مقدمة

نظرية الأعداد علم يعني بدراسة خواص الأعداد الصحيحة: $\cdots,-2,-1,0,1,2,\cdots$. على الرغم من أن الأعداد الصحيحة مألوفة وخواصها تبدو بسيطة إلا أنها علم عميق جداً. هناك عشرات المسائل التي لم تحل بعد في نظرية الأعداد نذكر بعضها:

(1) هل كل عدد زوجي $n > 2$ يكون مجموعاً لعددين أوليين؟

(2) هل يوجد عدد أولي على الصورة $2^{2^n} + 1$ و $n \geq 5$ ؟

(3) هل يوجد عدد غير منته من الأعداد التامة الزوجية وهل يوجد عدد تام فردي؟

(4) هل يوجد عدد غير منته من الأعداد الأولية التوأم (Twin primes) ؟

(5) هل يوجد عدد غير منته من الأعداد الأولية التي كل خاناتها الرقم 1 ؟

فيما يلي نعرض لبعض المفاهيم الأساسية في نظرية الأعداد مزودة ببعض الأمثلة المحلولة و مسائل اوليمبياد الرياضيات البسيطة . نرمز لمجموعة الأعداد الصحيحة بالرمز $\mathbb{Z} = \{0, \pm, 1, \pm 2, \pm 3, \cdots\}$ ولمجموعة الأعداد الصحيحة الموجبة بالرمز $\mathbb{Z}^+ = \{1, 2, 3, \cdots\}$.

قابلية القسمة
Divisibility

ليكن a, b عددين صحيحين. نقول أن $a \neq 0$ قاسم للعدد b أو b يقبل القسمة على a إذا وجد عدد صحيح q بحيث $b = qa$ ونعبر عن هذا بكتابة $a \mid b$. أيضا في هذه الحالة نقول أن b مضاعف لـ a أو a عامل من عوامل b. إذا كان a لا يقسم b فنكتب $a \nmid b$. إذا كان $a^\beta \mid b$ و $a^{\beta+1} \nmid b$، أي أن β أكبر قوة للعدد a بحيث $a^\beta \mid b$، فنكتب $a^\beta \mid\mid b$.

خصائص أساسية للقاسم

ليكن a, b, c أعداد صحيحة عندئذ

(1) إذا كان $a \mid b$ و $a \mid c$ فإن a يقسم أي تركيب خطي $bx + cy$ من b و c حيث x, y أعداد صحيحة. كحالة خاصة $a \mid (b \pm c)$ أي أن a يقسم مجموع العددين ويقسم الفرق بينهما.

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

(3) إذا كان $a \mid b$ فإن $ac \mid bc$ حيث $c \neq 0$.

(4) إذا كان $a \mid b$ و $b \mid a$ فإن $a = \pm b$.

(5) إذا كان $a \mid b$ و $b \neq 0$ فإن $|a| \leq |b|$.

(6) إذا كان $a \mid b$ و $b \neq 0$ فإن $\frac{b}{a} \mid b$.

سنبرهن بعضا من هذه الخصائص.

$(P1)$ بما أن $a \mid b$ و $a \mid c$ ، إذن يوجد عددين صحيحين m و n بحيث $b = ma$ و $c = na$ وعليه

$$bx + cy = (ma)x + (na)y = (mx + ny)\,a$$

ومنه $a \mid bx + cy$

$(P2)$ بما أن $a \mid b$ و $b \mid c$ ، إذن يوجد عددين صحيحين m و n بحيث $b = ma$ و $c = nb$ وبالتالي

$a \mid c$ وعليه $c = nb = n(ma) = (nm)a$

$(P5)$ إذا كان $a \mid b$ فإنه يوجد عدد صحِيح c بحيث $b = ac$. إذا $|a| \geq |a|$ $||$ $|b| = |c|$.

المربع الكامل والمكعب الكامل

نقول عن العدد الصحيح m أنه مربع كامل (مكعب كامل) إذا وجد عدد صحيح k بحيث $m = k^2$ ($m = k^3$). نقول أن m خال من التربيع إذا كان لا يقبل القسمة على أي عدد مربع $n > 1$. واضح أن 100^{999} مكعب كامل؟ هل هو مربع كامل؟ بين ذلك. مربع أي عدد صحيح إما أن يكون على الشكل $4m$ أو على الشكل $4m + 1$. حدد متى نحصل على هذه الصيغة أو تلك.

خوارزمية القسمة

إذا كان a, b عددين صحيحين بحيث أن $b \neq 0$ فإنه يوجد عددين صحيحين وحيدين q, r بحيث

$$a = qb + r, \quad 0 \leq r < |b|$$

العدد q يسمى خارج القسمة quotient والعدد r يسمى الباقي remainder.

إذ ا أخذنا الأعداد $8,9,10,11,12,13,14,15,16,17,18,19,$ قسمنا على 5 وسجلنا بواقي القسمة. ماذا سنجد؟ خذ الآن خمسة أعداد متتالية ولتكن $23,24,25,26,27$ وسجل بواقي قسمتها على 5. ماذا تلاحظ ؟ هل يوجد بينهما عددان لهما نفس الباقي ؟ عمم هذه النتيجة.

نلاحظ أن بواقي القسمة هي $3,4,0,1,2,3,4,0,1,2,3,4,0,\cdots$. في حالة الخمسة أعداد المتتالية نجد أن جميع البواقي مختلفة وهي $3,4,0,1,2$. يمكن أن نعمم النقاش ليشمل أي عدد n ونصل إلى نتيجتين هامتين هما: من بين n من الأعداد المتتالية يوجد عدد يقبل القسمة على n. ولكل واحد من هذه الأعداد باق مختلف عن الآخر عند قسمتها على n. حاصل ضرب n من الأعداد المتتالية يقبل القسمة على العدد n، أي أن $n \mid (k+1)(k+2)\cdots(k+n)$. وأكثر من ذلك فان $n! \mid (k+1)(k+2)\cdots(k+n)$.

قابلية القسمة على بعض الأعداد الصحيحة

ليكن $N = (a_n a_{n-1} \cdots a_1 a_0)_{10}$ عدداً عشرياً خاناته $a_0, a_1, \cdots, a_{n-1}, a_n$ حيث $a_n \neq 0$. يسمى الرقم a_n بالحد الأول للعدد N ويسمى الرقم a_0 بالحد الأخير للعدد N. العدد N يكتب على الصورة

$$\begin{aligned} N &= a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0 \\ &= 10(a_n \times 10^{n-1} + a_{n-1} \times 10^{n-2} + \cdots + a_2 \times 10 + a_1) + a_0 \\ &= 10(a_n a_{n-1} \cdots a_1)_{10} + a_0 \end{aligned}$$

لاحظ أن خانات أي عدد عشري تكون من المجموعة $\{0,1,,\cdots,9\}$. هناك أنظمة أعداد أخرى غير العشرية فالعدد الثنائي تكون خاناته من المجموعة $\{0,1\}$والعدد الثماني تكون خاناته من المجموعة $\{0,1,,\cdots,7\}$ وإذا كان $N = (a_n a_{n-1} \cdots a_1 a_0)_8$عدداً ثمانيا فان N يكتب على الصورة

$$N = a_n \times 8^n + a_{n-1} \times 8^{n-1} + \cdots + a_1 \times 8 + a_0$$

الآن نعطي اختبارات قابلية القسمة لبعض الأعداد الصحيحة:

ليكن $N = (a_n a_{n-1} \cdots a_1 a_0)_{10}$عدد عشرياً

(1) $2|N \Leftrightarrow 2|a_0 \Leftrightarrow a_0 \in \{0,2,4,6,8\}$.

(2) $3|N \Leftrightarrow 3|a_n + \cdots + a_1 + a_0$.

(3) $4|N \Leftrightarrow 4|(a_1 a_0)_{10} \Leftrightarrow 4|2a_1 + a_0$.

(4) $5|N \Leftrightarrow 5|a_0 \Leftrightarrow a_0 \in \{0,5\}$.

(5)و $6|N \Leftrightarrow 2|N$ $3|N$.

(6) $7|N \Leftrightarrow 7|(a_n a_{n-1} \cdots a_1)_{10} - 2a_0$.

(7) $8|N \Leftrightarrow 4|(a_2 a_1 a_0)_{10} \Leftrightarrow 8|4a_2 + 2a_1 + a_0$

(8) $9|N \Leftrightarrow 9|a_n + \cdots + a_1 + a_0$.

(9) $10|N \Leftrightarrow 10|a_0 \Leftrightarrow a_0 = 0$.

(10) $11|N \Leftrightarrow 11|(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots)$.

أمثلة

(1) إذا كان x, yعددين صحيحين مختلفين فإن $x - y|x^n - y^n$لجميع قيم n الصحيحة الموجبة وذلك لان $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$.

(2)أثبت أن $3^{2n} - 1$ يقبل القسمة على 8 حيث $n \geq 0$ عدد صحيح.

$(S2)$ باستخدام العلاقة من مثال(1):

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1})$$

نجد أن

$$3^{2n} - 1 = 9^n - 1 = (9-1)(9^{n-1} + 9^{n-2} + \cdots + 1)$$

أي أن $3^{2n} - 1 = 8k$ و $k \in \mathbb{Z}$.

(3) إذا كان $2^n \mid\mid 3^{1024} - 1$ أوجد n.

$(S3)$ لاحظ أولا أن $1024 = 2^{10}$، ثم بالتحليل

$$3^{2^{10}} - 1 = (3^{2^9} + 1)(3^{2^9} - 1) = (3^{2^9} + 1)(3^{2^8} + 1)(3^{2^7} + 1) \cdots (3^2 + 1)(3^2 - 1).$$

ليكن m عدد زوجي، من نظرية ذات الحدين لدينا

$$1 + 3^m = 1 + (4-1)^m = 1 + \sum_{k=0}^{m} 4^{m-k}(-1)^k \binom{m}{k} = 4a + 2$$

إذا $3^{2k} + 1$ لا يقبل القسمة على 4 أي أن $2 \mid\mid 3^{2k} + 1$ وبالتالي $n = 12$.

(4) أوجد جميع الأعداد الصحيحة n التي تحقق أن $\dfrac{5n+26}{2n+3} \in \mathbb{Z}$

$(S4)$

$$2n+3 \mid 5n+26 \Rightarrow 2n+3 \mid 2(5n+26) - 5(2n+3) = 37$$

$$\Rightarrow 2n+3 \mid 37 \Rightarrow 2n+3 \in \{\pm 1, \pm 37\}$$

وعليه $n \in \{-20, -2, -1, 17\}$.

تمارين

(A) إذا كان x, y عددين صحيحين فاثبت أن $17 \mid 2x + 3y \Leftrightarrow 17 \mid 9x + 5y$.

(B) اثبت أن $n^3 + (n+1)^3 + (n+2)^3$ يقبل القسمة على 9.

(C) ليكن n عدد صحيح موجب، لماذا $n^5 - n$ يقبل القسمة على 5 دائما؟

(D) أوجد جميع الأزواج الصحيحة الموجبة (m, n) التي تحقق المعادلة $m^2 - n! = 780$.

(E) (الأعداد الزوجية والفردية): نقول أن m عدد فردي إذا وجد $k \in \mathbb{Z}$ بحيث $m = 2k + 1$. والمجموعة $2\mathbb{Z} + 1 = \{\pm 1, \pm 3, \pm 5, \cdots\}$ تسمى مجموعة الأعداد الفردية. نقول أن m عدد زوجي إذا وجد $k \in \mathbb{Z}$ بحيث $m = 2k$ و $2\mathbb{Z} = \{0, \pm 2, \pm 4, \cdots\}$ تسمى مجموعة الأعداد الزوجية. من السهل التحقق من أن مجموع عددين زوجيين هو عدد زوجي وذلك لأن

$$2m + 2n = 2(m+n)$$

كذلك مجموع عددين فرديين هو عدد زوجي، مجموع عدد فردي مع عدد زوجي هو عدد فردي، حاصل ضرب عددين زوجيين هو عدد زوجي، حاصل ضرب عدد فردي في عدد زوجي هو عدد زوجي، وحاصل ضرب عددين

فرديين هو عدد فردي. أثبت انه إذا كان $a,b \in \mathbb{Z}$ فان $4 \mid a^2 - b^2$ إذا وإذا فقط كان a,b كلاهما زوجيان أو فرديان.

(F) هل توجد كثيرة حدود $p(x)$ معاملاتها أعداد صحيحة بحيث $p(1) = 2$ و $p(3) = 5$ ؟

(G) أثبت أنه لكل $n \in \mathbb{Z}$ ، $n > 11$ فإن العدد $n^2 - 19n + 89$ ليس مربعاً.

(H) إذا كان n مكعب كامل فأثبت أن $n^2 + 3n + 3$ ليس مكعب كامل.

(I) ليكن $a,b,c \in \mathbb{Z}$ ، أثبت أن $6 \left| a^3 + b^3 + c^3 \right. \Leftrightarrow 6 \left| a + b + c \right.$.

(J) أثبت أن العدد $\underbrace{11\cdots1}_{2011}\underbrace{55\cdots5}_{2010}6$ عدد مربع

القاسم المشترك الأكبر
Greatest Common Divisor

ليكن a,b عددين صحيحين ليس كلاهما صفر. نقول أن d قاسم مشترك للعددين a,b إذا كان $d \mid a,\ d \mid b$. نقول أن d هو القاسم المشترك الأكبر للعددين a,b إذا كان d هو أكبر قاسم مشترك لهما ونرمز لذلك بكتابة $d = (a,b)$ أو $d = \gcd(a,b)$. من هذا التعريف وباستخدام العلاقتين $(a,b) = (b,a)$ و $(a,b) = (a,-b)$ ينتج مباشرة أن

$$(a,b) = (b,a) = (a,-b) = (-a,-b) = (|a|,|b|)$$

و $(a,0) = |a|$ لكل عدد صحيح غير صفري a

يسمى العددان اللذان قاسمهما المشترك الأكبر يساوي 1 عددين أوليين نسبياً (Relatively primes). يمكن تمديد تعريف القاسم المشترك الأكبر ليشمل ثلاثة أعداد أو أكثر، فإذا كانت $a_1, a_2, \ldots, a_n$ أعداد صحيحة ليست جميعها أصفار فإن القاسم المشترك الأكبر لها ورمزه $(a_1, a_2, \ldots, a_n)$ هو أكبر القواسم المشتركة للأعداد.

إذا كان $(a_1, a_2, \ldots, a_n) = 1$ فإننا نقول أن الأعداد $a_1, a_2, \ldots, a_n$ أولية تبادليا. وإذا كانت $(a_i, a_j) = 1$ لكل $1 \le i < j \le n$ فإننا نقول أن $a_1, a_2, \ldots, a_n$ أولية نسبيا مثنى مثنى.من الواضح أن الأعداد الأولية مثنى مثنى هي أعداد أوليه تبادليا ولكن العكس غير صحيح دائما. المتطابقة التالية من النتائج الهامة التي لها استخدامات عدة وهي تبين أن القاسم المشترك الأكبر لعددين ليس كلاهما صفرا يمكن كتابته كتركيب خطي منهما.

متطابقة بيزوه Bézout

إذا كان a,b عددين صحيحين ليس كلاهما صفراً وكان $d = (a,b)$ فإنه يوجد عددين صحيحين x,y بحيث

$$ax + by = d$$

نتيجة 1

إذا كان $a_1, a_2, \cdots, a_n$ أعداد ليس جميعها أصفار فانه يوجد أعداد صحيحة $x_1, x_2, \cdots, x_n$ بحيث
$a_1x_1 + a_2x_2 + \cdots + a_nx_n = \gcd(a_1, a_2, \cdots, a_n)$.

نتيجة 2

العددين a, b أوليان نسبياً إذا وإذا فقط إذا وجد عددين صحيحين x, y بحيث $ax + by = 1$.

نتيجة 3

ليكن $a, b, c \in \mathbb{Z}$. توجد حلول صحيحة للمعادلة $ax + by = c$ إذا وفقط إذا كان $d|c$ ، حيث $d = \gcd(a, b)$. وعلاوة على ذلك إذا كان $d|c$ وكان x_0, y_0 حلا للمعادلة ، فان جميع الحلول تعطى بالصورة $x = x_0 + k\frac{b}{d}, \qquad y = y_0 - k\frac{a}{d}$ حيث $k \in \mathbb{Z}$.

خوارزمية إقليدس لإيجاد ق.م.أ

لخوارزمية القسمة استخدامات عدة في نظرية الأعداد من ضمنها إيجاد القاسم المشترك الأكبر حيث يتم استخدام الخوارزمية بشكل متكرر وتعرف هذه الطريقة الحسابية بخوارزمية إقليدس.

ليكن $a > b > 0$ عددين صحيحين، لإيجاد (a, b) نتبع الخوارزمية التالية

$$\begin{aligned}
a &= q_1 b + r_1, && 0 < r_1 < b.\\
b &= q_2 r_1 + r_2, && 0 < r_2 < r_1\\
r_1 &= q_3 r_2 + r_3, && 0 < r_3 < r_2\\
r_2 &= q_4 r_3 + r_4, && 0 < r_4 < r_3\\
&\vdots\\
r_{n-2} &= q_n r_{n-1} + r_n, && 0 < r_n < r_{n-1}\\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

حيث $r_{n+1} = 0$ ، أي أن r_n هو آخر باقي غير صفري.

لاحظ أن $b > r_1 > r_2 > r_3 > \ldots > r_n > r_{n+1}$ لذلك يجب أن ننتهي إلى باقي يساوي صفر ورمزنا له بـ r_{n+1}. في هذه الحالة فإن $(a, b) = r_n$ وذلك لأن

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_n, 0) = r_n$$

استخدم خوارزمية إقليدس لإيجاد x, y في متطابقة بيزوه للعددين (a, b): من خوارزمية إقليدس لدينا

$$r_1 = a - q_1 b,\ r_2 = b - q_2 r_1,\ r_3 = r_1 - q_3 r_2, \cdots,\ r_n = r_{n-2} - q_n r_{n-1}$$

لاحظ أن $r_1 = a - q_1 b$ تركيب خطي من a, b وبالتالي عند التعويض عن r_1 في $r_2 = b - q_2 r$ نحصل على $r_2 = ax_2 + by_2$ وهو تركيب خطي من a, b. بالمثل نعوض بهذه الصيغة عن r_2 في

$r_3 = r_1 - q_3 r_2$ لنحصل على تركيب خطي $r_3 = ax_3 + by_3$ وهكذا نستمر حتى ننتهي إلى $d = r_n = ax + by$.

خصائص القاسم المشترك الأكبر

لتكن a, b, c أعداد صحيحة عندئذ

(1) إذا كان n عدد صحيح فإن $(a,b) = (a, b+na)$ وكحالة خاصة $(a,b) = (a, b \pm a)$.

(2) إذا كان $a = qb + r$ فإن $(a,b) = (b,r)$، حيث q, r أعداد صحيحة.

(3) إذا كان $(a,b) = d$ فإن $(\frac{a}{d}, \frac{b}{d}) = 1$.

(4) إذا كان $a \mid c$ و $b \mid c$ وكان $(a,b) = 1$ فإن $ab \mid c$.

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

(6) إذا كان $(a,c) = 1 = (b,c)$ فإن $(ab, c) = 1$

(7) إذا كان $a \mid bc$ و $(a,b) = 1$ فإن $a \mid c$.

(8) إذا كان n عدد صحيح موجب فإن $(na, nb) = n(a,b)$.

(9) إذا كان $a \mid\mid c^{\alpha}$ و $b \mid\mid c^{\beta}$ حيث α, β صحيحة موجبة فإن $(a,b) \mid\mid c^{\min(\alpha,\beta)}$.

البرهان

نكتفي ببرهنة بعض الفقرات

$(P1)$ افرض أن $(a, b+na) = c$ و $(a,b) = d$. إذا d يقسم أي تركيب خطي من a, b. أي أن $d \mid b + na$ وبالتالي $d \mid a, b + na$. إذا $d \leq c$. بالمثل نثبت $d \geq c$ وبالتالي $d = c$.

$(P2)$ افرض $d_1 = (a,b)$ ، $d_2 = (b,r)$. بما أن $d_1 \mid r = a - qb$ فإن $d_1 \leq d_2$. بالمثل لاحظ أن $d_2 \mid a = qb + r$ إذا $d_2 \leq d_1$ وينتج لنا $d_1 = d_2$، أي أن $(a,b) = (b,r)$.

المضاعف المشترك الأصغر
Least common multiple

المضاعف المشترك الأصغر للعددين a, b هو أصغر مضاعف موجب لكل من a, b ويرمز له بالرمز $[a,b]$ أو $lcm(a,b)$. يمكن تمديد تعريف المضاعف المشترك الأصغر ليشمل ثلاثة أعداد أو أكثر فإذا كانت $a_1, a_2, \ldots, a_n$ أعداد صحيحة فإن مضاعفها المشترك الأصغر $[a_1, a_2, \ldots, a_n]$ هو أصغر المضاعفات المشتركة الموجبة لهذه الأعداد.

خصائص المضاعف المشترك الأصغر

ليكن m المضاعف المشترك الأصغر لعددين a, b عندئذ:

(1) $m = ax, m = by$ حيث $(x, y) = 1$.

(2) إذا كان m' مضاعف لكلا من a, b فإن $m \mid m'$.

(3) إذا كان n عدد صحيح موجب فإن $[na, nb] = n[a, b]$

(4) إذا كان $a \mid c,\ b \mid c$ فإن $[a,b] \mid c$.

(5) لأي عددين صحيحين $a,\ b > 0$ فإن $[a,b](a,b) = ab$ وكحالة خاصة $[a,b] = ab$ عندما $(a,\ b) = 1$.

ملاحظة:الصيغة الواردة في (5)غير صحيحة دائما لأكثر من عددين، أي أن

$\left[a_1, a_2, \cdots, a_n\right](a_1, a_2, \cdots, a_n)$ لا يساوي دائما $a_1 a_2 \cdots a_n$ لكل $n \geq 3$ و $a_i \in \mathbb{Z}^+$ ولكن تكون صحيحة في الحالة الخاصة التالية: إذا كانت $a_1, a_2, \cdots, a_n$ موجبة وأولية نسبيا مثنى مثنى فان $\left[a_1, a_2, \cdots, a_n\right] = a_1 a_2 \cdots a_n$

أمثلة

(1)أوجد القاسم المشترك الأكبر للعددين 2520و 154 ثم عبر عنه كتركيب خطي منهما.

$(S1)$أولا إيجاد $(2520,154)$:

$$2520 = 16 \times 154 + 56$$

$$154 = 2 \times 56 + 42$$

$$56 = 1 \times 42 + 14$$

$$42 = 3 \times 14$$

أي أن $(2520,154) = 14$.

ثانيا نوجد عددين صحيحين x, y بحيث $2520x + 154y = (2520,154$

$$14 = 56 - 1 \times 42$$

$$= 56 - 1(154 - 2 \times 56) = 3 \times 56 - 1 \times 154$$

$$= 3(2520 - 16 \times 154) - 1 \times 154 = 3 \times 2520 - 49 \times 154$$

أي أن $14 = (-49) \times 154 + 3 \times 2520$ز

(2)اثبت أن الكسر $\dfrac{12n+1}{30n+2}$ غير قابل للتحليل

$(S2)$ المطلوب إثبات أن $\gcd(12n+1, 30n+2) = 1$:

$$\gcd(12n+1, 30n+2) = \gcd(12n+1, 6n) = \gcd(1, 6n) = 1$$

حل آخر

بما أن $(12n+12)5 + (30n+2)(-2) = 1$ ، إذن من نتيجة 2 ،

$\gcd(12n+1, 30n+2) = 1$.

(3) ليكن n عدد صحيح، أثبت أن $\gcd(n^3+n^2-10n-1, n^2-3n+1) \mid 11$.

$(S3)$ ضع

$$d = \gcd(n^3+n^2-10n-1, n^2-3n+1)$$

$$\begin{aligned}
d &= \gcd(n^3+n^2-10n-1-n(n^2-3n+1), n^2-3n+1) \\
&= \gcd(4n^2-11n-1, n^2-3n+1) \\
&= \gcd(4n^2-11n-1-4(n^2-3n+1), n^2-3n+1) = \\
&= \gcd(n-5, n^2-3n+1) \\
&= \gcd(n-5, n^2-3n+1-n(n-5)) \\
&= \gcd(n-5, 2n+1) \\
&= \gcd(n-5, 2n+1-2(n-5)) \\
&= \gcd(n-5, 11) \mid 11
\end{aligned}$$

(4) إذا كان a,b أعداد صحيحة بحيث $[a,b]+(a,b)=a+b$ اثبت أن $a \mid b$ أو $b \mid a$.

$(S4)$ بفرض أن $d=(a,b)$ وعليه يمكن كتابه $a=md$ و $b=nd$ ويكون $(m,n)=1$ و وحيث أن $[a,b]=\dfrac{ab}{(a,b)}=mnd$. الآن بالتعويض في المعادلة الأصلية ، نحصل على

$mnd+d=md+nd$ أو $mn-m-n+1=0$ أو $(m-1)(n-1)=0$ وعليه

$m=1$ أو $n=1$ ويكون لدينا حالتان إما $a=d, \quad b=nd=na$ وعندها $a \mid b$ أو

$b=d, \quad a=md=mb$ وعندها $b \mid a$.

حل آخر، لدينا: $[a,b]+(a,b)=a+b$ وأيضا $[a,b](a,b)=ab$ وعليه فإن

المعادلة $x^2-(a+b)+ab=0$ يكون جذراها $a,\ b$ وأيضا في نفس الوقت جذراها $(a,b)\ ,[a,b]$ ومن ثم $\Big\{[a,b],\ (a,b)\Big\}=\Big\{a,\ b\Big\}$.

(5) أوجد $\gcd(2^{120}-1, 2^{70}-1)$.

$(S5)$

$$2^{120}-1=2^{50}(2^{70}-1)+2^{50}-1$$
$$2^{70}-1=2^{20}(2^{50}-1)+2^{20}-1$$
$$2^{50}-1=(2^{30}+2^{10})(2^{20}-1)+2^{10}-1$$
$$2^{20}-1=(2^{10}+1)(2^{20}-1)$$
وعليه $\gcd(2^{120}-1,2^{70}-1)=2^{10}-1$

تمارين

(A) ليكن $m,n\in\mathbb{Z}$. أوجد $\gcd(2^n,2m+1)$ ، $\gcd(6,2m+1)$ ، $\gcd(2n+2,2n+6)$ ، $\gcd(2^n-1,2^n+1)$

(B) أثبت أن الكسر $\dfrac{21n+4}{14n+3}$ في أبسط صورة لكل $n\in\mathbb{Z}^+$ $(IMO\ 1959)$.

(C) إذا كان $\gcd(a,b)=1$ فاثبت أن $3\left|\gcd(a+b,a^2-ab+b^2)\right.$.

(D) أثبت أن $\gcd(5a+3b,13a+8b)=\gcd(a,b)$.

(E) إذا كان $A=2n+3m+13,\quad B=3n+5m+1,\quad C=6n+8n-1$ فاثبت أن $77\left|\gcd(A,B,C)\right.$.

(F) احسب $\gcd(n!+1,(n+1)!+1)$ حيث n عدد صحيح موجب.

(G) ليكن n عدد صحيح أكبر من 2 ، أثبت انه يوجد ضمن الكسور $\dfrac{1}{n},\dfrac{2}{n},\cdots,\dfrac{n-1}{n}$ عدد زوجي من الكسور غير القابلة للتحليل

(H) أثبت أن حاصل ضرب أربعة أعداد صحيحة موجبة متتالية لا يمكن أي يكون قوي لعدد صحيح موجب.

(I) أوجد القاسم المشترك الأكبر للأعداد

$$2^{2^2}+2^{2^1}+1,\ 2^{2^3}+2^{2^2}+1,\ \ldots,\ 2^{2^{n+1}}+2^{2^n}+1,\ \ldots$$

(J) إذا كان $n,a,b\in\mathbb{Z}^+$ و $n>1$ فاثبت أن $\gcd(n^a-1,n^b-1)=n^{\gcd(a,b)}-1$

(K) رقم هاتفي، مكون من سبع خانات، إذا نقلت الخانات الأربع اليمنى إلى اليسار ونقلت الخانات الثلاث اليسرى إلى اليمين فإن الرقم الناتج أكبر من ضعف الرقم الأصلي بـ 1. أوجد رقم الهاتف.

الأعداد الأولية
Prime Numbers

نقول أن العدد الصحيح n عدد **أولي**(Prime) إذا كان $n>1$ و كانت مجموعة قواسمه الموجبة تحوي عنصرين فقط هما $1,n$. ونقول أن n عدد **مؤلف**(Composite) إذا كان $n>1$ و غير أولي. أي أن n عدد مؤلف إذا وجد عددان صحيحان a,b بحيث

$$n = ab, \qquad 1 < a, b < n$$

ملاحظات: أي عدد صحيح $n > 1$ إما أولي أو مؤلف.أي عدد زوجي أكبر من 2 يكون غير أولي وأي عدد أولي أكبر من 2 يكون فردي وأي عدد أولي اكبر من 3 يكون على الصورة $6k \pm 1$ لبعض $k \in \mathbb{Z}^+$.لكل عدد صحيح موجب n يوجد n من الأعداد الصحيحة المؤلفة المتتالية فالأعداد
$(n+1)!+2, (n+1)!+3, \cdots, (n+1)!+(n+1)$ جميعها مؤلفة. قد توجد صيغ تعتمد على n تولد أعداداً أولية لبعض قيم n فمثلا $n^2 - n + 41$ تعطي عدد أولي لكل $n = 0,1,2,\cdots,40$ بينما تفشل على سبيل المثال عند $n = 41$ وكذلك $n^2 - 79n + 1601$ تعطي عدد أولي لكل $n = 0,1,2,\cdots,79$ بينما تفشل عندما $n = 80$ ولكن لا توجد صيغ معروفة تعطى أعداد أولية دائما.

الأعداد الأولية التي اقل أو تساوي 100 هي:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,$$
$$43,\ 47,53,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97$$

وهي تمثل الحدود الأولى من متتابعة الأعداد الأولية (p_n) .

خصائص الأعداد الأولية

(1) أي عدد صحيح $n > 1$ إما يكون أوليا، أو يكون حاصل ضرب عدد منته من الأعداد الأولية.

(2) كل عدد صحيح $n > 1$ له قاسم أولي.

(3) إذا كان n عدد مؤلفا فإن له قاسم أولي p بحيث $p \le \sqrt{n}$

(4) إذا كان a, b عددين صحيحين و p عدد أولي بحيث $p \mid ab$ فإن $p \mid a$ أو $p \mid b$.

(5) إذا كان $n > 1$ عددا لا يوجد له أي قاسم أولي اقل من أو يساوي $\sqrt{n}$ فان n يجب أن يكون عددا أوليا.

نلاحظ أن توزيع الأعداد الأولية غير منتظم فمثلا عدد الأعداد الأولية من 1 إلى 100 هو 25 ومن 101 إلى 200 هو 21 ومن 201 إلى 300 هو 16 ومن 9900 إلى 10000 هو 9 . على الرغم من أن عدد الأعداد الأولية يتناقص إلا أن عدد الأعداد الأولية غير منتهي. توجد براهين عديدة لإثبات هذه النتيجة وكان أول برهان هو البرهان الذي قدمه العالم الإغريقي إقليدس قبل الميلاد في الجزء التاسع من كتابة المسمى " العناصر" Elements.

نظرية إقليدس

يوجد عدد غير منتهي من الأعداد الأولية

البرهان

سنستخدم البرهان بالتناقض. أفرض أن هناك عدد منتهي $p_1, p_2, \ldots, p_m$ من الأعداد الأولية. خذ العدد $p = p_1 p_2 \ldots p_m + 1$. العدد p لا يقبل القسمة على أي من p_i حيث $1 \le i \le m$. ولكن كل عدد طبيعي له قاسم أولي. إذا هناك قاسم أولي للعدد p ليس من ضمن $p_1, p_2, \ldots, p_m$ وهذا تناقض.

النظرية الأساسية في الحساب
The Fundamental Theorem of Arithmetic

النظرية الأساسية في الحساب

كل عدد صحيح $n > 1$ يمكن كتابته بشكل وحيد كحاصل ضرب لقوى أعداد أولية $p_1, p_2, \ldots, p_k$ ، أي

$$n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_k^{\alpha k}$$

إيجاد $\gcd, \operatorname{lcm}$ **باستخدام التحليل.**

إذا حللنا العددين الصحيحين a, b لعواملهما الأولية $a = p_1^{a1} p_2^{a2} \ldots p_k^{ak}$ ، $b = p_1^{b1} p_2^{b2} \ldots p_k^{bk}$ فإن $p_1^{min(a_1,b_1)}$ أكبر قوة ممكنة للأولي p_1 تقسم كلا من p_1^{a1}, p_1^{b1} . كذلك الحال مع بقية العوامل الأولية ولذلك

$$(a,b) = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} \ldots p_k^{min(a_k,b_k)} \qquad (*)$$

من جهة أخرى $p_1^{max(a_1,b_1)}$ هي أصغر قوة ممكنة للأولي p_1 ليكون مضاعف للعددين $p_1^{a_1}, p_1^{b_1}$ ولذلك

$$[a,b] = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} \ldots p_k^{max(a_k,b_k)} \qquad (**)$$

إذا كان $n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_k^{\alpha k}$ تحليل العدد n لعوامله الأولية وكان m قاسم موجب للعدد n فيجب أن تكون عوامله الأولية من بين العوامل $p_1, p_2, \ldots, p_k$. السؤال هو ما هي القوة الممكنة لعامل أولي مثل p_i ؟. يمكن أن تكون قوته $0, 1, 2, \ldots, \alpha_i$ أي أن هناك $\alpha_i + 1$ اختيار وبالتالي إذا رمزنا كانت لعدد قواسم n الموجبة بالرمز $\tau(n)$ فإن

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

أمثلة:

(1) اختبر ما إذا كانت الأعداد التالية أولية أم لا: $9901, \quad 2^{11} - 1, \quad 577, \quad 127.$

$(S1)$ العدد 127 أولي لأنه لا يقبل القسمة على أي من الأعداد الأولية التي اقل من أو يساوي 11وكذلك العدد أولي 577 لأنه لا يقبل القسمة على أي من الأعداد الأولية التي اقل من أو يساوي 23، بينما العدد $2^{11} - 1 = 2047$ عدد مؤلف لأنه يقبل القسمة على 23 والعدد 9901 عدد أولي لأنه لا يقبل القسمة على أي من الأعداد الأولية التي اقل من أو يساوي 97.

(2) أوجد جميع العوامل الأولية للمقدار $3^{18} - 2^{18}$

$(S2)$

$$\begin{aligned}3^{18}-2^{18} &= (3^9)^2-(2^9)^2 = (3^9-2^9)(3^9+2^9)\\ &= (3^3-2^3)(3^6+6^3+2^6)(3^3+2^3)(3^6-6^3+2^6)\\ &= (3-2)(3^2+6+2^2)(3^6+6^3+2^6)(3+2)(3^2-6+2^2)(3^6-6^3+2^6)\\ &= 5\times 7\times 19\times 577\times 1009\end{aligned}$$

العدد 577 أولي من المثال (1) ويمكن التحقق من أن 1009 عدد أولي.

(3) أوجد جميع الأعداد الأولية p بحيث كل من $4p^2+1$ و $6p^2+1$ عدد أولي.

$(S3)$ إذا كان آحاد العدد p إما 1 أو 9 فإن آحاد p^2 أيضا 1 وعليه آحاد $4p^2+1$ يساوي 5، أي أن $4p^2+1$ غير أولي في هذه الحالة.

إذا كان آحاد العدد p إما 3 أو 7 فإن آحاد p^2 هو 9 وعليه آحاد $6p^2+1$ يساوي 5، أي أن $6p^2+1$ غير أولي في هذه الحالة. الآن يتبقى إما $p=2$ أو $p=5$:

إذا كان $p=2$ فإن $4p^2+1=17$ أولي بينما $6p^2+1=25$ غير أولي. إذا كان $p=5$ فإن $4p^2+1=101$ أولي $6p^2+1=151$ أولي أيضا. إذاً يوجد عدد أولي وحيد هو $p=5$ عنده كل من $4p^2+1$ و $6p^2+1$ عدد أولي.

(4) أثبت أن أي عدد صحيح زوجي $n>8$ يمكن كتابته على صورة جمع ثلاثة أعداد أولية نسبيا مثنى مثنى.

$(S4)$ أي عدد صحيح زوجي يكون على الصورة $n=6k$ أو $n=6k+2$ أو $n=6k+4$ حيث $k\in\mathbb{Z}$.

إذا كان $n=6k$، $(k\geq 2)$ فان $n=2+3+(6k-5)$.

إذا كان $n=6k+2$، $(k\geq 2)$ فان $n=3+4+(6k-5)$.

إذا كان $n=6k+4$، $(k\geq 1)$ فان $n=2+3+(6k-1)$.

(6) أثبت أنه يوجد عدد غير منتهي من الأعداد الأولية التي على الصورة $4k+3$.

$(S6)$ الحل يعتمد على فكرة أن حاصل ضرب عددين على الصورة $4k+1$ يكون على نفس الصورة.

لنفرض أن هناك عدد منتهي من الأعداد الأولية التي على الصورة $4k+3$ هي $p_1,p_2,\ldots,p_t$. خذ العدد

$$N=4p_1p_2\ldots p_t-1=4(p_1p_2\ldots p_t-1)+3$$

العدد N لا يقبل القسمة على أي من p_i حيث $1\leq i\leq t$. ولكن كل عدد صحيح موجب أكبر من 1 له قاسم أولي. أيضا العدد N فردي لذلك كل عوامله الأولية فردية وحيث أنه على الشكل $4m+3$ فيجب أن يكون أحد عوامله الأولية على الصورة $4m+3$. إذا هناك قاسم أولي للعدد N ليس من ضمن $p_1,p_2,\ldots,p_t$ وهذا تناقض. إذا هناك عدد لا نهائي من الأعداد الأولية على الصورة $4k+3$.

(7) برهن على أن $\log 2$ عدد غير نسبي

$(S7)$ بفرض العكس، أي أن $\log 2$ عددا نسبيا وليكن $\log 2 = \frac{m}{n}$ بحيث $(m.n) = 1$.

$$\log 2 = \frac{m}{n} \Rightarrow 10^{\frac{m}{n}} = 2 \Rightarrow 10^m = 2^n \Rightarrow 2^m \times 5^m = 2^n$$

وهذا يناقض النظرية الأساسية في الحساب (الوحدانية)، إذن عكس الفرض هو الصحيح.

(8)إذا كان أحد العددين $2^n - 1$ أو $2^n + 1$ أولي فان الآخر يكون غير أولي، حيث $n \geq 3$

$(S8)$

الحل

العدد 2^n لا يقبل القسمة على 3 . إذا كان باقي قسمة 2^nعلى 3 يساوي 1 فان $2^n - 1$ يقبل القسمة على 3 وإذا كان باقي قسمة 2^nعلى 3 يساوي 2 فان $2^n + 1$ يقبل القسمة على 3وعليه أحد العددين $2^n - 1$ أو $2^n + 1$ يقبل القسمة على 3، فإذا كان كل من العددين أكبر من 3 فانه لا يمكن أن يكون العددين أوليين.

تمارين

(A)إذا كان $2^n - 1$ عدد أولي فان n عدد أولي.

(B)إذا كان p العدد 27000001 له أربعة عوامل أولية فأوجد مجموعهم.

(C)هل $4^{2009} + 2009^4$ عدد أولي؟

(D) أوجد جميع الحلول الصحيحة الموجبة للمعادلة $2^{2m} - 3^{2n} = 175$.

(E)إذا كان p عدد أولي أكبر من 3 فإن العدد $p^2 + 2$ مؤلف و $24 | p^2 - 1$.

(F) أوجد جميع الأعداد الأولية p, q التي تجعل $p^2 + pq + q^2$ مربع كامل

(G) إذا كان للمعادلة $x^2 - 2px + p^2 - 5p - 1 = 0$ جذرين صحيحين ، حيث p عدد أولي. أوجد القيم الممكنة للعدد p .

(H) حلل العدد 1001001001 إلى عوامله الأولية.

(I) أوجد جميع الأعداد الأولية p بحيث العدد $p^2 + 11$ له 6قواسم مختلفة من بينها العدد 1 والعدد نفسه.

(J) إذا كان p, q أوليان وكان $r = \frac{p^2 + q^2}{p + q}$ عدد صحيح فأثبت أن r أولي.

التطابقات قياس n

n Congruencies modulo

ليكن n عدد صحيح موجب. نقول أن العدد a يطابق العدد b قياس n ونرمز لذلك بالرمز $a \equiv_n b$ أو $a \equiv b \pmod{n}$ إذا كان $n \mid (a-b)$ و إذا كان $n \nmid (a-b)$ فإننا نقول أن a لا يطابق b قياس n ونرمز لذلك بالرمز $a \not\equiv b \pmod{n}$. وبكتابة مكافئه فان

$$a \equiv b \pmod{n} \Leftrightarrow \exists k \in \mathbb{Z} : \quad a = b + kn$$

لاحظ أن أي عدد صحيح a يطابق باقي قسمته على n قياس العدد n وذلك لان حسب خوارزمية القسمة $a = qn + r, \quad 0 \le r < n$ وعليه فان $a \equiv r \pmod{n}$.

خواص أساسية للتطابقات

لتكن $a,b,c,d \in \mathbb{Z}$ و $n \in \mathbb{Z}^+$ أعداد صحيحة

(1) $a \equiv a \pmod{n}$ (خاصية الانعكاس)

(2) $a \equiv b \pmod{n} \Leftarrow b \equiv a \pmod{n}$ (خاصية التناظر)

(3) $a \equiv b \pmod{n}$ و $b \equiv c \pmod{n} \Leftarrow a \equiv c \pmod{n}$ (خاصية التعدي)

(4) إذا كان $a \equiv b \pmod{n}$ وكان $m \mid n$ فان $a \equiv b \pmod{m}$.

(5) إذا كان $a \equiv b \pmod{n}$ و $c \equiv d \pmod{n}$ فإن

$a \pm c \equiv b \pm d \pmod{n}$ (قانون جمع(طرح) التطابقات)

$ac \equiv bd \pmod{n}$ (قانون ضرب التطابقات)

(6) بشكل أعم إذا كان $a_i \equiv b_i \pmod{n}$ لكل $i = 1,2,\ldots,k$ فإن

$$a_1 + a_2 + \cdots + a_k \equiv b_1 + b_2 + \cdots + b_k \pmod{n},$$

$$a_1 a_2 \cdots a_k \equiv b_1 b_2 \cdots b_k \pmod{n}.$$

وكحالة خاصة ، إذا كان $a \equiv b \pmod{n}$ فإن $a^k \equiv b^k \pmod{n}$ لكل $k \in \mathbb{Z}^+$

(7) $ac \equiv bc \pmod{n} \Leftrightarrow a \equiv b \pmod{\frac{n}{d}}$ ، حيث $d = (n,c)$

(8) إذا كان $a \equiv b \pmod{n_i}$ حيث $i = 1,2,\ldots,m$ فإن $a \equiv b \pmod{[n_1, n_2, \cdots, n_m]}$

وكحالة خاصة، إذا كانت $n_1, n_2, \cdots, n_m$ أعداد أولية نسبيا مثنى مثنى فإن $a \equiv b \pmod{n_1 n_2 \cdots n_m}$.

(9) إذا كان m عدد صحيح موجب فإن $(an+b)^m \equiv b^m \pmod{n}$.

مجموع المربعين

متى يكتب العدد الصحيح الموجب على صورة مجموع مربعين لعددين صحيحين ؟، فالعدد 3 لا يمكن كتابته على صورة مجموع مربعين وبصفة عامة أي عدد صحيح موجب n بحيث $n \equiv 3 \pmod{4}$ لا يمكن كتابته على صورة مجموع مربعين. العدد 5 يمكن كتابته على صورة مجموع مربعين على الصورة $5 = 1^2 + 2^2$.

نعرض بعض الخواص المتعلقة بكتابة العدد كمجموع مربعين

(1) إذا كان كل من m و n مجموع مربعين فإن mn كذلك

(2)العدد الأولي p يمكن كتابته كمجموع مربعين بطريقة وحيدة إذا وفقط إذا كان $p = 2$ أو $p \equiv 1 (\mathrm{mod}\, 4)$

(3)العدد الصحيح الموجب n يكون مجموع لمربعين إذا وفقط إذا كان أي قاسم أولي p للعدد n بحيث $p \equiv 3 (\mathrm{mod}\, 4)$ يظهر بقوة زوجية في تحليل العدد n إلى عوامله الأولية.

سنبرهن الخاصية (1) :

بفرض $m = a^2 + b^2$ و $n = c^2 + d^2$. عندئذ

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

ملاحظات

يمكن تعميم الخاصية (1) كما يلي: إذا كان كل من $n_1, n_2, \cdots, n_k$ مجموع مربعين فإن $n_1 n_2 \cdots n_k$ كذلك لكل $k \geq 1$. الخاصية (2) تزودنا باختبار لأولية العدد n ، عندما يكون $n \equiv 1 (\mathrm{mod}\, 4)$ ، فمثلا العدد $n = 221$ يطابق 1 قياس 4 وعليه إذا كان أوليا فإنه n يمكن كتابته بطريقة وحيدة كمجموع مربعين . ولكن $n = 10^2 + 11^2 = 5^2 + 14^2$ وبالتالي فإن n عدد مؤلف

أمثلة:

(1) أثبت أن $13^{682} \equiv 1 \mathrm{mod}\, 7$

$(S1)$ باستخدام خاصية (9): $(an + b)^m \equiv b^m \mod n$

$$13^{682} = (2 \times 7 - 1)^{682} \equiv (-1)^{682} \equiv 1 \mod 7$$

(2) اثبت أن $6^{n-1} + 6^{n-2} + \cdots + 6^1 + 1 - n$ تقبل القسمة على 5 لأي عدد صحيح موجب n .

$(S2)$ بما أن $6 \equiv 1 (\mathrm{mod}\, 5)$ فإن $6^m \equiv 1^m = 1 (\mathrm{mod}\, 5)$ حيث m صحيح موجب، إذا

$$6^{n-1} + 6^{n-2} + \cdots + 6^1 + 1 - n \equiv (1 + 1 + \cdots + 1 + 1) - n$$
$$\equiv n - n \equiv 0 (\mathrm{mod}\, 5)$$

.

(3) أثبت أن $3^{4n+2} + 5^{2n+1}$ يقبل القسمة على 14 حيث $n \geq 0$.

$(S3)$ لهذه المسألة عدة طرق منها الاستقراء الرياضي، لكن باستخدام التطابق نصل للجواب سريعا. لاحظ أن

$$3^{4n+2} + 5^{2n+1} = 9(81)^n + 5(25)^n$$

ولكن $81 \equiv -3 (\mathrm{mod} 14), \quad 25 \equiv -3 (\mathrm{mod} 14)$ إذا

$$(81)^n \equiv (-3)^n (\mathrm{mod} 14), \quad (25)^n \equiv (-3)^n (\mathrm{mod} 14)$$

وبالتالي

$$3^{4n+2} + 5^{2n+1} \equiv 9(-3)^n + 5(-3)^n \equiv 14(-3)^n \equiv 0 (\mathrm{mod} 14)$$

(4) أثبت أن في المتتابعة $a_n = 2^n - 3$ حيث $n \geq 0$ عدد لا نهائي من الحدود قابلة للقسمة على 5 وكذلك عدد لا نهائي من الحدود قابلة للقسمة على 13 ولكن ليس فيها أي حد يقبل القسمة على 5 و 13.

(S4) بما أن $2^3 \equiv 3 (\mathrm{mod}\, 5)$ وبما أن $2^4 \equiv 1 (\mathrm{mod}\, 5)$ فإن

$$2^{4k+3} - 3 \equiv (2^4)^k \cdot 2^3 - 3 \equiv 1.3 - 3 \equiv 0 (\mathrm{mod}\, 5).$$

بما أن $2^r \equiv 3 (\mathrm{mod}\, 5)$ متحققة فقط عندما $r = 3$ من بين الأعداد $0,1,2,3,4$ وعليه فان $5 \mid a_n$ فقط عندما $n = 4k + 3$.

بالمثل $2^4 \equiv 3 (\mathrm{mod}\, 13)$ و $(2^4)^3 \equiv 3^3 \equiv 1 \mathrm{mod}\, 13$ ولذلك

$$2^{12m+4} - 3 \equiv (2^{12})^m \cdot 2^4 - 3 \equiv 1.3 - 3 \equiv 0 (\mathrm{mod}\, 13)$$

وحيث $2^r \equiv 3 (\mathrm{mod}\, 13)$ إذا وإذا فقط $r = 4$ لكل $0 \leq r < 13$ فإن $13 \mid a_n$ فقط عندما $n = 12m + 4$. بما أنه لا يوجد عدد صحيح له الصورة $n = 12m + 4$ والصورة $n = 4k + 3$ فإنه لا يوجد حد من المتتابعة يقبل القسمة على 5 و 13.

(5) ليكن $x, y \in \mathbb{Z}$. $3 \left| x^2 + y^2 \right. \Leftrightarrow 3 | x, 3 \left| y \right.$

(S5) إذا كان $3 | x, 3 \left| y \right.$ فإن وضوحا $3 \left| x^2 + y^2 \right.$. نلاحظ أن $x^2 \equiv 0 \; or \; 1 (\mathrm{mod}\, 3)$ وعليه إذا كان $3 \left| x^2 + y^2 \right.$ فان $3 \left| x^2, 3 \right| y^2$ وعليه $3 | x, 3 | y$.

ملاحظة

التمرين السابق لا يتحقق لأي عدد أولي فمثلا $5 \left| 1^2 + 2^2 \right.$ بينما $5 \nmid 1$ و $5 \nmid 2$. هل يتحقق التمرين السابق للعدد الأولي $p = 7$ ؟.

(6) أثبت أنه إذا كان $a \equiv b (\mathrm{mod}\, n)$ فإن $a^n \equiv b^n (\mathrm{mod}\, n^2)$. هل العكس صحيح؟

(S6) بما أن $a \equiv b (\mathrm{mod}\, n)$ ، إذن $a = b + qn$ لعدد صحيح q . الآن من نظرية ذات الحدين

$$\begin{aligned} a^n - b^n &= (b + qn)^n - b^n \\ &= \binom{n}{1} b^{n-1} qn + \binom{n}{2} b^{n-2} q^2 n^2 + \cdots + \binom{n}{n} q^n n^n \\ &= n^2 \left(b^{n-1} q + \binom{n}{2} b^{n-2} q^2 + \cdots + \binom{n}{n} q^n n^{n-2} \right) \end{aligned}$$

وعليه $a^n \equiv b^n (\mathrm{mod}\, n^2)$. العكس غير صحيح، فمثلا $3^4 \equiv 1^4 (\mathrm{mod}\, 4^2)$ بينما $3 \not\equiv 1 (\mathrm{mod}\, 4)$.

حل آخر

لدينا $a^n - b^n = (a - b)(a^{n-1} + a^{n-2} b + \cdots + a b^{n-2} + b^{n-1})$ وحيث أن

$$a^{n-1-i} b^i \equiv a^{n-1-i} a^i \equiv a^{n-1} (\mathrm{mod}\, n)$$

إذن $(a^{n-1} + a^{n-2} b + \cdots + a b^{n-2} + b^{n-1}) \equiv n a^{n-1} \equiv 0 (\mathrm{mod}\, n)$، أي أن

$n^2 \mid a^n - b^n$ وبالتالي $n \mid (a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$ و $n \mid (a-b)$ وعليه
$a^n \equiv b^n \pmod{n^2}$.

(7)أكتب العدد 2009 كمجموع مربعين
$(S7)$بتحليل العدد 2009 إلى عوامله الأولية نجد أن $2009 = 7^2 \times 41$، إذن يمكن كتابته على صورة مجموع مربعين $2009 = 7^2 \times 41 = 7^2(4^2 + 5^2) = 28^2 + 35^2$.

نختم هذا الجزء بنظرية برهانها يعتمد على مواضيع سوف نتطرق إليها في الجزء الثاني من هذا العمل إنشاء الله وذلك لاستخدامها في إثبات أنه يوجد عدد غير منتهي من الأعداد الأولية التي على الصورة $4k+1$.

نظرية

ليكن p عدداً أوليا. عندئذ يوجد حل للتطابق $x^2 \equiv -1 \pmod{p}$ إذا وفقط إذا كان $p \equiv 1 \pmod{4}$. وعلاوة على ذلك إذا كان $p \equiv 1 \pmod{4}$ فإن $x = \left(\frac{p-1}{2}\right)!$ حلاً للتطابق.

تمارين

(A)أوجد آخر رقمين(خانتي الآحاد والعشرات) من العدد 7^{2010} .
(B) أثبت أن $2222^{5555} + 5555^{2222}$ يقبل القسمة على 7.
(C)أوجد آخر رقمين من العدد $229^{10} + 37^{10}$.
(D) أوجد آخر رقمين من العدد 2^{999}.
(E)إذا كان p عدداً أولياً و k عدد صحيح بحيث $1 \le k < p$ فأثبت أن $p \left| \binom{p}{k} \right.$ ، ثم استنتج أنه إذا كان a, b عددين صحيحين فإن $(a+b)^p \equiv a^p + b^p \pmod{p}$.
(F)حل المعادلة التالية في الأعداد الصحيحة $x^2 + y^2 = 3^{2008}$.
(G) عين الأعداد الصحيحة الموجبة m بحيث يكون $m! + 5$ مكعب كامل.
(H) أثبت أنه يوجد عدد غير منتهي من الأعداد الأولية التي على الصورة $4k+1$.
(I)أثبت أن $2^{11 \times 31} \equiv 2 \pmod{11 \times 31}$.
(J) أوجد المربعات الكاملة في المتتابعة
$1!,\ 1!+2!,\ 1!+2!+3!, 1!+2!+3!+4!,\ \ldots,\ 1!+2!+3!+\cdots+n!,\ \ldots,$
(K)أوجد باقي قسمة $17 + 177 + 1777 + \cdots + 1\underbrace{77\cdots7}_{20}$على 7 .

الحلول

قابلية القسمة

(A) إذا كان x, y عددين صحيحين فاثبت أن $17 \mid 2x+3y \Leftrightarrow 17 \mid 9x+5y$.

الحل

" $\Rightarrow$ "

$$17 \mid 2x+3y \Rightarrow 17 \mid 13(2x+3y) = (17x+34y)+(9x+5y)$$
$$\Rightarrow 17 \mid 9x+5y$$

" $\Leftarrow$ "

$$17 \mid 9x+5y \Rightarrow 17 \mid 4(9x+5y) = (34x+17y)+(2x+3y)$$
$$\Rightarrow 17 \mid 2x+3y$$

(B) اثبت أن $n^3+(n+1)^3+(n+2)^3$ يقبل القسمة على 9.

الحل

ضع $S = n^3+(n+1)^3+(n+2)^3$.

$$\begin{aligned} S &= n^3+(n+1)^3+(n+2)^3 \\ &= n^3+(n^3+3n^2+3n+1)+(n^3+6n^2+12n+8) \\ &= 3n^3+9n^2+15n+9 = 3n^3+15n+9(n^2+1) \\ &= 3n^3-3n+18n+9(n^2+1) \\ &= 3n(n^2-1)+9(n^2+2n+1) \end{aligned}$$

واضح أن كل من حدي المعادلة الأخيرة يقبل القسمة على 9 ، الحد الأول يتكون من العدد 3 مضروبا في ثلاثة أعداد صحيحة متتالية والثاني وضوحا يقبل القسمة على 9 .

(C) ليكن n عدد صحيح موجب، لماذا n^5-n يقبل القسمة على 5 دائما؟

الحل

ضع $S = n^5-n$.

$$S = n(n^4-1) = n(n^2-1)(n^2+1) = (n-1)n(n+1)(n^2+1)$$

أي عدد صحيح موجب n يكون على الصورة $n = 5k+i, \quad 0 \le i \le 4$ حيث $k \in \mathbb{Z}$.

إذا كان n يساوي $5k$ أو $5k+1$ أو $5k+4$ فان $5|S$. أما إذا كان $n=5k+2$ او $n=5k+3$ فان $5|S$ وذلك لان $5|n^2+1$. أكثر من ذلك يمكن إثبات أن $30|S$ وإذا كان n عدد فردي فان $240|S$.

(D) أوجد جميع الأزواج الصحيحة الموجبة (m,n) التي تحقق المعادلة $m^2-n!=780$.

الحل

إذا كان هناك حل فان $n\leq 5$ لأنه إذا كان $n>5$ فان $3|780+n!$ و $9\nmid 780+n!=m^2$ وبالتعويض بـ $n=1,2,3,4,5$ نجد أن $n=5$ و $m=30$ هو الحل الوحيد.

(E) إذا كان $a,b\in\mathbb{Z}$ فأثبت أن $4\mid a^2-b^2$ إذا وإذا فقط كان a,b كلاهما زوجيان أو فرديان.

الحل

افرض أن احدهما وليكن a فردي و b زوجي عندئذ $a^2-b^2=(a+b)(a-b)$ عبارة عن حاصل ضرب فرديين وبالتالي $4\nmid a^2-b^2$. الآن افرض أن كلاهما فرديان أو كلاهما زوجيان إذا $a+b,a-b$ زوجيان وبالتالي $a^2-b^2=(a+b)(a-b)$ يقبل القسمة على 4.

(F) هل توجد كثيرة حدود $p(x)$ معاملاتها أعداد صحيحة بحيث $p(1)=2$ و $p(3)=5$ ؟

الحل

بفرض توجد كثيرة حدود $p(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$ حيث $a_i\in\mathbb{Z},\quad i=0,1,\cdots,n$ و $p(3)=5\quad p(1)=2$.

$$p(1)=2\Rightarrow a_n+a_{n-1}+...+a_1+a_0=2$$

$$p(3)=5\Rightarrow 3^na_n+3^{n-1}a_{n-1}+...+3a_1+a_0=5$$

بالطرح، نحصل على

$(3^n-1)a_n+(3^{n-1}-1)a_{n-1}+...+(3-1)a_{10}=3$ ، تناقض، 2 تقسم الطرف الأيسر لان: $2|3^i-1$ لكل $i=1,2,\cdots,n$ بينما 2 لا قسم 3 (الطرف الأيمن). إذاً لا توجد مثل هذه كثيرة الحدود.

لاحظ أن $a-b|p(a)-p(b)$ لكل $a,b\in\mathbb{Z}$ و $a\neq b$.

(G) أثبت أنه لكل $n>11$ فان العدد $n^2-19n+89$ ليس مربعا

الحل

سوف نثبت أن العدد $n^2-19n+89$ يقع بين عددين مربعين متتاليين لكل $n>11$.

$$n^2-19n+89=n^2-18n+81-(n-8)=(n-9)^2-(\underbrace{n-8}_{>0})<(n-9)^2$$

$$n^2-19n+89=n^2-20n+100+n-11=(n-10)^2+\underbrace{n-11}_{>0}>(n-10)^2$$

أي أن $(n-10)^2<n^2-19n+89<(n-9)^2$.

(H) إذا كان n مكعب كامل فأثبت أن n^2+3n+3 ليس مكعب كامل.

الحل

بفرض العكس أن n^2+3n+3 عدد مكعب كامل وحيث أن n مكعب كامل ، إذاً $n(n^2+3n+3)$ مكعب كامل، ولكن

$$n(n^2+3n+3)=n^3+3n^2+3n=(n+1)^3-1$$

وهذا تعارض لان $(n+1)^3-1$ لا يمكن أن يكون عدد مكعب كامل.

(I)ليكن $a,b,c\in\mathbb{Z}$، أثبت أن $6\left|a^3+b^3+c^3\right.\Leftrightarrow 6\left|a+b+c\right.$.

الحل

لاحظ أن $a^3+b^3+c^3-(a+b+c)=6k$ حيث $k\in\mathbb{Z}$. وينتج المطلوب مباشرة.

(J)أثبت أن العدد $\underbrace{11\cdots1}_{2011}\underbrace{55\cdots5}_{2010}6$ عدد مربع

الحل

ليكن $N=\underbrace{11\cdots1}_{2010}\underbrace{55\cdots5}_{2009}6$

$$N=\underbrace{11\cdots1}_{2011}\times10^{2011}+\underbrace{55\cdots5}_{2010}\times10+6$$

$$=\frac{1}{9}(10^{2011}-1)\times10^{2011}+\frac{5}{9}(10^{2010}-1)\times10+6$$

$$=\frac{1}{9}[(10^{4022}-10^{2011}+5\times10^{2011}+4]$$

$$=\frac{1}{9}[(10^{4022}+4\times10^{2011}+4]$$

$$=(\frac{10^{2011}+2}{3})^2=(\frac{1\underbrace{00\cdots0}_{2010}2}{3})^2=(\underbrace{33\cdots3}_{2010}2)^2$$

القاسم المشترك الأكبر والمضاعف المشترك الأصغر

(A)ليكن $m,n \in \mathbb{Z}$. أوجد $\gcd(2^n, 2m+1)$، $\gcd(6, 2m+1)$ ،
$\gcd(2n+2, 2n+6)$، $\gcd(2^n - 1, 2^n + 1)$

الحل

$\gcd(2^n, 2m+1) = 1$ و $\gcd(6, 2m+1) \mid 3$ و

$$\gcd(2n+2, 2n+6) = \gcd(2n+2, 2n+6-2n-2) = \gcd(2n+2, 4) = 2 \ or \ 4$$

$$\gcd(2^n - 1, 2^n + 1) = \gcd(2^n - 1, 2^n + 1 - 2^n + 1) = \gcd(2^n - 1, 2) = 1.$$

(B)أثبت أن الكسر $\dfrac{21n+4}{14n+3}$ في أبسط صورة لكل $n \in \mathbb{Z}^+$ $(IMO\ 1959)$.

الحل

المطلوب إثبات أن $\gcd(21n+4, 14n+3) = 1$.

بما أن $(21n+4)(-2) + (14n+3) \times 3 = 1$ إذا $\gcd(21n+4, 14n+3) = 1$.

(C)إذا كان $\gcd(a,b) = 1$ فاثبت أن $\gcd(a+b, a^2 - ab + b^2) \mid 3$.

الحل

بفرض $d = \gcd(a+b, a^2 - ab + b^2)$،

$$d \mid (a+b)^2 - a^2 + ab - b^2 = 3ab$$

أيضا $d \mid 3b(a+b)$ ومنها $d \mid 3b^2$ وبالمثل $d \mid 3a^2$ وعليه

$$d \mid (3a^2, 3b^2) = 3(a^2, b^2) = 3(a,b)^2 = 3.$$

(D) أثبت أن $\gcd(5a+3b, 13a+8b) = \gcd(a,b)$.

الحل

بفرض $d_1 = \gcd(a,b)$ و $d_2 = \gcd(5a+3b, 13a+8b)$.

بما أن

$$d_1 \mid a, \quad d_1 \mid b \Rightarrow d_1 \mid 5a+3b, \quad d_1 \mid 13a+8b \Rightarrow d_1 \mid d_2 \cdots (1)$$

أيضا

$$d_2 \mid 5a+3b, \quad d_2 \mid 13a+8b \Rightarrow d_2 \mid 8(5a+3b)-3(13a+8b)=a,$$
$$d_2 \mid (-13)(5a+3b)+5(13a+8b)=b$$
$$\Rightarrow d_2 \mid d_1 \cdots (2)$$

من (1) و (2) ينتج المطلوب.

(E) إذا كان $C=6n+8n-1$ $B=3n+5m+1,$ $A=2n+3m+13,$ فاثبت أن $77 \mid \gcd(A,B,C)$.

الحل

ليكن $d=\gcd(A,B,C)$. إذا d كان هو القاسم المشترك الأكبر للأعداد A,B,C فإن d يقسم كل من

$$E=3A-C=m+40,$$
$$F=2B-C=2m+3$$

وأيضا يقسم $G=2E-F=77$ ومن ثم d يجب أن يكون قاسما لـ 77.

(F) احسب $\gcd(n!+1,(n+1)!+1)$ حيث n عدد صحيح موجب.

الحل

$$\gcd(n!+1,(n+1)!+1)=\gcd(n!+1,(n+1)!+1-(n+1)(n+1))$$
$$=\gcd(n!+1,n)=1$$

(G) ليكن n عدد صحيح أكبر من 2 ، أثبت انه يوجد ضمن الكسور $\frac{1}{n},\frac{2}{n},\cdots,\frac{n-1}{n}$ عدد زوجي من الكسور غير القابلة للتحليل.

الحل

الفكرة في أن الكسر $\frac{k}{n}$ غير قابل للتحليل إذا وفقط إذا كان الكسر $\frac{n-k}{n}$ غير قابل للتحليل، وذلك لان $\gcd(k,n)=\gcd(n-k,n)$. إذا كان الكسرين $\frac{k}{n}$ و $\frac{n-k}{n}$ مختلفين لكل k فإن مجموع الكسور غير القابلة للتحليل زوجي. إذا كان $\frac{k}{n}=\frac{n-k}{n}$ لـ $k\in\mathbb{Z}^+$ فان $n=2k$ وعليه $\frac{k}{n}=\frac{k}{2k}=\frac{1}{2}$ كسر قابل للتحليل وتؤول هذه إلى الحالة الأولى.

(H) حاصل ضرب أربعة أعداد صحيحة موجبة متتالية لا يمكن أي يكون قوي لعدد صحيح موجب.

الحل

بفرض $n(n+1)(n+2)(n+3)=m^k$ حيث $n,m,k\in\mathbb{Z}^+$ و $k>1$

$$n(n+1)(n+2)(n+3)=(n^2+3n)(n^2+3n+2)=m^k$$

بمـــا أن $\gcd(n^2+3n,n^2+3n+2)=2$ ، إذن $\gcd(\frac{n^2+3n}{2},\frac{n^2+3n+2}{2})=1$

وعليه $\frac{n^2+3n}{2}=a^k$ و $\frac{n^2+3n+2}{2}=b^k$ ومنها $b^k-a^k=1$ ولا يوجد عددين موجبين الفرق بين قواهما يساوي 1.

ملاحظة إذا أضفنا لهذا الضرب العدد 1 فان العدد يصبح مربع كامل.

$$\begin{aligned}n(n+1)(n+2)(n+3)+1&=(n^2+3n)(n^2+3n+2)+1\\&=(n^2+3n)^2+2(n^2+3n)+1\\&=((n^2+3n)+1)^2\end{aligned}$$

(I) أوجد القاسم المشترك الأكبر للأعداد

$$2^{2^2}+2^{2^1}+1,\ 2^{2^3}+2^{2^2}+1,\ ...,\ 2^{2^{n+1}}+2^{2^n}+1,\ ...$$

الحل

اجعل $a_i=2^{2^i}+2^{2^{i-1}}+1$.

$$a_m=2^{2^m}+2^{2^{m-1}}+1=(2^{2^{m-1}}+1)^2-2^{2^{m-1}}=(2^{2^{m-1}}+1-2^{2^{m-2}})(2^{2^{m-1}}+1+2^{2^{m-2}})$$

إذا $a_m=(2^{2^{m-1}}+1-2^{2^{m-2}})a_{m-1}$ وبالتالي $a_{m-1}\mid a_m$. إذا القاسم المشترك الأكبر هو أول حد في المتتابعة وهو $a_2=21$.

(J)إذا كان $n,a,b\in\mathbb{Z}^+$ و $n>1$ فاثبت أن $\gcd(n^a-1,n^b-1)=n^{\gcd(a,b)}-1$

الحل

بدون فقد العمومية نفرض أن $a\geq b$. إذن

$$\gcd(n^a-1,n^b-1)=\gcd(n^a-1-n^{a-b}(n^b-1),n^b-1)=\gcd(n^{a-b}-1,n^b-1)$$

وبهذا نصل إلى المطلوب، تذكر أن $\gcd(a,b)=\gcd(a-b,b)$.

(K)رقم هاتفي، مكون من سبع خانات، إذا نقلت الخانات الأربع اليمنى إلى اليسار ونقلت الخانات الثلاث اليسرى إلى اليمين فإن الرقم الناتج أكبر من ضعف الرقم الأصلي بـ 1. أوجد رقم الهاتف.

الحل

نفرض أن yx هو رقم الهاتف حيث x رقم مكون من أربع خانات و y رقم مكون من ثلاث خانات. من المعطيات $2(y\times 10000+x)+1=x\times 1000+y$ ومنها نجد أن $998x-19999y=1$. الآن، نبحث عن القاسم المشترك الأكبر للعددين 998 و 19999:

$$\begin{aligned}19999 &= 20\times 998+39\\ 998 &= 25\times 39+23\\ 39 &= 1\times 23+16\\ 23 &= 1\times 16+7\\ 16 &= 2\times 7+2\\ 7 &= 3\times 2+1\\ 2 &= 2\times 1+0\end{aligned}$$

وعليه $\gcd(998,19999)=1$ ، نستخدم خوارزمية إقليدس لإيجاد x,y ، بإجراء عملية عكسية لما تم أعلاه نجد أن $1=435\times 19999-998\times 8717$ وعليه يكون $y=435, \quad x=8717,$ ويكون رقم الهاتف هو $8717-435$.ملاحظة هذا الرقم وحيد: لان جميع الحلول x,y تعطى من نتيجة 3 وتكون على الصورة

$$x=8717-19999k$$

$$y=435-998k$$

حيث $k\in\mathbb{Z}$ ويكون كل من x,y موجبين إذا كان $k\leq 0$ والحالة الوحيدة التي يكون فيه الرقم x يتكون من أربع خانات و y من ثلاث خانات هي عندما $k=0$.

الأعداد الأولية والنظرية الأساسية في الحساب

(A)إذا كان 2^n-1 عدد أولي فان n عدد أولي.

الحل

الإثبات بواسطة المكافئ العكسي. ليكن $n=mt$ عدد مؤلف حيث $1<m,t<n$ ونجد أن $2^n-1=2^{mt}-1=(2^m)^t-1=(2^m-1)k$ ومنها $2^m-1\big|2^n-1$ و $2^n-1>1$ عدد مؤلف، لاحظ أن $k>1$.

(B)إذا كان p العدد 27000001 له أربعة عوامل أولية فأوجد مجموعهم.

الحل

$$\begin{aligned}27000001 &= 27\times 10^6+1\\ &= (3\times 10^2)^3+1\\ &= (300+1)(300^2-300+1)\\ &= 301(300^2+2\times 300+1-3\times 300)\\ &= 7\times 43((300+1)^2-30^2)\\ &= 7\times 43(301-30)(301+30)\\ &= 7\times 43\times 271\times 331\end{aligned}$$

ويمكن التحقق من أن كل من 271 و 331 عدد أولي. ويكون مجموعهم مساويا 652.

(C) هل $4^{2009}+2009^4$ عدد أولي؟

الحل

بتطبيق متباينة صوفي جيرمين للمقدار $2009^4+4\times(4^{502})^4$.

متطابقة صوفي جيرمين Sophie Germain :

$$\begin{aligned}a^4+4b^4 &= a^4+4a^2b^2+4b^4-4a^2b^2\\ &= (a^2+2b^2)^2-(2ab)^2\\ &= (a^2+2b^2-2ab)(a^2+2b^2+2ab)\end{aligned}$$

(D)أوجد جميع الحلول الصحيحة الموجبة للمعادلة $2^{2m}-3^{2n}=175$

الحل

واضح أن $m>n$.فكرة الحل التحليل ومناقشة الحالات تبعا للنظرية الأساسية في الحساب

$$2^{2m}-3^{2n}=(2^m-3^n)(2^m+3^n)=7\times 5^2 \quad .$$

لاحظ أن $(2^m-3^n)<(2^m+3^n)$ وعليه يكون لدينا الحالات:

$$(2^m-3^n)=1,\quad (2^m+3^n)=175\cdots(1)$$

$$(2^m-3^n)=5,\quad (2^m+3^n)=35\cdots(2)$$

$$(2^m-3^n)=7,\quad (2^m+3^n)=25\cdots(3)$$

ونجد أن المعادلة (3) فقط التي لها حل هو $m=4$ و $n=2$.

(E)إذا كان p عدد أولي أكبر من 3 فإن العدد p^2+2 مؤلف و $24|\,p^2-1$

الحل

أي عدد أولي أكبر من 3 يكون على الصورة $6k\pm 1$ حيث $k\in\mathbb{Z}^+$ وعليه يكون

$3 \mid p^2 + 2$ ، أي أن $p^2 + 2 = 36k^2 \pm 12k + 3$

وأيضا $p^2 - 1 = 12k(3k \pm 1)$ وحيث أن $k(3k \pm 1)$ عدد زوجي لجميع $k \in \mathbb{Z}^+$ ، إذن

$24 \mid p^2 - 1$.

(F) أوجد جميع الأعداد الأولية p, q التي تجعل $p^2 + pq + q^2$ مربع كامل

الحل

بفرض $p^2 + pq + q^2 = n^2$ حيث n عدد صحيح موجب

$$p^2 + pq + q^2 = n^2 \Rightarrow (p+q)^2 - pq = n^2 \Rightarrow (p+q)^2 - n^2 = pq$$
$$\Rightarrow (p+q-n)((p+q+n) = pq$$

إذن $((p+q+n) = pq \quad (p+q-n) = 1,$ لان $p+q-n \neq p, q$

ومنها $2p + 2q = pq + 1$ وعليه $pq - 2p - 2q + 4 = 3$

ومنها $(p-2)(q-2) = 3$ ويكون $p = 3$ و $q = 5$ أو العكس.

(G) إذا كان للمعادلة $x^2 - 2px + p^2 - 5p - 1 = 0$ جذرين صحيحين ، حيث p عدد أولي.

أوجد القيم الممكنة للعدد p .

الحل

$$x_{1,2} = \frac{2p \pm \sqrt{4p^2 - 4(p^2 - 5p - 1)}}{2}$$
$$= p \pm \sqrt{5p+1}$$

لكي يكون للمعادلة جذرين صحيحين لابد أن يكون $5p + 1$ مربع كامل. ليكن $5p + 1 = n^2$ حيث n عدد صحيح موجب. $5p = (n-1)(n+1)$ وعليه $n - 1 = 5$ أو $n + 1 = 5$ ونجد أن p يساوي 3 أو 7 .

(H) حلل العدد 1001001001 إلى عوامله الأولية.

الحل

$$1001001001 = 1001 \times 10^6 + 1001$$
$$= 1001(10^6 + 1)$$
$$= 7 \times 11 \times 13((10^2)^3 + 1)$$
$$= 7 \times 11 \times 13 \times 101 \times 9901$$

(I) أوجد جميع الأعداد الأولية p بحيث العدد $p^2 + 11$ له 6 قواسم مختلفة من بينها العدد 1 والعدد نفسه

الحل

إذا كان p عدد أولي أكبر من 3 فإن $p = 6k \pm 1, \quad k \in \mathbb{Z}$

$$\Rightarrow p^2 = 36k^2 \pm 12k + 1$$

$$\Rightarrow p^2 + 11 = 36k^2 \pm 12k + 12$$

$$\Rightarrow 12 \mid p^2 + 11$$

وحيث أن $p^2 + 11 > 12$ و العدد 12 له 6 قواسم هي $1,2,3,4,6,12$. إذن $p^2 + 11$ له أكثر من 6 قواسم.

يتبقى حالتين هما $p = 2$ و $p = 3$:

إذا كان $p = 2$ فإن $p^2 + 11 = 15$ له أربعة قواسم فقط.

إذا كان $p = 3$ فإن $p^2 + 11 = 20$ له ستة قواسم بالضبط. إذاً $p = 3$ هو الحل الوحيد.

(J) إذا كان p, q أوليان وكان $r = \dfrac{p^2 + q^2}{p + q}$ عدد صحيح فأثبت أن r أولي.

الحل

إذا كان $p = q$ واضح أن $r = \dfrac{p^2 + q^2}{p + q} = \dfrac{p^2}{2p} = p$ وهو أولي. لنفرض الآن أن $p \neq q$ أن $r = \dfrac{p^2 + q^2}{p + q}$ عدد صحيح. بما أن $p^2 + q^2 = (p + q)^2 - 2pq$ فإن $p + q \mid 2pq$ ولكن $(p + q, pq) = 1$ لأن $(p + q, p) = 1, (p + q, q) = 1$. إذا $p + q \mid 2$ وهذا مستحيل.

التطابقات قياس n

(A) أوجد آخر رقمين(خانتي الآحاد والعشرات) من العدد 7^{2010} .

الحل

بما أن $7^4 = 49^2 = (50 - 1)^2 \equiv 1 (\mathrm{mod}\, 100)$

إذا $7^{2010} = (7^4)^{502} \times 7^2 \equiv 1^{502} \times 49 \equiv 49 (\mathrm{mod}\, 100)$ **وعليه فإن آخر رقمين هما** 49

(B) أثبت أن $2222^{5555} + 5555^{2222}$ يقبل القسمة على 7

الحل

$$2222 \equiv 3 (\mathrm{mod}\, 7)$$

$$3^3 = 27 \equiv -1 (\mathrm{mod}\, 7)$$

$$2222^{5555} \equiv 3^{5553+2} \equiv 3^{3k+2} \equiv (-1)^k \cdot 3^2 \equiv -9 \equiv -2 (\mathrm{mod}\, 7)$$

لاحظ أن k عدد فردي. بالمثل

$$5555 \equiv 4(\mathrm{mod}\,7)$$

$$3^3 = 27 \equiv -1(\mathrm{mod}\,7)$$

$$5555^{2222} \equiv 4^{2220+2} \equiv 4^{3m+2} \equiv (-1)^m \cdot 4^2 \equiv 16 \equiv 2(\mathrm{mod}\,7)$$

لاحظ m زوجي. بالجمع نصل للمطلوب.

(C)أوجد آخر رقمين من العدد $229^{10} + 37^{10}$.

الحل

سنستخدم الخاصية: إذا كان $a \equiv b\,(\mathrm{mod}\,n)$ فإن $a^n \equiv b^n\,(\mathrm{mod}\,n^2)$.

$$229 \equiv 29 \equiv -1\ (\mathrm{mod}\,10) \Rightarrow 229^{10} \equiv (-1)^{10} \equiv 1\ (\mathrm{mod}\,100)$$

$$37 \equiv 7\ (\mathrm{mod}\,10) \Rightarrow 37^{10} \equiv 7^{10} \equiv (50-1)^5 \equiv 250-1 \equiv 49\ (\mathrm{mod}\,100)$$

إذا $229^{10} + 37^{10} \equiv 1 + 49 \equiv 50\ (\mathrm{mod}\,100)$ والباقي يكون 50.

(D) أوجد آخر رقمين من العدد 2^{999}.

الحل

لاحظ أولا أن: $2^{10} \equiv -1(\mathrm{mod}\,25)$ وعليه فان

$$2^{997} = (2^{10})^{99}.2^7 \equiv (-1).3(\mathrm{mod}\,25) \equiv 22(\mathrm{mod}\,25)$$

ومنها نجد أن

$$2^2.2^{997} \equiv 4.22(\mathrm{mod}\,100) \equiv 88(\mathrm{mod}\,100)$$

لاحظ استخدمنا: $a \equiv b(\mathrm{mod}\,n) \Leftrightarrow am \equiv bm(\mathrm{mod}\,mn)$ لكل $m \in \mathbb{Z}^+$.

حل آخر: $2^{12} \equiv -4(\mathrm{mod}\,100)$ ومنها $2^{72} = (2^{12})^6 \equiv -4(\mathrm{mod}\,100)$ وأيضا $2^{432} = (2^{72})^6 \equiv -4(\mathrm{mod}\,100)$ وعليه $2^{864} \equiv 16(\mathrm{mod}\,100)$.

أيضا $2^{60} \equiv -24(\mathrm{mod}\,100)$ ومن ثم $2^{999} \equiv 88(\mathrm{mod}\,100)$.

(E)إذا كان p عدداً أولياً و k عدد صحيح بحيث $1 \le k < p$ فأثبت أن $p \left| \binom{p}{k} \right.$.

الحل

بما أن $k\binom{p}{k} = p\binom{p-1}{k-1}$، إذن $p \mid k\binom{p}{k}$ وحيث أن $\gcd(k,p) = 1$ أذن $p \left| \binom{p}{k} \right.$، الجزء الثاني ينتج مباشرة من نظرية ذات الحدين واستخدام الجزء الأول.

(F) حل المعادلة التالية في الأعداد الصحيحة $x^2 + y^2 = 3^{2008}$.

الحل

بما أن $x^2+y^2 \equiv 3^{2008} \equiv 0 \pmod 3$ وحيث أنه لأي عدد صحيح a فان $a^2 \equiv 0 \ or \ 1 \pmod 3$ وعليه $x^2+y^2 \equiv 0 \pmod 3$ إذا وإذا فقط $3 \mid x,y$. إذا افرض أن $x=3x_1$ و $y=3y_1$ وبالتعويض في المعادلة والقسمة على 3^2 نستنتج أن ${x_1}^2+{y_1}^2=3^{2006}$. بتكرار نفس الإجراء مرات متعاقبة يتولد متتابعة $(x_k)_{k=1}^{1004}$ وأخرى $(y_k)_{k=1}^{1004}$ بحيث $x=3^{1004}x_{1004}$ و $y=3^{1004}y_{1004}$ و ${x_{1004}}^2+{y_{1004}}^2=1$ وهذه لها الحلول الأربعة $(\pm 1,0),\ (0,\pm 1)$. إذا المعادلة الأصلية لها الحلول $(\pm 3^{1004},0),\ (0,\pm 3^{1004})$.

(G) حدد الأعداد الصحيحة الموجبة m بحيث يكون $m!+5$ مكعب كامل.

الحل

دراسة هذه المسألة قياس 7 سيكون مناسب جدا، وهذه إستراتيجية مهمة.

بما أن $m \equiv 0,1,2,3,4,5,6 \pmod 7$ نريد أن نرى بواقي m^3 لذلك سنكتب بواقي القسمة على 7 بالشكل $m \equiv 0,\pm 1,\pm 2,\pm 3 \pmod 7$ حتى يسهل حساب المكعبات.

بالتكعيب وفقا للخاصية $a^k \equiv b^k \pmod n$ نجد أن $m^3 \equiv 0,\pm 1 \pmod 7$. إذا باقي مكعب أي عدد لدى قسمته على 7 هو 0 أو ± 1. لذلك إذا كانت $m \geq 7$ فإن $m!+5$ ليس مكعب كامل لأن

$$m!+5 \equiv 0+5 \equiv 5 \pmod 7$$

يبقى فقط فحص $m!+5$ عندما $m<7$:

$$m=6,\ m!+5=5(6\cdot 4\cdot 3\cdot 2+1)=5\cdot 145=5^2\cdot 29$$

$$m=5,\ m!+5=5(4\cdot 3\cdot 2+1)=5\cdot 25=5^3$$

عندما $m=4,3,2,1$ فإن $m!+5=29,11,7,6$ على الترتيب. إذا $m!+5$ مكعب كامل فقط عندما $m=5$.

(H) أثبت أنه يوجد عدد غير منتهي من الأعداد الأولية التي على الصورة $4k+1$.

الحل

بفرض يوجد عدد منتهٍ من الأعداد الأولية التي على الصورة $4k+1$، هي $p_1<p_2<...<p_t$. خذ العدد $N=(2p_1p_2...p_t)^2+1$. بما أن $N>1$ عدد فردي، إذا يوجد له قاسم أولي $p>2$. أي أن $(2p_1p_2...p_t)^2 \equiv -1 \pmod p$ وعليه p يجب أن يكون على الصورة $4n+1$ حيث $n \in \mathbb{Z}^+$ و بما أن $p_{1,}p_2,...,p_t$ هي جميع الأعداد التي على الصورة $4k+1$ فإن $p=p_i$ حيث $1 \leq i \leq t$ وبالتالي $p \mid N$ و $p \mid (2p_1p_2...p_t)^2$ وعليه $p \mid N-(2p_1p_2...p_t)^2=1$ وهذا مستحيل. إذن عكس الفرض هو الصحيح.

(I)أثبت أن $2^{11\times 31} \equiv 2(\mathrm{mod}\, 11\times 31)$

الحل: باستخدام الخاصية (8): $a \equiv b(\mathrm{mod}\, n_1),\ \ a \equiv b(\mathrm{mod}\, n_2)$ إذا وإذا فقط .

$a \equiv b\,(\mathrm{mod}[n_1, n_2])$.

نستنتج أن

$2^{11\times 31} \equiv 2(\mathrm{mod}\, 11\times 31)$ إذا وإذا فقط $2^{11\times 31} \equiv 2(\mathrm{mod}\, 11)$ و $2^{11\times 31} \equiv 2(\mathrm{mod}\, 31)$. بما أن $2^5 \equiv 32 \equiv -1\ (\mathrm{mod}\, 11)$ فإن

$$2^{11\times 31} \equiv 2^{5(68)+1} \equiv (-1)^{68}\cdot 2^1 \equiv 2\,\mathrm{mod}\, 11$$

بالمثل حيث أن $2^5 \equiv 1(\,\mathrm{mod}\, 31)$ نستنتج أن $2^{11\times 31} \equiv 2(\mathrm{mod}\, 31)$ ويثبت المطلوب.

(J) أوجد المربعات الكاملة في المتتابعة

$$1!,\ 1!+2!,\ 1!+2!+3!,1!+2!+3!+4!,\ \ldots,\ 1!+2!+3!+\cdots+n!,\ \ldots$$

الحل

بفرض $S_n = 1!+2!+3!+\cdots+n!$

من خلال الحساب يتضح أن الحدود من S_1 إلى S_4 ليس بينها مربع كامل سوى S_1, S_3 .

الآن افرض $n \geq 5$. لدينا $S_n = (1!+2!+3!+4!)+5!+\cdots+n! = 33+5!+\cdots+n!$

$S_n - 3 = 30+5!+\cdots+n!$ كل حد من حدود $5!+\cdots+n!$ يقبل القسمة على 5 وعليه فإن $S_n - 3$ يقبل القسمة على 5 . بمعنى آخر $S_n \equiv 3(\mathrm{mod}\, 5)$. هذا التطابق قياس 5 مستحيل التحقق عندما يكون S_n مربع كامل وذلك لان لأي عدد طبيعي k فإن $k \equiv 0,\pm 1,\pm 2(\mathrm{mod}\, 5)$ وعليه فإن $k^2 \equiv 0,1,4(\mathrm{mod}\, 5)$ إذا S_n ليس مربع كامل لكل $n \geq 5$.

(K)أوجد باقي قسمة $17+177+1777+\cdots+1\underbrace{77\cdots 7}_{20}$على 7 .

الحل

ضع $S = 17+177+1777+\cdots+1\underbrace{77\cdots 7}_{20}$.

$$S \equiv \sum_{k=1}^{20} 10^k (\mathrm{mod}\, 7) \equiv 3(3+2+6+4+5+1)+3+2 \equiv 5(\mathrm{mod}\, 7)$$