفاتيح، ومع التطور الهائل في وسائل الاتصالات واستخدام البريد الإلكتروني في التواصل، أصبحنا في أمس الحاجة إلى التوصل إلى حل مسألة توزيع المفاتيح، إن هذا هو الذي دفع كلاً من وايتفيلد ديفي (*Whitfield Diffie*) ، مارتن هيلمان (*Martin Hellman*) ، رالف ميركل (*Ralph Merkle*) إلى الاستمرار في محاولة

حل هذه المسألة إلى أن توصلوا في العام ١٩٧٤م إلى حلها، كما أنهم وضعوا الفكرة الأساسية لأنظمة تعمية حديثة مفاتيحها غير سرية وتسمى أنظمة التعمية المعلنة المفاتيح. ومن الممكن وصف عمل هذه الأنظمة على النحو التالي:

لنفرض أن أحمد المقيم في الرياض يريد أن يرسل رسالة سرية إلى بدر المقيم في جدة ولكن لم يسبق لهما أن اتفقا على مفتاح سري. من الواضح أنه لا يمكن لأحمد أن يضمن سرية الرسالة دون أن يلتقي ببدر أولا ويتفقا على مفتاح سري أو أن يستخدما أحداً موثوقاً به لتوصيل المفتاح السري. ومن الواضح أيضاً أنه لا يمكن لأحمد أن يستخدم وسيلة اتصال معلنة، مثل الهاتف أو البريد الالكتروني لإرسال المفتاح إلى بدر ومن ثم استخدامه لتعمية الرسالة دون المخاطرة بكشف هذه الرسالة من قبل عدوان. إن حل هذه المسألة هو الدافع الرئيس الذي أدى الى ابتكار أنظمة التعمية المعلنة المفاتيح حيث يكون مفتاح التعمية في هذه الأنظمة معلناً ولكن يصعب على عدوان معرفة مفتاح كشف المعمى دون الوصول إلى معلومات سرية يعرفها بدر فقط .

على الرغم من أن أنظمة التعمية المعلنة المفاتيح حلت المشكلة الرئيسة في نظرية التعمية وهي مسألة توزيع المفاتيح، إلا أن لها سلبياتها، إذ أن عملية التعمية تستغرق في العادة زمناً أطول من نظيرتها في الأنظمة التقليدية ويرجع ذلك إلى العمليات الحسابية المعقدة التي تُجرى لتنفيذ عملية التعمية. ولذا فإن استخداماتها تكون محدودة جداً مثل التوقيع الالكتروني وتوزيع المفاتيح ومن ثم استخدام هذه المفاتيح لتعمية الرسالة باستخدام الأنظمة التقليدية.

إن أهم هذه الأنظمة هو نظام *RSA* الذي يعتمد على صعوبة مسألة تحليل الأعداد. قبل أن ندرس أنظمة التعمية المعلنة المفاتيح نقوم بالتحضير لذلك بدراسة أحد الأنظمة التقليدية وهو نظام القوة ذو المفتاح السري.

(٩,٣,١) نظام القوة (*Exponentiation Cipher*)

يعتمد نظام القوة على إيجاد قوة عدد قياس n وهو نظام سري المفتاح تم اكتشافه من قبل بوليش وهيلمان (*Pohlig and Hellman*) في العام ١٩٧٨م.

تعريف (٩,٨)

ليكن p عدداً أولياً فردياً. وليكن $P=C=\mathbb{Z}_m$ حيث $m\in\mathbb{Z}^+$ وليكن $K=\{(a,b):ab\equiv 1(\mathrm{mod}\,p-1)\}$. لكل $k=(a,b)\in K$ تعرف دالتا التعمية وكشف المعمى على النحو التالي:

$$x\in\mathbb{Z}_m \text{ لكل } e_k(x)\equiv x^a(\mathrm{mod}\,p)$$

$$x\in\mathbb{Z}_m \text{ لكل } d_x(x)\equiv x^b(\mathrm{mod}\,p)$$

سنبرهن الآن دالة كشف المعمى هي بالفعل معكوس لدالة التعمية.

مبرهنة (٩,١)

في نظام القوة للتعمية يكون $d_k(e_k(x))\equiv x(\mathrm{mod}\,p)$ لكل $x\in\mathbb{Z}_m$.

البرهان

بما أن $ab\equiv 1(\mathrm{mod}\,p-1)$ فإن $ab=1+\alpha(p-1)$ حيث $\alpha\in\mathbb{Z}$ ، وباستخدام مبرهنة فيرما الصغرى نجد أن :

- $d_k(e_k(x)) \equiv d_k(x^a) \equiv x^{ab} \equiv x(x^{p-1})^a \equiv x \pmod{p}$

ملحوظة

لاجراء عملية التعمية وكشف المعمى في أنظمة التعمية التي سندرسها في هذا الفصل نقوم بمقابلة حروف الهجائية الانجليزية مع أعداد $\mathbb{Z}_{26}$ ، كما في الأنظمة التقليدية مع ملاحظة جعل جميع الأعداد المقابلة للحروف مكونة من رقمين وذلك بوضع الرقم 0 على اليسار إذا احتاج الأمر إلى ذلك. فمثلاً الحرف b يقابل 01 بدلاً من 1 وهكذا. كذلك، إذا كان العدد المقابل للرسالة أكبر من العدد الأولي p فإننا نقوم بتقسيم العدد المقابل للرسالة إلى مجموعات من الأعداد بحيث يكون العدد في كل مجموعة أصغر من p ، فمثلاً إذا كان $p=1009$ وكانت الرسالة 211208001323 فنقسم الرسالة إلى مجموعات من الأعداد تحتوي كل منها على ثلاثة أرقام مثلاً فنحصل على: 323 208 211 ثم نقوم بتعمية كل مجموعة من مجموعات الأعداد على حدة.

مثال (٩,١٣)

عند استخدام أحمد لنظام القوة حيث $p=101$ و $a=3$ أرسل الرسالة المعماة التالية إلى بدر: 1417172711176576077614. جد الرسالة الواضحة.

الحل

يقوم بدر بحساب $b \equiv a^{-1} \pmod{100}$ مستخدماً خوارزمية إقليدس فيجد أن $b \equiv 67 \pmod{100}$. وعليه فإن دالة كشف المعمى هي $d_k(x) \equiv x^{67} \pmod{101}$. وبتقسيم الرسالة المعماة إلى مجموعات كل منها مكونة

من رقمين وحساب $d_k(x)$ لكل منها يحصل بدر على النص الواضح التالي:

06141403121417130813306 .

وبإيجاد الحروف المكافئة يكون النص الواضح: *good morning* □

ملحوظات

(١) لاحظ أنه إذا حصل محلل التعمية على a و p وعلى جزء من الرسالة الواضحة x وما يقابله من الرسالة المعماة y فلمعرفة مفتاح كشف المعمى b يجب أن يقوم بحل التطابق $y = x^b \pmod p$. أي يلزمه حساب اللوغاريتم المنفصل $b \equiv \log_x(y) \pmod p$ ، وحل هذه المسألة لإيجاد $0 \le b \le p-1$ بمعرفة x ، y ، p يدعى مسألة اللوغاريتم المنفصل (DLP) والنص العام لهذه المسألة هو:

ليكن p عدداً أولياً وليكن $\alpha \in \mathbb{Z}_p^*$ جذراً بدائياً وليكن $\beta \in \mathbb{Z}_p^*$. جد عدداً وحيداً غير سالب $x \le p-2$ بحيث يكون $\alpha^x \equiv \beta \pmod p$.

(٢) إذا كان طول العدد الأولي p يساوي 150 مرتبة عشرية ويوجد على الأقل قاسم أولي كبير للعدد $p-1$ فلا توجد خوارزمية حدودية لحل مسألة اللوغاريتم المنفصل، لأنه من المعتقد أن هذه المسألة تكافيء مسألة التحليل وبهذا يكون نظام القوة آمناً لأنه لا توجد خوارزمية حدودية لتحليل الأعداد (ومن ثم لحساب اللوغاريتم المنفصل). أما إذا كانت جميع القواسم الأولية للعدد $p-1$ صغيرة فإنه توجد خوارزميات حدودية لحساب اللوغاريتم المنفصل وللتفاصيل انظر [1].

(٩,٣,٢) نظام *RSA* للتعمية (*RSA cryptosystem*)

تعتمد أنظمة التعمية معلنة المفاتيح ومنها نظام *RSA* على الدوال وحيدة الاتجاه ذات الباب السري ويمكن تعريف هذه الدوال على النحو التالي:

تعريف (٩,٩)

نقول إن الدالة الأحادية $f: P \to C$ وحيدة الاتجاه (*one-way function*) ، إذا كان "من السهل" حساب $f(x)$ لكل $x \in P$ ولكن إذا كان $y \in \mathrm{Im}(f)$ عشوائياً فإن إيجاد $x \in P$ بحيث يحقق $f(x) = y$ يكون صعباً حسابياً. أي أنه من السهل حساب f ولكن من الصعب حساب f^{-1}.

ملحوظة

لاحظ أن تعريف الدالة وحيدة الاتجاه ليس دقيقاً بالمعنى الرياضي لأنه لا يمكن تقديم تعريف رياضي دقيق لمعنى "صعب حسابياً" . وعلى الرغم من ذلك فالتعريف يؤدي المطلوب منه لغرض التعمية.

إن دالة التعمية المستخدمة في نظام القوة هي دالة وحيدة الإتجاه، حساب معكوسها يعتمد على إيجاد اللوغاريتم المنفصل وهذا صعب حسابياً كما بينا سابقاً.

تعريف (٩,١٠)

لتكن $f: P \to C$ دالة وحيدة الاتجاه. نقول إن f دالة ذات باب سري (trapdoor) أو f دالة تعمية لنظام معلن المفتاح إذا وجدت معلومات سرية (*trapdoor information*) بحيث يصبح من السهل إيجاد $x \in P$ لكل $y \in \mathrm{Im}(f)$ حيث $f(x) = y$ ولكنه يكون من الصعب الحصول على x بدون هذه المعلومات السرية.

نستطيع الآن تقديم تعريف لأنظمة التعمية معلنة المفاتيح.

تعريف (٩,١١)

يتكون نظام التعمية معلن المفتاح من فضاء مفاتيح K ودالتي تعمية وكشف المعمى e_k و d_k لكل $k \in K$ بحيث يكون:

(١) e_k هي معكوس الدالة d_k.

(٢) e_k دالة معلنة و d_k دالة سرية.

(٣) e_k دالة وحيدة الاتجاه.

من الواضح من تعريف (٩,١١) أن أنظمة التعمية معلنة المفتاح تعتمد أساساً على وجود دوال وحيدة الاتجاه، ولقد تبين أن المكان الأنسب للبحث عن مثل هذه الدوال هو نظرية الأعداد مما أتاح لهذه النظرية أن تلعب دوراً أساسياً في أنظمة التعمية الحديثة. سنقدم الآن أول هذه الأنظمة وهو نظام *RSA* ونوضح كيفية استخدامه على مرحلتين هما مرحلة توليد المفاتيح ومرحلة التعمية وكشف المعمى.

توليد مفتاح *RSA* :

يقوم كل من أحمد وبدر بتنفيذ الخطوات التالية:

(١) توليد عددين أوليين عشوائيين $p \neq q$ (ويفضل أن يكونا من الطول نفسه) .

(٢) حساب كل من $n = pq$ و $\varphi(n) = (p-1)(q-1)$. يسمى العدد n مقياس النظام *RSA* .

(٣) اختيار عدد عشوائي a ، $1 < a < \varphi(n)$ بحيث يكون $\gcd(a, \varphi(n)) = 1$. يسمى a عدد قوة التعمية لنظام *RSA* .

(٤) استخدام خوارزمية إقليدس لإيجاد النظير الضربي للعدد a قياس $\varphi(n)$. أي إيجاد العدد الوحيد b، $1<b<\varphi(n)$ الذي يحقق $ab \equiv 1(\mathrm{mod}\ \varphi(n))$. يسمى b عدد قوة كشف المعمى لنظام RSA .

(٥) المفتاح المعلن لنظام RSA هو (n,a) والمفتاح السري هو b ، p ، q .

عمليتا التعمية وكشف المعمى في نظام RSA :

إذا أراد أحمد إرسال رسالة معماة إلى بدر فإنه يقوم بتنفيذ الخطوات التالية:

(١) يحصل أحمد على مفتاح بدر المعلن (n,a).

(٢) يقوم بإيجاد المكافيء العددي لحروف الرسالة.

(٣) يقوم بتقسيم العدد المكافيء للرسالة إلى مجموعات متساوية الطول وليكن l (في العادة l يحقق $26^l < n < 26^{l+1}$).

(٤) يستخدم أحمد دالة التعمية e_k لتعمية مجموعات أعداد النص الواضح x على النحو التالي:

$$y = e_k(x) = x^a (\mathrm{mod}\ n)$$

وذلك باستخدام خوارزمية التربيع.

(٥) يقوم أحمد بإرسال جميع أعداد النص المعمى y إلى بدر.

(٦) عند استلام بدر للرسالة المعماة يقوم باستخدام دالة كشف المعمى d_k للحصول على أعداد النص الواضح x على النحو التالي:

$$x = d_k(y) \equiv y^b (\mathrm{mod}\ n) \ .$$

مثال (٩,١٤)

لنفرض أن أحمد يريد تعمية الرسالة *golden ratio* باستخدام نظام *RSA* حيث $p=23$ ، $q=43$ ، $a=5$. لاحظ أن $n=pd=989$ وأن $\varphi(n)=924$. بما أن $26^2<989<26^3$ فإن أحمد يختار الطول $l=2$. بتحويل الرسالة الواضحة إلى المكافيء العددي وتقسيم المكافيء العددي إلى مجموعات كل منها مكون من رقمين نجد أن :

06 14 11 03 04 13 17 00 19 08 14

يقوم أحمد باستخدام خوارزمية التربيع لحساب $e_k(x)\equiv x^5 \pmod{989}$ لكل x فيجد أن الرسالة المعماة هي:

853 797 833 243 35 418 642 0 632 131 799

ولكشف المعمى يقوم بدر أولاً بحساب النظير الضربي للعدد a قياس $\varphi(n)=924$ مستخدماً خوارزمية إقليدس ليجد أن $b=185$. ومن ثم يقوم بحساب $x=d_k(y)=y^b \pmod{n}$ لكل y ليحصل على الرسالة الواضحة. على سبيل المثال، كشف المعمى 35 يكون على النحو التالي:

$$35^2 = 1225 \equiv 236 \pmod{989}$$
$$35^4 = 55696 \equiv 312 \pmod{989}$$
$$35^8 = 97344 \equiv 422 \pmod{989}$$
$$35^{16} = 178084 \equiv 64 \pmod{989}$$
$$35^{32} = 4096 \equiv 140 \pmod{989}$$
$$35^{64} = 19600 \equiv 809 \pmod{989}$$
$$35^{128} = 654481 \equiv 752 \pmod{989}$$

ولذا فإن: $d_k(35)\equiv 35^{185}=35^{128}\times 35^{32}\times 35^{16}\times 35^8\times 35\equiv 4 \pmod{989}$ □

ملحوظات

(١) لاحظ أن العددين الأوليين في المثال (٩,١٤) صغيران ، ولذا كان من السهل حساب داليّ التعمية وكشف المعمى باستخدام آلة حاسبة عادية. ولكن في التطبيقات الحقيقية يكون طول كل من p و q يساوي 154 مرتبة عشرية (512 مرتبة ثنائية) . ولذا فإن طول n يساوي 308 مرتبة عشرية (1024 مرتبة ثنائية). وفي هذه الحالة يتم حساب كل من دالة التعمية وكشف المعمى باستخدام برامج مثل *Mathematica* أو *Maple* .

(٢) لتنفيذ نظام *RSA* نحتاج إلى توليد a عشوائياً، كما نحتاج إلى توليد عددين أوليين p و q كبيرين بطريقة عشوائية. إحدى طرائق توليد الأعداد الأولية العشوائية تتم أولاً بتوليد عدد صحيح فردي كبير جداً وليكن m ثم نقوم باستخدام أحد اختبارات الأوليات لاختبار أولية m ، فإذا كان m مؤلفاً فإننا نختبر $m+2$ ونستمر على هذا المنوال حتى نحصل على عدد أولي أكبر من أو يساوي m.

(٣) إذا كان المكافيء العددي x للرسالة الواضحة أكبر من n فإنه من المهم أن نقسم الرسالة x إلى مجموعات من الأعداد كل منها أصغر من n (كما هو مبين في الخطوة (٣) من الخوارزمية) ، وإلا فإنه عند كشف المعمى لن نحصل على العدد x مرة أخرى، ويعود السبب إلى أننا عند تعمية x نقوم باختزاله قياس n . على سبيل المثال ، إذا كان $x=ij=0809$ ، $p=7$ ، $q=5$، $n=35$ ، $\varphi(n)=24$ ، $a=b=5$ فإن $x>n$. ويكون:

$y = e_k(x) \equiv 809^5 \equiv 9 \pmod{35}$ وعليه فإن $d_k(y) \equiv 9^5 \equiv 04 \pmod{35}$.

أي أن $d_k(y) = e$ وليس ij .

سنبرهن الآن أن e_k هي بالفعل معكوس الدالة d_k في نظام RSA .

مبرهنة (٩,٢)

إذا كان $n = pq$ حيث p ، q عددان أوليان وكانت $e_k(x) \equiv x^a \pmod{n}$ ، $d_k(x) \equiv x^b \pmod{n}$ حيث $ab \equiv 1 \pmod{\varphi(n)}$ فإن $d_k(e_k(x)) \equiv x \pmod{n}$ لكل x .

البرهان

بما أن $d_k(e_k(x)) \equiv d_k(x^a) \equiv x^{ab} \pmod{n}$ فيكفي إثبات أن $x^{ab} \equiv x \pmod{n}$. ولإنجاز ذلك نبرهن أن $x^{ab} \equiv x \pmod{p}$ وأن $x^{ab} \equiv x \pmod{q}$ ومن نحصل على المطلوب. لبرهان أن $x^{ab} \equiv x \pmod{p}$ لاحظ أولاً أن $ab \equiv 1 \pmod{\varphi(n)}$. عندئذ، $ab - 1 = t\varphi(n)$ حيث $t \in \mathbb{Z}$.

أي أن $ab = 1 + t(p-1)(q-1)$.

لنفرض أولاً أن $\gcd(x,p) > 1$ (أي أن $p \mid x$). عندئذ ، $x \equiv 0 \pmod{p}$ و $x^{ab} \equiv 0 \pmod{p}$. أما إذا كان $\gcd(x,p) = 1$ فنرى أن

$$\begin{aligned} x^{ab} &\equiv x^{1+t(p-1)(q-1)} \pmod{p} \\ &\equiv x\,(x^{p-1})^{t(q-1)} \pmod{p} \\ &\equiv x\,(1)^{t(q-1)} \pmod{p} \\ &\equiv x \pmod{p} \end{aligned}$$

وبالمثل $x^{ab} \equiv x \pmod{q}$ ◆

(٩,٣,٣) أمن نظام *RSA* (*Security of RSA system*)

يعتمد أمن نظام *RSA* على مسألة تدعى مسألة *RSA* وتوصف على النحو التالي:

ليكن $n = pq$ حيث p و q عددان أوليان فرديان مختلفان. وليكن $a \in \mathbb{Z}^+$ بحيث يكون $\gcd(a, \varphi(n)) = 1$ وليكن $y \in \mathbb{Z}^+$. عين عدداً صحيحاً x يحقق $x^a \equiv y \pmod{n}$.

لاحظ أن مسألة *RSA* تكافيء مسألة إيجاد $\sqrt[a]{y} \pmod{n}$.

لكسر نظام *RSA* يكون على محلل التعمية الحصول على x حيث $x^a \equiv y \pmod{n}$. أي يجب على محلل التعمية حل مسألة *RSA* . هناك إجماع عام على أن مسألة *RSA* تكافيء مسألة تحليل العدد n ولكنه لا يوجد برهان لذلك. وعليه إذا استطاع محلل التعمية أن يحلل العدد n فإنه يكون قد كسر نظام *RSA* . نناقش هنا هذه المسألة ونستعرض طرائق أخرى معلومة لمحاولة كسر نظام *RSA* .

(١) تحليل نظام *RSA* بمعرفة $\varphi(n)$.

إن معرفة $\varphi(n)$ تكافيء تحليل العدد n ومن ثم يتم كسر النظام. وهذا ما توضحه المبرهنة التالية:

مبرهنة (٩,٣)

ليكن $n = pq$ حيث p و q عددان أوليان فرديان مختلفان. عندئذ ، إن معرفة $\varphi(n)$ تكافيء تحليل n .

البرهان

لنفرض أن $n=pq$ و $\varphi(n)$ معلومان. بما أن $\varphi(n)=(p-1)(q-1)$

وأن $q=\frac{n}{p}$

فإن $\varphi(n)=(p-1)\left(\frac{n}{p}-1\right)=(p-1)\left(\frac{n-p}{p}\right)$.

ونرى أن $p\varphi(n)=(p-1)(n-p)pn-p^2-n+p$. أي أن

$p^2+[\varphi(n)-n-1]p+n=0$. وبحل المعادلة التربيعية نحصل على p و q .

برهان العكس واضح لأنه لو كان $n=pq$ تحليلاً للعدد n فإننا نستطيع حساب $\varphi(n)$ من الصيغة $\varphi(n)=(p-1)(q-1)$ ◆

ملحوظة

لاحظ أن جذري المعادلة $p^2+[\varphi(n)-n-1]p+n=0$ هما العددان p و q حيث $n=pq$.

مثال (٩,١٥)

لنفرض أن $n=89747027$ وأن عدوان استطاع معرفة أن $\varphi(n)=89728056$ فاحسب كلاً من p و q .

الحل

بالتعويض في المعادلة $p^2+[\varphi(n)-n-1]p+n=0$ نجد أن:

$p^2-18972p+89747027=0$ وبحل هذه المعادلة نحصل على $p=8999$ أو $p=9973$ □

(٢) تحليل نظام *RSA* بمعرفة b

إن معرفة b تؤدي إلى وجود خوارزمية لتحليل n ومن ثم كسر النظام، كما هو مبين في المبرهنة التالية:

مبرهنة (٩,٤)

ليكن $n=pq$ حيث p و q عددان أوليان فرديان مختلفان، عندئذ ، تحليل n يكافيء معرفة b .

البرهان

لنفرض أن p و q معلومان. عندئذ، نستطيع حساب $\varphi(n)=(p-1)(q-1)$ ومن ثم نستخدم خوارزمية إقليدس لحساب b حيث $ab\equiv 1(\mathrm{mod}\ \varphi(n))$.

ولبرهان العكس ، نفرض أن b معلوم. بما أن $ab\equiv 1(\mathrm{mod}\ \varphi(n))$ فإن $ab-1=k\varphi(n)$ حيث $k\in\mathbb{Z}$. ومنه نجد أن $x^{ab-1}=(x^{\varphi(n)})^k\equiv 1(\mathrm{mod}\ n)$.

بوضع $ab-1=2^j m$ حيث m عدد فردي نجد أن $x^{2^j m}\equiv 1(\mathrm{mod}\ n)$. الآن نبحث عن x الذي يحقق أيضاً $x^{2^{j-1}m}\not\equiv \pm 1(\mathrm{mod}\ n)$. فيكون $\gcd(x^{2^{j-1}m}-1,n)>1$ أو $\gcd(x^{2^{j-1}m}+1,n)>1$. وبالتالي نحصل على تحليل n ◆

(٣) تحليل النظام باستخدام قوة صغيرة a لدالة التعمية.

عند التطبيق العملي لنظام *RSA* يكون من المناسب اختيار قوة صغيرة a لدالة التعمية لتسريع عملية التعمية، فمثلاً إذا كان $a=3$ فإن عملية التعمية تكون سريعة جداً حيث يلزمنا لتنفيذها عملية ضرب واحدة وعملية تربيع واحدة قياس n

. ولكن مثل هذا الاختيار يقلل من أمن النظام، ولرؤية ذلك، نفرض أن أحمد يريد إرسال الرسالة نفسها لعدد من الأشخاص مستخدماً المفتاح المعلن لكل منهم لتعمية الرسالة. إذا اعترض عدوان هذه الرسائل وكان عددها أكبر من أو يساوي $a=3$ فيكون بإمكانه كسر النظام، على سبيل المثال، إذا كانت الرسائل هي:

$$y_1 = e_{k_1}(x) \equiv x^3 (\text{mod } n_1)$$
$$y_2 = e_{k_2}(x) \equiv x^3 (\text{mod } n_2)$$
$$y_3 = e_{k_3}(x) \equiv x^3 (\text{mod } n_3)$$

وبما أن الأعداد n_1, n_2, n_3 أولية نسبياً زوجاً زوجاً على الأرجح فإن عدوان يستطيع استخدام مبرهنة الباقي الصينية لإيجاد الحل الوحيد $0 \le z < n_1 n_2 n_3$ للنظام:

$$z \equiv y_1 (\text{mod } n_1)$$
$$z \equiv y_2 (\text{mod } n_2)$$
$$z \equiv y_3 (\text{mod } n_3)$$

وبما أن $x^3 < n_1 n_2 n_3$ فنرى $x^3 = z$. وبالتالي يمكن إيجاد x بأخذ الجذر التكعيبي للعدد z.

(٩,٣,٤) نظام رابن للتعمية (*Rabin Cryptosystem*)

إن الصفة الأهم التي يجب أن يتمتع بها أي نظام تعمية معلن المفتاح هي أن تكون مسألة تحليل النظام مكافئة لمسألة حسابية معروف أنها صعبة الحل. فأمن نظام *RSA* يعتمد على صعوبة مسألة تحليل العدد n ، إلا أنه لا يوجد برهان على أن هاتين المسألتين متكافئتين. أما نظام رابن فيعتمد أمنه على مسألة إيجاد الجذور التربيعية للرواسب التربيعية قياس n التي قدمناها في الفصل الثامن ويوجد برهان

على أن هذه المسألة تكافيء مسألة تحليل العدد n ومن ثم يكون لدينا نظام تعمية معلن المفتاح آمن (انظر [1]) .

وإليك خوارزميتي توليد مفاتيح نظام رابن وعملية التعمية وكشف المعمى.

توليد مفتاح نظام رابن :

يقوم كل من أحمد وبدر بتنفيذ الخطوات التالية:

(١) توليد عددين أوليين عشوائيين مختلفين p و q لهما الطول نفسه.

(٢) حساب $n = pq$. العدد n هو مقياس نظام رابن.

(٣) المفتاح المعلن هو n والمفتاح السري هو p و q .

عمليتا التعمية وكشف المعمى في نظام رابن:

إذا أراد أحمد إرسال رسالة إلى بدر فإنه يقوم بتنفيذ الخطوات التالية:

(١) يحصل أحمد على مفتاح بدر المعلن n.

(٢) يقوم بإيجاد المكافيء العددي للنص الواضح في المجال $0,1,2,\ldots,n-1$.

(٣) يستخدم أحمد دالة التعمية e_k لتعمية النص الواضح x على النحو التالي:

$$y = e_k(x) \equiv x^2 \pmod{n}$$

(٤) يقوم أحمد بإرسال y إلى بدر.

(٥) عند استلام بدر لرسالة أحمد المعماة يقوم باستخدام دالة كشف المعمى

$$x = d_k(y) \equiv \sqrt{y} \pmod{n}$$

لإيجاد الجذور التربيعية الأربعة x_1,x_2,x_3,x_4 فيكون النص الواضح هو أحد هذه الجذور التربيعية.

ملحوظة

من الواضح أن بدر سيواجه مشكلة معرفة أي من الجذور الأربعة x_1 ، x_2 ، x_3 ، x_4 هو الرسالة الواضحة. إذا كُشِف المعمى إلى لغة مقروءة فإن هذه المشكلة سهلة الحل. أما إذا كُشف المعمى إلى كلمات ثنائية غير مفهومة فمن الممكن ألا توجد وسيلة سهلة لمعرفة الجذر التربيعي المقابل للنص الواضح. توجد طرائق عديدة للتغلب على هذه المشكلة، إحداها هي قيام أحمد بتذييل الرسالة الواضحة بمعلومات إضافية قبل عملية التعمية. على سبيل المثال، إضافة كلمة ثنائية ثابتة الطول في نهاية الرسالة. وعند استلام بدر للرسالة المعماة وإيجاد الجذور التربيعية الأربعة فإنه وباحتمال كبير جداً يكون واحد فقط من هذه الجذور يحتوي على المعلومات الإضافية ومن ثم يختاره بدر على أنه الرسالة الواضحة.

مثال (٩,١٦)

أراد أحمد تعمية الرسالة $x=1101$ مستخدماً نظام رابن حيث $n=11021=103\times107$ وقبل إجراء عملية التعمية ذيل الرسالة بأن كرر الثلاث مراتب الأخيرة منها. بين كيف يتمكن بدر من معرفة النص الواضح x بعد كشف المعمى للرسالة التي استقبلها.

الحل

يقوم أحمد بتعمية الرسالة $x'=1101101=109$ ليحصل على :

$$(x') \equiv (109)^2 \equiv 860 (\text{mod } 11021)$$

عند استلام بدر الرسالة يقوم بحساب الجذور التربيعية للعدد 860 قيـــاس 11021 على النحو التالي:

بما أن

$$\left(\frac{860}{103}\right) = \left(\frac{36}{103}\right) = \left(\frac{6}{103}\right)^2 = 1$$

$$\left(\frac{860}{107}\right) = \left(\frac{4}{107}\right) = \left(\frac{2}{107}\right)^2 = 1$$

فإن $860 \in \mathbb{Q}_{103}$ ، $860 \in \mathbb{Q}_{107}$. ولذا فإن $860 \in \mathbb{Q}_{11021}$. وبحل التطابقات :

$$x^2 \equiv 860 \equiv 36 (\text{mod } 103)$$

$$x^2 \equiv 860 \equiv 4 (\text{mod } 107)$$

نجد أن $x \equiv \pm 6 (\text{mod } 103)$ وأن $x \equiv \pm 2 (\text{mod } 107)$. وباستخدام مبرهنة الباقي الصينية لحل كل من الأنظمة :

(أ) $x \equiv 6 (\text{mod } 103)$ ، $x \equiv 2 (\text{mod } 107)$

(ب) $x \equiv 6 (\text{mod } 103)$ ، $x \equiv -2 (\text{mod } 107)$

(ج) $x \equiv -6 (\text{mod } 103)$ ، $x \equiv 2 (\text{mod } 107)$

(د) $x \equiv -6 (\text{mod } 103)$ ، $x \equiv -2 (\text{mod } 107)$

يحصل بدر على الجذور التربيعية:

$$x_1 = 212 = 11010100$$

$$x_2 = 109 = 1101101$$

$$x_3 = 10912 = 10101010100000$$

$$x_4 = 10809 = 10101000111001$$

وبملاحظة أن x_2 هو الوحيد من بينها الذي تكررت مراتبه الثلاث الأخيرة فإن بدر يستنتج أن $x' = 1101101$ ومن ثم فإن $x = 1101$ □

(٩,٣,٥) خطة ديفي وهيلمان لتبادل المفاتيح

(Diffie – Hellman Key Exchange Protocol)

تعد هذه الخطة أول وأفضل خطة وضعت لتبادل المفاتيح السرية عبر قنوات مفتوحة. جاء اكتشاف هذه الخطة بعد محاولات عديدة من قبل ديفي وهيلمان لحل مشكلة توزيع المفاتيح، وحفز هذا الاكتشاف العديد من الباحثين حيث تم إجراء العديد من التعديلات على هذه الخطة إضافة إلى اكتشاف المزيد من الخطط المختلفة الأخرى. ومن الممكن وصف هذه الخطة على النحو التالي:

إن أراد أحمد وبدر إنشاء مفتاح سري لإستخدامه في عملية التعمية فإنهما ينفذان ما يلي:

(١) يتفقان على عدد أولي p كبير جداً (طوله 1024 مرتبة ثنائية) وعلى عنصر بدائي $\alpha \in \mathbb{Z}_p^*$ ويعلنان كلاً من p و α .

(٢) يختار أحمد عدداً سرياً x ويختار بدر عدداً سرياً y بحيث يكون $1 \le x \le p-2$ و $1 \le y \le p-2$.

(٣) يقوم أحمد بحساب $\alpha^x \pmod p$ ويرسل الناتج إلى بدر ويقوم بدر بحساب $\alpha^y \pmod p$ ويرسل ناتج ذلك إلى أحمد .

(٤) يقوم كل من أحمد وبدر بحساب المفتاح السري k كالتالي:

$$k = (\alpha^y)^x \equiv (\alpha^x)^y \pmod p$$

إذا اعترض عـــدوان الرســـالتين $\alpha^x \pmod p$ و $\alpha^y \pmod p$ فإنـــه لا يستطيع معرفة المفتاح k لأنه يتوجب عليه حساب $\alpha^{xy} \pmod p$. أي حـــل مسألة ديفي وهيلمان وهي كما بينا سابقاً من المسائل الصعبة. ولكـــن عـــدوان يستطيع قراءة رسائل أحمد وبدر بطريقة تدعى الهجوم المتطفل (*intruder attack*) والتي يمكن انجازها بتنفيذ الخطوات التالية:

(١) يختار عدوان عدداً z.

(٢) يقوم عدوان باعتراض الرسالتين α^x و α^y .

(٣) يقوم عدوان بإرسال α^z إلى كل من أحمد وبدر (يعتقد أحمد أنه اســـتقبل α^y ويعتقد بدر أنه استقبل α^x).

(٤) يقـــوم عـــدوان بحـــساب كـــل مـــن $k_{AO} \equiv (\alpha^x)^z \pmod p$ و $k_{OB} \equiv (\alpha^y)^z \pmod p$.

(٥) ولاعتقاد أحمد أنه استقبل α^y فإنه يقوم بحساب $k_{AO} \equiv (\alpha^z)^x \pmod p$.

(٦) وبالمثل يقوم بدر بحساب $k_{OB} \equiv (\alpha^z)^y \pmod p$.

(٧) لنفرض الآن أن أحمد يريد إرسال رسالة m إلى بدر فإنه يستخدم المفتـــاح k_{AO} ويقوم بإرسال $e_{k_{AO}}(m)$.

(٨) يعترض عدوان الرسالة $e_{k_{AO}}(m)$ ويعيد تعميتها باستخدام المفتاح k_{AO} . ثم يقرأ الرسالة ويعيد تعميتها باستخدام المفتاح k_{OB} ويرسل $e_{k_{OB}}(m)$ إلى بدر الذي يعيد تعميتها باستخدام مفتاح إعادة التعمية $d_{k_{OB}}$ دون أن يعلـــم أن هناك من اعترضها.

يوجد العديد من الخطط لتجنب مثل هذا الهجوم (انظر [1]).

تمارين (٩,٣)

(١) استخدم نظام القوة لإيجاد النص الواضح للرسالة *BJAMMJYK* حيث $p=29$ و $a=5$.

(٢) استخدم نظام القوة لإيجاد النص الواضح للرسالة :

1213 0902 0509 1208 1234 1103 1374

حيث $p=2591$ ، $a=13$.

(٣) استخدم نظام القوة لإيجاد النص الواضح للرسالة :

2199 1745 1745 1206 2437 2425 1729
1619 0935 0960 1072 1541 1701 1553
0735 2064 1351 1704 1841 1459

حيث $p=2633$ ، $a=29$.

(٤) إذا اعترض عدوان الرسالة التالية المعماة بنظام القوة حيث $p=29$.

04 19 19 11 04 24 09 15 15

وعلم أن النص المعمى 24 يقابل النص الواضح 20 فهل يستطيع عدوان إيجاد الرسالة الواضحة؟

(٥) إذا كان $p=31$ ، $a=11$ في نظام القوة فجد مفتاح كشف المعمى b .

(٦) استخدم نظام *RSA* لتعمية الرسالة : *no such agency* إذا علمت أن

$n=97\times167=16199$ و $b=11957$.

(٧) اقرأ الرسالة التالية المعماة بنظام *RSA* علماً بأن $n=43\times59=2537$ وأن $a=13$ وأن $l=4$.

0095 1648 1410 1299 0811 2333 2132 0370 1185 1457 1084

وعلماً بأن $l=4$.

(٨) أعد التمرين (٧) إذا كان $n=2669$ للرسالة المعماة:

1215 1224 1471 0023 0116

(٩) استخدم نظام *RSA* لتعمية الرسالة *"small encryption exponents"* علماً بأن $n=18923$ ، $b=1216$ ، $l=2$.

(١٠) استخدم نظام *RSA* لتعمية الرسالة:

"if I feel unhappy I do mathematics to become happy, if I am happy I do mathematics to keep happy"

علماً بأن $n=31313$ ، $a=4913$ ، $l=3$.

(١١) إذا كانت قوة التعمية $a=\frac{\varphi(n)}{2}+1$ في نظام *RSA* فأثبت أن $e_k(x)\equiv x \pmod n$ ومن ثم فإنه يمكن كسر النظام في هذه الحالة.

(١٢) قام أحمد بإرسال الرسالة المعماة $y\equiv x^a \pmod n$ بنظام *RSA* إلى بدر. اعترض عدوان الرسالة وقام باستبدالها بالرسالة $y'\equiv yz^a \pmod n$ حيث z عدد عشوائي أولي نسبياً مع n اختاره عدوان وأرسل y' إلى بدر . عند استقبال بدر لهذه الرسالة قام بحساب $x'\equiv (y')^b \pmod n$ وأعاد x' إلى أحمد ، بين كيف يتمكن عدوان من الحصول على الرسالة الواضحة x (ومن ثم كسر النظام) بمعرفة x'.

(١٣) إذا استطاع عدوان أن يحصل على نص واضح x في نظام *RSA* بحيث يكون $\gcd(x,n)>1$ فهل يستطيع أن يكسر النظام؟

(١٤) ليكن $n=pq$ حيث p و q عددان أوليان فرديان مختلفان وليكن $\lambda=lcm(p-1,q-1)$.

(أ) هل $\lambda=\varphi(n)$ ؟ لماذا؟

(ب) هل يمكن تصميم نظام تعمية معلن المفتاح يشبه نظام RSA باستخدام λ عوضاً عن $\varphi(n)$؟

(ج) إذا كانت إجابة الفقرة (ب) "نعم" فأثبت أن $d_k(e_k(x))=x$ لكل $x \in \mathbb{Z}_n$.

(١٥) استخدم نظام رابن لتعمية الرسالة $x=101110$ بعد تذيلها بتكرار الثلاث مراتب الأخيرة حيث $n=5177=31\times167$. بين كيف يتمكن بدر من معرفة النص الواضح عند كشف الرسالة المعماة.

(١٦) استقبل بدر الرسالة المعماة التالية بنظام رابن حيث $n=77$: 1000111 . إذا علم أن أحمد قد ذيل النص الواضح بتكرار المرتبتين الأخيرتين فهل يستطيع بدر الحصول على النص الواضح قبل تذيله؟

(١٧) استقبل بدر الرسالة المعماة 42 بنظام رابن حيث $n=209=11\times19$. جد جميع النصوص الواضحة الممكنة.

نبذة عن حياة رون رايفست
Biography of Ron Rivest



ولد : عام ١٩٤٧ في نيويورك

حصل رون رايفست على درجة البكالوريوس في الرياضيات من جامعة ييل في العام ١٩٦٩م وعلى درجة الدكتوراه في علوم الحاسب في العام ١٩٧٤م من جامعة ستانفورد.

يعمل رون رايفست حالياً أستاذاً في قسم الهندسة الكهربائية وعلوم الحاسب في معهد مساشوتستس للتقنية (*MIT*) . شارك في تأليف كتاب مقدمة في الخوارزميات. كما أنه عضواً في مختبر علوم الحاسب والذكاء الإصطناعي للمعهد. إن أهم انجازاته العلمية هو مشاركته مع شامير وأدلمان (*Shamir and Adleman*) في اكتشاف نظام التعمية ذو المفتاح المعلن *RSA* الذي أدى إلى فوزهم بجائزة تورينغ (*Turing*) في العام ٢٠٠٢م.

ومن انجازاته أيضاً اكتشافه لخوارزميات التعمية *RC2* ، *RC4* ، *RC5* ومشاركته في اكتشاف الخوارزمية *RC6* لأنظمة التعمية متماثلة المفاتيح. كما أنه مكتشف دوال التمويه التعمية *MD2* ، *MD4* ، *MD6* .

علاوة على جائزة تورينغ فقد حصل رون رايفست على العديد من الجوائز الأخرى منها: جائزة كوجي كوبياشي (*Koji Kobayashi*) في الحاسبات ووسائل الاتصال في العام ٢٠٠٠م، جائزة أمن المعلومات ، جائزة *MITC* عن انجازاته العلمية في العام ٢٠٠٥م. كما حصل على درجة الدكتوراه الفخرية من جامعة روما.

الفصل العاشر

تطبيقـــات
APPLICATIONS

قدمنا في الفصل التاسع مبادئ في علم التعمية كتطبيق على نظرية الأعـــداد وفي هذا الفصل ، اخترنا أربع تطبيقات أخرى هي المربع الـــسحري ، والأعـــداد العشوائية وجَدْل كوابل الهاتف وتطبيق على صيغة موبياس للتعاكس.

(١٠,١) المربعات السحرية
Magic Squares

المربع السحري من الدرجة n هو عبارة عن شبكة مربعة تحوي الأعداد من 1 إلى n^2 بحيث يكون مجموع الأعداد في كل صف أو عمود أو أي من القطرين متساوياً ويساوي عدداً T . نوضح الفكرة من خلال المثالين التاليين:

مثال (١٠,١)

المربع التالي هو مربع سحري من الدرجة 3

8	1	6
3	5	7
4	9	2

لاحظ أن المربع يحوي الأعداد 1 إلى 9 وإن $T=15$ □

مثال (١٠,٢)

المربع التالي هو مربع سحري من الدرجة 4

1	14	15	4
12	7	6	9
8	11	10	5
13	2	3	16

يحوي هذا المربع الأعداد من 1 إلى 16 ، كما أن $T=34$ □

تزودنا المبرهنة التالية بصيغة لحساب T للمربع السحري من الدرجة n .

مبرهنة (١٠,١)

إذا كان S مربعاً سحرياً من الدرجة n فإن $T=\frac{n(n^2+1)}{2}$.

البرهان

باستخدام الاستقراء الرياضي على n نعلم أن:

$$1+2+3+\ldots+n^2=\frac{n^2(n^2+1)}{2}$$

لذا فإن مجموع جميع أعداد المربع السحري من الدرجة n يساوي $\frac{n^2(n^2+1)}{2}$. وبما أن مجموع أعداد أي صف من صفوف المربع يساوي T وعدد هذه الصفوف يساوي n فنرى أن مجموع أعداد المربع يساوي nT .

إذن، $nT=\frac{n^2(n^2+1)}{2}$. ويكون $T=\frac{n(n^2+1)}{2}$ ◆

إن عملية انشاء مربعات سحرية من درجة محددة n قد شغلت الكثيرين من علماء الرياضيات مثل فيرما وأويلر بالإضافة إلى الآلاف من الهواة. ولقد ابتكرت طرائق عديدة لإنشاء مربعات سحرية من درجة محددة ومع ذلك عجزت جميع هذه الطرائق عن احصاء جميع المربعات السحرية من الدرجة n .

في هذا البند سنعرض طريقة لإنشاء مربعات سحرية تعتمد على فكرة التطابقات وأنظمة الرواسب قياس العدد n . ولكن قبل البدء بشرح هذه الطريقة دعنا نعرض بعض الحقائق والأفكار التي سنستعين بها.

مبرهنة (١٠,٢)

يمكن كتابة أي عدد من 1 إلى n^2 بطريقة وحيدة على الصورة :

$$nq+r \quad \text{حيث} \quad 0\le q\le n-1 \quad \text{و} \quad 1\le r\le n$$

البرهان

لنفرض أن $1\le x\le n^2$. عندئذ ، استناداً إلى خوارزمية القسمة يوجد عددان وحيدان q_1 و r_1 يحققان

$$x-1=nq_1+r_1 \quad \text{حيث} \quad 0\le r_1\le n-1 \ .$$

ومن ذلك نرى أن $x = nq_1 + (r_1 + 1)$. وبوضع $q = q_1$ و $r = r_1 + 1$ نجد أن

$x = nq + r$ حيث $0 \le q \le n-1$ و $1 \le r \le n$.

ولبرهان الوحدانية نفرض أن

$x = nq + r$ حيث $0 \le q \le n-1$ و $1 \le r \le n$

وأن

$x = nq_1 + r_1$ حيث $0 \le q_1 \le n-1$ و $1 \le r_1 \le n$.

عندئذ ، $x - 1 = nq + (r-1)$ و $x - 1 = nq_1 + (r_1 - 1)$

ومن وحدانية خوارزمية القسمة نجد أن $q = q_1$ و $r - 1 = r_1 - 1$ ويكون $q = q_1$ و $r = r_1$ ◆

تعريف (١٠,١)

إذا كان $x = nq + r$ حيث $1 \le x \le n^2$ ، $0 \le q \le n-1$ ، $1 \le r \le n$ فإننا نسمي العدد q المركبة الأولى للعدد x والعدد r المركبة الثانية للعدد x .

نقدم الآن فكرة المربعات المساعدة التي ستعيننا في إنشاء المربعات السحرية .

تعريف (١٠,٢)

لتكن S شبكة مربعة تحوي الأعداد من 1 إلى n^2 . المربع الناشيء من S بكتابة المركبة الأولى للأعداد من 1 إلى n^2 يسمى مربعاً مساعداً من النوع الأول ونرمز له بالرمز A_1 ، والمربع الناشيء من S بكتابة المركبة الثانية للأعداد من 1 إلى n^2 يسمى مربعاً مساعداً من النوع الثاني ونرمز له بالرمز A_2 .

مثال (١٠,٣)

المربعات المساعدة للمربعين السحريين الـــواردين في المثـــالين (١٠,١) و (١٠,٢) هي :

2	0	1
0	1	2
1	2	0

A_1

2	1	3
3	2	1
1	3	2

A_2

0	3	3	0
2	1	1	2
1	2	2	1
3	0	0	3

A_1

1	2	3	4
4	3	2	1
4	3	2	1
1	2	3	4

A_2

□

ملحوظة

في المثال (١٠,٣) لاحظ أن المربعات المساعدة لها خاصية ثبات المجمـــوع للصفوف والأعمدة والقطرين ،كما في المربع السحري ولكن هذا ليس بالضرورة صحيحاً في كل المربعات السحرية وهو ما يوضحه المثال التالي:

مثال (١٠,٤)

المربعان المساعدان للمربع السحري

1	2	15	16
12	14	3	5
13	7	10	4
8	11	6	9

هما

1	2	3	4
4	2	3	1
1	3	2	4
4	3	2	1

A_2

0	0	3	3
2	3	0	1
3	1	2	0
1	2	1	2

A_1

لاحظ ، على سبيل المثال ، أن مجموع أعداد الصف الأول في المربع A_1 يساوي 6 أما مجموع أعداد أحد القطرين يساوي 7 □

ملحوظة

سنشير إلى المربعات المساعدة التي تتمتع بخاصة ثبات المجموع للصفوف والأعمدة والقطرين بالمربعات السحرية المساعدة.

إن فكرة الخوارزمية اليت نستخدمها في هذا البند لإنشاء مربعات سحرية تستند إلى الحقيقة التي تتضمنها المبرهنة التالية:

مبرهنة (١٠,٣)

إذا كان A_1 و A_2 مربعين سحريين مساعدين من النوع الأول والثاني للشبكة المربعة S من الدرجة n فإن S تشكل مربعاً سحرياً بشرط أن تكون أعداد S جميعها مختلفة.

البرهان

لتكن $x_1, x_2, \ldots, x_n$ عناصر أحد صفوف S . عندئذ ، $x_i = ny_i + z_i$ ، $1 \le i \le n$ حيث y_i عنصر في نفس الصف في المربع A_1 و z_i عنصر في نفس الصف في المربع A_2 . وبذلك نجد أن

$$\sum_{i=1}^{n} x_i = n\sum_{i=1}^{n} y_i + \sum_{i=1}^{n} z_i$$

ولكن من الفرض لدينا $\sum_{i=1}^{n} y_i = C_1$ و $\sum_{i=1}^{n} z_i = C_2$ حيث C_1 و C_2 عـــددان ثابتان لا يعتمدان على اختيار الصف . إذن ،

$$\sum_{i=1}^{n} x_i = nC_1 + C_2$$

وهو عدد ثابت . وكذلك الحال بالنسبة للأعمدة والقطرين سيكون مجموع كل منها يساوي $nC_1 + C_2$.

الآن لاحـــظ أن العـــدد $x_i = ny_i + z_i$ يحقـــق $1 \le x_i \le n^2$ لأن $0 \le y_i \le n-1$ و $0 \le z_i \le n$. ولكون أعداد S جميعها مختلفة فإن S تحـــوي الأعداد من 1 إلى n^2 وبهذا تكون S مربعاً سحرياً ◆

سنبين فيما يلي كيفية إنشاء مربعات سحرية مساعدة.

تعريف (١٠,٣)

نقول إن الدالة $f : \mathbb{Z} \to \{0,1,2, \ldots, n-1\}$ دالة تطابقية قياس n إذا تحقق ما يلي: $f(x) = f(y)$ إذا وفقط إذا كان $x \equiv y \pmod{n}$.

مثال (١٠,٥)

إذا كان n عدداً فردياً وكانت $f(x)\equiv 2x \pmod n$ (أي أن $f(x)$ يساوي باقي قسمة $2x$ على n) فإن f دالة تطابقية قياس n لأن:

$$f(x)=f(y)\Leftrightarrow 2x\equiv 2y \pmod n$$
$$\Leftrightarrow x\equiv y \pmod n$$

لأن $(2,n)=1$ □

ملحوظة

من التعريف نستنتج أن الدالة f تتعين من معرفة قيمها على نظام رواسب تام قياس n.

نقدم الآن خطوات الخوازمية التي تنشيء المربعين السحريين المساعدين A_1 و A_2 ومن ثم المربع السحري وسنقصر دراستنا على الحالة التي يكون فيها n عدداً فردياً لأنها الأبسط ، أما الحالة التي يكون فيها n عدداً زوجياً فهي أكثر تعقيداً .

تقدم المبرهنة التالية خطوات إنشاء المربع السحري المساعد A_1 .

مبرهنة (١٠,٤) [إنشاء A_1]

ليكن n عدداً فردياً . الخطوات التالية تنشيء المربع A_1 :

(١) أنشيء شبكة مربعة تحوي n من الصفوف و n من الأعمدة.

(٢) رقّم الصفوف من الأعلى إلى الأسفل والأعمدة من اليسار إلى اليمين بالأعداد $0,1,2,\ldots,n-1$.

(٣) كوِّن دالة تطابقية f قياس n تحقق $f(n-1)=\frac{n-1}{2}$.

(٤) ضع في المربع (i,j) العدد $f(i+j)$.

عندئذ، الشبكة المربعة هي مربع سحري حيث $T=\frac{(n-1)n}{2}$.

البرهان

في الصف i : إذا كان $f(i+j_1)=f(i+j_2)$ فإن $i+j_1\equiv i+j_2(\text{mod } n)$ مما يجعل $j_1\equiv j_2(\text{mod } n)$. ونرى أن $j_1=j_2$ لأن $0\le j_1,j_2\le n-1$.

وبهذا تكون جميع الأعداد $f(i+j)$ في الصف i مختلفة. أي أن الصف i يحوي جميع الأعداد $0,1,2,\ldots,n-1$ الذي مجموعها يساوي $\frac{(n-1)n}{2}$.

ونفس الكلام ينطبق على الأعمدة.

القطر النازل : يحوي القطر النازل الأعداد $f(i+i)=(f\,2i)$ وهي أعداد مختلفة لأنه لو كان $f(2i_1)=f(2i_2)$ فإن $2i_1\equiv 2i_2(\text{mod } n)$ ويكون $i_1\equiv i_2(\text{mod } n)$ لأن $(2,n)=1$. وبهذا نحصل على المساواة $i_1=i_2$ لأن $0\le i_1,i_2\le n-1$. إذن ، القطر النازل يحوي الأعداد $0,1,2,\ldots,n-1$ بترتيب معين ومجموعها يساوي $\frac{(n-1)n}{2}$.

القطر الصاعد: هذا القطر يحوي الأعداد $f(i+j)=f(n-1)$. ولكي يكون فيه المجموع مطابقاً للمجاميع السابقة فلا بد أن يكون $n\,f(n-1)=\frac{(n-1)n}{2}$.

أي أن يكون $f(n-1)=\frac{n-1}{2}$.

◆ إذن ، الشبكة المربعة الناتجة هي مربع سحري فيه $T=\frac{(n-1)n}{2}$

مثال (١٠,٦)

إذا كان $n=5$ وكانت الدالة التطابقية f معرفة على النحو التالي:

$$f(0)=1, f(1)=4, f(2)=3, f(3)=0, f(4)=\frac{5-1}{2}=2$$

فإن المربع السحري المساعد A_1 هو :

	0	1	2	3	4
0	$f(0+0)$	$f(0+1)$	$f(0+2)$	$f(0+3)$	$f(0+4)$
1	$f(1+0)$	$f(1+1)$	$f(1+2)$	$f(1+3)$	$f(1+4)$
2	$f(2+0)$	$f(2+1)$	$f(2+2)$	$f(2+3)$	$f(2+4)$
3	$f(3+0)$	$f(3+1)$	$f(3+2)$	$f(3+3)$	$f(3+4)$
4	$f(4+0)$	$f(4+1)$	$f(4+2)$	$f(4+3)$	$f(4+4)$

أي أن :

	0	1	2	3	4
0	1	4	3	0	2
1	4	3	0	2	1
2	3	0	2	1	4
3	0	2	1	4	3
4	2	1	4	3	0

لاحظ أن $T=\frac{4\times5}{2}=10$ □

ننتقل الآن إلى إنشاء المربع السحري المساعد A_2 .

مبرهنة (١٠,٥)

ليكن n عدداً فردياً. الخطوات التالية تنشيء المربع A_2 :

(١) انشيء شبكة مربعة تحوي n من الصفوف والأعمدة .

(٢) رقّم الصفوف من الأعلى إلى الأسفل والأعمدة من اليسار إلى اليمين بالأعداد $0,1,2,\ldots,n-1$.

(٣) كوّن دالة تطابقية g قياس n تحقق $g(0)=\frac{n-1}{2}$.

(٤) ضع في المربع (i,j) العدد $g(i-j)+1$.

عندئذ، الشبكة المربعة الناتجة هي مربع سحري حيث $T=\frac{n(n+1)}{2}$.

البرهان

في الصف i : إذا كان $g(i-j_1)+1=g(i-j_2)+1$ فإن $g(i-j_1)=g(i-j_2)$ ، ونرى أن $i-j_1=i-j_2 \pmod n$ ، وبهذا يكون $j_1\equiv j_2 \pmod n$. وينتج عن ذلك المساواة $j_1=j_2$ لأن $0\le j_1,j_2\le n-1$.

إذن، القيم $g(i-j)+1$ في الصف الواحد مختلفة وتحقق $1\le g(i-j)+1\le n$.

وعليه فمجموع كل صف يساوي

$$1+2+\ldots+n=\frac{n(n+1)}{2}$$

ومجموع كل عمود يساوي ايضاً $\frac{n(n+1)}{2}$ مع تبرير مشابه لما ذكر أعلاه.

القطر النازل : كل من أعداد القطر النازل يساوي $g(0)+1$ $g(i-j)+1=g(0)+1$.

ولكي يكون مجموع عناصر القطر مساوياً للعدد $\frac{n(n+1)}{2}$ ، علينا اختيار g بحيث تحقق القيمة $g(0)$ التالي:

$$n(g(0)+1)=\frac{n(n+1)}{2}$$

أي $$g(0)+1=\frac{n+1}{2}$$

أي $$g(0)=\frac{n-1}{2}$$

وهذا هو بالضبط الشرط (٣) في المبرهنة .

القطر الصاعد : لدينا في هذا القطر ، $i+j=n-1$ وبهذا يكون $i-j=2i-n-1$. فإذا كان $g(i_1-j_1)+1=g(i_2-j_2)+1$. فنجد

$$g(i_1-j_1)=g(i_2-j_2)\Rightarrow i_1-j_1\equiv i_2-j_2(\text{mod } n)$$
$$\Rightarrow 2i_1-n-1\equiv 2i_2-n-1(\text{mod } n)$$
$$\Rightarrow 2i_1\equiv 2i_2(\text{mod } n)$$
$$\Rightarrow i_1\equiv i_2(\text{mod } n)$$

ولكون $0\le i_1,i_2\le n-1$ فنجد أن $i_1=i_2$. ومن ثم يكون $j_1=j_2$.

إذن، الأعداد $g(i-j)+1$ على القطر الصاعد كلها مختلفة وهي من بين الأعداد $1,2,\dots,n$. وعليه يكون مجموعها يساوي $\frac{n(n+1)}{2}$ أيضاً. ونخلص إلى أن الشبكة المربعة الناتجة هي مربع سحري فيه $T=\frac{n(n+1)}{2}$ ◆

مثال (١٠,٧)

إذا كان $n=5$ وكانت الدالة التطابقية g معرفة على النحو التالي:

$$g(0)=\frac{n-1}{2}=2,\ g(1)=3,\ g(2)=4,\ g(3)=0,\ g(4)=1$$

فإن المربع السحري المساعد A_2 هو :

	0	1	2	3	4
0	$g(0)+1$	$g(-1)+1$	$g(-2)+1$	$g(-3)+1$	$g(-4)+1$
1	$g(1)+1$	$g(0)+1$	$g(-1)+1$	$g(-2)+1$	$g(-3)+1$
2	$g(2)+1$	$g(1)+1$	$g(0)+1$	$g(-1)+1$	$g(-2)+1$
3	$g(3)+1$	$g(2)+1$	$g(1)+1$	$g(0)+1$	$g(-1)+1$
4	$g(4)+1$	$g(3)+1$	$g(2)+1$	$g(1)+1$	$g(0)+1$

أي أن

	0	1	2	3	4
0	3	2	1	5	4
1	4	3	2	1	5
2	5	4	3	2	1
3	1	5	4	3	2
4	2	1	5	4	3

لاحظ أن $T=\frac{5\times 6}{2}=15$ □

نحن الآن جاهزون لإنشاء مربع سحري من الدرجة n حيث n عدد فردي.

مبرهنة (١٠,٦)

إذا كان A_1 و A_2 المربعين السحريين المساعدين المنشأين بخطوات المبرهنتين (١٠,٥) و (١٠,٦) فإن المربع

$$M = nA_1 + A_2$$

هو مربع سحري حيث عمليتا الجمع والضرب بعدد هما كما في المصفوفات.

البرهان

من المبرهنة (١٠,٣) يكفي أن نبرهن أن الأعداد في M مختلفة. لنفرض أن

$$nf(i_1 + j_1) + g(i_1 - j_1) + 1 = nf(i_2 + j_2) + g(i_2 - j_2) + 1$$

فنجد من وحدانية التمثيل للأعداد $1, 2, \ldots, n^2$ أن

$$f(i_1 + j_1) = f(i_2 + j_2)$$

و

$$g(i_1 - j_1) = g(i_2 - j_2)$$

ولكون f و g دالتين تطابقتين نحصل على

$$i_1 + j_1 \equiv i_2 + j_2 \pmod{n}$$
$$i_1 - j_1 \equiv i_2 - j_2 \pmod{n}$$

وبجمع المعادلتين مرة وطرحهما مرة أخرى نجد أن

$$2i_1 \equiv 2i_2 \pmod{n}$$

$$2j_1 \equiv 2j_2 (\text{mod } n)$$

ومن ذلك نحصل على

$$i_1 \equiv i_2 (\text{mod } n)$$

$$j_1 \equiv j_2 (\text{mod } n)$$

لأن $(2,n)=1$. وهذا يؤدي إلى أن

$i_1 = i_2$ و $j_1 = j_2$ لأن $0 \le i_1, i_2, j_1, j_2 \le n-1$.

وينتج عن ذلك أن أعداد M مختلفة ويكون مربعاً سحرياً ◆

مثال (١٠,٨)

المربع $M = 5A_1 + A_2$ هو مربع سحري من الدرجة 5 حيـــث A_1 و A_2 هما المربعان السحريان المساعدان الواردان في المثال (١٠,٦) والمثال (١٠,٧) .

M =

8	22	16	5	14
24	18	2	11	10
20	4	13	7	21
1	15	9	23	17
12	6	25	19	3

لاحظ أن $M = \frac{n(n^2+1)}{2} = \frac{5 \times 26}{2} = 65$ □

تمارين (١٠,١)

(١) أنشيء مربعاً سحرياً من الدرجة 5 .

(٢) أنشيء مربعاً سحرياً من الدرجة 7 .

(٣) أنشيء مربعاً سحرياً من الدرجة 9.

(٤) إذا كان A مربعاً سحرياً من الدرجة n وكان المربع B هو المربع الذي نحصل عليه بطرح كل عدد من أعداد A من العدد n^2+1 فأثبت أن B مربعاً سحرياً (يسمى المربع السحري المتمم للمربع A) .

(٥) جد المربعات السحرية المتممة للمربعات السحرية التي أنشأتها في (١)، (٢) ، (٣) .

(١٠,٢) الأعداد العشوائية
Random Numbers

المتتالية التي لا تربط بين عناصرها أي علاقة رياضية معروفة تسمى متتالية "عشوائية" . ولهذه المتتالية تطبيقات عديدة في التقنية الحديثة وخاصة في مجال التعمية. على سبيل المثال ، إذا رمينا قطعة نقود بحيث نرمز لظهور الصورة بالرمز 1 وظهور الكتابة بالرمز 0 فنحصل على 0 أو 1 في كل رمية، وبالتكرار نحصل على متتالية من الأرقام الثنائية العشوائية. ومن الواضح أن هذه الطريقة بطيئة خاصة إذا كانت هناك حاجة إلى توليد متتالية أعداد طويلة جداً. ولذا فالوسيلة المثلى لتوليد متتالية أعداد عشوائية تكون باستخدام الحاسب الآلي. وهنا تظهر المشكلة حيث لا يوجد تعريف رياضي دقيق للأعداد العشوائية. ولذا عند استخدام برامج الحاسب الآلي لتوليد متتالية من الأعداد فهذه الأعداد ليست عشوائية بالمطلق لأن الحاسب

مكون من عدد منته من الحالات ومن ثم فإن المتتالية المولّدة تكون دورية. ولكنها تؤدي الغرض، ولهذا السبب تسمى هذه البرامج مولدات الأعداد شبه العـــشوائية *(pseudorandom number generators)* وإذا كانت دورة المتتالية شبه العشوائية كبيرة جداً فمن الممكن استخدامها لأغراض عديدة كالتعمية وغيرها.

يوجد العديد من الطرق لتوليد المتتالية شبه العشوائية وأكثر هـــذه الطـــرق شيوعاً هي طريقة التطابقات الـــضربية*(multiplicative congruential method)* والتي سنناقشها في هذا البند.

ليكن $n>1$ ولتكن $S=\{1,2,3,\ldots,n-1\}$ وليكن $a\in S$. تعرف دالة التطابق الضربي $L:S\to S$ على النحو التالي :

$$L(x)\equiv ax \pmod n \quad \text{لكل } x\in S \ .$$

تولّد لنا الدالة L استقرائياً متتالية $x_0,x_1,x_2,\ldots$ من الأعداد الصحيحة كالتالي:

(١) $x_0\in S$.

(٢) $x_{i+1}=L(x_i),i\geq 0$. أي أن $x_{i+1}\equiv ax_i \pmod n$.

يسمى العنصر الابتدائي x_0 بالبذرة (*seed*) لأنه يحدد لنا تماماً حدود المتتالية إذا علمنا كلاً من a و n . كما يسمى العدد a بالضارب (*multiplier*) .

المبرهنة التالية تزودنا بصيغة مغلقة لحساب حدود المتتالية:

مبرهنة (٧,١٠)

إذا كانت $\{x_i\}$ هي المتتالية المعرفة أعلاه فإن $x_k\equiv a^k x_0 \pmod n$ لكل $k\geq 1$.

البرهان

باستخدام الاستقراء الرياضي على k.

بما أن $x_1 \equiv ax_0 \pmod{n}$ فإن العبارة صحيحة عندما $k=1$. لنفرض الآن أن العبارة صحيحة عند k. عندئذ، $x_{k+1} \equiv ax_k \equiv aa^k x_0 \equiv a^{k+1}x_0 \pmod{n}$

وبالتالي فإن العبارة صحيحة عند $k+1$ ◆

مثال (٩,١٠)

إذا كان $n=15$ ، $a=2$ ، $x_0=3$ فإن متتالية التطابق الضربي التي نحصل عليها هي:

$$3,6,12,9,3,6,\ldots$$ □

لاحظ أن المتتالية في المثال (٩,١٠) تبدأ بالتكرار بعد الحد الرابع. يسمى طول المتتالية الجزئية قبل بداية التكرار بطول الدورة. وبما أن S مجموعة منتهية فإنه لا بد من تكرار المتتالية $x_0,x_1,x_2,\ldots$ ولكننا نأمل عند توليد الأعداد أن يكون طول الدورة هو n. لاحظ أيضاً أننا لو أخذنا $x_0=5$ و $a=1$ لحصلنا على المتتالية $x_0=x_1=x_2=\ldots=5$ مما يتعارض مع مفهوم العدد العشوائي. كما أننا لو أخذنا $x_0=5$ و $a=3$ لحصلنا على $x_1 \equiv 2\times 5 \equiv 0 \notin S$. ولذا لكي تكون طريقة التطابق الضربي قابلة للتطبيق فإننا نطمح إلى أن تتحقق الشروط التالية:

(١) يجب أن يكون المقياس n كبيراً كبراً كافياً لكي نحصل على أعداد عشوائية كبيرة مختلفة.

(٢) يفضل اختيار $a>1$ و n بحيث يكون $ax_k \not\equiv 0 \pmod{n}$ لكل k.

(٣) أن يكون طول دورة المتتالية $x_0,x_1,x_2,\ldots$ أكبر ما يمكن.

تزودنا المبرهنة التالية بالشرط اللازم لتحقيق (٢):

مبرهنة (١٠,٨)

إذا كان $\gcd(a,n)=1$ فإن $ax_k \not\equiv 0 \pmod n$ لكل $k \geq 1$.

البرهان

لنفرض أن $\gcd(a,n)=1$ ولنفرض لغرض التناقض أنه يوجد k حيث $ax_k \equiv 0 \pmod n$ عندئذ، $a^k x_0 \equiv 0 \pmod n$. أي أن $n \mid a^k x_0$. وبما أن $\gcd(a^k,n)=1$ (لماذا؟) فإن $n \mid x_0$. وهذا تناقض لأن $x_0 < n$ ◆

ولتحقيق الشرط (٣)، لاحظ أن $x_k \equiv a^k x_0 \pmod n$ لكل $k \geq 1$، ولذا فطول الدورة هو أصغر عدد صحيح موجب k يحقق $x_k = x_0$. أي أنه أصغر عدد صحيح موجب يحقق $x_0 \equiv a^k x_0 \pmod n$. ومن ثم إذا اخترنا البذرة x_0 بحيث يكون $\gcd(x_0,n)=1$ فإن طول الدورة هو أصغر عدد صحيح k يحقق $a^k \equiv 1 \pmod n$. وبما أن $\gcd(a,n)=1$ فنجد من مبرهنة أويلر أن $a^{\varphi(n)} \equiv 1 \pmod n$. ولذا فإن طول الدورة أقل من أو يساوي $\varphi(n)$. ولذا فإنه عند تطبيق طريقة التطابق الضربي عادة ما يكون القباس n عدداً أولياً. وبناء على ذلك إذا اخترنا n عدداً أولياً واخترنا a جذراً بدائياً قياس n فيكون $a^{\varphi(n)} = a^{n-1} \equiv 1 \pmod n$ وبهذا نحصل على أكبر طول دورة.

ملحوظة

عند تطبيق طريقة التطابقات الضربية لتوليد أعداد عشوائية فغالباً ما نختار عدداً أولياً كبيراً كقياس بحيث يتناسب مع سعة الحاسب الآلي المستخدم لتنفيذ

الطريقة. وبما أنه يتم تمثيل الأعداد الصحيحة بأعداد ثنائية تحتوي على 32 رقماً ثنائياً في معظم الحاسبات فإن عدد ميرسين الأولي $M_{31}=2^{31}-1$ هو المرشح الأفضل. ومن المعلوم أن العدد 7 جذر بدائي قياس M_{31} . ولكن عند استخدامنا للعدد 7 كضارب فإن الأعداد الأولية المولّدة تكون صغيرة نسبياً. ولذا فنستعيض عن العدد 7 بجذر بدائي أكبر حيث نعلم أن 7 جذر بدائي قياس M_{31} إذا وفقط إذا كان $\gcd(t,\varphi(M_{31}))=\gcd(t,M_{31}-1)=1$. وبما أن $\gcd(5,M_{31}-1)=\gcd(13,M_{31}-1)=1$ فإن كل من $7^5=16807$ و $7^{13}=252246292$ جذر بدائي قياس M_{31}. وعادة ما يؤخذ أحدهما كضارب.

تمارين (٢,١٠)

(١) عين الخمسة عشر حداً الأولى من متتالية التطابقات الضربية المعطاة ثم جد طول دورة كل منها.

(أ) $x_{k+1}\equiv 5x_k \pmod 9$ ، $x_0=6$.

(ب) $x_{k+1}\equiv 4x_k \pmod{25}$ ، $x_0=2$.

(ج) $x_{k+1}\equiv 3x_k \pmod{10}$ ، $x_0=2$.

(٢) إذا كانت متتالية التطابقات الضربية معرفة على النحو التالي:

$$x_{k+1}\equiv ax_k+c \pmod n \quad \text{لكل } k\geq 1 .$$

حيث $a,c,x_0\in\{1,2,\ldots,n\}$ لكل $c\neq 0$ فأثبت أن:

$$x_{k+1}=a^k x_0+c\left(\frac{a^k-1}{a-1}\right) \pmod n \quad \text{لكل } k\geq 1 .$$

(٣) عين طول الدورة لكل من متتاليات التطابقات الضربية التالية:

(أ) $x_{k+1} \equiv 3x_k + 4 \pmod{12}$ ، $x_0 = 5$.

(ب) $x_{k+1} \equiv 7x_k + 4 \pmod{19}$ ، $x_0 = 3$.

(ج) $x_{k+1} \equiv 5x_k + 2 \pmod{19}$ ، $x_0 = 6$.

(د) $x_{k+1} \equiv 4x_k + 7 \pmod{25}$ ، $x_0 = 2$.

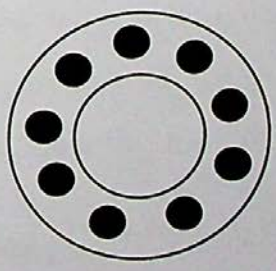
(٤) من الممكن توليد أعداد عشوائية باستخدام متتالية فيبوناتشي على النحو التالي:

$x_{k+1} \equiv x_k + x_{k-1} \pmod{n}$ لكـــل $k \geq 2$. حيـــث $0 \leq x_0, x_1 < n$ بذرتان. احسب الثمانية حدود الأولى من المتتاليـــة المولـــدة باســـتخدام متتاليـــة فيبوناتشي حيث $n = 31$ ، $x_0 = 1$ ، $x_1 = 24$.

(٥) أثبت أن 7 جذر بدائي للعدد $M_{31} = 2^{31} - 1$.

(١٠,٣) جَدْل كوابل الهاتف
Splicing Telephone Cables

تتكون كوابل الهاتف من طبقات متمركزة (متحدة المركـــز) والطبقـــات بدورها مكونة من أسلاك نحاسية معزولية ، ويتم انتاج الكوابل على شكل قطـــع بأطوال مختلفة . الشكل التالي يبين مقطع عرضي لطبقة كابل هاتفي



مقطع عرضي لطبقة كابل هاتفي

يتم إنشاء خطوط الهاتف بجدل قطع من الكوابل بعضها مع بعض، وعندما يتجاور سلكان من طبقة واحدة في عدد من قطع الكابل فإنه غالباً ما ينتج عن ذلك تداخل بين الخطوط ما يسبب تشويش في المكالمات الهاتفية. وعليه فعملية جدل قطع الكوابل يجب أن تحقق الخاصية التالية:

إذا تجاور سلكا طبقة واحدة من قطعة ما فالسلكان يجب أن لا يتجاورا في الطبقة نفسها في القطع القريبة من تلك القطعة.

لإنجاز ذلك نقوم بإنشاء نظام جدل بسيط حيث نفرض أن لدينا طبقة مكونة من الأسلاك $1,2,\ldots,n$. ولنفرض أن $r\in\mathbb{Z}$ أولي نسبياً مع n (يسمى العدد r مدى نظام الجدل). نقوم بوصل السلك j حيث $1\le j\le n$ في القطعة S_1 مع السلك $M(j)$ في القطعة المجاورة S_2 حيث $M(j)$ هو أصغر عدد صحيح موجب يحقق:

$$M(j)\equiv 1+(j-1)r \pmod n$$

لاحظ أنه عند جدل سلك من القطعة S_1 مع سلك من القطعة المجاورة S_2 فإنه يتم تحديد موقع السلك في القطعة S_2 ليكون على بعد $r \pmod n$ من آخر سلك تم جدله في هذه القطعة S_2. كما أن سلكان مختلفان في القطعة S_1 يقابلان سلكان مختلفان في القطعة المجاورة S_2 . ولرؤية ذلك، نفرض أن السلكان i و j في القطعة S_1 مختلفان ولكن $M(i)=M(j)$ في القطعة المجاورة S_2. عندئذ ،

$$\begin{aligned} M(i)=M(j) &\Rightarrow 1+(i-1)r\equiv 1+(j-1)r \pmod n \\ &\Rightarrow ir\equiv jr \pmod n \\ &\Rightarrow i\equiv j \pmod n \\ &\Rightarrow i=j \end{aligned}$$

لأن $(n,r)=1$ وأن $1\le i,j\le n$.

مثال (١٠,١٠)

إذا أردنـــا وصـــل الأســـلاك 12, ... ,2, 1 بمـــدى $r=5$ فـــإن

$M(j)\equiv 1+5(j-1) \pmod{12}$ ونحصل على التقابل

$1\leftrightarrow M(1)=1$ $\quad$ $7\leftrightarrow M(7)=7$

$2\leftrightarrow M(2)=6$ $\quad$ $8\leftrightarrow M(8)=12$

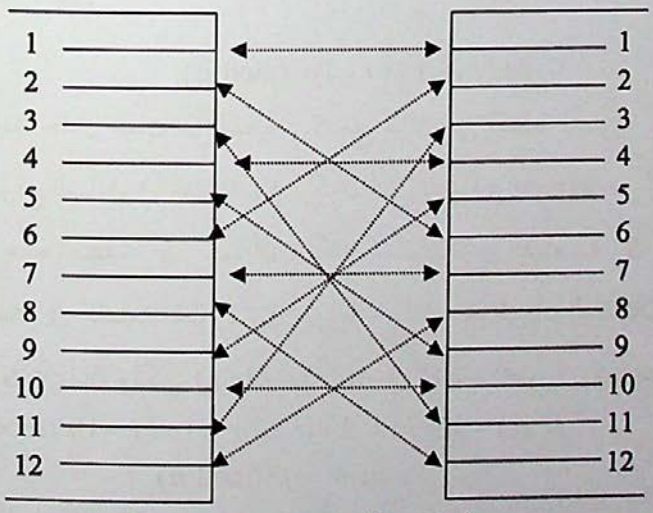
$3\leftrightarrow M(3)=11$ $\quad$ $9\leftrightarrow M(9)=5$

$4\leftrightarrow M(4)=4$ $\quad$ $10\leftrightarrow M(10)=10$

$5\leftrightarrow M(5)=9$ $\quad$ $11\leftrightarrow M(11)=3$

$6\leftrightarrow M(6)=2$ $\quad$ $12\leftrightarrow M(12)=8$

وهذا موضح في الشكل التالي:



جدل 12 سلك بمدى يساوي 5 □

تبين لنا المبرهنة التالية التقابل بين أسلاك القطعة الأولى من الكابل وأسلاك القطعة k من الكابل نفسه.

مبرهنة (١٠,٩)

لنفرض أن $M_k(j)$ هو موقع السلك في القطعة k حيث $k \geq 2$ المجدول مع السلك j من القطعة الأولى. عندئذ:

$$M_k(j) \equiv 1+(j-1)r^{k-1} \pmod{n}$$

البرهان

بالاستقراء الرياضي على k . العبارة صائبة عندما $k=2$ لأن

$$M_2(j) \equiv 1+(j-1)r \pmod{n}$$

لنفرض الآن أن العبارة صحيحة عند $k=m \geq 2$.

$$\begin{aligned} M_{m+1}(j) &\equiv 1+(M_m(j)-1)r \pmod{n} \\ &\equiv 1+[(j-1)r^{m-1}]r \pmod{n} \\ &\equiv 1+(j-1)r^m \pmod{n} \end{aligned}$$

وبهذا تكون العبارة صائبة عندما $k=m+1$ ومن ثم نحصل على المطلوب ◆

لاحظ أنه بعد إنجاز عدد k من الجدلات ، فاستناداً إلى المبرهنة (١٠,٩) نجد أن سلكين متجاورين في الموقعين j و $j+1$ يتم وصلهما بسلكين في الموقعين $M_k(j)$ و $M_k(j+1)$ على التوالي.

الآن، يكون السلكان $M_k(j)$ و $M_k(j+1)$ متجاورين إذا وفقط إذا كان

$$M_k(j)-M_k(j+1)\equiv\pm1(\text{mod } n)$$
$$\Leftrightarrow 1+(j-1)r^k-(1+jr^k)\equiv\pm1(\text{mod } n)$$
$$\Leftrightarrow r^k\equiv\pm1(\text{mod } n)$$

فلذا لكي يكون تجاور السلكين $M_k(j)$ و $M_k(j+1)$ في قطعة أبعد ما يمكن من القطعة التي يتجاور فيها السلكان j و $j+1$ فيجب إيجاد عدد k يحقق

$$r^k\equiv\pm1(\text{mod } n)$$

تعريف (١٠,٤)

ليكن $n\in\mathbb{Z}^+$ وليكن العدد r أولي نسبياً مع n . تعرف القوة ±1 للعدد r قياس n (±1- *exponent of r modulo n*) على أنه أصغر عـــدد صـــحيح موجب k يحقق $r^k\equiv\pm1\ (\text{mod } n)$. سنرمز لأكبر عدد k يحقق ذلك بـــالرمز $\lambda_0(n)$.

لاحظ أنه لإنجاز عملية جدل ملائمة بمدى r فإننا نسعى لإيجـــاد $\lambda_0(n)$. والمبرهنة التالية تجد لنا هذا العدد بدلالة القوة الشاملة الصغرى $\lambda(n)$ للعدد n .

مبرهنة (١٠,١٠)

ليكن n عدداً صحيحاً أكبر من 2 .

(أ) إذا وجد جذر بدائي للعدد n فإن $\lambda_0(n)=\dfrac{\varphi(n)}{2}=\dfrac{\lambda(n)}{2}$

(ب)في حالة عدم وجود جذر بدائي للعدد n يكون $\lambda_0(n)=\lambda(n)$.

البرهان

انظر [131] ◆

مثال (١٠,١١)

إذا أردنا جدل 144 سلكاً بمدى $r=3$ فجد $\lambda_0(144)$.

الحل

بما أن $144=2^4\times3^2$ فإنه لا يوجد جذر بدائي للعدد 144. إذن،

$$\lambda_0(144)=\lambda(144)=[2^2,6]=12$$

تمارين (١٠,٣)

(١) جد $\lambda_0(n)$ لكل من الأعداد التالية:

(أ) 22 (ب) 222 (ج) 884 (د) 99

(٢) صمم نظام جدل لكوابل الهاتف عدد أسلاكه

(أ) 50 (ب) 125

(٧,٤) تطبيقات على صيغة موبياس للتعاكس
Applications of The Möbius Inversion Formula

هناك العديد من التطبيقات المهمة على صيغة موبياس للتعاكس في الجبر ونظرية التركيبات والفيزياء وغيرها. نقدم هنا تطبيقان لهذه الصيغة.

لنفرض أن لدينا n من المدعوين (رجال وفتيان) على وليمة عشاء ونود إجلاسهم حول مائدة مستديرة تحوي عدداً n من الكراسي. بما أنه من الممكن أن

يجلس رجلاً (M) أو فتى (B) على أي من الكراسي فإن عدد الطرق المختلفة التي يمكن أن يجلس فيها المدعوين يساوي 2^n .

الآن ، إذا قمنا بتدوير جميع المدعوين بمقعد واحد حول المائدة فمن الممكن أن ينتج عن ذلك تغيير في نمط الجلوس ولكن بعد تدوير المدعوين n من التدويرات المتالية فإننا نحصل على النمط الأساسي مرة أخرى.

دعنا نقول إن دورة نمط الجلوس يساوي d إذا حصلنا على النمط الأساسي للمرة الأولى بعد d من التدويرات (أي إذا قمنا بتدوير النمط فإننا نحصل بالضبط على d من الأنماط المختلفة) . على سبيل المثال دورة النمط $MMM \ldots M$ تساوي1 ، وإذا كان n عدداً زوجياً فإن دورة النمط $BMBM \ldots BM$ تساوي 2 .

لنفرض الآن أن $f(d)$ هو عدد الأنماط المختلفة ذات الدورة d. سنوظف صيغة موبياس للتعاكس لحساب العدد $f(d)$.

مبرهنة (١٠,١١)

إذا كانت دورة النمط تساوي d فإن d يقسم n.

البرهان

استناداً إلى خوارزمية القسمة نستطيع إيجاد q و r يحققان

$$n = qd + r \quad ، \quad 0 \le r \le d$$

وبملاحظة أنه يمكن الحصول على النمط الأساسي بعد d من التدويرات وبعد n من التدويرات ومن ثم بعد $r = n - qd$ من التدويرات. وبما أن $r < d$ فمن تعريف الدورة نجد أن $r = 0$ وبهذا يكون d يقسم n ◆

مبرهنة (١٠,١٢)

$$f(d)=\sum_{c\mid d}2^c\,\mu(d/c)$$

البرهان

لكل d ، عدد الأنماط المختلفة ذات الدورة d يعتمد فقط على d ولا يعتمد على $n=qd$. وذلك لأننا نحصل على النمط qd بتكرار قالب يحتوي على d من الأشخاص M أو B بعدد q من المرات ، علاوة على أن هذا النمط ليس تكراراً لقوالب أصغر وأن عدد القوالب من الطول d يعتمد فقط على d. وعليه فلكل $d \mid n$ نحصل على $f(d)$ من الأنماط المختلفة من الدورة d.

وبهذا يكون $\sum_{d\mid n} f(d)$ يساوي العدد الكلي للأنماط وهذا بدوره يساوي 2^n.

إذن، $\sum_{d\mid n} f(d)=2^n$.

وباستخدام صيغة موبياس للتعكاس نجد أن

$$f(n)=\sum_{d\mid n}2^d\,\mu(n/d)$$

وباستبدال الترميز نجد أن

$$\blacklozenge\quad f(d)=\sum_{c\mid d}2^c\;\mu\,(d/c)$$

مثال (١٠,١٢)

عدد الأنماط المختلفة ذات الدورة 14 يساوي

$$f(14)=\sum_{c\mid 14}2^c\;\mu\,(14/c)$$

$$= 2\times\mu(14)+2^2\times\mu(7)+2^7\times\mu(2)+2^{14}\times\mu(1)$$
$$= 2-2^2-2^7-2^7+2^{14} = 16254$$

وبهذا يكون عدد الأنماط المختلفة ذات الدورة 14 هو $f(14)=16254$ □

ننتقل الآن إلى تطبيق جبري.

تعريف (١٠,٥)

تُعرف كثيرة الحدود الدويرانية *(cyclotomic polynomial)* على النحو التالي:

$$\Phi_n(x)=\prod_{d\mid n}(x^d-1)^{\mu(n/d)}$$ حيث $n\in\mathbb{Z}^+$.

لاحظ أن درجة $\Phi_n(x)$ هي $\sum_{d\mid n} d\,\mu(n/d)=\varphi(n)$.

كما أنه من المعلوم أن $\Phi_n(x)$ كثيرة حدود واحدية غير قابلة للتحليل معاملاتها أعداد صحيحة.

لاحظ أنه باستخدام صيغة موبياس للتعاكس (باستخدام الضرب بدل الجمع) نجد أن

$$x^n-1=\prod_{d\mid n}\Phi_d(x)$$

ولذا فإن كثيرات الحدود الدويرانية تستخدم لتحليل كثيرة الحدود x^n-1 إلى عوامل غير قابلة للتحليل.

مثال (١٠,١٣)

استخدم كثيرات الحدود الدويرانية لتحليل كثيرة الحدود x^6-1.

الحل

$$x^6-1=\prod_{d\mid 6}\Phi_d(x)=\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)$$

ولكن

$$\Phi_1(x)=x-1$$
$$\Phi_2(x)=(x-1)^{-1}(x^2-1)=x+1$$
$$\Phi_3(x)=(x-1)^{-1}(x^3-1)=x^2+x+1$$
$$\Phi_6(x)=(x-1)(x^2-1)^{-1}(x^3-1)^{-1}(x^6-1)$$
$$=\frac{(x-1)(x^3-1)(x^3+1)}{(x-)(x+1)(x^3-1)}$$
$$=\frac{x^3+1}{x+1}=x^2-x+1$$

إذن، $x^6-1=(x-1)(x+1)(x^2+x+1)(x^2-x+1)$ □

تمارين (١٠,٤)

(١) احسب عدد الأنماط ذات الدورات 2 ، 3 ، 4 .

(٢) إذا كان المدعون هم رجال ، سيدات، شبان ، فتيات فما هو عدد الأنمـــاط المختلفة من الدورة d؟

(٣) احسب $\Phi_n(x)$ لكل n ، $1\le n\le 9$.

(٤) إذا كان p عدداً أولياً فأثبت أن $\Phi_{p^2}(x)=\Phi_p(x^p)$.

(٥) حلل x^9-1 إلى عوامل غير قابلة للتحليل.

الجداول
Tables

جدول (١) : الأعداد الأولية التي تقل عن العدد 10000

2	103	241	401	571	739	919	1093
3	107	251	409	577	743	929	1097
5	109	257	419	587	751	937	1103
7	113	263	421	593	757	941	1109
11	127	269	431	599	761	947	1117
13	131	271	433	601	769	953	1123
17	137	277	439	607	773	967	1129
19	139	281	443	613	787	971	1151
23	149	283	449	617	797	977	1153
29	151	293	457	619	809	983	1163
31	157	307	461	631	811	991	1171
37	163	311	463	641	821	997	1181
41	167	313	467	643	823	1009	1187
43	173	317	479	647	827	1013	1193
47	179	331	487	653	829	1019	1201
53	181	337	491	659	839	1021	1213
59	191	347	499	661	853	1031	1217
61	193	349	503	673	857	1033	1223
67	197	353	509	677	859	1039	1229
71	199	359	521	683	863	1049	1231
73	211	367	523	691	877	1051	1237
79	223	373	541	701	881	1061	1249
83	227	379	547	709	883	1063	1259
89	229	383	557	719	887	1069	1277
97	233	389	563	727	907	1087	1279
101	239	397	569	733	911	1091	1283

تابع جدول (١)

1289	1487	1669	1889	2099	2311	2539	2729
1291	1489	1693	1901	2111	2333	2543	2731
1297	1493	1697	1907	2113	2339	2549	2741
1301	1499	1699	1913	2129	2341	2551	2749
1303	1511	1709	1931	2131	2347	2557	2753
1307	1523	1721	1933	2137	2351	2579	2767
1319	1531	1723	1949	2141	2357	2591	2777
1321	1543	1733	1951	2143	2371	2593	2789
1327	1549	1741	1973	2153	2377	2609	2791
1361	1553	1747	1979	2161	2381	2617	2797
1367	1559	1753	1987	2179	2383	2621	2801
1373	1567	1759	1993	2203	2389	2633	2803
1381	1571	1777	1997	2207	2393	2647	2819
1399	1579	1783	1999	2213	2399	2657	2833
1409	1583	1787	2003	2221	2411	2659	2837
1423	1597	1789	2011	2237	2417	2663	2843
1427	1601	1801	2017	2239	2423	2671	2851
1429	1607	1811	2027	2243	2437	2677	2857
1433	1609	1823	2029	2251	2441	2683	2861
1439	1613	1831	2039	2267	2447	2687	2879
1447	1619	1847	2053	2269	2459	2689	2887
1451	1621	1861	2063	2273	2467	2693	2897
1453	1627	1867	2069	2281	2473	2699	2903
1459	1637	1871	2081	2287	2477	2707	2909
1471	1657	1873	2083	2293	2503	2711	2917
1481	1663	1877	2087	2297	2521	2713	2927
1483	1667	1879	2089	2309	2531	2719	2939

تابع جدول (١)

2953	3191	3407	3617	3847	4057	4283	4523
2957	3203	3413	3623	3851	4073	4289	4547
2963	3209	3433	3631	3853	4079	4297	4549
2969	3217	3449	3637	3863	4091	4327	4561
2971	3221	3457	3643	3877	4093	4337	4567
2999	3229	3461	3659	3881	4099	4339	4583
3001	3251	3463	3671	3889	4111	4349	4591
3011	3253	3467	3673	3907	4127	4357	4597
3019	3257	3469	3677	3911	4129	4363	4603
3023	3259	3491	3691	3917	4133	4373	4621
3037	3271	3499	3697	3919	4139	4391	4637
3041	3299	3511	3701	3923	4153	4397	4639
3049	3301	3517	3709	3929	4157	4409	4643
3061	3307	3527	3719	3931	4159	4421	4649
3067	3313	3529	3727	3943	4177	4423	4651
3079	3319	3533	3733	3947	4201	4441	4657
3083	3323	3539	3739	3967	4211	4447	4663
3089	3329	3541	3761	3989	4217	4451	4673
3109	3331	3547	3767	4001	4219	4457	4679
3119	3343	3557	3769	4003	4229	4463	4691
3121	3347	3559	3779	4007	4231	4481	4703
3137	3359	3571	3793	4013	4241	4483	4721
3163	3361	3581	3797	4019	4243	4493	4723
3167	3371	3583	3803	4021	4253	4507	4729
3169	3373	3593	3821	4027	4259	4513	4733
3181	3389	3607	3823	4049	4261	4517	4751
3187	3391	3613	3833	4051	4271	4519	4759
					4273		

تابع جدول (١)

4783	4999	5233	5477	5693	5903	6173	6373
4787	5003	5237	5479	5701	5923	6197	6379
4789	5009	5261	5483	5711	5927	6199	6389
4793	5011	5273	5501	5717	5939	6203	6397
4799	5021	5279	5503	5737	5953	6211	6421
4801	5023	5281	5507	5741	5981	6217	6427
4813	5039	5297	5519	5743	5987	6221	6449
4817	5051	5303	5521	5749	6007	6229	6451
4831	5059	5309	5527	5779	6011	6247	6469
4861	5077	5323	5531	5783	6029	6257	6473
4871	5081	5333	5557	5791	6037	6263	6481
4877	5087	5347	5563	5801	6043	6269	6491
4889	5099	5351	5569	5807	6047	6271	6521
4903	5101	5381	5573	5813	6053	6277	6529
4909	5107	5387	5581	5821	6067	6287	6547
4919	5113	5393	5591	5827	6073	6299	6551
4931	5119	5399	5623	5839	6079	6301	6553
4933	5147	5407	5639	5843	6089	6311	6563
4937	5153	5413	5641	5849	6091	6317	6569
4943	5167	5417	5647	5851	6101	6323	6571
4951	5171	5419	5651	5857	6113	6329	6577
4957	5179	5431	5653	5861	6121	6337	6581
4967	5189	5437	5657	5867	6131	6343	6599
4969	5197	5441	5659	5869	6133	6353	6607
4973	5209	5443	5669	5879	6143	6359	6619
4987	5227	5449	5683	5881	6151	6361	6637
4993	5231	5471	5689	5897	6163	6367	6653
			5693				

تابع جدول (١)

6659	6871	7121	7393	7603	7867	8111	8363
6661	6883	7127	7411	7607	7873	8117	8369
6673	6899	7129	7417	7621	7877	8123	8377
6679	6907	7151	7433	7639	7879	8147	8387
6689	6911	7159	7451	7643	7883	8161	8389
6691	6917	7177	7457	7649	7901	8167	8419
6701	6947	7187	7459	7669	7907	8171	8423
6703	6949	7193	7477	7673	7919	8179	8429
6709	6959	7207	7481	7681	7927	8191	8431
6719	6961	7211	7487	7687	7933	8209	8443
6733	6967	7213	7489	7691	7937	8219	8447
6737	6971	7219	7499	7699	7949	8221	8461
6761	6977	7229	7507	7703	7951	8231	8467
6763	6983	7237	7517	7717	7963	8233	8501
6779	6991	7243	7523	7723	7993	8237	8513
6781	6997	7247	7529	7727	8009	8243	8521
6791	7001	7253	7537	7741	8011	8263	8527
6793	7013	7283	7541	7753	8017	8269	8537
6803	7019	7297	7547	7757	8039	8273	8539
6823	7027	7307	7549	7759	8053	8287	8543
6827	7039	7309	7559	7789	8059	8291	8563
6829	7043	7321	7561	7793	8069	8293	8573
6833	7057	7331	7573	7817	8081	8297	8581
6841	7069	7333	7577	7823	8087	8311	8597
6857	7079	7349	7583	7829	8089	8317	8599
6863	7103	7351	7589	7841	8093	8329	8609
6869	7109	7369	7591	7853	8101	8353	8623

تابع جدول (١)

8627	8837	9091	9337	9547	9803
8629	8839	9103	9341	9551	9811
8641	8849	9109	9343	9587	9817
8647	8861	9127	9349	9601	9829
8663	8863	9133	9371	9613	9833
8669	8867	9137	9377	9619	9839
8677	8887	9151	9391	9623	9851
8681	8893	9157	9397	9629	9857
8689	8923	9161	9403	9631	9859
8693	8929	9173	9413	9643	9871
8699	8933	9181	9419	9649	9883
8707	8941	9187	9421	9661	9887
8713	8951	9199	9431	9677	9901
8719	8963	9203	9433	9679	9907
8731	8969	9209	9437	9689	9923
8737	8971	9221	9439	9697	9929
8741	8999	9227	9461	9719	9931
8747	9001	9239	9463	9721	9941
8753	9007	9241	9467	9733	9949
8761	9011	9257	9473	9739	9967
8779	9013	9277	9479	9743	9973
8783	9029	9281	9491	9749	
8803	9041	9283	9497	9767	
8807	9043	9293	9511	9769	
8819	9049	9311	9521	9781	
8821	9059	9319	9533	9787	
8831	9067	9323	9539	9791	

جدول (٢) أصغر قاسم أولي

يعطينا هذا الجدول أصغر قاسم أولي لكل عدد مؤلف أقل من 10000

ما عدا التي تقبل القسمة على أي من الأعداد الأولية 2,3,5,7,11

169	13	713	13	1037	17	1387	19	1751	17
221	13	731	17	1073	29	1391	13	1763	41
147	13	767	13	1079	13	1403	23	1769	29
289	17	799	19	1081	23	1411	17	1781	13
299	13	793	13	1121	19	1417	13	1807	13
323	17	799	17	1139	17	1457	31	1817	23
361	19	817	19	1147	31	1469	13	1819	17
377	13	841	29	1157	13	1501	19	1929	31
391	17	851	23	1159	19	1513	17	1843	19
403	13	871	13	1189	29	1517	37	1849	43
437	19	893	19	1207	17	1537	29	1853	17
481	13	899	29	1219	23	1541	23	1891	31
493	17	901	17	1241	17	1577	19	1909	23
527	17	923	13	1247	29	1591	37	1919	19
529	23	943	23	1261	13	1633	23	1921	17
533	13	949	13	1271	31	1643	31	1927	41
551	19	961	31	1273	19	1649	17	1937	13
559	13	989	23	1313	13	1651	13	1943	29
589	19	1003	17	1333	31	1679	23	1957	19
611	13	1007	19	1339	13	1681	41	1961	37
629	17	1027	13	1343	17	1691	19	1963	13
667	23	1037	17	1349	19	1703	13	2021	43
689	13	1073	17	1357	23	1711	29	2033	19
697	17	1007	19	1363	29	1717	17	2041	13
703	19	1027	13	1369	37	1739	37	2047	23

تابع جدول (٢)

2059	29	2479	37	2869	19	3173	19	3551	53
2071	19	2483	13	2873	13	3193	31	3569	43
2077	31	2489	19	2881	43	3197	23	3587	17
2117	29	2491	47	2899	13	3211	13	3589	37
2119	13	2501	41	2911	41	3233	53	3599	59
2147	19	2507	23	2921	23	3239	41	3601	13
2159	17	2509	13	2923	37	3247	17	3677	23
2171	13	2533	17	2929	29	3263	13	3629	19
2173	41	2537	43	2941	17	3277	29	3649	41
2183	37	2561	13	2951	13	3281	17	3653	13
2197	13	2567	17	2977	13	3289	19	3667	19
2201	31	2573	31	2983	19	3317	37	3679	13
2209	47	2581	29	2987	29	3317	31	3683	29
2227	17	2587	13	2993	41	3337	47	3713	47
2231	23	2599	23	3007	31	3341	13	3721	61
2249	13	2603	19	3013	23	3349	17	3737	37
2257	37	2623	43	3029	13	3379	17	3743	19
2263	31	3627	37	3043	17	3379	31	3749	23
2279	43	2641	19	3053	43	3383	17	3757	13
2291	29	2669	17	37	37	3397	43	3763	53
2323	23	2701	37	3077	17	3401	19	3781	19
2327	13	2743	13	3097	19	3403	41	3791	17
2329	17	2743	41	3103	29	3419	13	3799	29
2353	13	2759	31	3107	13	3427	23	3809	13
2363	17	2771	17	3127	53	3431	47	3811	37
2369	23	2773	47	3131	31	3439	19	3827	43
2407	29	2809	53	3133	13	3473	23	3841	23
2413	19	2813	29	3139	43	3481	59	3859	17
2419	41	2831	19	3149	47	3497	13	3869	53
2449	31	2839	17	3151	23	3503	31	3887	13
2461	23	2867	47	3161	29	3523	13	3901	47

تابع جدول (٢)

3937	31	4267	17	4601	43	4913	17	5267	23
3953	59	4303	13	4607	17	4927	13	5287	17
4307	13	4607	17	4927	13	5287			
3959	37	4309	31	4633	41	4981	17	5311	47
3961	17	4313	19	4661	59	4997	19	5317	13
3973	29	4321	29	4667	13	5017	29	5021	17
3977	41	4331	61	4681	31	5029	47	5329	73
3979	23	4343	43	4687	43	5041	71	5339	19
3991	13	4351	19	4693	13	5053	31	5353	53
4009	19	4369	17	4699	37	5057	13	5359	23
4031	29	4379	29	4709	17	5063	61	5363	31
4033	37	4381	13	4717	53	5069	37	5371	41
4043	13	4387	41	4727	29	5097	17	5377	19
4061	31	4393	23	4747	47	5111	19	5389	17
4063	17	4399	53	4757	67	5103	17	5429	61
4069	13	4427	19	4769	19	5129	23	5447	13
4087	61	4429	43	4771	13	5141	53	5449	53
4097	17	4453	61	4777	17	5143	37	5461	43
4117	23	4479	41	4811	17	5149	19	5473	13
4121	13	4471	17	4819	61	5161	13	5491	17
4141	41	4489	67	4841	47	5177	31	5497	23
4163	23	4451	13	4843	29	5183	71	5513	37
4171	43	4531	23	4847	37	5191	29	5539	29
4181	37	4537	13	4849	13	5207	41	5543	23
4183	47	4541	19	4853	23	5213	13	5549	31
4187	53	4553	29	4859	43	5219	17	5561	67
4189	59	4559	47	4867	31	5221	23	5567	19
4199	13	4573	17	4883	19	5239	13	5587	37
4223	41	4577	23	4891	67	5249	29	5597	29
4237	19	4579	19	4867	59	5251	59	5603	13
4247	31	4589	13	4901	13	5263	19	5609	71

تابع جدول (٢)

5611	31	5963	67	6289	19	6617	13	6943	53
5617	41	5969	47	6313	59	6623	37	6953	17
5627	17	5977	43	6319	71	6631	19	6973	19
5629	13	5983	31	6331	13	6641	29	6989	29
5633	43	5989	53	6341	17	6647	17	7003	47
5671	53	5993	13	6371	23	6649	61	7009	43
5681	13	6001	17	6386	13	6667	59	7031	79
5699	41	6019	13	6401	37	6683	41	7033	13
5707	13	6023	19	6403	19	6697	37	7037	31
5713	29	6031	37	6407	43	6707	19	7061	23
5723	59	6049	23	6409	13	6731	53	7067	37
5729	17	6059	73	6431	59	6739	23	7081	73
5759	13	6071	13	6437	41	6749	17	7087	19
5767	73	6077	69	6439	47	6751	43	7093	41
5771	29	6103	17	6443	17	6757	29	7097	47
5773	23	6107	31	6463	23	6767	67	7099	31
5777	53	6109	41	6467	29	6773	13	7111	13
5809	37	6119	29	6487	13	6799	13	7123	17
5833	19	6137	17	6493	43	6817	17	7141	37
5837	13	6157	47	6497	73	6821	19	7153	23
5891	43	6161	61	6499	67	6847	41	7157	17
5893	71	6169	31	6509	23	6851	13	7163	13
5899	17	6179	37	6511	17	6859	19	7169	67
5909	19	6187	23	6527	61	6877	13	7171	71
5911	23	6191	41	6533	47	6889	71	7181	43
5917	61	6227	13	6539	13	6889	83	7199	23
5921	31	6233	23	6541	31	6893	61	7201	19
5933	17	6239	17	6557	79	6901	67	7223	31
5941	13	6241	79	6583	29	6913	31	7241	13
5947	19	6253	13	6593	19	6929	13	7261	53
5959	59	6283	61	6613	17	6931	29	7267	13

تابع جدول (٢)

7277	19	7597	71	7913	41	8203	13	8497	29
7279	29	7613	23	7921	89	8207	29	8505	47
7289	37	7619	19	7939	17	8213	43	8509	67
7291	23	7627	29	7943	13	8227	19	8531	19
7303	67	7631	13	7957	73	8249	73	8549	83
7313	71	7633	17	7961	19	8251	37	8551	17
7319	13	7657	13	7967	31	8257	23	8557	43
7327	17	7661	47	7969	13	8279	17	8567	13
7339	41	7663	79	7979	79	8299	43	8579	23
7361	17	7697	43	7981	23	8303	19	8587	31
7363	37	7709	13	7991	61	8321	53	8593	13
7367	53	7729	59	7999	19	8333	13	8611	70
7373	73	7739	71	8003	53	8339	31	8621	37
7379	47	7747	61	8021	13	8341	19	8633	89
7387	83	7751	23	8023	71	8347	17	8639	53
7391	19	7769	17	8027	23	8357	61	8651	41
7397	13	7771	19	8033	29	8359	13	8653	47
7409	31	7781	31	8047	13	8381	17	8671	13
7421	41	7783	43	8051	83	8383	83	8683	19
7423	13	7787	13	8077	41	8399	37	8711	31
7429	17	7801	29	8083	59	8401	31	8717	23
7439	43	7807	37	8119	23	8411	13	8749	13
7453	29	7811	73	8131	47	8759	47	8759	19
7463	17	7813	13	8137	79	8417	19	8773	31
7471	31	7831	41	8143	17	8441	23	8777	67
7493	59	7837	17	8149	29	8453	79	8791	59
7501	13	7849	47	8153	31	8471	43	8797	13
7519	73	7859	29	8159	41	8473	37	8801	13
7431	17	7871	17	8177	13	8479	61	8809	23
7543	19	7891	13	8189	19	8483	17	8843	37
7571	67	7897	53	8201	59	8489	13	8851	53

تابع جدول (٢)

8857	17	9179	67	9523	89	9847	43
8873	19	9193	29	9529	13	9853	59
8881	83	9197	17	9553	41	9869	71
8891	17	9211	61	9557	19	9881	41
8903	29	9217	13	9563	73	9893	13
8909	59	9223	23	9571	17	9899	19
8917	37	9253	19	9577	61	9913	23
8927	79	9259	47	9589	43	9917	47
8947	23	9263	59	9593	53	9937	19
8975	13	9269	13	9599	29	9943	61
8959	17	9271	73	9607	13	9953	37
8977	47	9287	37	9617	59	9959	23
8983	13	9299	17	9637	23	9971	13
8989	89	9301	71	9641	31		
8983	17	9307	41	9659	13		
9017	71	9313	67	9671	19		
9019	29	9329	19	9673	17		
9047	83	9347	13	9683	23		
9061	13	9353	47	9701	89		
9071	47	9367	17	9703	31		
9073	43	9379	83	9707	17		
9077	29	9389	41	9272	71		
9083	31	9407	23	9731	37		
9089	61	9409	97	9761	43		
9101	19	9451	13	9763	13		
9113	13	9469	17	9773	29		
9131	23	9481	19	9797	97		
9139	13	9487	53	9799	41		
9143	41	9503	13	9809	17		
9167	89	9509	37	9827	31		
9169	53	9517	31	9841	13		

جدول (٣) : قيم لبعض الدوال العددية

n	ϕ	τ	σ
1	1	1	1
2	1	2	3
3	2	2	4
4	2	3	7
5	4	2	6
6	2	4	12
7	6	2	8
8	4	4	15
9	6	3	13
10	4	4	18
11	10	2	12
12	4	6	28
13	12	2	14
14	6	4	24
15	8	4	24
16	8	5	31
17	16	2	18
18	6	6	39
19	18	2	20
20	8	6	42
21	12	4	32
22	10	4	36
23	22	2	24
24	8	8	60

تابع جدول (٣)

n	ϕ	τ	σ
25	20	3	31
26	12	4	42
27	18	4	40
28	12	6	56
29	28	2	30
30	8	8	72
31	30	2	32
32	16	6	63
33	20	4	48
34	16	4	54
35	24	4	48
36	12	9	91
37	36	2	38
38	18	4	60
39	24	4	56
40	16	8	90
41	40	2	42
42	12	8	96
43	42	2	44
44	20	6	84
45	24	6	84
46	22	4	72
47	46	2	48
48	16	10	124
49	42	3	57

تابع جدول (٣)

n	ϕ	τ	σ
50	20	6	93
51	32	4	72
52	24	6	98
53	52	2	54
54	18	8	120
55	40	4	72
56	24	8	120
57	36	4	80
58	28	4	90
59	58	2	60
60	16	12	168
61	60	2	62
62	30	4	96
63	36	6	104
64	32	7	127
65	48	4	84
66	20	8	144
67	66	2	68
68	32	6	126
69	44	4	96
70	24	8	144
71	70	2	72
72	24	12	195
73	72	2	74
74	36	4	114

جدول (٤) : الكسر المتواصل للعدد $\sqrt{d}$

d	$\sqrt{d}$	d	$\sqrt{d}$
2	$[1; \overline{2}]$	28	$[5; \overline{3, 2, 3, 10}]$
3	$[1; \overline{1, 2}]$	29	$[5; \overline{2, 1, 1, 2, 10}]$
5	$[2; \overline{4}]$	30	$[5; \overline{2, 10}]$
6	$[2; \overline{2, 4}]$	31	$[5; \overline{1, 1, 3, 5, 3, 1, 1, 10}]$
7	$[2; \overline{1, 1, 1, 4}]$	32	$[5; \overline{1, 1, 1, 10}]$
8	$[2; \overline{1, 4}]$	33	$[5; \overline{1, 2, 1, 10}]$
10	$[3; \overline{6}]$	34	$[5; \overline{1, 4, 1, 10}]$
11	$[3; \overline{3, 6}]$	35	$[5; \overline{1, 10}]$
12	$[3; \overline{2, 6}]$	37	$[6; \overline{12}]$
13	$[3; \overline{1, 1, 1, 1, 6}]$	38	$[6; \overline{6, 12}]$
14	$[3; \overline{1, 2, 1, 6}]$	39	$[6; \overline{4, 12}]$
15	$[3; \overline{1, 6}]$	40	$[6; \overline{3, 12}]$
17	$[4; \overline{8}]$	41	$[6; \overline{2, 2, 12}]$
18	$[4; \overline{4, 8}]$	42	$[6; \overline{2, 12}]$
19	$[4; \overline{2, 1, 3, 1, 2, 8}]$	43	$[6; \overline{1, 1, 3, 1, 5, 1, 3, 1, 1, 12}]$
20	$[4; \overline{2, 8}]$	44	$[6; \overline{1, 1, 1, 2, 1, 1, 1, 12}]$
21	$[4; \overline{1, 1, 2, 1, 1, 8}]$	45	$[6; \overline{1, 2, 2, 2, 1, 12}]$
22	$[4; \overline{1, 2, 4, 2, 1, 8}]$	46	$[6; \overline{1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12}]$
23	$[4; \overline{1, 3, 1, 8}]$	47	$[6; \overline{1, 5, 1, 12}]$
24	$[4; \overline{1, 8}]$	48	$[6; \overline{1, 12}]$
26	$[5; \overline{10}]$	50	$[7; \overline{14}]$
27	$[5; \overline{5, 10}]$	51	$[7; \overline{7, 14}]$

d	$\sqrt{d}$	d	$\sqrt{d}$
52	$[7; \overline{4, 1, 2, 1, 4, 14}]$	76	$[8; \overline{1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16}]$
53	$[7; \overline{3, 1, 1, 3, 14}]$	77	$[8; \overline{1, 3, 2, 3, 1, 16}]$
54	$[7; \overline{2, 1, 6, 1, 2, 14}]$	78	$[8; \overline{1, 4, 1, 16}]$
55	$[7; \overline{2, 2, 2, 14}]$	79	$[8; \overline{1,7,1,16}]$
56	$[7; \overline{2, 14}]$	80	$[8; \overline{1, 16}]$
57	$[7; \overline{1, 1, 4, 1, 1, 14}]$	82	$[9; \overline{18}]$
58	$[7; \overline{1, 1, 1, 1, 1, 1, 14}]$	83	$[9; \overline{9, 18}]$
59	$[7; \overline{1, 2, 7, 2, 1, 14}]$	84	$[9; \overline{6, 18}]$
60	$[7; \overline{1, 2, 1, 14}]$	85	$[9; \overline{4, 1, 1, 4, 18}]$
61	$[7; \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$	86	$[9; \overline{3, 1, 1, 1, 8, 1, 1, 1, 3, 18}]$
62	$[7; \overline{1, 6, 1, 14}]$	87	$[9; \overline{3, 18}]$
63	$[7; \overline{1, 14}]$	88	$[9; \overline{2, 1, 1, 1, 2, 18}]$
65	$[8; \overline{16}]$	89	$[9; \overline{2, 3, 3, 2, 18}]$
66	$[8; \overline{8, 16}]$	90	$[9; \overline{2, 18}]$
67	$[8; \overline{5, 2, 1, 1, 7, 1, 1, 2, 5, 16}]$	91	$[9; \overline{1, 1, 5, 1, 5, 1, 1, 18}]$
68	$[8; \overline{4, 16}]$	92	$[9; \overline{1, 1, 2, 4, 2, 1, 1, 18}]$
69	$[8; \overline{3, 3, 1, 4, 1, 3, 3, 16}]$	93	$[9; \overline{1, 1, 1, 4, 6, 4}, \overline{1, 1, 1, 18}]$
70	$[8; \overline{2, 1, 2, 1, 2, 16}]$	94	$[9; \overline{1, 2, 3, 1, 1, 5, 1, 8,}$ $\overline{1, 5, 1, 1, 3, 2, 1, 18}]$
71	$[8; \overline{2, 2, 1, 7, 1, 2, 2, 16}]$	95	$[9; \overline{1, 2, 1, 18}]$
72	$[8; \overline{2, 16}]$	96	$[9; \overline{1, 3, 1, 18}]$
73	$[8; \overline{1, 1, 5, 5, 1, 1, 16}]$	97	$[9; \overline{1, 5, 1, 1, 1, 1, 1}, \overline{1, 5, 1, 18}]$
74	$[8; \overline{1, 1, 1, 1, 16}]$	98	$[9; \overline{1, 8, 1, 18}]$
75	$[8; \overline{1, 1, 1, 16}]$	99	$[9; \overline{1, 18}]$

جدول (٥) : أصغر جذر بدائي g قياس العدد الأولي p حيث $p < 1000$

p	g	p	g	p	g	p	g	p	g	p	g
2	1	109	6	269	2	439	15	617	3	811	3
3	2	113	3	271	6	443	2	619	2	821	2
5	2	127	3	277	5	449	3	631	3	823	3
7	3	131	2	281	3	457	13	641	3	827	2
11	2	137	3	283	3	461	2	643	11	829	2
13	2	139	2	293	2	463	3	647	5	839	11
17	3	149	2	307	5	467	2	653	2	853	2
19	2	151	6	311	17	479	13	659	2	857	3
23	5	157	5	313	10	487	3	661	2	859	2
29	2	163	2	317	2	491	2	673	5	863	5
31	3	167	5	331	3	499	7	677	2	877	2
37	2	173	2	337	10	503	5	683	5	881	3
41	6	179	2	347	2	509	2	691	3	883	2
43	3	181	2	349	2	521	3	701	2	887	5
47	5	191	19	353	3	523	2	709	2	907	2
53	2	193	5	359	7	541	2	719	11	911	17
59	2	197	2	367	6	547	2	727	5	919	7
61	2	199	3	373	2	557	2	733	6	929	3
67	2	211	2	379	2	563	2	739	3	937	5
71	7	223	3	383	5	569	3	743	5	941	2
73	5	227	2	389	2	571	3	751	3	947	2
79	3	229	6	307	5	577	5	757	2	953	3
83	2	233	3	401	3	587	2	761	6	967	5
89	3	239	7	409	21	593	3	769	11	971	6
97	5	241	7	419	2	599	7	773	2	977	2
101	2	251	6	421	2	601	7	787	2		
103	5	257	3	431	7	607	3	797	2		
107	2	263	5	433	5	613	2	809	3		

إجابات وإرشادات لتمارين مختارة
Answers and Hints for Selected Exercises

تمارين (١,١)

(١) خطوة الاستقراء : لنفرض أن العبارة صائبة عندما $n = k \geq 6$.

$$2^{k+1} = 2 \times 2^k > 2(k^2 + 19) = k^2 + k^2 + 38 > k^2 + 2k + 38$$
$$> k^2 + 2k + 1 + 19 = (k+1)^2 + 19$$

ولذا فإن العبارة صائبة عندما $n = k + 1$.

(١٦) خطوة الاستقراء : لنفرض أن العبارة صائبة عندما $n = k \geq 2$.

$$\sum_{i=1}^{k+1} \frac{1}{\sqrt{i}} = \sum_{i=1}^{k} \frac{1}{\sqrt{i}} + \frac{1}{\sqrt{k+1}} > \sqrt{k} + \frac{1}{\sqrt{k+1}}$$

لاحظ أن $\sqrt{k}\sqrt{k+1} > k$. ولذا فإن

$$\sqrt{k}\sqrt{k+1} > \Rightarrow \sqrt{k}\sqrt{k+1} + 1 > k + 1 \Rightarrow \sqrt{k} + \frac{1}{\sqrt{k+1}} > \frac{k+1}{\sqrt{k+1}}$$

$$\Rightarrow \sqrt{k} + \frac{1}{\sqrt{k+1}} > \frac{1}{\sqrt{k+1}}$$

ونخلص إلى أن العبارة صائبة عندما $n = k + 1$.

(١٩) خطوة الاستقراء : لنفرض أن $\prod_{i=1}^{k}(1+a_i) \geq 1 + \sum_{i=1}^{k} a_i$.

$$\prod_{i=1}^{k+1}(1+a_i)=(1+a_{k+1})\prod_{i=1}^{k}(1+a_i)\geq(1+a_{k+1})(1+\sum_{i=1}^{k}a_i)$$
$$=1+\sum_{i=1}^{k}a_i+a_{k+1}+a_{k+1}\sum_{i=1}^{k}a_i=1+\sum_{i=1}^{k+1}a_i+a_{k+1}\sum_{i=1}^{k}a_i$$
$$\geq 1+\sum_{i=1}^{k+1}a_i$$

إذن ، العبارة صائبة عندما $n=k+1$.

(٣٠) خطوة الاستقراء: نفرض أن العبارة صائبة لكل $n=0,1,\ldots,k$

$$a_{k+1}=-2a_k+3a_{k-1}=-2[1-(-3)^k+3[1-(-3)^{k-1}]$$
$$=-2+2(-3)^k+3+(-3)^k=1+3(-3)^k=1-(-3)^{k+1}$$

وبالتالي فإن العبارة صائبة عندما $n=k+1$.

(٣٤) خطوة الاستقراء : نفرض أن العبارة صائبة لكل $n=2,3,\ldots,k$.

$$f_{k+7}=f_{k+6}+f_{k+5}=4f_{k+3}=f_k+4f_{k+2}+f_{k-1}$$
$$=4(f_{k+3}+f_{k+2})+(f_k+f_{k-1})=4f_{k+4}+f_{k+1}$$

إذن، العبارة صائبة عندما $n=k+1$.

(٤٩) استخدم أولاً الاستقراء الرياضي على n لاثبات أن

$f_2f_n+f_3f_{n+1}=f_{n+3}$ وأن $f_1f_n+f_2f_{n+1}=f_{n+2}$

ثم بعد ذلك استخدم الاستقراء الرياضي على m .

(٥١) (أ) $a_{k+1}=\sqrt{2+a_k}<\sqrt{2+2}=2$.

(ب) نفرض أن a_k عدد كسري، إذا كان $a_{k+1}=\sqrt{2+a_k}$ عدداً كسرياً فإن $a_{k+1}=\sqrt{2+a_k}=\frac{m}{n}$. عندئذ ، $a_k=\frac{m^2-2n^2}{n^2}$ عدداً كسرياً مما يناقض الفرض.

(ج) بالاستقراء الرياضي على n : لنفرض أن $a_k<a_{k+1}$

$$a_{k+1}=\sqrt{2+a_k}<\sqrt{2+a_{k+1}}=a_{k+2}$$

(د) لنفرض أن $\lim_{n\to\infty}a_n=L$. عندئذ ، $\lim_{n\to\infty}a_{n+1}=L$.

وبما أن $a_{n+1}=\sqrt{2+a_n}$ فإن $L=\sqrt{2+L}$. ومنه فإن $L^2-L-2=0$.

أي أن $L=2$ أو $L=-1$. ولكن عناصر المتتالية موجبة، إذن $L=2$.

تمارين (١,٢)

(١) ضع $2^n=(1+1)^n$ واستخدم مبرهنة ذات الحدين.

(٢) $2^{99}\times3^{101}\binom{200}{99}$.

(٤) استخدم الاستقراء الرياضي.

(٦) لاحظ أن $0=(1+(-1))^n$ ثم استخدم مبرهنة ذات الحدين.

(٨) استخدم التمرين (١) .

تمارين (١,٣)

(١) 64 (٢) 9 (٣) 18 (٤) 4 (٥) 29

(٦)

$$64=512\times2+320\times(-3)$$

$$9 = 963 \times (-15) + 657 \times 22$$

$$18 = 252 \times 4 + 198 \times (-5)$$

(٧) 35 (٨) 5 (٩) 4 (١٠) 1

(١١) $x = 28$ ، $y = -16$ ، $z = -1$ (أجوبة أخرى ممكنة).

(١٢) $x = 45$ ، $y = 5$ ، $z = 1$ ، $w = -15$ (أجوبة أخرى ممكنة).

(١٣) لا، لأن $7 \mid a$ و $7 \mid b$ يؤدي إلى أن $7 \mid 500$ وهذا مستحيل.

(١٤) إذا كان $\frac{a}{b} + \frac{c}{d} = n \in \mathbb{Z}$ فإن $ad = b(dn - c)$ وهذا يكون $b \mid ad$ ومن ثم $b \mid d$. وبالمثل $d \mid b$. وعليه $b = d$ وهذا مستحيل.

(١٧) إذا كان $(n, n-2) = d$ فإن $d \mid 2$. ومنه $d = 1$ أو $d = 2$. وبما أن n فردي فإن $d \neq 2$. إذن ، $d = 1$.

(١٨) لاحظ أن $6(7k+6) + (-7)(6k+5) = 1$.

(١٩) إلى (٣٠) استخدم الاستقراء الرياضي.

(٣١) $3 + 108 \ldots 111 = 111 \ldots 111 = n$ والعدد $n = 4k + 3$ لا يمكن أن يكون مربعاً كاملاً.

(٣٢) $n^6 = (n^2)^3 = (n^3)^2$ لكل $n \in \mathbb{Z}^+$.

(٣٥) إذا كان $(a,c) = d$ فإن $d \mid a$ و $d \mid c$. وبما أن $a \mid b$ فإن $d \mid b$. ولذا فإن $d = 1$.

(٣٦) ادرس الحالات $n = 5k \pm 1$ و $n = 5k \pm 2$.

(٣٧) بما أن $(n,10) = 1$ فإن $(n,5) = 1$ ومن ثم استخدم التمرين (٣٦) .

(٤١) $11^{10} - 1 = (11-1)(11^9 + 11^8 + 11^7 + \ldots + 11^2 + 11 + 1)$

وأحاد كل من الأعداد العشرة في المجموع يساوي 1. ولذا فإن 10 يقسم المجموع. ومن ثم 100 يقسم $11^{10}-1$.

(٤٢) لا: $1\mid 1$ و $1\mid 2$ ولكن $1\nmid 1+2$ و $1\nmid 1+1$.

(٤٤) 40 (٤٥) 467 (٤٦) 533 (٤٧) 250 .

(٥٦) انظر التمرين (٧) من التمارين المحلولة.

(٥٧) لاحظ أن $(a,a+2)$ يساوي 2 إذا كان a زوجياً ويساوي 1 إذا كان a فردياً.

تمارين (١,٤)

(١) $x=-22+5k$ ، $y=11-2k$ حيث $k\in\mathbb{Z}$.

(٢) $x=20+9k$ ، $y=-15-7k$ حيث $k\in\mathbb{Z}$.

(٣) $(60,18)=3$ لا يقسم 97 ومن ثم لا يوجد حلول صحيحة.

(٤) $x=500+5k$ ، $y=-4250-43k$ حيث $k\in\mathbb{Z}$.

(٥) $x=54-k$ ، $y=10-k$ حيث $k\in\mathbb{Z}$.

(٦) $x=7k$ ، $y=30-15k$ حيث $k\in\mathbb{Z}$.

(٧) $x=14+17k$ ، $y=-1-7k$ حيث $k\in\mathbb{Z}$.

(٨) $x=-55+38k$ ، $y=22-15k$ حيث $k\in\mathbb{Z}$.

(٩) $x=15+14k$ ، $y=-78-73k$ حيث $k\in\mathbb{Z}$.

(١٠) لا توجد حلول صحيحة.

(١١) $(1,66)$ ، $(12,4)$.

(١٢) لا توجد حلول صحيحة موجبة.

(١٣) (2,7) ، (5,5) ، (8,3) ، (11,1).

(١٤) (9,71) ، (30,40) ، (51,9) .

(١٥) يوجد عدد غير منته من الحلول الصحيحة الموجبة.

(١٦) (1,27) ، (8,16) ، (15,5) .

(١٧) يوجد عدد غير منته من الحلول الصحيحة الموجبة.

(١٨) $x = y = 10$ فقط.

(١٩) لا يوجد حلول صحيحة موجبة.

(٢٠) يوجد عدد غير منته من الحلول الصحيحة الموجبة.

(٢١) $x = 8 + 2k$ ، $y = -48 - 15k - 5t$ ، $z = 16 + 5k + 2t$.

(٢٢) $x = 2 - 3k + 2t$ ، $y = 3 + 7k + 2t$ ، $z = t$.

(٢٣) يوجد 27 حل موجب أحدها (2,3,4,5) .

(٢٤) $x = -1 + 44k$ ، $y = 2 - 50k$ ، $z = 1 - 27k$.

(٢٥) توجد أربعة حلول موجبة أحدها (162,41,67) .

(٢٦) الحل العام: $x = 60 - 4k$ ، $y = 27 + k$ ، $z = k$.

والحلول الموجبة نحصل عليها عندما $1 \le k \le 14$.

(٢٧) يلزمنا إيجاد الحلول الموجبة للنظام $x + y + z = 41$ و $48x + 36y + 4z = 480$ والحل الموجب الوحيد هو $x = 5$ ، $y = 3$ ، $z = 33$.

(٢٨) $M = 4128$.

(٢٩) إما 4, 1, 5, 90 أو 4, 2, 2, 92 .

تمارين (١,٥)

(١) $(11101001000)_2$.

(٢) $(10705679)_{10}$.

(٣) $(10111110110011)_2$.

(٤) $(3DE9)_{16}$.

(٥) $(111001)_2$.

(٦) $(F01D)_{16}$.

(٧) $(34132)_5$.

(٨) $(21131)_5$.

(٩) $(2620)_{10}$.

(١٠) $(1001101000001011)_2$.

تمارين (٢,١)

(٣) لا : ضع $a=p$ و $b=p^3$.

(٤) لا : ضع $a=p=2$.

(٥) $p=3$ فقط.

(٨) لا : ضع $a=8$ و $b=4$ (أجوبة أخرى ممكنة).

(٩) (أ) $p=19$. (ب) $p=5$.

(١٠) بما أن $2p+2=2(p+1)$ فيكفي اثبات أن $6 \mid (p+1)$. الآن ، بما أن p فردي فإن $2 \mid (p+1)$. أثبت أن $3 \mid (p+1)$ بدراسة الحالتان $p=3k+1$ و $p=3k+2$.

(١١) حلل مجموع المكعبين.

(١٢) حلل الفرق بين مكعبين ثم استنتج المطلوب.

(١٣) $n=25=9+4^2$.

(١٤) $a^4+4=(a^2+2)^2-4a^2=(a^2+2-4a)\,(a^2+2+4a)$.

(١٥) $8^n+1=(2^n)^3+1$ مجموع مكعبين.

(١٦) إذ كان $n=2k$ فإن $n=2(k-3)+6$ و $k\geq 5$

وإذا كان $b=2k+1$ فإن $n=2(k-4)+9$ و $k\geq 5$.

(١٨) ادرس الحالات $p=5k+r$ ، $r=1,2,3,4$.

(١٩) لاحظ أن $\left(\frac{p}{k}\right)=p\frac{(p-1)!}{k!(p-k)!}$ لا يقسم المقام.

(٢٣) خطأ : ضع $p=a=2$ ، $b=4$ ، $m=1$.

(٢٤) العكس غير صحيح : ضع $n=11$.

(٢٥) أدرس الحالتين $2^n=3k+1$ و $2^n=3k+2$.

(٢٦) ادرس الحالات $p=3$ ، $p=3k+1$ ، $p=3k+2$.

(٣٠) إذا كان $2^a \,||\, n!$ و $5^b \,||\, n!$ فإن $a>b$ و $n!=2^a5^b m$ حيث $(m,10)=1$. إذن، $10^b \,||\, n!$ ومن ثم $\frac{n!}{10^b}=2^{a-b}m$ عدد زوجي.

(٣١) إذا كان $10^a \,||\, 169!$ فإن $2^a \,||\, 169!$ و $5^b \,||\, 169!$ وأن $b<a$. عندئذ، عدد أصفار $169!$ هو $[\frac{169}{5}]+[\frac{169}{25}]+[\frac{169}{125}]=33+6+1=40$.

(٣٢) عدد الأصفار هو : $124-49=75$.

(٣٣) لنفرض أن $M=1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}$. ولنفرض أن k هو أكبر عدد صحيح يحقق $2^k\leq n$ و P حاصل ضرب جميع الأعداد الفردية التي لا تزيد عن n . عندئذ ، $2^{k-1}PM=A+2^{k-1}P(\frac{1}{2^k})=A+\frac{1}{2}P$

(٢٩) إما 4, 1, 5, 90 أو 4, 2, 2, 92 .

تمارين (١,٥)

(١) $(11101001000)_2$.

(٢) $(10705679)_{10}$.

(٣) $(10111110110011)_2$.

(٤) $(3DE9)_{16}$.

(٥) $(111001)_2$.

(٦) $(F01D)_{16}$.

(٧) $(34132)_5$.

(٨) $(21131)_5$.

(٩) $(2620)_{10}$.

(١٠) $(1001101000001011)_2$.

تمارين (٢,١)

(٣) لا : ضع $a=p$ و $b=p^3$.

(٤) لا : ضع $a=p=2$.

(٥) $p=3$ فقط.

(٨) لا : ضع $a=8$ و $b=4$ (أجوبة أخرى ممكنة).

(٩) (أ) $p=19$. (ب) $p=5$.

(١٠) بما أن $2p+2=2(p+1)$ فيكفي اثبات أن $6 \mid (p+1)$. الآن ، بما أن p فردي فإن $2 \mid (p+1)$. أثبت أن $3 \mid (p+1)$ بدراسة الحالتان $p=3k+1$ و $p=3k+2$.

(١١) حلل مجموع المكعبين.

(١٢) حلل الفرق بين مكعبين ثم استنتج المطلوب.

(١٣) $n=25=9+4^2$.

(١٤) $a^4+4=(a^2+2)^2-4a^2=(a^2+2-4a)(a^2+2+4a)$.

(١٥) $8^n+1=(2^n)^3+1$ مجموع مكعبين.

(١٦) إذ كان $n=2k$ فإن $n=2(k-3)+6$ و $k\geq 5$

وإذا كان $b=2k+1$ فإن $n=2(k-4)+9$ و $k\geq 5$.

(١٨) ادرس الحالات $p=5k+r$ ، $r=1,2,3,4$.

(١٩) لاحظ أن $\left(\frac{p}{k}\right)=p\frac{(p-1)!}{k!(p-k)!}$ لا يقسم المقام.

(٢٣) خطأ : ضع $p=a=2$ ، $b=4$ ، $m=1$.

(٢٤) العكس غير صحيح : ضع $n=11$.

(٢٥) أدرس الحالتين $2^n=3k+1$ و $2^n=3k+2$.

(٢٦) ادرس الحالات $p=3$ ، $p=3k+1$ ، $p=3k+2$.

(٣٠) إذا كان $2^a \| n!$ و $5^b \| n!$ فإن $a>b$ و $n!=2^a5^b m$ حيث $(m,10)=1$. إذن، $10^b \| n!$ ومن ثم $\frac{n!}{10^b}=2^{a-b}m$ عدد زوجي.

(٣١) إذا كان $10^a \| 169!$ فإن $2^a \| 169!$ و $5^b \| 169!$ وأن $b<a$. عندئذ، عدد أصفار $169!$ هو $40=33+6+1=[\frac{169}{5}]+[\frac{169}{25}]+[\frac{169}{125}]$.

(٣٢) عدد الأصفار هو : $75=49-124$.

(٣٣) لنفرض أن $M=1+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{n}$. ولنفرض أن k هو أكبر عدد صحيح يحقق $2^k\leq n$ و P حاصل ضرب جميع الأعداد الفردية التي لا تزيد عن n . عندئذ ، $2^{k-1}PM=A+2^{k-1}P(\frac{1}{2^k})=A+\frac{1}{2}P$

حيث A عدد صحيح. ولذا لا يمكن أن يكون M عدداً صحيحاً.

(٣٦) $\sqrt{2}+\sqrt{3}$ جذراً لكثيرة الحدود x^4-10x^2+1.

(٣٩) (ب) لنفرض أن $[a,b]=m$ وأن $(a,m)=d$. عندئذ، $m=ca$ و $d=ax+my$. الآن:

$$d=ax+my=ax+cay=a(x+cy)\Rightarrow a\mid d$$

ولكن $d\mid a$. إذن، $a=d$.

(٤٠) حلل الأعداد إلى قوى عواملها الأولية.

تمارين (٢,٢)

(٣) إذا كان $p=p_i$ فإن $p\mid N$. وبما أن $p\mid(N-1)$ فإن $p\mid 1$ وهذا مستحيل.

(٥) لنفرض أن $p_1<p_2<\ldots<p_n$ هي جميع الأعداد الأولية التي على الصورة $6k-1$ وليكن $N=6p_1p_2\ldots p_n-1$. لاحظ أن N على الصورة $6k-1$. إذا كان جميع القواسم الأولية للعدد N على الصورة $6k+1$ فإن N على الصورة $6k+1$. ولذا فإنه يوجد قاسم أولي $p\mid N$ على الصورة $p=6k-1$. إذن، $p=p_i$ ومن ثم فإن $p\mid 1$ وهذا مستحيل.

(٩) لنفرض أن $a+nb=p$ عدداً أولياً ولنفرض أن $n_k=n+kp$ حيث $k=1,2,\ldots$. سنبرهن أن $a+n_kb$ مؤلف لكل $k=1,2,3,\ldots$.

$$a+n_kb=a+(n+kb)p=a+nb+kbp=p+kbp=p(1+kb)$$

ولهذا فإن $p \mid (a+n_k b)$ لكل $k \geq 1$.

(١٠) افرض أن $p \neq 2$ ثم أدرس الحالتين $p = 4k+1$ و $p = 4k+3$.

(١٤) إذا كان $a = 1$ فمن الواضح وجود عدد غير منته من الأوليات على الصورة $k+b$. لنفرض إذن أن $a > 1$. بما أن $(a,b) = 1$ فإن $(a^n,b) = 1$ لكل $n \geq 1$. بما أن $(a,b) = 1$ فإن $(a^n,b) = 1$ لكل $n \geq 1$ ونجد من الفرض عدداً أولياً p على الصورة $a^n k+b$. أي على الصورة $am+b$ حيث $p > a^n$ لكل $n \geq 1$. ونخلص إلى وجود عدد غير منته من الأوليات على الصورة المطلوبة.

(١٥) بما أن $n > 7$ عدد فردي فإن $n-3 > 4$ عدد زوجي ومن ثم $n-3 = p+q$. أي أن $n = 3+p+q$.

تمارين (٢,٣)

(١) إذا كان a فردياً فإن a^m+1 عدد زوجي أكبر من 2 . ولذا فهو مؤلف. إذن، a عدد زوجي. واثبات أن m قوة للعدد 2 يماثل اثبات المبرهنة (٢,١٤).

(٥) خاطيء : بوضع $a = 12$ و $n = 2$ نجد $N = 12^4+1 = 20737 = 89 \times 233$ وكل من العددين 89 و 233 ليس عدداً لفيرما.

(٦) استخدم الاستقراء الرياضي لإثبات أن $F_n - 7$ يقسم 10 .

(٧) استخدم الاستقراء الرياضي لاثبات أن $F_n + 4$ يقسم 3.

تمارين (٢,٤)

(٣) (أ) $k=8$ (ب) $k=4$ (ج) $k=10$.

(٤) (أ) $k=3$ (ب) $k=4$ (ج) $k=2$.

(٥) العدد في الفقرة (ب) لا يقبل القسمة وأعداد باقي الفقرات تقبل القسمة.

(٦) كل من (أ) و (ب) لا يقبل القسمة على 9 وكل من (ج) و (د) يقبل.

(٧) (ب) يقبل القسمة على 7 ولا يقبل القسمة على 11 أو 13 .

(١٤) $2^{18}+1=4(2^4)^4+1=(2\times2^8+2\times2^4+1)(2\times2^8-2\times2^4+1)=545\times481$

تمارين (٣,١)

(١) 1 (٢) 8 (٣) 6 (٤) 1 (٥) 1 (٦) 9

(٧) إلى (١٥) : استخدم حوارزمية التربيع.

(٢٧) خطأ : لاحظ أن $3\equiv1(\text{mod }2)$ ولكن $3\not\equiv1(\text{mod }4)$.

(٢٨) بما أن k فردي فإن:

$$11^{2k}+19^{2k}=(121)^k+(120)^k\equiv(121)^k+(-121)^k\equiv0(\text{mod }241)$$

(٢٩) استخدم $p\equiv\pm1(\text{mod }3)$.

(٣٢) $x=6,y=2$ أو $x=2,y=6$.

(٣٣) $x=2,y=3$ أو $x=y=7$.

(٣٤) العكس غير صحيح : $(3,5)=(2,5)=1$ ولكن $2\not\equiv3(\text{mod }5)$.

(٣٩) خطأ : $9\equiv16(\text{mod }7)$ ولكن $3\not\equiv4(\text{mod }7)$.

(٤٠) خطأ : ضع $a=3$ ، $b=4$ ، $k=2$ ، $j=9$ ، $n=7$.

(٤٣) $a^2 \equiv b^2 \pmod p \Leftarrow p \mid (a-b)(a+b) \Leftarrow p \mid a-b$ أو $p \mid a+b$.

(٤٤) بما أن $a^k \equiv b^k \pmod m$ فإن $ba^k = b^{k+1} \pmod m$ ، ولذا فإن $ba^k \equiv a^{k+1} \pmod m$. وبما أن $(a,m)=1$ فإن $(a^k,m)=1$. وبهذا يكون $b \equiv a \pmod m$.

العبارة خاطئة عندما يكون $(a,m)>1$: ضع $m=a=4$ ، $b=k=2$.

(٤٧) (أ) $\{\pm1, \pm3, \pm5, 7\}$ (أجوبة أخرى ممكنة).

(ب) $\{0, \pm2, \pm4, \pm6\}$ (أجوبة أخرى ممكنة).

(ج) $\{2,3,5,7,11,13,29\}$ (أجوبة أخرى ممكنة).

(٤٨) لا: لأنه لا يوجد $x \in \mathbb{Z}$ يحقق $x^2 \equiv 3 \pmod 7$.

(٥١) لا: لاحظ أن $1 \not\equiv m-1 \pmod m$ ولكن $1^2 \equiv (m-1)^2 \pmod m$.

(٥٥) $\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} i \equiv \frac{n(n+1)}{2} \equiv 0 \pmod n$.

(٥٦) $(160)^{-1} \equiv 205 \pmod{841}$.

(٥٧) $c(ac^{-1}-bd^{-1}) \equiv acc^{-1}-bcd^{-1} \equiv acc^{-1}-bdd^{-1} \equiv a-b \equiv 0 \pmod m$

ولذا فإن $ac^{-1}-bd^{-1} \equiv 0 \pmod m$.

تمارين (٢, ٣)

(١) 107 (٢) 1239 (٣) لا يوجد حلول.

(٤) $x=-10+26k$ حيث $0 \le k \le 6$.

(٥) $x=4+5k$ حيث $k=0,1,2$.

(٦) 198 (٧) لا يوجد حلول (٨) $x=4+7k$ ، $0\le k\le 5$.

(٩) 1 (١٠) $x=4+5k$ ، $0\le k\le 71$ (١١) 812

(١٢) 1596 (١٣) 968 (١٤) $x=13+67k$ ، $0\le k\le 10$.

(١٥) 15 (١٦) $x=2+7k$ ، $k=0,1$ (١٧) لا يوجد حلول.

(١٨) 18 (١٩) 293 (٢٠) 1816 (٢١) 35 .

(٢٢) $x=16+21k$ ، $0\le k\le 3$.

(٢٣) $x=17+126k$ ، $0\le k\le 5$.

(٢٤) 624 (٢٥) 103 (٢٦) 453 .

(٢٧) يوجد 14 حل هي: (8,0) ، (6,1) ، (4,2) ، (2,3) ، (0,4) ، (11,5) ، (9,6) ، (7,7) ، (5,8) ، (3,9) ، (1,10) ، (12,11) ، (10,12) .

(٢٨) يوجد عشرة حلول. (٢٩) يوجد 12 حلاً. (٣٠) يوجد 16 حلاً.

(٣١) يوجد 27 حلاً. (٣٢) لا يوجد حلول. (٣٣) يوجد 14 حلاً.

(٣٤) لا يوجد حلول.

(٣٥) يوجد 5 حلول هي : (4,0) ، (2,1) ، (0,2) ، (3,3) ، (1,4) .

(٣٦) يوجد 16 حلاً.

تمارين (٣,٣)

(١) $23 \pmod{105}$. (٢) $2055 \pmod{2889}$.

(٣) $58 \pmod{60}$. (٤) $74 \pmod{990}$.

(٥) $815 \pmod{1260}$. (٦) $1272 \pmod{2310}$.

(٧) $106 \pmod{252}$.
(٨) $12113 \pmod{20128}$.
(٩) $62 \pmod{140}$.
(١٠) $3041 \pmod{5040}$.
(١١) $6 \pmod{210}$.
(١٢) $150999 \pmod{554268}$.
(١٣) $1423 \pmod{2310}$.
(١٤) $88 \pmod{105}$.
(١٥) $104 \pmod{180}$.
(١٦) $33 \pmod{30}$.
(١٧) $100 \pmod{210}$.
(١٨) النظام غير منسجم.
(١٩) $44 \pmod{840}$.
(٢٠) النظام غير منسجم.
(٢١) $148 \pmod{210}$.
(٢٢) النظام غير منسجم.
(٢٣) $1413 \pmod{2200}$.
(٢٤) النظام غير منسجم.
(٢٥) $1829 \pmod{8180}$.
(٢٦) $327 \pmod{380}$.
(٢٧) $104 \pmod{165}$
(٢٨) $222 \pmod{529}$
(٢٩) $33 \pmod{276}$ (٣٠) 62 (٣١) 350 (٣٢) 17 (٣٣) 59
(٣٤) 1103 (٣٥) 3424 ، 4425 (٣٦) 129 (٣٧) 73800
(٣٨) 119 (٣٩) 15 ، 8 ، 23 على التوالي.
(٤٠) $2 \pmod{55}$ أو $46 \pmod{55}$.
(٤١) حلول التطابقات هي: $\pm 3 \pmod{67}$ ، $\pm 5 \pmod{11}$ ، $\pm 2 \pmod{13}$
وبهذا يلزمنا حل 8 أنظمة من التطابقات هي
$x \equiv a \pmod{7}$ ، $x \equiv b \pmod{11}$ ، $x \equiv c \pmod{13}$ حيث
$a = \pm 3$ ، $b = \pm 5$ ، $c = \pm 2$ لنحصل على حلول النظام الأصلي وهي:
$x = \pm 115$, ± 171 , ± 193 , $\pm 479 \pmod{1001}$.

تمارين (٣,٤)

(١) $x=7$ ، $y=8$ (٢) $x=10$ ، $y=11$.

(٣) لا يوجد حلول (٤) حلان: ($x=6$ ، $y=7$) و ($x=19$ ، $y=20$)

(٥) $x=6$ ، $y=1$. (٧)ثلاث حلول: $x=0,3,4$ و $y=7,4,1$ على التوالي.

(٨) $x=9$ ، $y=21$ (٩) جميع الأزواج المرتبة (x,x) .

(١٠) لا يوجد حلول (١١) $x=0$ ، $y=1$ ، $z=2$.

(١٢) $x=1$ ، $y=z=0$ (١٣) $x=y=z=w=5$.

(١٤) $x=3$ ، $y=4$ ، $z=1$ (١٥) لا يوجد حلول.

(١٦) ثلاث حلول: $x=7, 10, 13$ ، $y=1, 1, 1$ ، $z=0, 9, 3$ على التوالي.

تمارين (٣,٥)

(١) 13 (٢) 28

(٣) بما أن $1000000 \equiv 4 \pmod 6$ فإن $2^{1000000} \equiv 2^4 \equiv 16 \equiv 2 \pmod 7$.

(٥) لاحظ أولاً أن $2222 \equiv 2 \pmod 6$ وأن $5555 \equiv 5 \pmod 6$.

(٧) مماثل للتمرين المحلول (٦) (٨) استخدم التمرين (٧) .

(١٠) بما أن $\varphi(100)=40$ وأن $9^9 \equiv (9^3)^3 \equiv 9^3 \equiv 9 \pmod{40}$ فإن $9^{9^9} \equiv 9^9 \pmod{100}$. ولكن باستخدام خوارزمية التربيع نجد أن $9^9 \equiv 89 \pmod{100}$.

(١٥) 26 (١٦) 79 .

(١٩) أثبت أن $a^{pq} \equiv a \pmod{p}$ وأن $a^{pq} \equiv a \pmod{q}$.

(٢١) جميع الأعداد n حيث n و $n+1$ مؤلفان.

(٢٢) استخدام مبرهنة فيرما الصغرى. (٢٣) استخدم مبرهنة أويلر.

(٢٥) (ب) $304x^{303} + 204x^{202} - 104x^{101} \equiv x^3 + 2x^2 - 3x$

$$\equiv x(x-1)(x+3) \pmod{101}$$

ولذا فإن $x \equiv 0, 1, -3 \pmod{101}$.

(٢٧) باستخدام مبرهنة ويلسن لدينا:

$$-1 \equiv (p-1)! = (p-1)(p-2)(p-3)! \equiv (-1)(-2)(p-3)! \pmod{p}$$

وبهذا يكون $2(p-3)! \equiv -1 \pmod{p}$.

(٢٩) استخدم مبرهنة فيرما الصغرى ومبرهنة ويلسن.

(٣٤) (أ) $n = p-1$ ، $p > 5$ أولي (ب) $n = p-1$ ، p أولي.

(٣٧) بما أن $a^p \equiv b^p \pmod{p}$ فإن $a \equiv b \pmod{p}$. الآن ضع $a = b + kp$

ثم استخدم مبرهنة ذات الحدين.

(٣٨) احسب $k! \binom{p-1}{k} \pmod{p}$.

(٣٩) أثبت أولاً أن $(a-1)(1+a+a^2+\ldots+a^{\varphi(m)-1}) \equiv 0 \pmod{m}$ ثم

استخدم $(a-1, m) = 1$ لتحصل على المطلوب.

(٤٢) لنفرض أن $a \not\equiv 0 \pmod{p}$. عندئذ يوجد نظير ضربي c للعدد a قياس p. الآن:

$$a^2 + b^2 \equiv 0 \pmod{p} \Rightarrow (ac)^2 + (bc)^2 \equiv 0 \pmod{p}$$

$$\Rightarrow 1 + (bc)^2 \equiv 0 \pmod{p} \Rightarrow (bc)^2 \equiv -1 \pmod{p}$$

وهذا مستحيل لأن $p \equiv 3 \pmod 4$. إذن $a \equiv 0 \pmod p$ وبالمثل ، $b \equiv 0 \pmod p$.

(٤٣) لاحظ أن $x^2 + 1 = 23y \equiv 0 \pmod{23}$. وبما أن $23 \equiv 3 \pmod 4$ فإنه لا يوجد حل للمعادلة.

(٤٥) خطأ : ضع $p = 13$ و $a = 5$. ولاحظ أن $5^8 \equiv 5^4 \equiv 1 \pmod{13}$ ولكن 8 لا يقسم 12 .

(٤٧) لاحظ أولاً أن $2^2 \equiv 1 \pmod{2^n - 1}$ ولكل $1 \le k < n$ لدينا $2 \le 2^k < 2^n$. ولهذا $2^k \not\equiv 1 \pmod{2^n - 1}$. إذن رتبة 2 قياس $2^n - 1$ تساوي n وبهذا نرى أن n يقسم $\varphi(2^n - 1)$.

(٥٠) (ب) $x \equiv 27 \pmod{68}$ للتطابق الاول $x \equiv 11 \pmod{68}$ للثاني.

(٥٣) بما أن p يقسم $2^q + 1$ فإن $2^q \equiv -1 \pmod p$. عندئذ، $2^{2q} \equiv 1 \pmod p$ ، ومن ثم فإن $ord_p(2) \mid 2q$. وعليه يكون $ord_p(2) = 2$ أو $ord_p(2) = 2q$ (لا يمكن أن يكون $ord_p(2) = q$ لأن $2^q \equiv -1 \pmod p$). إذا كان $ord_p(2) = 2$ فإن $p = 3$. أما إذا كان $ord_p(2) = 2q$ فإن $2q \mid (p-1)$.

(٥٧) لاحظ أولاً أن $a^2 + a + 1 \equiv 0 \pmod p$. احسب الآن $(a+1)^3 \pmod p$.

(٥٩) $M_p(M_p + 2) = (2^{(q-1)/2} - 1)(2^{(q+1)/2} + 1) = 2^{q-1} - 1 \equiv 0 \pmod q$

(٦٠) لا: لأن $p = 29$ ، $q = 59$ ، $59 \nmid M_{29}$ ، $59 \mid M_{29} + 2$.

(٦٥) و (٦٦) : استخدم التمرين (٦٤).

(٦٧) 15 شبه أولي للأساس 4 ولكن $N=\frac{4^{15}-1}{3}$ ليس شبه أولي للأساس 4 . لاحظ أن $(4-1,\ 15)\neq 1$. وأن $4^{15}\equiv 1(\text{mod } N)$ ولكن $N-1=\frac{4(14^4-1)}{3}$ لا يقبل القسمة 3 ومن ثم لا يقبل القسمة على 15 .

(٦٨) (ب) ضع $m=3$ في الفقرة (أ) لتجد أن p يقسم كل من الأعداد 2^2-1 ، 5^2-1 ، 7^2-1 وهذا مستحيل.

(ج) ضع $m=5$ واستخدم الفقرة (أ)

(د) إذا كان $n<91$ شبه أولي للأساس 3 فإن $n=pq$ حيث كل من p و q أولي أكبر من 5. أي أن $n=49$ أو $n=77$ وكلاهما ليس شبه أولي للأساس 3.

تمارين (٦,٣)

(١) $x\equiv 64(\text{mod } 5^3)$ (٢) $x\equiv -31(\text{mod } 5^3)$.

(٣) حلا التطابق $f(x)\equiv 0\ (\text{mod } 5)$ هما $s_1=\pm 1$.

عندما $s_1=1$ يكون للتطابق $f(x)\equiv 0(\text{mod } 5^2)$ خمسة حلول هي 1 ، 6 ، 11 ، 16 ، 21 . أما عندما $s_1=-1$ فإن له حل وحيد هو 9.

(٤) $f(x)\equiv 2x^2+1\ (\text{mod } 3)$ وحلا التطابق $f(x)\equiv 0(\text{mod } 3)$ هما $s=\pm 1$.

كما أن $f(x)\equiv 3x+3(\text{mod } 7)$ وحلا التطابق $f(x)\equiv 0(\text{mod } 7)$ هما

$s=-2,3$. باستخدام مبرهنة الباقي الصينية نجد أن حلول التطابق $f(x)\equiv 0 \pmod{21}$ هي 5 ، 10 ، 17 ، 19 .

(٥) (أ) 1 ، 3 (ب) 6 (ج) 6 .

(٦) (أ) 2 ، 4 ، 6 (ب) 20 ، 37 ، 39 (ج) 37 ، 137 ، 167 .

(٧) 3 ، 13 ، 18 ، 33 .

(٨) (أ) 22 (ب) 2 ، 9 ، 16 ، 23 ، 30 ، 37 ، 44

(ج) 184 ، 373 ، 562 ، 751 ، 940 ، 1129 ، 1318 .

(٩) (أ) 7 (ب) 23 (ج) 3257 .

(١٠) (أ) 0 ، 3 (ب) 6 ، 7 (ج) 7 ، 15 ، 16 ، 24 .

(١١) الاجابة لا في الحالتين (١٢) الاجابة نعم.

(١٣) (أ) يوجد حلان للتطابق $x^2\equiv 1 \pmod{p_i^{\alpha_i}}$ لكل $1\le i\le r$.

ولذا فعدد حلول $x^2\equiv 1 \pmod{m}$ يساوي 2^r.

(ب) باستخدام الفقرة (أ) يوجد أربع قواسم أولية للعدد m . ولذا فإن

$$m=3\times 5\times 7\times 11=1155$$

(ج) $m=2^k n$ حيث n فردي. للتطابق $x^2\equiv 1 \pmod{2^k}$ حل واحد عندما $k=1$ ، حلان عندما $k=2$ ، أربع حلول عندما $k\ge 3$. ولذا فإن أصغر m هو $8\times 3\times 5=120$.

(١٥) $f(x)=x^p-x+1\equiv x-x+1\equiv 1\not\equiv 0 \pmod{p}$

(١٧) العدد المطلوب يحقق التطابق $x^2\equiv x \pmod{10^5}$. بحل هذا التطابق نجد أن $x=0,1\,9376,\,90625$. ويكون العدد المطلوب هو 90625 .

(١٨) لنفرض أن $f(x)=x^2-a$. من الواضح أنه إذا كان $f(x)\equiv 0 \pmod{p^{k+1}}$ قابلاً للحل فإن $f(x)\equiv 0 \pmod{p^k}$ قابل للحل. وبالعكس ، إذا كان s حلاً للتطابق $f(x)\equiv 0 \pmod{p^k}$ فإن $p\nmid s$ (لأن $(a,p)=1$) . وبهذا نرى أن $p\nmid f'(s)=2s$ ومن ثم استناداً إلى المبرهنة (٣,٥٠) يكون التطابق $f(x)\equiv 0 \pmod{p^{k+1}}$ قابلاً للحل.

(٢١) حل واحد فقط (٢٢) حلان (٢٣) لا توجد حلول.

(٢٤) حل واحد فقط (٢٥) 4 حلول (٢٦) 8 حلول.

(٢٧) لا توجد حلول.

تمارين (٤,١)

(١) (18, 24, 30) ، (18, 80, 82) .

(٢) (7, 24, 25) ، (143, 24, 145) .

(٣) (21, 20, 29) ، (21, 220, 221) .

(٤) (119, 44, 125) (٥) (63, 16, 65) ، (12, 16, 20) ، (30, 16, 34) .

(٦) (35, 12, 37) ، (35, 612, 513) ، (35, 84, 91) ، (35, 120, 125) .

(٨) أثبت أن كل من 3 ، 4 ، 5 يقسم xyz .

(٩) كل من $x^2+y^2=1^2$ و $x^2+y^2=2^2$ غير قابل للحل.

(١٣) $y\equiv 2 \pmod 4 \Rightarrow 2mn\equiv 2 \pmod 4 \Rightarrow mn\equiv 1 \pmod 4$

وهذا مستحيل لأن mn عدد زوجي.

(١٤) $p = z = k(m^2+n^2)$. بما أن p أولي وأن $m^2+n^2 > 1$ فإن $k = 1$.

إذن، $p = m^2+n^2$ وبهذا يكون $p \equiv 1 \pmod 4$ (أنظر مبرهنة (٤,٨))

(١٦) $x+(x+1) = y^2 \Rightarrow 2x+1 = y^2 \Rightarrow (x+1)^2 = x^2+2x+1 = x^2+y^2$

تمارين (٤,٢)

(١) (أ) 7^2+7^2 (ب) $343 = 7^3$ لا يمكن كتابته كمجموع مربعين.

(ج) $735 = 3\times5\times7^2$ ولذا لا يمكن كتابته كمجموع مربعين.

(د) $1428 = 2^2\times3\times7\times17$ ولذا لا يمكن كتابته كمجموع مربعين.

(س) $4680 = 2^3\times3^2\times5\times13 = (2^2+2^2)(3^2+0^2)(2^2+1^2)(3^2+2^2)$

$= (6^2+6^2)(4^2+7^2) = (-18)^2+(66)^2$

(ص) $5525 = 5^2\times13\times17 = (62)^2+(41)^2 = 7^2+(74)^2$

(م) $14365 = 5\times13^2\times17 = (21)^2+(118)^2$

(هـ) $229320 = 2^3\times3^2\times7^2\times5\times13 = (126)^2+(462)^2$

(و) $16660 = 2^2\times5\times17\times7^2 = (28)^2+(126)^2$

(٣) على الأقل عدد واحد من بينها يطابق 3 قياس 4 .

(٤) $2p-1 = n^2 \Rightarrow p = \dfrac{n^2+1}{2} = \left(\dfrac{n-1}{2}\right)^2+\left(\dfrac{n+1}{2}\right)^2$

(٥) لا يوجد، لأنه لو كان $n^2=x^2+y^2$ فإن جميع قواسم n^2 الأولية لا يمكن أن تكون على الصورة $4k+3$ وهذا تناقض لأن 3 يقسم n^2 .

(٦) لاحظ أن $a^2+b^2\not\equiv 3 \pmod 9$ أو 6.

(٨) أحدهما ليس على الصورة $4^m(8k+7)$.

(١١) يوجد عدد غير منته من الأعداد الأولية التي على الصورة $p=4k+3$.

ولذا $p-1=4k+2$ ليس على الصورة $4^m(8k+7)$. إذن $p-1=a^2+b^2+c^2$ وبهذا يكون $p=a^2+b^2+c^2+1$.

(١٢) إذا كان n ليس على الصورة $4^m(8k+7)$ فإن n مجموع ثلاث مربعات ومن ثم مجموع أربع مربعات.

إذا كان n على الصورة $4^m(8k+7)$ فإن

$n-4^m=4^m(8k+6)=a^2+b^2+c^2\Rightarrow n=a^2+b^2+c^2+(2^m)^2$.

تمارين (٤,٣)

(٣) إذا كان $p\nmid xyz$ فإن p لا يقسم أي منها. ولذا فإن

$x^{p-1}\equiv y^{p-1}\equiv z^{p-1}\equiv 1 \pmod p$ وبهذا يكون

$2=1+1\equiv x^{p-1}+y^{p-1}\equiv z^{p-1}\equiv 1 \pmod p$ وهو مستحيل.

(٤) لاحظ أن $x^p+y^p-z^p\equiv x+y-z\equiv 0 \pmod p$.

(٧) لاحظ أن

$x^4-4y^4=z^2 \Rightarrow (x^4-4y^4)^2=z^4 \Rightarrow (2xy)^4+z^4=(x^4+4y^4)^2$

(٩) افرض وجود حل ثم استخدم ثلاثيات فيثاغورس.

(١٠) و (١١) استخدم ثلاثيات فيثاغورس.

(١٢) $x=3k^2-1$ ، $y=k(k^2-3)$ ، $z=k^2+1$ حيث $k\in\mathbb{Z}$.

(١٣) إذا كان $a^2+b^2=c^2$ و $a^2-b^2=d^2$ فإنه سيوجد حل للمعادلة $x^4-y^4=z^2$ وهذا مستحيل.

(١٤) إذا كان اثنان منهما مربعان كاملان فإن للمعادلة $x^4+y^4+z^2$ أو للمعادلة $x^4-y^4=z^2$ حل وهذا مستحيل.

(١٥) الحلول هي: $x=\pm1$ و $y=0$.

(١٧) إذا كان $\frac{1}{2}xy=2c^2$ و $x^2+y^2=z^2$ فإننا سنحصل على تناقض لتمرين (٧).

(١٨) بضرب المعادلتين نحصل على المعادلة $x^4-y^4=(zw)^2$ والتي ليس لها حلول.

(١٩) اطرح المعادلتين واستخدم تمرين (١٨).

(٢٠) $x=8n^4+1$ و $y=8n^3$ حل للنظام لكل $n\in\mathbb{Z}^+$

تمارين (١,٥)

(١) $5112=2^3\times3^2\times71$ ، $\tau(5112)=24$ ، $\sigma(5112)=14040$ ، $\sigma_2(5112)=33167324000$.

(٢) $\tau(509)=2$ ، $\tau(20!)=41040$ ، $\tau(1128)=16$.

(٣) $\sigma(509)=510$ ، $\sigma(20!)=26495791882560$ ، $\sigma(1128)=2880$

(٤) $\sigma_2(4)=63$ ، $\sigma_2(9)=364$ ، $\sigma_2(36)=22932$.

(٥) $\sigma_3(4)=511$ ، $\sigma_3(9)=9841$ ، $\sigma_3(36)=5028751$ ،

(١٢) (أ) $100=2\times50=4\times25=5\times20=10\times10=2\times2\times25$

$=4\times5\times5=2\times2\times5\times5$

ولذا فإن: $n=p_1p_2^{49}$ ، $n=p_1^3p_2^{24}$ ، $n=p_1^4p_2^{19}$ ،

$n=p_1^9p_2^9$ ، $n=p_1p_2p_3^{24}$ ، $n=p_1^3p_2^4p_3^4$ ، $n=p_1p_2p_3^4p_4^4$

وأصغر هذه الأعداد هو $n=2^4\times3^4\times5\times7$.

(١٣) (أ) لا يوجد (ب) $n=2\times11=22$.

(ج) 3×17 أو 2×23 أو 5×11 أو 1×71 .

(د) لا يوجد (هـ) 2×13 أو 5×2^2 (و) $2^2\times3^2$

(١٤) (أ) $n=p$ عدد أولي. (ب) $n=p^2$ حيث p عدد أولي.

(١٥) $n=2^km^2$.

(١٧) لاحظ أنه إذا كان p مؤلفاً فإن له ثلاث قواسم على الأقل.

(١٨) بوضع $n=p^{k-1}$ نجد أن $\tau(n)=k$.

(٢٣) إذا كان $n=ab$ حيث $1\le a\le b<n$ فإن $a\le\sqrt{n}$ أو $b\le\sqrt{n}$. ولذا فإن $\tau(n)\le\sqrt{n}+\sqrt{n}=2\sqrt{n}$.

(٢٦) $\sigma(p+2)=(p+2)+1=p+3=(p+1)+2=\sigma(p)+2$.

(٢٧) $\sigma(p^\alpha)=1+p+p^2+\ldots+p^\alpha\equiv1+1+\ldots+1\equiv\alpha+1\pmod 4$.

(٣٦) لاحظ أن $g(n)=\sum_{d|n} f(d)$ حيث f هي الدالة المقدمة في التمرين (٣٥) وبهذا تكون g دالة ضربية. لاحظ أيضاً أن $g(2^k)=1$ و $g(p^k)=k+1$.

(٤٠) لاحظ أنه إذا كان $(m,n)=1$ فإن $d^2 \mid mn$ إذا وفقط إذا كان $d=ab$ حيث $a^2 \mid m$ و $b^2 \mid n$ ويصبح البرهان كما في المبرهنة (٥,٦).

تمارين (٥,٢)

(٢) غير تام لأن M_{11} غير أولي (٣) غير تام لأن M_{29} غير أولي.

(٤) $\sigma(p^k)=1+p+p^2+\ldots+p^k=\frac{p^k-1}{p-1}<p^k<2p^k$

(٥) $\sum_{d|n}\frac{1}{d}=\frac{\sigma(n)}{n}=\frac{2n}{2}=2$.

(٦) استخدم التمرين (٥).

(١٠) $n=2^{p-1}(2^p-1)$. وبما أن $n>6$ فإن p فردي. لاحظ أن

$$2^{p-1}\equiv 1,4,7,1,4,7,\ldots \pmod 9$$

$$2^{p}\equiv 1,7,4,1,7,4,\ldots \pmod 9$$

لكل عدد فردي p. ومن ثم تحصل على المطلوب.

(١١) $\sigma(pq)=(p+1)(q+1)=pq+(p+q)+1<2pq$.

(١٥) $\sigma(n)=\sigma(3)\sigma(2^k)=4(2^{k+1}-1)>6\times 2^k=2n$.

(١٧) أثبت أن كل من 2^p-1 و 2^{p-1} يطابق 1 قياس 6 .

(٢٢) $\sigma(3n)=\sigma(3)\sigma(n)=4(3n)$.

تمارين (٥,٣)

(٢) ناقش الحالتان n فردي و n زوجي. (٣) استخدم التمرين المحلول (٢).

(٤) (ب) لاحظ أن $f(n)=\sum_{d\mid n}\mu(d)\,\tau(d)$ ضربية وأن $f(p_i^{\alpha_i})=-1$.

(د) لاحظ أن $f(n)=\sum_{d\mid n} d\,\mu(d)$ ضربية وأن $f(p_i^{\alpha_i})=1-p_i$.

(٥) (أ) $\left(\frac{3}{2}\right)^k$ (ب) $\prod_{i=1}^{k}(1+\frac{1}{p_i+1})$.

(٦) (أ) $f(n)=\varphi(n)$ (ج) $f(n)=0$.

تمارين (٥,٤)

(١) (أ) 1152 (ب) 226800 (ج) 2002 (د) 2160

(هـ) 5760 (و) 414720

(٢) كل منها يساوي 2592 .

(٣) (أ) 35 ، 39 ، 45 ، 52 ، 56 ، 70 ، 72 ، 78 ، 84 ، 90.

(ب) 31 ، 62 .

(ج) 73 ، 91 ، 95 ، 111 ، 117 ، 135 ، 146 ، 148 ، 152،

182 ، 190 ، 216 ، 222 ، 228، 234 ، 252، 270.

(د) لا يوجد لأن $\varphi(x)$ زوجي لكل $x>2$.

(٤) بما أن 2×7^m يقبل القسمة على 2 ولا يقبل القسمة على 4 فنجد استناداً إلى التمرين المحلول (٧) أن $x=p^k$ أو $x=2p^k$ حيث $p\equiv 3 \pmod 4$ عدد أولي. في الحالتين $\varphi(x)=p^{k-1}(p-1)$. ومنه فإن $p^{k-1}(p-1)=2\times 7^m$ يؤدي إلى أن $k=1$ وأن $p-1=2\times 7^m$. أي أن $p=2\times 7^m+1$. ولكن $7^m\equiv 1 \pmod 3$ وبهذا يكون $p=2\times 7^m+1\equiv 0 \pmod 3$ ليس أولياً وهذا مستحيل.

(٨) $n=4$.

(١١) إذا كان $p^2\mid n$ حيث p أولي فإن $p\mid \varphi(n)$. ولذا فإن $p\mid (n-1)$ أي أن $p\mid 1$ وهذا مستحيل.

(١٤) 4 ، p^k ، $2p^k$ حيث $p\equiv 3 \pmod 4$ أولي.

(١٧) بما أن $6\mid n$ فإن $n=2^k\,3^j\,m$ حيث $(2,m)=(3,m)=1$.

$$\varphi(n)=2^{k-1}3^j\left(1-\frac{1}{3}\right)\varphi(m)=2^k3^{j-1}\varphi(m)\le 2^k3^{j-1}m=\frac{n}{3}$$ إذن

(١٨) ضع $n=2^{2k+1}$ فيكون $\varphi(n)=2^{2k}=(2^k)^2$.

(١٩) $\varphi(n^2)+\varphi((n+1)^2)=n\varphi(n)+(n+1)\varphi(n+1)\le n(n-1)+(n+1)n=2n^2$

ونحصل على المساواة إذا كان n أو $n+1$ أوليان وهذا مستحيل لأن أحدهما فردي والآخر زوجي.

(٢١) جد $m=2p$ حيث p أولي و $2p+1$ مؤلف (يوجد عدد غير منته من الأعداد p التي تحقق ذلك) ثم استخدم تمرين (٢٠) .

(٢٣) ضع $n=2^{k_0}\,p_1^{k_1}\,p_2^{k_2}\dots p_t^{k_t}$ وأثبت أن $\varphi(n)\ge 2^{k_0-1}\,p_1^{\frac{k_1}{2}}\dots p_t^{\frac{k_t}{2}}$.

(٢٤) لاحظ أن $\varphi(n)=n\prod_{i=1}^{t}\left(1-\frac{1}{p_i}\right)$ وأن $1-\frac{1}{p_i}=\frac{p_i-1}{p_i}\ge\frac{1}{2}$.

$$\sum_{d\mid n}\mu(d)\varphi(d)=\prod_{p\mid n}(1-\varphi(p))=\prod_{p\mid n}(1-(p-1))=\prod_{p\mid n}(2-p) \quad (٣٢)$$

تمارين (٥,٥)

(١) استخدم صيغة موبياس وعكسها.

(٣) لنفرض أن $h=f*g$ وأن $(m,n)=1$. عندئذ،

$h(mn)=\sum_{d\mid mn} f(d)g(\frac{mn}{d})$. والباقي يماثل برهان النتيجة (٥,١٥).

(٦) بما أن $f*f^{-1}=I$ وكل من I و f دالة ضربية فإن f^{-1} دالة ضربية (باستخدام تمرين (٥)).

(٨) بما أن $\varphi=\mu*\mathrm{E}$ فإن $\varphi^{-1}=\mu^{-1}*\mathrm{E}^{-1}$. ولكن E دالة ضربية تماماً. إذن، باستخدام تمرين (٧) نجد أن $\mathrm{E}^{-1}=\mu\mathrm{E}$. وعليه فإن $\varphi^{-1}=\mu^{-1}*\mu\mathrm{E}=U*\mu\mathrm{E}$. الآن :

$$\varphi^{-1}(n)=\sum_{d\mid n}U(d)\mu\mathrm{E}(\frac{n}{d})=\sum_{d\mid n}\mu(\frac{n}{d})\mathrm{E}(\frac{n}{d})=\sum_{d\mid n}\mu(\frac{n}{d})\frac{n}{d}$$

$$=\sum_{d\mid n}\mu(d)d=\prod_{p\mid n}(1-p)$$

$$\sum_{d\mid n}f(d)=\sum_{d\mid n}f(d)\,U(\frac{n}{d})=(f*U)(n) \quad (١٢)\ .$$

وبما أن f ضربية فإن $f*U$ ضربية وبهذا يكون

$$(f*U)(n)=\prod_{p\mid n}(f*U)(p)$$

$$=\prod_{p\mid n}(f(1)U(1)+f(p)U(p))=\prod_{p\mid n}(1+f(p))$$

تمارين (٦,١)

(١) (أ) $[3; 7, 16]=[3; 7, 15, 1]$ (ب) $[0; 6, 2, 2]=[0; 6, 2, 1, 1]$.

(ج) $[3; 4, 2, 5]=[3; 4, 2, 4, 1]$.

(د) $[-1; 1, 1, 1, 2, 6]=[-1; 1, 1, 1, 2, 5, 1]$.

(هـ) $[-1; 1, 22, 3, 1, 1, 2, \overline{2}]=[-1; 1, 22, 3, 1, 1, 2, 1, 1]$

(و) $[0; 20, 1, 8, 1, 1, 2]=[0; 20, 1, 8, 1, 1, 1, 1]$.

(٢) (أ)

k	a_k	p_k	q_k	p_k/q_k
0	-3	-3	1	$-3/1$
1	4	$4\times(-3)+1=-11$	$4\times1+0=4$	$-11/4$
2	2	$2\times(-11)+(-3)=-25$	$2\times4+1=9$	$-25/9$
3	5	$5\times(-25)+(-11)=-136$	$5\times9+4=49$	$-136/49$

ولذا فإن $-136/49=[-3; 4, 2, 5]$.

(ب) $13/8$ (ج) $661/150$ (د) $321/460$

(هـ) $355/113$ (و) $3/2$.

(٧) $\frac{p_k}{p_{k-1}}=\frac{a_k p_{k-1}+p_{k-2}}{p_{k-1}}=a_k+\frac{1}{\frac{p_{k-1}}{p_{k-2}}}$. وبما أن $p_{k-2}<p_{k-1}$ فإن

$\frac{p_k}{p_{k+1}}=[a_k; \frac{p_{k-1}}{p_{k-2}}]$. ولكن $\frac{p_{k-1}}{p_{k-2}}=a_{k-1}+\frac{1}{\frac{p_{k-2}}{p_{k-3}}}$. إذن

$\frac{p_k}{p_{k-1}}=[a_k; a_{k-1}, \frac{p_{k-2}}{p_{t-3}}]$. وبالاستمرار على هذا المنوال نجد أن

$$\frac{p_k}{p_{k-1}} = [a_k ; a_{k-1}, \dots , a_1, \frac{p_0}{p_{-1}}] = [a_k ; a_{k-1}, \dots , a_1, a_0]$$

(٩) $\frac{f_{n+1}}{f_n} = [1; 1, 1, \dots , 2] = [1; 1, 1, \dots , 1, 1]$.

تمارين (٦,٢)

(١) (أ) $a_0 = [\alpha_0] = 2, \ \alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{\sqrt{6}+2}{2}$

$$a_1 = [\alpha_1] = 2, \ \alpha_2 = \frac{1}{\alpha_1 - a_1} = \sqrt{6}+2$$

$$a_2 = [\alpha_2] = 4, \ \alpha_3 = \frac{1}{\alpha_2 - \alpha_2} = \frac{\sqrt{6}+2}{2}$$

ولذا فإن $\sqrt{6}$ دوري وأن $\sqrt{6} = [2; 2, 4, 2, 4, \dots]$.

(ب) $\sqrt{5} = [2; 4, 4, 4, \dots]$ (ج) $\sqrt{15} = [3; 1, 6, 1, 6, \dots]$

(د) $\sqrt[3]{2} = [1; 3, 1, 5, 1, \dots]$ (هـ) $\frac{e^2-1}{e^2+1} = [0; 1, 3, 5, 7, \dots]$

(و) $2\pi = [6; 3, 1, 1, 7, \dots]$.

(٢) لنفرض أن العدد المطلوب هو α . عندئذ ،

$\alpha = 2 + \frac{1}{[2; 2, 2, \dots]} = 2 + \frac{1}{\alpha}$. ولذا فإن $\alpha^2 - 2\alpha - 1 = 0$ ويكون

$\alpha = \sqrt{2} - 1$.

(ب) $\alpha = \sqrt{3}+1$ (ج) $\alpha = \frac{\sqrt{15}-6}{3}$ (د) $\alpha = \frac{\sqrt{13}-1}{2}$.

(٤)

k	a_k	p_k	q_k	c_k
0	1	1	1	1/1
1	2	$2\times1+1=3$	$2\times1+0=2$	3/2
2	3	$3\times3+1=10$	$3\times2+1=7$	10/7
3	a	$a\times10+3=10a+3$	$a\times7+2=7a+2$	

ولذا فإن $\alpha=\dfrac{10a+3}{7a+2}$.

(٨) باستخدام التعريف (٦,٥) نجد أن $\sqrt{2}=[1;\ 2,\ 2,\ 2,\ \ldots.\ ]$. الآن

k	a_k	p_k	q_k
0	1	1	1
1	2	3	2
2	2	7	5
3	2	17	12
4	2	41	29
5	2	99	70
6	2	239	169

وبهذا استناداً إلى المبرهنة (٥,١٦) نجد أن 99/70 هو أفضل تقريب كسري للعدد $\sqrt{2}$ من بين جميع التقريبات التي مقاماتها لا تزيد عن 70 . واستناداً إلى المبرهنة (٥,١٣) نجد أن:

$$|\sqrt{2}-99/70|<\frac{1}{70\times169}=8453\times10^{-8}<85\times10^{-6}\ .$$

(١١) لاحظ أن $|\sqrt{6}-22/9|=0.05045\ldots<\dfrac{1}{2\times9^2}=0.006172\ldots$.

إذن 22/9 متقارب للعدد $\sqrt{6}$.

(١٣) بما أن $|\alpha-\dfrac{p_k}{q_k}|<\dfrac{1}{q_k\,q_{k+1}}$ فباستخدام جدول تمرين (٨) نجد أن

$$0<\left|\frac{99}{70}-\frac{a}{b}\right|<\left|\sqrt{2}-\frac{99}{70}\right|<\frac{1}{70\times169}$$

وبالضرب بالعدد $70b$ نحصل على $0<|99b-70a|<\frac{b}{169}$.

وبما أن $|99b-70a|$ عدد صحيح موجب فإن $\frac{b}{169}>1$. إذن، $b>169$.

(١٩) استناداً إلى المبرهنة (٦,١٣) لدينا:

$$0<\left|\frac{a}{b}-\frac{p_k}{q_k}\right|<\left|\alpha-\frac{p_k}{q_k}\right|<\frac{1}{q_k q_{k+1}}$$

وبضرب طرفي المتباينة بالعدد bq_k نجد أن $0<|aq_k-bp_k|<\frac{b}{q_{k+1}}$.

وبهذا يكون $\frac{b}{q_{k+1}}>1$. أي أن $b>q_{k+1}$.

(٢٢) بما أن $|b\alpha-a|\geq\frac{1}{b}$ فإن $\left|\alpha-\frac{a}{b}\right|\geq\frac{1}{b^2}$ واستناداً إلى المبرهنة (٦,١٣)

لا يمكن أن يكون $\frac{a}{b}$ متقارباً للعدد α.

(٢٥) لـيكن $\alpha=[0;n,1,n]=\frac{n+1}{n(n+2)}$. عندئـذ ، $p_1=1$ ، $q_1=n$ ،

$p_3=n+1$ ، $q_3=n(n+1)$. ويكون

$$\left|\alpha-\frac{p_1}{q_1}\right|=\left|\frac{p_3}{q_3}-\frac{p_1}{q_1}\right|=\frac{1}{n(n+2)}=\frac{1}{q_2^2(1+\frac{2}{n})}$$

وإذا اخترنا n يحقق $\frac{1}{1+\frac{2}{n}}>1-\varepsilon$ نحصل على $\left|\alpha-\frac{p_1}{q_1}\right|>\frac{1-\varepsilon}{q_1^2}$.

تمارين (٦,٣)

(١) (أ) $\sqrt{31}=[5;\overline{1,1,3,5,3,1,1,10}]$.

(ب) $\sqrt{46}=[6;\overline{1,2,1,1,2,6,2,1,1,2,1,12}]$.

(ج) $\sqrt{76}=[8;\overline{1,2,1,1,5,4,5,1,1,2,1,1,16}]$.

(د) $\sqrt{47}=[6;\overline{1,5,1,12}]$. (هـ) $\sqrt{130}=[11;\overline{2,2,22}]$.

(و) $\frac{7+\sqrt{130}}{9}=[\overline{2;22,2}]$ (ز) $\frac{2+\sqrt{10}}{2}=[\overline{2;1,1}]$

(٢) (أ) $\frac{23+\sqrt{29}}{10}$ (ب) $\frac{-1+\sqrt{5}}{2}$ (ج) $\frac{8+\sqrt{82}}{6}$

(د) $\frac{25-\sqrt{5}}{10}$ (هـ) $\frac{1+\sqrt{3}}{2}$ (و) $3-\sqrt{3}$

(ز) $\frac{15+\sqrt{257}}{8}$ (ح) $\frac{-1+\sqrt{77}}{2}$ (ط) $\frac{10+\sqrt{37}}{3}$.

(٣) (أ)

k	r_k	s_k	a_k
0	0	1	n
1	n	2	n
2	n	1	2n
3	n	2	

$\sqrt{n^2+1}=[n;\overline{n,2n}]$.

(ب) $\sqrt{9803}=[99;\overline{99,198}]$ ، $\sqrt{291}=[17;\overline{17,34}]$.

(ج) $\sqrt{11666}=[108;\overline{108,216}]$.

(٩) (أ) و (ح) غير مختزل وما عدا ذلك فهو مختزل.

(١٠) إذا كان $b\neq s$ فإن $\sqrt{d}=\frac{br-as}{s-b}\in Q$ وهذا مستحيل.

(١٤) (أ) $s_{18}=16$ و $p_7=494881$. إذن $(494877,n)=293$ و $(494885,n)=3413$. وبهذا يكون $n=293\times3413$.

تمارين (٦,٤)

(١) (أ) $x^2+3y^2>4$ إلا إذا كان $y=0$ أو $y=\pm1$.

الحلول هي $(\pm2,0)$ ، $(\pm1,\pm1)$.

(٢) (أ) $(x+y)(x-y)=8=1\times8=2\times4=4\times2=8\times1$

جميع الأنظمة الناتجة ليس لها حل ما عدا النظام $x+y=4$ ، $x-y=2$

وحل هذا النظام هو $(3,1)$.

(٣) $(5,1)$ ، $(1549\ ،\ 5585)$ ، $(7249325, 20106001)$.

(٤) الحل الأساسي للمعادلة $x^2-82y^2=-1$ هو $(9,1)$.

ولذا يكون (x_2,y_2) الحل الأساسي للمعادلة $x^2-82y^2=1$ حيث $(x_2,y_2)=(163,18)$. وبهذا يكون $x_2+y_2\sqrt{82}=(9+\sqrt{82})^2$.

(٧) بما أن $9943\equiv3\pmod4$ فيوجد قاسم أولي للعدد 9943 على الصورة $4k+3$ ومن ثم المعادلة غير قابلة للحل.

(١٠) بالتجريب $(10,1)$ هو الحل الأساسي للمعادلة $x^2-99y^2=1$ وجميع الحلول هي (x_n,y_n) حيث $x_n+y_n\sqrt{99}=(10+\sqrt{99})^n$ ، $n\geq1$. أما المعادلة $x^2-99y^2=-1$ فهي غير قابلة للحل لأن $x^2\not\equiv-1\pmod3$.

(١٥) لاحظ أن $\sqrt{23}=[4;\overline{1,3,1,8}]$ ، ولذا فإن $m=4$ وأن $(p_3,q_3)=(24,5)$ هو الحل الأساسي. وبما أن $(24+5\sqrt{23})^2=1151+240\sqrt{23}$ فإن الحل الثاني هو $(1151,240)$. ولذا لا يوجد حلول تحقق $24<x<1151$.

(١٦) للمعادلة $x^2-2y^2=1$ عدد غير منته من الحلول الموجبة، فإذا كان (a,b) حل فإن $n=a^2$ ، $n+1=a^2+1$ ، $n-1=2b^2=b^2+b^2$.

(١٨) $(k,1)$ حل موجب للمعادلة $x^2-(k^2-1)y^2=1$. فإذا كان (a,b) حل للمعادلة $x^2-(k^2-1)y^2=-1$ فإن $a<k$ و $b<1$ وهذا مستحيل.

(٢١) إذا كان (a,b) حلاً فإن $(a^2-19b^2)(a^2+19b^2)=-p$ وبهذا يكون $a^2-19b^2=-1$ و $a^2+19b^2=p$. ولكن طول دورة $\sqrt{19}$ زوجي وبهذا فإن $a^2-19b^2\neq-1$ وهذا تناقض.

تمارين (١, ٧)

(١) $\varphi(17)=16$ والقاسم الأولي الوحيد للعدد 16 هو 2 وأن $3^8=-1 \pmod{17}$. إذن، 3 جذر بدائي قياس العدد 17 والجذور البدائية الأخرى هي:

$3^3\equiv10,\ 3^5\equiv5,\ 3^7\equiv11,\ 3^9\equiv14,\ 3^{11}\equiv7,\ 3^{13}\equiv12,\ 3^{15}\equiv6$.

(٧) 3 جذر بدائي قياس 7 و $3^6=729\not\equiv1 \pmod{7^2}$ وبهذا يكون 3 جذراً بدائياً قياس 7^2 ومن ثم قياس 7^k لكل $k\geq1$.

(٨) بما أن 3 جذر بدائي قياس 7^k (تمرين ٧) فإنه جذراً بدائياً قياس 2×7^k لكل $k \geq 1$.

(٩) 2 جذر بدائي قياس 19 ولكنه ليس جذراً بدائياً قياس 17.

(١٦) $\varphi(\varphi(n))=1 \Leftarrow \varphi(n)=1$ أو $\varphi(n)=2 \Leftarrow n=2,3,4,6$.

(١٨) بما أن $ord_n(a^k)=\frac{ord_n(a)}{(k\,,\,ord_n(a))}$ فإن $ord_n(a^k)\leq ord_n(a)$.

وبما أن a^k جذر بدائي قياس n فإن $ord_n(a^k)=\varphi(n)$. ومنه فإن $ord_n(a)\geq\varphi(n)$ وبهذا يكون $ord_n(a)=\varphi(n)$. وبالتالي فإن a جذر بدائي قياس n.

(٢١) لا : لاحظ أن $(7-1)^{\frac{7-1}{2}}\equiv(-1)^{\frac{7-1}{2}}\equiv-1 \pmod 7$ ولكن 6 ليس جذراً بدائياً قياس 7.

(٢٤) عدد الجذور البدائية غير المتطابقة قياس p^2 هو $\varphi(\varphi(p^2))=(p-1)\varphi(p-1)$. كل منها جذر بدائي قياس p^k، ولذا يكون كل منها جذر بدائي قياس p^2 وهذا يعني أن كل منها يطابق إحدى جذور p^2 البدائية.

(٢٧) $ord_{M_n}(2)=n<2^n-2=\varphi(M_n)$.

تمارين (٧,٢)

(١)

a	1	2	3	4	5	6	7	8	9	10	11	12
$\log_2(a)$	12	1	4	2	9	5	11	3	8	10	7	6

(أ) $x = 2,11 \pmod{13}$ (ب) $x \equiv 5 \pmod{13}$ (ج) $x \equiv 1,5,9 \pmod{13}$

(د) لا يوجد حل.

(٦) $4x^{12} \equiv -23 \pmod{29} \Leftrightarrow 4x^{12} \equiv 6 \pmod{29} \Leftrightarrow 2x^{12} \equiv 3 \pmod{29}$

$\Leftrightarrow 2x^{12} \equiv -26 \pmod{29} \Leftrightarrow x^{12} \equiv -13 \pmod{29} \Leftrightarrow x^{12} \equiv 16 \pmod{29}$

$\Leftrightarrow 12\log_2(x) \equiv \log_2(16) \pmod{28} \Leftrightarrow 12\log_2(x) \equiv 4 \pmod{28}$

$\Leftrightarrow 3\log_2(x) \equiv 1 \pmod{7} \Leftrightarrow \log_2(x) \equiv 5 \pmod{7}$

$\Leftrightarrow \log_2(x) \equiv 5, 12, 19, 26 \pmod{28}$

$\Leftrightarrow x \equiv 2^5, 2^{12}, 2^{19}, 2^{26} \pmod{29}$

$\Leftrightarrow x \equiv 3, 7, 26, 22 \pmod{29}$

(٧) $x \equiv 2^{14}, 2^{34}, 2^{54}, 2^{74}, 2^{94} \equiv 20, 70, 85, 96, 30 \pmod{101}$.

(٨) $x \equiv 2^{17} \equiv 33 \pmod{59}$.

(٩) $x \equiv 7^9, 7^{23}, 7^{37}, 7^{51}, 7^{65} \equiv 47, 53, 22, 52, 39 \pmod{71}$.

(١٠) لاحظ أن 2 جذر بدائي قياس 19 وأن $\log_2(5) = 16$. إذن $5 \equiv 2^{16} \pmod{19}$. الآن :

$x = 5^{4^3} \equiv 2^{16\times 4^3} \pmod{19} \Rightarrow \log_2(x) \equiv 16\times 4^3 \log_2(2) \pmod{18}$

$\Rightarrow \log_2(x) \equiv (-2)\times(-2)\times 4\times 1 \equiv 16 \pmod{18}$

إذن، $x \equiv 2^{16} \equiv 5 \pmod{19}$.

(١١) $3^{3^3} \equiv 14 \pmod{17}$.

(١٤) بما أن $p=3k+2$ فإن $(3,p-1)=(3,3k+1)=1$. ومن مبرهنة فيرما لدينا $a^{p-1}\equiv 1 \pmod p$. إذن $a^{(p-1)/(3,p-1)}\equiv 1 \pmod p$ واستناداً إلى النتيجة (٦,١٩) نجد أن $x^3\equiv a \pmod p$ قابل للحل.

(١٧) لاحظ أنه لا توجد جذور بدائية للعدد $1323=3^3\times 7^2$.

ولكن كل من التطابقين $x^{13}\equiv 10 \pmod{27}$ و $x^{13}\equiv 10 \pmod{49}$ قابل للحل وبالتالي يمكن ايجاد حل للتطابق الأصلي باستخدام مبرهنة الباقي الصينية.

(١٩) إرشاد: انظر التمرين المحلول (١).

تمارين (٧,٣)

(١) (أ) $\lambda(120)=[2,2,4]=4$ (ب) $\lambda(180)=[2,6,4]=12$

(٢) لاحظ أن $36=2^3\times 3^2$ وأن $\lambda(36)=[2,6]=6$.

لإيجاد a حيث $ord_{36}(a)=6$ نختار الجذر البدائي 2 للعدد 6 ثم نستخدم مبرهنة الباقي الصينية لحل التطابقين $a\equiv 3 \pmod 4$ و $a\equiv 2 \pmod 9$ لنجد أن $a\equiv 11 \pmod{46}$.

(٤) $\lambda(65520)=12$ ومن ثم نحصل على المطلوب.

(٧) لنفرض أن $p_i-1=2b_i$ لكل $1\le i\le t$. عندئذ ،

$\varphi(n)=2^t b_1 b_2 \dots b_t$ و $\lambda(n)=2[b_1,b_2,\dots b_t]$.

ونحصل على المطلوب لأن $[b_1,b_2,\dots,b_t]\le b_1 b_2,\dots b_t$.

تمارين (٨,١)

(١) $x \equiv 5,9 \pmod{11}$ (٢) لا يوجد حلول.

(٣) $1^2, 2^2, 3^2 \equiv 1, 4, 2 \pmod 7$.

(٥) $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2 \equiv 1, 4, 9, 16, 8, 2, 15, 13 \pmod{17}$

(٩) (أ) $x \equiv \pm 49^{15} \equiv \pm 7 \pmod{59}$ (ب) $x \equiv \pm 6^{11} \equiv \pm 7 \pmod{43}$

(ج) $x \equiv \pm 36^{26} \equiv \pm 6 \pmod{103}$ (د) $x \equiv \pm 4^{26} \equiv \pm 2 \pmod{107}$

(١٠) لا ، لأن : $x^2 \equiv a \pmod{pq} \Leftarrow x^2 \equiv a \pmod p$.

(١١) يحل كل من التطابقين $x^2 \equiv 860 \equiv 36 \pmod{103}$ و $x^2 \equiv 860 \equiv 4 \pmod{107}$ نجد أن ± 6 حلاً للتطابق الأول وأن ± 2 حلاً التطابق الثاني. وباستخدام مبرهنة الباقي الصينية نجد أن الحلول هي ± 109 و ± 212.

تمارين (٨,٢)

(١) (أ) -1 (ب) -1 (ج) -1 (د) 1

(٣) لاحظ أن $\frac{p-1}{2}$ هو عدد الرواسب التربيعية وهو أيضاً عدد الرواسب غير التربيعية.

(٤) $\left(\frac{1+a^{-1}}{p}\right) = \left(\frac{a^2(1+a^{-1})}{p}\right) = \left(\frac{a(a+aa^{-1})}{p}\right) = \left(\frac{a(a+1)}{p}\right)$.

(٥) استخدم تمرين (٤). (٦) استخدم تمرين (٥) .

(٧) لاحظ أن $(\frac{1}{p}) = 1 = (\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.

(١٢) استخدم معيار أويلر.

(١٣) p يقسم a^2+b^2 يؤدي إلى أن $a^2 \equiv -b^2 \pmod{p}$. ولذا

$1=(\frac{a^2}{p})=(\frac{-b^2}{p})=(\frac{-1}{p})$. وبهذا يكون $p=1 \pmod 4$.

تمارين (٨,٣)

(١) نعم (٢) نعم (٣) نعم (٤) 1 (٥) 1

(٦) 1 (٧) −1 (٨) −1 (٩) 1 (١٠) 1

(١٢) $5 \in Q_p \Leftrightarrow p \equiv \pm 1 \pmod 5$.

(١٣) $6 \in Q_p \Leftrightarrow p \equiv \pm 1, \pm 5 \pmod{24}$.

(١٤) $7 \in Q_p \Leftrightarrow p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}$

(١٥) $10 \in Q_p \Leftrightarrow p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}$

(١٦) $p \neq 13 \Leftrightarrow 169=13^2 \in Q_p$.

(١٧) إذا كان $a=bc$ فإن b أو c راسب غير تربيعي قياس p.

(١٩) (أ) غير قابل للحل. (ب) قابل للحل.

(ج) غير قابل للحل. (د) قابل للحل.

(٢٠) $x \equiv 8,11 \pmod{13}$.

(٢١) (أ) $x \equiv \pm 39 \pmod{59}$ (ب) $x \equiv 5, 37 \pmod{59}$.

(٢٢) بما أن $4 \equiv 1 \pmod 3$ فإن $p=4^n+1 \equiv 2 \pmod 3$. كما أن

$p \equiv 1 \pmod 4$. إذن، $(\frac{3}{p})=(\frac{p}{3})=(\frac{2}{3})=-1$.

(٢٣) لاحظ أن $N = 3 \pmod 5$. ولذا إذا كان $N = m^2 \equiv 3 \pmod 5$ فـإن $3 \in Q_5$ وهذا مستحيل.

(٢٤) افـــــرض أن $N = 5(n!)^2 - 1$ وأن $p \mid N$ أولي وأثبـــــت أن $p \equiv -1 \pmod{10}$. وبما أن $p > n$ فإنه يوجد عدد غير منته من الأوليات التي على الصورة $10\ k - 1$.

(٢٦) (أ) $p \mid n^2 + 1 \Leftrightarrow n^2 \equiv -1 \pmod p \Leftrightarrow (\frac{-1}{p}) = 1 \Leftrightarrow p \equiv 1 \pmod 4$.

(٢٧) $$(\frac{13}{p}) = (\frac{p}{13}) = (\frac{q + 26k}{13}) = (\frac{q}{13}) = (\frac{13}{q})$$

(٣٠) بما أن $q \mid M_p$ فإن $2^p \equiv 1 \pmod q$ وبهذا يكون $(2^{\frac{p+1}{2}})^2 \equiv 2^{p+1} \equiv 2 \pmod q$. أي أن 2 راسب تربيعي قياس q وبهـــذا يكون $q \equiv \pm 1 \pmod 8$.

تمارين (٨,٤)

(١) $x \equiv \pm 7 \pmod{43}$.

(٢) $x \equiv \pm 14 \pmod{97}$.

(٣) $x \equiv \pm 7 \pmod{41}$.

(٤) $x \equiv \pm 81 \pmod{311}$.

(٥) غير قابل للحل .

(٦) $x \equiv \pm 12 \pmod{103}$.

(٧) غير قابل للحل.

(٨) $x \equiv \pm 54 \pmod{97}$.

(٩) $x \equiv \pm 22 \pmod{397}$.

(١٠) $x \equiv \pm 29 \pmod{401}$.

تمارين (٨,٥)

(١) $x \equiv \pm 3 \pmod 7$ حلاً التطابق $x^2 \equiv 2 \pmod 7$.

و $x \equiv \pm 6 \pmod{17}$ حلاً التطابق $x^2 \equiv 2 \pmod{17}$.

ولذا حلول التطابق هي: $x \equiv \pm 11, \pm 45 \pmod{119}$.

(٢) التطابق $x^2 \equiv 3 \pmod 5$ غير قابل للحل ومن ثم التطابق الأصلي غير قابل للحل.

(٣) ± 75773 ، ± 126351 . (٤) ± 109 ، ± 212 .

(٥) ± 1 ، ± 4 . (٧) ± 47 ، ± 96 ، ± 135 ، ± 278 .

(٨) غير قابل للحل (٩) غير قابل للحل.

(١٠) ± 1 ، ± 13 ، ± 15 ، ± 27 .

تمارين (٨,٦)

(١) (أ) -1 (ب) 1 (ج) 1 (د) -1 .

(٢) (أ) -1 (ب) 1 (ج) -1 (د) 1 .

(٤) (أ) $\left(\frac{5}{11111}\right) = \left(\frac{3}{11111}\right) = \left(\frac{2}{11111}\right) = 1$ و $\left(\frac{7}{11111}\right) = -1$.

(٥) $m \equiv 1, 7, 11, 17, 43, 49, 53, 59 \pmod{60}$.

(٧) استخدم التمرين (٣) من تمارين (٨,٢).

تمارين (٩,١)

(٢) gaul is divided into three parts .

(٣) we will meet at midnight .

(٥) proceed meeting as agreed .

(٦) (أ) FEXENZMBMKJNHMGMYZMN .

(ب) please send money .

(٨) $A^{-1}=\begin{bmatrix}17 & 5\\ 18 & 23\end{bmatrix}$ والرسالة هي : gold .

(٩) أضف الحرف A في آخر الرسالة ، $A^{-1}=\begin{bmatrix}6 & 21 & 11\\ 21 & 25 & 16\\ 19 & 3 & 7\end{bmatrix}$ والرسالة هي:

stop pamentx.

(١٠) $A^{-1}=\begin{bmatrix}5 & 17\\ 20 & 9\end{bmatrix}$ والرسالة هي: help .

(١١) $A^{-1}=\begin{bmatrix}14 & 11\\ 17 & 10\end{bmatrix}$ ، QVNAYQHI ، attack .

(١٢) $A^{-1}=\begin{bmatrix}20 & 23\\ 17 & 4\end{bmatrix}$ والرسالة هي: hill .

تمارين (٩,٢)

(١) attack .

(٢) $k=11$ ، we will meet midnight .

(٤) $k=(1,11)$. (٥) $k=(11,19)$.

(٦) $k=(11,18)$ والرسالة : surrender immediately .

(٧) $k=(3,7)$ والرسالة : send in the troops .

(٨) $k=(5,4)$ والرسالة : success at last .

(٩) توجد 9 قيم لكل من a و b وبالتجريب نجد أن $d_k(x)\equiv 7x+18 \pmod{27}$ وتكون الرسالة: i am in rio .

(١٠) $k=(3,18)$ (١١) $k=(19,20)$.

(١٢) $k=(9,2)$ والرسالة : affine .

(١٣) $k=(3,5)$ والرسالة: buy telecom shares .

(١٤) للنظام $13a+b\equiv 20$ و $25a+b\equiv 0$ حلان أحدهما هو $(a,b)=(7,7)$ يصلح كمفتاح تعمية.

(١٥) $k=(5,10)$.

(١٦) $k=(7,18)$ والرسالة :

in order to succeed in this life you have to work very hard and respect competition

(١٧) توجد 12 قيمة ممكنة لكل من a و b.

(١٨) الدالة ليست أحادية ومن ثم لا تصلح كدالة تعمية.

(١٩) (أ) للتطابق $5x+18\equiv 0 \pmod{26}$ حلان ولذا فإن النظام يثبت حرفين.

(ب) الرسالة : summer is coming .

(٢٠) $\{(1,0),(1,13),(-1,b): b\in \mathbb{Z}_{26}\}$.

(٢١) $k=(3,17)$ يصلح كمفتاح تعمية.

(٢٢) $A=\begin{bmatrix}23 & 17\\ 21 & 2\end{bmatrix}$.

(٢٣) $A=\begin{bmatrix}3 & 10\\ 9 & 7\end{bmatrix}$ والرسالة : beware of the messenger .

(٢٤) $A^{-1}=\begin{bmatrix}15 & 25\\ 19 & 9\end{bmatrix}$ والرسالة: get butter and guns .

(٢٥) لا، لأن المصفوفة $X=\begin{bmatrix}18 & 14\\ 19 & 15\end{bmatrix}$ غير قابلة للعكس قياس 26.

(٢٦) $A=\begin{bmatrix}5 & 22\\ 1 & 1\end{bmatrix}$.

(٢٧) $A^{-1}=\begin{bmatrix}18 & 21 & 19\\ 13 & 18 & 3\\ 3 & 19 & 11\end{bmatrix}$ والرسالة هي: send roses and caviar jamesbond

(٢٩) $\begin{bmatrix}x\\ y\end{bmatrix}=\begin{bmatrix}16n\\ 2n\end{bmatrix}$ حيث $n=0, 1, 2, \ldots, 12$.

تمارين (٩,٣)

(١) 15 04 00 12 12 04 20 15 .

(٣) $b=2269$ والرسالة الواضحة هي:

this is an example of an exponentiation cipher

(٤) مفتاح كشف المعمى $b=\log_{20}(24) \pmod{28}$.

(٥) مفتاح كشف المعمى هو $b=11$.

(٦) $a=797$ والرسالة المعماة هي :

14238 7052 4454 2444 2684 14560
0 3314 11500 14238 2684 10952

(٧) $b=937$ والرسالة الواضحة هي:

1520 0111 0802 1004 2402 1724
1519 1406 17010 1507 2423

(٨) الرسالة الواضحة هي: best wishes

(١١) $e_k(x) \equiv x^a \equiv x\,(x^{p-1})^{(q-1)/2} \equiv x \pmod p$. وبالمثل ،

$e_k(x) \equiv x \pmod q$.

(١٢) $x' \equiv (y')^b \equiv (yz^a)^b \equiv y^b z^{ab} \equiv y^b z \equiv xz \pmod n$. وعليه فإن:

$x \equiv x' z^{-1} \pmod n$.

(١٤) (أ) $\lambda \neq \varphi(n)$.

(ب) نعم ، ضع $k = \{(n,p,q,a,b) : n = pq, ab \equiv 1 \pmod \lambda\}$

(١٥) $x = 101110$ ، $x' = 101110110 = 374$ ، $(x')^2 \equiv 97 \pmod{5177}$.

وبإيجاد جذور 97 التربيعية قياس 5177 نجد :

$x_1 = 3133 = 110000111101,\ x_2 = 2044 = 11111111100$

$x_3 = 374 = 10110110,\ x_4 = 4803 = 1001011000011$

ومن ثم يستنتج أحمد أن $x' = x_3$ ومن ثم يحصل على $x = 101110$.

(١٦) $71 = 1000111$ والجذور التربيعية قياس 77 هي:

$15 = 1111$ ، $29 = 1101101$ ، $48 = 110000$ ، $62 = 111110$ ، ولذا يكون النص الواضح 11 أو 1100 .

(١٧) $x = 135,\ 173,\ 36,\ 74$.

تمارين (١٠,٢)

(١) (ج) ... 2, 6, 8, 4, 2, 6, 8, وطول الدورة 4 .

(٣) (أ) ... 5, 7, 1, 7, 1, 7, 1, وطول الدورة 2 .

(ب) ... 3, 7, 8, 6, 2, 0, 4, 5, 3, وطول الدورة 8.

(٤) 1, 24, 25, 18, 12, 30, 11, 10, 21 .

حلول تمارين (١٠,٣)

(١) (أ) $\lambda_0(22)=\frac{\varphi(22)}{2}=10$.

(ب) $\lambda_0(222)=\lambda(222)=36$.

(ج) $\lambda_0(884)=\lambda(884)=48$.

(د) $\lambda_0(99)=\lambda(99)=30$.

(٢) (أ) بما أن $50=2\times5^2$ فإن $\lambda_0(50)=\frac{\varphi(50)}{2}=10$.

الآن نبحث عن مدى r يحقق $r^{10}\equiv\pm1 \pmod{50}$ فنجد أن $r=3$.

(ب) بما أن $125=5^3$ فإن $\lambda_0(125)=\frac{\varphi(125)}{2}=50$. نبحث الآن عن مدى r يحقق $r^{50}\equiv\pm1 \pmod{125}$ فنجد أن $r=2$.

حلول تمارين (١٠,٤)

(١) 2 ، 6 ، 12 .

(٢) $\sum_{d\mid n} f(d)=4^n$ ومن ثم فإن $f(d)=\sum_{c\mid d} 4^c\,\mu(\frac{d}{c})$.

(٣)

$$\Phi_1(x)=x-1$$
$$\Phi_2(x)=x+1$$
$$\Phi_3(x)=x^2+x+1$$
$$\Phi_4(x)=x^2+1$$
$$\Phi_5(x)=x^4+x^3+x^2+x+1$$
$$\Phi_6(x)=x^2-x+1$$
$$\Phi_7(x)=x^6+x^5+x^4+x^3+x^2+x+1$$
$$\Phi_8(x)=x^4+1$$
$$\Phi_9(x)=x^6+x^3+1$$

المراجـــع
Bibliography

[1] سمحان، معروف عبد الرحمن والذكير، فوزي أحمد ، نظرية التعميـــة ، دار الخريجي للنشر والتوزيع، ١٤٢٩هـــ/٢٠٠٨م.

[2] سمحان، معروف عبد الرحمن والسحياني ، علي عبد الله والذكير، فـــوزي أحمد ، الجبر الخطي وتطبيقاته، الطبعة الثالثة، دار الخريجي للنشر والتوزيع، ١٤٣٠هـــ/٢٠٠٩م.

[3] سمحان، معروف عبد الرحمن وأبو مريفة، فدوى سلامة ، أسس الرياضيات، الطبعة الثانية، دار الخريجي للنشر والتوزيع، ١٤٢٧هـــ/ ٢٠٠٦م.

[4] سمحان، معروف عبد الرحمن وأبو عمه، عبد الرحمن محمد سليمان والذكير، فوزي أحمد، قاموس العلوم الرياضية ، النشر العلمي والمطابع ، منـــشورات جامعة الملك سعود ، ١٤٢٢هـــ/٢٠٠١م.

[5] Adams W. W. and Goldstein L. J., *Introduction to Number Theory*, Prentice-Hall, Englewood Cliffs, New Jersey, 1976.

[6] Adleman L. M., "A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography," *Proc. 20th IEEE Found. Comput. Sci. Symp.* (1979), 55-60.

[7] Adleman L. M., Pomerance C., and Rumely R. S., "On distinguishing prime numbers from composite numbers," *Annals of Mathematics*, Volume 117 (1983), 173-206.

[8] Alford W. R., A. Granville, and C. Pomerance, "There Are Infinitely Many Carmichael Numbers," *Ann. Math.,* Volume 140 (1994), 703-722.

[9] Andrews A.J. and Bell J.M. Number Theory with Applications, Prentice Hall, 1996.

[10] Apostol T. A., *Introduction to Analytic Number Theory,* Springer-Verlag, New York, 1976.

[11] Archibald R. G., *An Introduction to the Theory of Numbers,* Merrill, Columbus, Ohio, 1970.

[12] Beilcr A. H., *Recreations in the 'Theory of Numbers,* 2nd ed., Dover, New York, 1966.

[13] Beker H. and Piper F., *Cipher Systems,* Wiley, New York, 1982.

[14] Bell E. T., *Men of Mathematics,* Simon and Schuster, New York, 1965.

[15] Bell E. T., *The Development of Mathematics,* 2nd ed., McGraw-Hill, New York, 1945.

[16] Berge C., *Principles of Combinatorics,* Academic Press, New York, 1971.

[17] Bolker IE. D., *Elementary Number Theory,* Benjamin, New York, 1970.

[18] Borevich Z. 1. and Shafarevich I. R., *Number Theory,* Academic Press, New York, 1966.

[19] Bosworth B., *Codes, Ciphers, and Computers,* Hayden, Rochelle Park, New Jersey, 1982.

[20] Boyer C. B., *A History of Mathematics.* Wiley, New York, 1968.

[21] Brent R P. and Pollard J. M., "Factorization of the Eighth Format Number," *Math, of Comput.,* Volume 36, No. 154 (1981), 627-630.

[22] Brent R. P., "Improved Techniques for Lower Bounds for Odd Perfect Numbers," *Mathematics of Computation,* Volume 57 (1991), 857-868.

[23] Brent R. P., "Irregularities in the Distribution of Primes and Twin Primes," *Math. Comput.,* Volume 29 (1975), 43-56.

[24] Bressoud D.M., *Factorization and Primality Testing,* Springer-Verlag, New York, 1989.

[25] Brillhart J., "Fermat's factoring method and its variants," *Congressus Numerantium,* Volume 32 (1981), 29-48.

[26] Brillhart J., Lehmer D.H., Selfridge J.L., Tuckerman B., Wagstaff S.S., Jr., *Factorizations ofb"± 1, b = 2,3,5,6,7,10,11,12 up to high powers,* revised ed., American Mathematical Society, Providence, Rhode Island, 1988.

[27] Burnett I. A., *Elements of Number 'Theory,* Prindle, Weber, and Schmidt, Boston, 1969.

[28] Burton D. M., *Elementary Number Theory,* 3rd ed., Win. C. Brown, Dubuque, Iowa, 1994.

[29] Burton D. M., *The History of Mathematics,* Allyn and Bacon, Boston, 1985.

[30] Cajori F., *A History of Mathematics,* 2nd ed., Macmillan, New York, 1961.

[31] Carmichael R. D., "On Composite Numbers P Which Satisfy the Format Congruence $a^{p-1} \equiv 1 \bmod p$," *Amer. Math. Monthly,* Volume 19, No. 2 (1912), 22-27.

[32] Carmichael R. D., *The Theory of Numbers and Diophantine Analysis,* Dover, New York, 1959 (reprint of the original 1914 and 1915 editions).

[33] Chaum D., ed.. *Advances in Cryptology - Proceedings of Crypto 83,* Plenum. New York, 1984.

[34] Chaum D., Rivest R. L., Sherman A.T., eds.. *Advances in Cryptology -Proceedings of Crypto 82,* Plenum, New York,

1983.

[35] Cipra B., "Big Number Breakdown,", *Science,* Volume 248 (1990), 1608.

[36] Cipra B., "PCs Factor a 'Most Wanted' Number," *Science,* Volume 242 (1988), 1634-1635.

[37] Cohen L. W. and Ehrlich G., *The Structure of the Real Number System,* Van Nostrand Reinhold, New York, 1963.

[38] Cohn H., *Advanced Number Theory,* Dover, New York, 1980.

[39] Colquitt W. N. and Welsh L., Jr., "A New Mersenne Prime," *Mathematics of Computation,* Volume 56 (1991), 867-870.

[40] Coppersmith D., "Cryptography," *IBM J. Res. Develop.,* Volume 31, No. 2 (1987), 244-248.

[41] Crandall R., Doenias J., Norrie C., and J. Young, "The Twenty-Second Fermat Number Is Composite," *Math. Comput,* Volume 64 (1995), 863-868.

[42] Dantzig T., *Number: The Language of Science,* 4th ed., Macmillan, New York, 1954.

[43] Davenport H., *The Higher Arithmetic,* 6th ed., Cambridge University Press, New York, 1992.

[44] Denning D.E.R., *Cryptography and Data Security,* Addison-Wesley, Reading, Massachusetts, 1982.

[45] Dickson L. E., *History of the Theory of Numbers,* three volumes, Chelsea, New York, 1952 (reprint of the 1919 original).

[46] Dickson L. E., *Studies in the Theory of Numbers,* Chelsea, New York, 1957.

[47] Dickson L.E., *Introduction to the Theory of Numbers,* Dover, New York 1957 (reprint of the original 1929 edition).

[48] Dime W. and Hellman M. E., "New Directions in Cryptography," *IEEE Trans. Inform. Theory,* Volume IT-22, No. 6 (1976), 644-654.

[49] Dixon J. D., "Factorization and primality tests," *American Mathematical Monthly,* Volume 91 (1984), 333-353.

[50] Dudley U., *Elementary Number Theory,* 2nd ed.. Freeman, New York, 1969.

[51] Ecuyer P. L, "Efficient and Portable Combined Random Number Generators," *Commun. ACM,* Volume 31 (1988), 742-774.

[52] Edwards H. M., *Fermat's Last Theorem,* Springer-Verlag, New York, 1977.

[53] Eves H., *An Introduction to the History of Mathematics* , 5th ed., Saunder, Philadelphia, 1983.

[54] Ewing J., " 2^{86243} - 1 is prime," *The Mathematical Intelligencer,* Volume 5 (1983), 60.

[55] Eynden C. V., *Elementary Number Theory,* McGraw-Hill, New York, 1987.

[56] Fishman G. S. and L. R. Moore, "A Statistical Evaluation of Multiplicative Congruential Random Number Generators with Modulus 2^{31} — 1," *J. Amer. Statist. Assoc,* Volume 77 (1982), 129-136.

[57] Fishman G. S. and Moore L. R. III, "An Exhaustive Analysis of Multiplicative Congruential Random Generators with Modulus 2^{31} — 1," *SI AM J. Sci. Statist. Comput,* Volume 7, No. 1 (1986), 24-45.

[58] Flath D., *Introduction to Number Theory,* Wiley, New York, 1989.

[59] Freund J. E., "Round robin mathematics," *American Mathematical Monthly,* Volume 63 (1956), 112-114.

[60] Friedman W.F., *Elements of Cryptanalysis,* Aegean Park Press,

Laguna Hills, California, 1978.

[61] Gauss C. F., *Disquisitiones Arithmeticae,* Yale, New Haven, Connecticut, 1966.

[62] Gersho A., ed.. *Advances in Cryptography,* Dept. of Electrical and Computer Engineering, Univ. Calif. Santa Barbara. 1982.

[63] Gilbert J. and Gilbert L., *Elements of Modern Algebra,* 4th ed. PWS-KeNT, Boston, 1995.

[64] Gioia A. A., *The Theory of Numbers,* Markham, Chicago 1970.

[65] Grosswald E., *Representations of Integers as Sums of Squares,* Springer-Verlag, New York, 1985.

[66] Grosswald E., *Topics from the Theory of Numbers,* 2nd ed., Birkhauser, Boston, 1982.

[67] Gupta H., *Selected Topics in Number Theory,* Abacus Press, Kent, England, 1980.

[68] Guy R. K., *Unsolved Problems in Number Theory,* Springer-Verlag, New York, 1981.

[69] Guy R.K., "How to factor a number" *Proceedings of the Fifth Manitoba Conference on Numerical Mathematics,* Utilitas, Winnepeg, Manitoba, 1975, 49-89.

[70] Hagis P., Jr., "Sketch of a proof that an odd perfect number relatively prime to 3 has at least eleven prime factors," *Mathematics of Computations,* Volume 46(1983), 399-404.

[71] Hardy G. H. and Wright E. M., *An Introduction to the Theory of Numbers,* 5th ed., Clarendon Press, Oxford, 1979.

[72] Head A. K., "Multiplication modulo n," *BIT,* Volume 20 (1980), 115-116.

[73] Hellman M. E., "The Mathematics of Public-Key Cryptography," *Sci. Amer.,* Volume 241, August (1979), 146-157.

[74] Hua L., *Introduction to Number Theory,* Springer-Verlag, New York 1982.

[75] Ingham A.E., *The Distribution of Prime Numbers,* Cambridge University Press, New York, 1992.

[76] Ireland K. and Rosen M. I., *A Classical Introduction to Modern Number Theory,* Springer-Verlag, New York, 1982.

[77] Kahn D., *The Codebreakers: The Story of Secret Writing,* Macmillan, 1908.

[78] Khinchin A. Ya., *Continued Fractions,* The University of Chicago Press, Chicago, 1904.

[79] Kirch A.M., *Elementary Number Theory: A Computer Approach,* Intext, New York, 1974.

[80] Klein H. A., *The Science of Measurement: A Historical Survey,* Dover, New York, 1988.

[81] Kline M., *Mathematical Thought from Ancient to Modern Times,* Oxford University Press, New York, 1972.

[82] Koblitz N., a *Course in Number Theory and Cryptography,* Springer-Verlag, New York, 1987.

[83] Kolata G., "Factoring Gets Easier," *Science,* Volume 222 (1983), 999-1001.

[84] Konheim A.G., *Cryptography: A Primer,* Wiley. New York. 1981.

[85] Kranakis E., *Primality and Cryptography,* Wiley-Teubner, Stuttgart, West Germany, 1986.

[86] Kullback S., *Statistical Methods in Cryptanalysis,* Aegean Park Press, Laguna Hills, California, 1976.

[87] Lagarias J. C. and Odlyzko A. M., "New algorithms for computing *n(x),*" Bell Laboratories Technical Memorandum TM-82-11218-57.

[88] Lagarias J. C., Miller V. S., and Odlyzko A. M., "Computing π(x): The Meisscl-Lehrner Method," *Math. Comput.,* Volume 44 (1985), 537-500.

[89] Landau E., *Elementary Number Theory,* Chelsea, New York, 1958.

[90] Lawther H. P., Jr., "An application of number theory to the splicing of telephone cables," *American Mathematical Monthly,* Volume 42 (1935), 81-91.

[91] LeVeque W. J., *Elementary Theory of Numbers,* Dover, New York, 1990.

[92] Lehmer D. H. and Powers R. E., "On factoring large numbers," *Bulletin of the American Mathematical Society,* Volume 37 (1931), 770-776.

[93] Lenstra A.K. and Lenstra II. W., editors Jr., , *The Development of the Number Field Sieve,* Springer-Verlag, New York 1993.

[94] Lenstra H. W., Jr., "Primality testing," *Studieweek Getaltheorie en Computers,* 1-5 September 1980, Stichting Mathematisch Centrum, Amsterdam, Holland.

[95] Libbrecht U., *Chinese Mathematics in the Thirteenth Century, The Shu-sfru chiu-chang ofCh'in Chiu-shao:'* MIT, 1973.

[96] Long C. T., *Elementary Introduction to Number Theory,* 2nd ed.. Heath, Lexington, Massachusetts, 1972.

[97] Loxton J.H., editor, *Number Theory and Cryptography,* Cambridge University Press, Cambridge, England, 1990.

[98] Marsaglia G., "Random Numbers Fall Mainly in the Planes," *Proc. Nat. Acad. Sci. U.S.A.,* Volume 01 (1908), 25-28.

[99] Merkle R.C., *Secrecy, Authentication, and Public Key Systems,* UMI Research Press, Ann Arbor, Michigan, 1982.

[100] Meyer C. H. and Matyas S. M., *Cryptography: A New Dimension in Computer Data Security,* Wiley, New York, 1982.

[101] Millane R. P., "A Product Form of the Mobius Transform," *Phys. Lett. A,* Volume 102 (1992), 213-214.

[102] Miller G. L., "Riemann's hypothesis and tests for primality," *Proceedings of the Seventh Annual ACM Symposium on the Theory of Computing,* 234-239.

[103] Monier L., "Evaluation and comparison of two efficient probablistic primality testing algorithms. *Theoretical Computer Science,* Volume I I (1980), 97-108.

[104] Newman J. R., *The World of Mathematics,* Simon &; Schuster, New York, 1950.

[105] Niven I., Zuckerman H.S., and Montgomery H.L., *An Introduction to the Theory of Numbers,* 5th ed., Wiley, New York, 1991.

[106] Olmsted J. M. H., *The Real Number System,* Appleton-Centuxy-Crofts, New York, 1962.

[107] Ore O., *An Invitation to Number Theory,* Random House, New York, 1967.

[108] Ore., *Number Theory and its History,* McGraw-Hill, New York, 1948.

[109] Parady B. K., Smith J. R., and Zarantonell S. o, "Largest Known Twin Primes," *Math. Comput,* Volume 55 (1990), 381-382.

[110] Park S. K. and Miller K. W., "Random Number Generators: Good Ones Are Hard to Find," *Commun. ACM,* Volume 31 (1988), 1192-1201.

[111] Pettofrezzo A. J. and Byrkit D. R., *Elements of Number Theory,* Prentice-Hall, Englewood Cliffs, New Jersey, 1970.

[112] Pfleeger C.P., *Security in Computing,* Prentice Hall,

Englewood Cliffs, New Jersey, 1989.

[113] Pohlig S. and Hellman M., "An Improved Algorithm for Computing Logarithms over *GF(j>)* and Its Cryptographic Significance," *IEEE Trans. Inform. Theory,* Vol. IT-24, No. 1 (1978), 106-110.

[114] Pollard J. M., "A Monte Carlo Method for Factorization," *Nordisk Tidskrift for Informationsbehandling (BIT),* Volume 15 (1975), 331-334.

[115] Pollard J. M., "Theorems on Factorization and Primality Testing," *Proc. Cambridge Philos. Soc.,* Volume 76 (1974), 521-528.

[116] Pollard J. M., "Theorems on Factorization and Primality Testing." *Proceedings of the Cambridge Philosophical Society,* Volume 76 (1974), 521-528.

[117] Pollard J. M.. "A Monte Carlo Method for Factorization," *Bit,* (1975), 331-334.

[118] Pomerance C., "Recent developments in primality testing." *The Mathematical Intelligencer,* Volume 3 (1981), 97-105.

[119] Pomerance C., "The search for prime numbers," *Scientific American,* Volume 247(1982), 136-147.

[120] Pomerance C., ed., *Cryptology and Computational Number Theory,* American Mathematical Society, Providence, Rhode Island, 1990.

[121] Pomerance C., *Lecture Notes on Primality Testing and Factoring,* The Mathematical Association of America, Washington, D.C., 1984.

[122] Rabin M., "Probabilistic Algorithm for Testing Primality," *J. Number Theory,* Volume 12 (1980), 128-138.

[123] Rademacher H., *Lectures on Elementary Number Theory,* Blaisdell, New York 1964, reprint Krieger, 1977.

[124] Ribenboim P., *13 Lectures on Fermat's Last Theorem,* Springer-Verlag, New York, 1979.

[125] Ribenboim P., *The Book of Prime Number Records,* 2nd ed., Springer-Verlag, New York, 1989.

[126] Ribenboim P., *The Little Book of Big Primes,* Springer-Verlag, New York, 1991.

[127] Riesel H., *Prime Numbers and Computer Methods for Factorization,* Birkhiiuser, Boston, 1985.

[128] Rivest R. L., Shamir A., and Adleman L., "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Commun. ACM,* Volume 21, No. 2 (1978), 120-126.

[129] Robbins N., *Beginning Number Theory,* Wm. C. Brown, Dubuque, Iowa, 1993.

[130] Roberts J., *Elementary Number Theory,* MIT Press, Cambridge, Massachusetts, 1977.

[131] Rosen K. H., *Elementary Number Theory and Its Applications,* 3d ed., Addison-Wesley, Reading, Mass., 1993.

[132] Rosser J. B. and Schoenfeld L., "Approximate Formulas for Some Functions of Prime Numbers," *Illinois J. Math.,* Volume 6 (1962), 64-94.

[133] Salomaa A., *Public-Key Cryptography,* Springer-Verlag, New York, 1990.

[134] Scharlau W. and Opolka H., *From Fermat to Minkowski, Lectures on the Theory of Numbers and its Historical Development,* Springer-Verlag, New York, 1985.

[135] Schimmel A., *The Mystery of Numbers,* Oxford University Press, New York, 1993.

[136] Schroeder M. R., *Number Theory in Science and Communication,* 2nd ed., Springer-Verlag, Berlin, 1986.

[137] Seberry J. and Pieprzyk J., *Cryptography: An Introduction to*

Computer Security, Prentice Hall, New York, 1989.

[138] Shanks D., *Solved and Unsolved Problems in Number Theory,* Chelsea, New York, 1985.

[139] Shapiro H. S., *Introduction to the Theory of Numbers,* Wiley, New York, 1983.

[140] Shockley J. E., *Introduction to Number Theory,* Holt, Rinehart, and Winston, 1967.

[141] Sierpinski W., *A Selection of Problems in the Theory of Numbers,* Pergammon Press, New York, 1964.

[142] Sierpinski W., *Elementary Theory of Numbers,* Polski Akademic Nauk, Warsaw, 1964.

[143] Sierpinski W., *250 Problems in Elementary Number Theory,* Polish Scientific Publishers, Warsaw, 1970.

[144] Simmons G. J., ed., *Secure Communications and Asymmetric Cryptosystems,* AAAS Selected Symposium Series 69, Westview Press, Boulder, Colorado, 1982.

[145] Sinkov A., *Elementary Cryptanalysis,* Mathematical Association of America, Washington, D.C., 1966.

[146] Smith D. E., *A Source Book in Mathematics,* Dover, New York, 1959.

[147] Smith D. E., *History of Mathematics,* Dover, New York, 1958.

[148] Solovay R. and Strassen V., "A Fast Monte-Carlo Test for Primality," *SI AM J. Compxd.,* Volume 6, No. 1 (1977), 84-85. "Erratum: A Fast Monte-Carlo Test for Primality," *SI AM J. CornpuL,* Volume 7, No. 1 (1978), 118.

[149] Stark H. M., *An Introduction to Number Theory,* Markham, Chicago, 1970; reprint MIT Press, Cambridge, Massachusetts, 1978.

[150] Stewart B. M., *Theory of Numbers,* 2ndod., Macmillan, New York, 1964.

[151] Strayer J. K., *Elementary Number Theory,* PWS Publishing Company, Boston, 1993.

[152] Todd J. A., "A Combinatorial Problem," *./. Math. Phys.,* Volume 12 (1933), 321-333.

[153] Vajda S., *Fibonacci & Lucas Numbers and the Golden Section: Theory and Applications,* Ellis Horwood, Chichester, England, 1989.

[154] Vanden Eyden C., *Number Theory,* International Textbook, Scranton, Pennsylvania, 1970.

[155] Vinogradov I. M., *Elements of Number Theory,* Dover, New York, 1954.

[156] Wagstaff S. S. and Smith J.W., "Methods of factoring large integers," in *Number Theory, New York, 1984-1985,* Lecture Notes in Mathematics, Volume 1240, Springer-Verlag, Berlin, 1987,281-303.

[157] Wagstaff S. S., "Using computers to teach number theory," *SIAM News,* Volume 19(1986), 14 and 18.

[158] Weil A., *Number Theory: An approach through history from Hummurapi to Legendre,* Birkhauser, Boston, 1984.

[159] Western A. E. and Miller J. C., *Tables of Indices and Primitive Roots,* Royal Society Mathematical Tables, Vol. 9, Cambridge University Press, Cambridge, 1968.

[160] Williams H. C., "The influence of computers in the development of number theory," *Computers and Mathematics with Applications,* Volume 8 (1982), 75-93.

[161] Williams H. C., ed., *Advances in Cryptology - CRYPTO '85,* Springer-Verlag, Berlin, 1986.

[162] Williams H.C., "An overview of factoring," in *Advances in Cryptology, Proceedings of Crypto 83,* Plenum, New York, 1984, 87-102.

[163] Williams H.C., "Primality testing on a computer", *Ars*

Combinatorial, Volume 5 (1978), 127-185.

[164] Wright H. N., *First Course in Theory of Numbers,* Wiley, New York, 1939.

[165] Wunderlich M. C. and Kubina J.M., "Extending Waring's conjecture to 471,600,000," *Mathematics of Computation,* Volume 55 (1990), 815-820.

[166] Wunderlich M. C., "Implementing the continued fraction algorithm on parallel machines," *Mathematics of Computation,* Volume 44 (1985), 251-260.

دليـــل الأســمـــاء

Index of names

الاسم	الصفحة	الاسم بالأحرف اللاتينية
آتكن	٨٨	Atkin
أدلمان	٥٩٠	Adleman
ادموند لاندو	٨٧ ، ٩٣	Edmund Landau
إقليدس	٣١، ٧٠ ، ٣٠٩	Euclid
أندرو وايلز	٢٧٧ ، ٢٩١	Andrew Wiles
أويلر	٥٤ ، ٩٩ ، ٢٣٧ ، ٣٠٩ ، ٣١١، ٣٤٨	Euler
أيفوري	١٨٩	Ivory
بابادابولس	١٠١	Papadopoulos
باسكارا	٥٨ ، ٤٢٤	Bhaskara
باورز	١٠٢	Powers
برون	١٢٢	Brun
بيكر	٥٤٧	Beker

الاسم	الصفحة	الاسم بالأحرف اللاتينية
بواسن	٩١	Poussin
بوست	٣٠	Post
بوليش	٥٦٩	Pohilg
بيانو	١	Peano
بايبر	٥٤٧	Piper
بيرتراند	٩٤	Bertrand
بيرفوتشن	١٠٢	Pervouchin
بيزو	٣١	Bezout
بيل	٣٤٨ ، ٤٢٦	Pell
تشبشيف	٩٤	Chebysheve
تشن	٩٥	Chen
تشيرش	٣٠	Church
تورينغ	٣٠ ، ٥٩٠	Turing
ثابت بن قرة	٣١٣، ٣٤٦	Thabit Ibn Quraa
جاكوبي	٥٢٥	Jacobi
جاوس	٩١ ، ٢٣٥	Gauss
جولدباخ	١٢٤	Goldhach
الخوارزمي	٧١	Al-Khwarizmi
دبنر	٨٨	Dubner

الاسم	الصفحة	الاسم بالأحرف اللاتينية
ديوفنتاس	٧٢	Diophatus
رابن	٥٨١	Rabin
راف ميركل	٥٦٧	Ralph Merkle
رافائيل بومباي	٣٤٨	Rafael Bombelli
رامانجان	١٢٢	Ramanujan
رون رايفست	٥٩٠	Ron Rivest
ريتشارد تايلر	٢٧٧	Richard Taylor
ريجيز	١٠١	Regius
ريمان	١٢٢	Reimann
سيلبرج	٩١ ، ١٢٢	Selberg
سيلفستر	٩٤	Sylvester
شامير	٥٩٠	Shamir
شانكس	٤٩٩	Shanks
فيبوناتشي	١١	Fibanacci
فيجينير	٥٣٥	Vigenere
فيرما	٩٨ ، ٢٨٩	Fermat
فيثاغورس	٢٣٩	Phythagoras
القيصر	٥٤١	Ceasar
كاتالدي	١٠١	Cataldi

الاسم	الصفحة	الاسم بالأحرف اللاتينية
كارمايكل	٢٠٥	Carmichael
كراندال	١٠١	Crandall
الكندي	٥٤٧	Al-Kindi
كيلر	١٠٠	Keller
لاجرانج	٢١٩ ، ٣٤٨ ، ٤٦٥	Lagrange
لامير	٢٠٢	Lehmer
لوقا	١٢ ، ١٠٢	Lucas
ليجندر	٩١ ، ٢٦٣ ، ٥٢٣	Legendre
مارتن هيلمان	٥٦٧	Martin Hellman
مانجولد	٢٩٤	Mangoldt
مانفرد توبيلك	٩٠	Manfred Toplic
ماير	١٠١	Mayer
موبياس	٣١٧	Mobius
ميرسين	٩٨ ، ٣٤٥	Mersenne
هادامار	٩١	Hadamard
هاردي	٩٥	Hardy
هالي	٤٦٥	Hally
هورنر	١٨٩	Horner
هيك	١٢٢	Hecke

الاسم	الصفحة	الاسم بالأحرف اللاتينية
هيل	٥٣٩	Hill
هيلمان	٥٦٩	Hellman
وايتفيلد ديفي	٥٦٧	Whitfield Diffie

دليـــل الرمـوز

Sumbols Index

الرمز	المعنى	الصفحة
$\mathbb{Z}$	الأعداد الصحيحة	١
$\mathbb{N}$	الأعداد الطبيعية	٣
$\mathbb{Z}^+$	الأعداد الصحيحة الموجبة	٤
$\leq$	علاقة الترتيب	٤
$P(n)$	جملة مفتوحة مجالها $\mathbb{Z}$	٥
$\sum$	سيجما (رمز المجموع)	٦
$\prod$	باي (رمز الضرب)	٦
$\{a_n\}$	متتالية	٩
$\{f_n\}$	متتالية فيوناتشي	١١
Φ	المجموعة الخالية	١٣
$\forall$	المسور الشامل (لكل)	١٣
$\binom{n}{k}$	معامل ذي الحدين	١٩
$n!$	مضروب العدد n	١٩

الرمز	المعنى	الصفحة
$a \mid b$	a يقسم b	٢٣
$a \nmid b$	a لا يقسم b	٢٣
$\lvert a \rvert$	القيمة المطلقة للعدد a	٢٦
(a,b)	القاسم المشترك الأعظم للعددين a و b	٢٧
$(a,b)=1$	عددان أوليان نسبياً	٣١
$(a_1, a_2, \dots, a_n)$	القاسم المشترك الأعظم للأعداد $a_1, \dots, a_n$	٣٦
$[a,b]$	المضاعف المشترك الأصغر للعددين a و b	٤٠
$[a_1, a_2, \dots, a_n]$	المضاعف المشترك الأصغر للأعداد $a_1, \dots, a_n$	٤٢
$[x]$	أكبر عدد صحيح لا يزيد عن x	٤٣
$[x]$	فصل تكافؤ x	١٣٧
$(a_m a_{m-1} \dots a_1 a_0)_k$	تمثيل العدد للأساس k	٦٧
E	مجموعة الأعداد الزوجية	٧٦
$\min\{a,b\}$	أصغر العددين a و b	٧٧
$\max\{a,b\}$	أكبر العددين a و b	٧٧

الرمز	المعنى	الصفحة
$p^a \| \| n$	$p^a \mid n$ و $p^{a+1} \nmid n$	٧٧
$\pi(x)$	عدد الأعداد الأولية التي لا تزيد عن x	٩١
F_n	عدد فيرما من الرتبة n	٩٨
M_n	عدد ميرسين من الرتبة n	١٠٢
$a \equiv b (\mathrm{mod}\ n)$	a يطابق b قياس n	١٢٦
$a \not\equiv b (\mathrm{mod}\ n)$	a لا يطابق b قياس n	١٢٦
$a^{-1} (\mathrm{mod}\ n)$	النظير الضربي للعدد a قياس n	١٣٢
$\mathbb{Z}_n$	مجموعة فصول تكافؤ علاقة التطابق قياس n	١٣٧
$\oplus$	عملية الجمع على $\mathbb{Z}_n$	١٣٧
$\odot$	عملية الضرب على $\mathbb{Z}_n$	١٣٧
$\varphi(n)$	دالة أويلر	١٤٢
U_n	$\{[a] \in \mathbb{Z}_n : (a,n) = 1\}$	١٤٢
A^{-1}	معكوس المصفوفة A	١٨٣
$\det A$	محدد المصفوفة A	١٨٣
$adj\ A$	المصفوفة المصاحبة للمصفوفة A	١٨٤

الرمز	المعنى	الصفحة
$ord_n(a)$	رتبة a قياس n	١٩٨
$\deg f$	درجة كثيرة الحدود f	٢١٨
$\Lambda(n)$	دالة مانجولد	٢٩٤
$\sum_{d\mid n}$	مجموع على قواسم العدد n الموجبة	٢٩٦
$\tau(n)$	عدد قواسم n الموجبة	٢٩٨
$\sigma(n)$	مجموع قواسم n الموجبة	٢٩٨
$\sigma_k(n)$	مجموع قواسم n الموجبة مرفوعة للقوة k	٢٩٨
$\lambda(n)$	دالة ليوفيل	٣٠٧
$H(n)$	الوسط التوافقي	٣١٤
$\mu(n)$	دالة موبياس	٣١٧
$f * g$	ضرب دريشليه	٣٣٩
$[a_0; a_1, a_2, \ldots, a_n]$	كسر متواصل منته	٣٤٩
$[a_0; a_1, a_2, \ldots]$	كسر متواصل غير منته	٣٦٣
$[a_0; a_1, \ldots, a_n, \overline{c_1, \ldots c_{m-1}}]$	كسر متواصل دورته m	٣٨١
$[\overline{a_0; a_1, a_2, \ldots, a_{m-1}}]$	كسر متواصل دوري تماماً	٣٨١

الرمز	المعنى	الصفحة
$\log_r(a) \pmod n$	اللوغاريتم المنفصل للعدد a للأساس r قياس n	٤٥٠
$ind_r(a)$	دليل a للأساس r	٤٥٠
$\lambda(n)$	القوة الشاملة الصغرى	٤٦٠
Q_n	مجموعة الرواسب التربيعية قياس n	٤٧٠
$\left(\frac{a}{p}\right)$	رمز ليجندر (p عدد أولي)	٤٧٥
$\left(\frac{a}{m}\right)$	زمر جاكوبي (m عدد فردي)	٥١٠
DES	نظام التعمية القياسي	٥٤٤
DLP	مسألة اللوغاريتم المنفصل	٥٧١
RSA	نظام التعمية RSA	٥٧١
A_1	مربع مساعد من النوع الأول	٥٩٦
A_2	مربع مساعد من النوع الثاني	٥٩٦
$\lambda_0(n)$	أكبر عدد صحيح k يحقق $r^k \equiv \pm 1 \pmod n$	٦١٧

الرمز	المعنى	الصفحة
$\Phi_n(x)$	كثيرة الحدود الدويرانية	٦٢١

كشاف وثبت المصطلحات

Subject Index

المصطلح	الصفحة	ما يقابله باللغة الانجليزية
اختبار بين	٤٩١	Pepin test
اختبار لوقا	٢١١	Lucas test
اختبارات القسمة	١٠٨	Divislbility tests
اختيار النص الواضح	٥٤٦ ، ٥٥٨ ، ٥٦١	Chosen plaintext
اختيار النص المعمى	٥٤٦، ٥٥٩، ٥٦١	Chosen ciphertext
أرقام (أو مراتب)	٦٥	Digits
أساس	٦٥	Base
الأعداد الأولية	٧٣	Prime numbers
الأعداد الصحيحة	١	Integers
أعداد تامة زوجية	٣٠٩ ، ٣١٠	Even perfect numbers
أعداد شبه عشوائية	٦٠٩	Pseudorandom numbers
أعداد عشوائية	٦٠٨	Random numbers
أعداد فيرما	٩٨ ، ٩٩	Fermat numbers

المصطلح	الصفحة	ما يقابله باللغة الانجليزية
أعداد كارمايكل	١٩٣، ٢٠٤، ٤٦٢	Carmichael numbers
أعداد ميرسين	٩٨، ١٠٢، ٣١٠	Mersenne numbers
أعداد ميرسين الأولية	١٠٢	Mersenne prime numbers
أمن نظام RSA	٥٧٨	Security of RSA system
أنظمة أحادية	٥٣٥	Monoalphabetic
أنظمة التطابقات الخطية	١٦٤، ١٨١	Systems of linear congrueces
أنظمة التعمية الحديثة	٥٦٧	Contemporary cryptosystems
أنظمة الرواسب	١٣٧	Residue systems
أنظمة تعددية	٥٣٥	Polyalphabetic systems
أنظمة تعمية ذات مفتاح سري	٥٢٨	Secret key ciphers
أنظمة تعمية ذات مفتاح معلن	٥٢٨، ٥٦٨، ٥٧٣	Public key ciphers
أوليان نسبياً	٣١	Relatively prime
أولية جمعاً	٣٨	Mutually prime
باقي القسمة	٢٦	Remainder
بذرة	٦٠٩	Seed

المصطلح	الصفحة	ما يقابله باللغة الانجليزية
تحليل (كسر) التعمية	٥٢٨ ، ٥٤٣	Cryptanalysis
تحليل النظام التآلفي	٥٥٥	Cryptanalysis of affine cipher
تحليل نظام الإزاحة	٥٤٩	Cryptanalysis of shift cipher
تحليل نظام التعويض	٥٥١	Cryptanalysis of snbstitution cipher
تحليل نظام فيجينير	٥٥٨	Cryptanalysis of Vigenere Cipher
تحليل نظام هيل	٥٥٩	Cryptanlaysis of Hill Cipher
تذيل	٥٨٣	Padding
تركيب خطي	٣١	Linear combination
التطابقات التربيعية	٤٦٧	Quadratic congruences
تطابقات خطية	١٤٩	Linear congruences
تطابقات خطية بمتغيرين	١٥٧	Linear congruences in two variables
تطابقات كثيرات الحدود	٢١٧	Polynomial conguences
التعريف الاستقرائي	٩	Inductive definition
التعمية	٥٢٧، ٥٢٨	Cryptography
التلاف	٣٣٩	Convolution
تمثيل الأعداد الصحيحة	٦٥	Representations of integers
تمهيدية إقليدس	٣٦	Euclidean lemma
تمهيدية جاوس	٤٨٢	Gauss lemma
توائم أولية	٨٧	Twin primes

المصطلح	الصفحة	ما يقابله باللغة الانجليزية
توليد مفتاح RSA	٥٧٣	Generating RSA key
توليد مفتاح نظام رابن	٥٨٢	Generating key for Rabin cryptosystem
ثلاثي فيثاغورس	٢٣٩ ، ٢٤٠	Phythogorean triple
ثلاثي فيثاغورس بدائي	٢٤١	Primitive Phythagoren triple
ثلاثيات أولية	٨٩	Triple primes
جَدل كوابل الهاتف	٦١٣	Splicing telephone cables
جذر بدائي	٤٢٧	Primitive root
جذر تربيعي	٤٩٩	Square root
حدس بيرتراند	٩٤	Bertrand conjecture
حدس جولدباخ	٩٤	Goldbach's conjecture
حدس فيرما	٢٧٦	Fermat Conjecture
حل أساسي	٤٠٤	Fundamental solution
حلقة إبدالية بمحايد	١٣٧	Commutative ring with unity
خارج القسمة	٢٦	Quotient
خطة ديفي وهيلمان	٥٨٥	Diffie-Hellmen Protocol
فضاء المفاتيح	٥٣٠	Keyspace
خوارزمية	٣٠ ، ٧١	Algorithm
خوارزمية إقليدس	٢٩	Euclidean algorithm

المصطلح	الصفحة	ما يقابله باللغة الانجليزية
خوارزمية إقليدس الموسعة	٣٣	Extended Euclideen algorithm
خوارزمية التربيع والضرب	١٣٥	Square and multiply algorithm
خوارزمية القسمة	٢٥	Division algorithm
خوارزمية شانكس	٤٩٩	Shanks algorithm
دالة أويلر	١٤٢ ، ١٩٧ ، ٣٢٥	Euler's function
دالة تطابق ضربي	٦٠٩	Multiplicative congruential function
دالة تطابقية	٥٩٩	Congruent function
دالة تعمية	٥٣٠	Encryption function
دالة ذات باب سري	٥٧٢	Trapdoor function
دالة ضربية	٢٩٣ ، ٢٩٤	Multiplicative function
دالة ضربية تماماً	٢٩٤	Completely multiplicative function
دالة عددية	٢٩٣	Arithmetic function
دالة كشف المعمى	٥٣٠	Decryption function
دالة مانجولد	٢٩٤ ، ٣٢١	Mangoldt function
دالة موبياس	٣١٧	Mobius function
دالة وحيدة الاتجاه	٥٧٢	One-way function
دورة الكسر المتواصل	٣٨١	Period of a continued fraction
راسب تربيعي	٤٧٠	Quadratic residue

المصطلح	الصفحة	ما يقابله باللغة الانجليزية
راسب غير تربيعي	٤٧٠	Quadratic nonresidue
راسب من الدرجة k	٤٥٣	Residue of degree k
رتبة العدد قياس n	١٩٨	Order of an element module n
رمز جاكوبي	٥١٠	Jacobi symbol
رمز ليجندر	٤٧٤ ، ٤٧٥	Legendre symbol
شبه أولي للأساس a	٢٠١	Pseudomprime to the base a
صيغة موبياس للتعاكس	٣١٧ ، ٣١٨، ٦١٨	Mobius inversion formula
ضارب	٦٠٩	Multiplier
ضرب دريشليه	٣٣٩	Dirichlet product
طبقات متمركزة	٦١٣	Concentric layers
طريقة الاستنفاد	٥٤٤ ، ٥٥٩	Exhaustion method
طريقة التطابقات الضربية	٦٠٩	Multiplicative congruential method
طريقة أويلر	٥٤	Euler method
طريقة أويلر للتحليل	١١٨	Euler factorization method
طريقة فيرما المعممة	١١٧	Genaralization fermat method
طريقة فيرما للتحليل	١١٤	Fermat factorization method
عامل	٢٣	Factor

ما يقابله باللغة الانجليزية	الصفحة	المصطلح
Prime number	٧٣ ، ٧٤	عدد أولي
Perfect number	٣٠٨	عدد تام
Automorph number	١٧٧	عدد ذاتي الشكل
Abundant number	٣٠٨	عدد زائد
Random number	٢٠٤	عدد عشوائي
Quadratic irrational	٣٨١	عدد غير كسر تربيعي
Reducible quadratic irrational	٣٨٩	عدد غير كسري تربيعي مختزل
Composite number	٧٤	عدد مؤلف
Deficient number	٣٠٨	عدد ناقص
Amicable pair	٣١٣	عددان متحابان
Arthmetica	٧٢	علم الحساب
Least element	١٣	عنصر أصغري
Irreducible	٨٠	غير قابلة للتحليل
Divisibility	٢٣	قابلية القسمة
Greatest common divisor	٢٧ ، ٧٧	القاسم المشترك الأعظم
The law of quadratic reciprocity	٤٨٢، ٤٨٨، ٤٨٩، ٥١٦	قانون التعاكس التربيعي
Smallest universal exponent	٤٦٠	القوة الشاملة الصغرى

المصطلح	الصفحة	ما يقابله باللغة الانجليزية
قوة شاملة	٤٥٩ ، ٦١٧	Universal exponent
كتاب العناصر	٧٠	Elements
كثيرة حدود دويرانية	٦١٥	Cyclotomic polynomial
كثيرة حدود واحدية	٧٩	Monic polynomial
الكسر المتواصل للعدد $\sqrt{d}$	٣٩١	Continued fraction for $\sqrt{d}$
كسر متواصل دوري تماماً	٣٨١ ، ٣٨٩	Purely periodic continued fraction
كسر متواصل منته بسيط	٣٤٩	Finite simple continued fraction
الكسور المتواصلة	٣٤٧	Continued fractions
الكسور المتواصلة الدورية	٣٨٠	Periodic continued fractions
الكسور المتواصلة المنتهية	٤٣٩	Finite continued fractions
الكسور المتواصلة غير المنتهية	٣٦٢	Infinite continued fractions
كلمة سر	٥٣٦	Keyword
لوغاريتم منفصل	٤٥٠	Discrete logarithm
المبدأ الأول للاستقراء الرياضي	٥	First principle of mathematical induction
مبدأ الترتيب الحسن	١٣	Well-ordering principle

المصطلح	الصفحة	ما يقابله باللغة الانجليزية
المبدأ الثاني للاستقراء الرياضي	١٠	Second principle of mathematical induction
مبدأ كرتكشوف	٥٤٧	Kerchkoff's principle
المبرهنة الأساسية في الحساب	٧٤ ، ٧٥	The fundamental theorem of arthmetic
مبرهنة الأعداد الاولية	٩١	Prime number theorem
مبرهنة الباقي الصينية	١٦٨	Cheinese remainder theorem
مبرهنة أويلر	١٩٧	Euler's theorem
مبرهنة دريشلية	٩٠ ، ١٩٠	Dirichlet theorem
مبرهنة ذات الحدين	١٩ ، ٢١	Binomial theorem
مبرهنة فيثاغورس	٢٤٠	Phythagoras theorem
مبرهنة فيرما الصغرى	١٩٢ ، ١٩٣	Fermat little theorem
مبرهنة فيرما الكبرى	٢٧٦	Fermat last theorem
مبرهنة لاجرانج	٢١٩ ، ٣٨٦	Lagrange theorem
مبرهنة ويلسن	١٩١	Wilson's theorem
متتالية فيبوناتشي	١١ ، ١٦	Fibonancci sequence
متتالية لوقا	١٢ ، ١٦	Lucas sequence
مثلث فيثاغورس	٢٤٠	Phythagoras triangle
مجموع أربع مربعات	٢٦٣	Sum of four squares

المصطلح	الصفحة	ما يقابله باللغة الانجليزية
مجموع ثلاث مربعات	٢٦٢	Sum of three squares
مجموع مربعين	٢٥٢	Sum of two squares
مدى نظام الجدْل	٦١٤	Range of splicing system
مرافق	٣٨٥	Conjugate
مربع سحري	٥٩٣	Magic square
مربع سحري متمم	٦٠٨	Complementary magic square
مربع سحري مساعد	٥٩٧	Supportive magic square
مرشح آراتوستينس	١١٢	Sieve of Eratoshenes
مركبة أُولى	٥٩٦	First component
مركبة ثانية	٥٩٦	Second component
مسألة RSA	٥٧٨	RSA problem
مسألة اللوغاريتم المنفصل	٥٧١	Discrete logarithm problem
مسلمات بيانو	١	Peano axioms
مشتقة كثيرة الحدود	٢٢٢	Derivative of a polynomial
مضاعف	٢٣	Multiple
المضاعف المشترك الأصغر	٤٠ ، ٧٧	Least common multiple
مضروب العدد	١٩	Factorial
معادلات ديوفنتية خطية	٤٩	Linear Diophantine equations
معادلة بيزو	٣١	Bezout's equation

المصطلح	الصفحة	ما يقابله باللغة الانجليزية
معادلة بيل	٣٤٨ ، ٤٠٢	Pell equation
معامل ذي الحدين	١٩	Bionomial coefficient
معرفة النص المعمى فقط	٥٤٦ ، ٥٥٩	Standard data encryption
معرفة النص الواضح	٥٤٦ ، ٥٥٨ ، ٥٦٠	Known ciphertext only
معكوس مصفوفة قياس m	١٨٣	Inverse of a matrix modulo m
معلومات سرية	٥٧٢	Trapdoor information
معيار أويلر	١٩٢ ، ٤٧٥	Eurler's criterion
مفتاح RSA السري	٥٧٤	RSA secret key
مفتاح RSA المعلن	٥٧٤	RSA public key
مفتاح تعمية	٥٢٨ ، ٥٢٩	Cipher Key
مفتاح تعمية سري	٥٢٨ ، ٥٣٤	Secert Cipher Key
مفتاح تعمية معلن	٥٢٨ ، ٥٤٣	Public cipher key
مفتاح رابن السري	٥٨٢	Rabin secret key
مفتاح رابن المعلن	٥٨٢	Rabin public key
مقارب	٣٥٦	Convergent
النص الواضح	٥٣٩ ، ٥٣٠	Plaintext
نص مُعَمى	٥٢٩ ، ٥٣٠	Ciphertext
نظام RSA	٥٧١	RSA Cryptosystem

المصطلح	الصفحة	ما يقابله باللغة الانجليزية
نظام الإزاحة	٥٣١ ، ٥٣٢	Shift cipher
نظام البيانات القياسي	٥٤٤	Standard data encryption
النظام التآلفي	٥٣٤	Affine cipher
نظام التعويض	٥٣٣	Substitution cipher
النظام الثنائي	٦٥	Binary system
نظام الرواسب التام القياسي	١٣٨	Standard complete residue system
النظام الستة عشري	٦٨	Hexadecimal system
النظام العشري	٦٥	Decimal system
نظام القيصر	٥٤١	Ceasar cipher
نظام تعمية	٥٢٧	Cryptosystem (Cipher system)
نظام تعمية تقليدي	٥٢٨ ، ٥٣٠	Classical Cryptosystem
نظام رابن	٥٨١	Rabin Cryptosystem
نظام رواسب تام	١٣٨	Complete residue system
نظام رواسب مختزل	١٤٠	Reduced residue system
نظام فينجينير	٥٣٥ ، ٥٣٦	Vigenere cipher
نظام منسجم	١٧١	Compatible system
نظام هيل	٥٣٩	Hill cipher
نظام هيل التآلفي	٥٤٠	Hill affine cipher

المصطلح	الصفحة	ما يقابله باللغة الانجليزية
نظير ضربي	١٣١	Multiplicative inverse
الهجوم المتطفل	٥٨٦	Intruder attack
الوسط التوافقي	٣١٤	Harmonic mean
يطابق	١٢٦	Congruent to
يُعمى	٥٢٩	Encipher (Encrypt)
يفك التعمية	٥٢٩	Decipher (Decrypt)
يقسم	٢٣	Divide

$$2^{43112609} - 1$$

$$= 31647026933025592314$$

.....

.....

.....

$$800221811666697152511$$

ردمك: ٨-١٨٤-٤٥-٩٩٦٠-٩٧٨

101000626