قابليــة القسمــة

Divisor

تعريف :

نقول إن العدد الصحيح a ، حيث $a \neq 0$ ، قاسما (divisor) للعدد الصحيح b ونكتب $a \mid b$ إذا وفقط إذا وجد عدد صحيح c يحقق المساواة b=ca. كما نقول إن a عامل من عوامل b أو b قابل للقسمة على a أو b من مضاعفات a . وإذا كان لا يقسم b، نكتب $a \not| b$

على سبيل المثال :

$$3 \mid 15 \quad , \quad 7 \mid 28, \quad 3 \not| 7 \quad , \quad 4 \not| 10 \quad , \quad 7 \not| 2 \quad , \quad 8 \not| 2$$

مبرهنة :

لتكن a,b,c أعداد صحيحة . عندئذ :

(1) إذا كان $a \mid b$ و $a \mid c$ فإن $a \mid (bx + cy)$ لجميع الأعداد الصحيحة x,y .

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

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

(4) إذا كان a>0 ، b >0 وكان $a \mid b$ فإن $a \leq b$.

(5) إذا كان $a \mid b$ فإن $|a| \mid |b|$.

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

البرهان :

(1) بما أن $a \mid b$ و $a \mid c$ فإنه يوجد عددان صحيحان s,t بحيث b=as، c=at

وعليه فإن :

Bx+cy=asx+aty=a(sx+ty)

ومنه نجد أن : $a \mid (bx + cy)$.

(2) بما أن $a \mid b$ و نعلم أن $a \mid a$. إذن من (1) نستنتج أن $a \mid (ax+by)$ لجميع قيم x,y .
وبإختيار x=0 و y=c نحصل على $a \mid bc$.

(3) بما أن $a \mid b$ و $b \mid c$ فإنه يوجد عددان صحيحان s,t بحيث b=as، c=bt
وعليه فإن : c=ast . ومنه نجد أن $a \mid c$.

(4) بما ان $a \mid b$ فإن b=ac حيث $c \in Z$ ، بما أن a>0 ، b >0 فإن c >0 . ومنه نجد أن
$c \geq 1$ لأن c عدد صحيح موجب . وبالتالي فإن $b = ac \geq a$.

(5) بما أن $a \mid b$ فإن b=ac حيث $c \in Z$ ، بأخذ القيمة المطلقة للطرفين نحصل على :
$|b| = |a||c|$ ومنه $|b| \geq |a|$.

(6) بما أن $a \mid b$ و $b \mid a$ فإن $|a| \leq |b|$ وكذلك $|b| \leq |a|$ وبإستخدام (4) نجد ان :
$|a| \leq |b|$ وكذلك $|b| \leq |a|$وهذا يعني أن $|a| = |b|$ وبالتالي $a = \pm b$.

مبرهنة (خوارزمية القسمة): (division algorithm)

ليكن a عدداً صحيحاً موجباً وليكن b عدداً صحيحاً . عندئذ ، يوجد عددان صحيحان وحيدان r,q بحيث يتحقق التالي :

b=qa+r حيث $0 \leq r < a$.

مثال :

برهن أن أي عدد صحيح فردي يمكن كتابته على الصورة 4k+1 أو 4k+3 حيث $k \in Z$.

الحل :

بأخذ a=4 واستخدام خوارزمية القسمة نستطيع كتابة أي عدد صحيح b على الصورة 4k+r حيث r=0,1,2,3 . ومنه نجد أن أي عدد فردي يكتب على الصورة 4k+1 أو 4k+3 لأن 4k ، 4k+2 عددان زوجيان .

مبرهنة :

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

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

علماً أن المعاملات a_t تأخذ قيم صحيحة بين العددين 0 و k-1 و $a_m \neq 0$.

ملاحظة :

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

$$a_m k^m + a_{m-1} k^{m-1} + ... + a_2 k^2 + a_1 k + a_0$$

مثال :

اكتب العدد 37 للأساس k=2 .

الحل :

$$\begin{aligned} 37 &= 2(18)+1 & q_1 &= 18 > k \\ 18 &= 2(9)+0 & q_2 &= 9 > k \\ 9 &= 2(4)+1 & q_3 &= 4 > k \\ 4 &= 2(2)+0 & q_4 &= 2 \geq k \\ 2 &= 2(1)+0 & q_5 &= 1 < k \end{aligned}$$

نضع $q_5 = a_5$ فنحصل على التمثيل :

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

مثال :

اكتب العدد 61469 للأساس k=16 .

الحل :

$$\begin{aligned} 61469 &= 16(3841)+13 & q_1 &= 3841 > k \\ 3841 &= 16(240)+1 & q_2 &= 240 > k \\ 240 &= 16(15)+0 & q_3 &= 15 < k \end{aligned}$$

نضع $q_3 = a_3$ فنحصل على التمثيل :

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

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

القاسم المشترك الأعظم : (Greatest common divsor)

تعريف :

ليكن a,b عددين صحيحين ليس كلاهما صفراً . نقول أن d هو القاسم المشترك الأعظم للعددين a,b ونرمز لذلك بالرمز d=(a,b) إذا تحقق ما يلي :

(1) $d>0$.

(2) $d|a$ و $d|b$.

(3) إذا كان $c|a$ و $c|b$ ، $c>0$ فإن $c \le d$

مثال :

(27,41)=1 , (-3,-9)=3 , (6,9)=3 , (5,15)=5 ,(7,16)=1.

مبرهنة :

إذا كان a,b عددين صحيحين ليس كلاهما صفراً فإنه يوجد عددان x_0, y_0 بحيث $d=(a,b)=ax_0+by_0$. أي أن (a,b) تركيباً خطياً (linear combination) من a,b .

ملاحظة :

العددين x_0, y_0 ليسا وحيدين فعلى سبيل المثال :

إن (15,24)=3

وإن :

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

نتيجة :

إذا كان d=(a,b) وكان c|a و c|b فإن c|d .

إحدى طرق إيجاد القاسم المشترك الأعظم هي خوارزمية اقليدس (Euclidean algorithm) والتي نمهد لها بما يلي :

تمهيدية :

إذا كان $b=qa+r$ فإن $(a,b)=(a,r)$.

البرهان :

ليكن $d=(a,b)$. بما أن $d|a$ و $d|b$ فإن $d|(qa+r)$. ومنه نجد أن $d|r$.

نفرض الآن أن $c|r$ و $c|a$. من الواضح أن $c|(qa+r)$. وعليه فإن $c|b$ وبذلك نكون قد برهنا أن c قاسم مشترك لكل من a,b وعليه $c \le d$ أي أن $d=(a,r)$.

تمهيدية :

إذا كان a,b عددين صحيحين ليس كلاهما صفراً فإن :

(1) $(a,b)=(-a,b)=(a,-b)=(-a,-b)$.

(2) $(a,0)=a$ إذا كان $a>0$.

مبرهنة : خوارزمية إقليدس (Euclidean algorithm)

ليكن $b \ge a > 0$ عددين صحيحين . من خوارزمية القسمة لدينا :

$$\begin{aligned}
0<r_1<a \quad &, \quad b=aq_1+r_1 \\
0<r_2<r_1 \quad &, \quad a=r_1q_2+r_2 \\
0<r_3<r_2 \quad &, \quad r_1=r_2q_3+r_3 \\
&\vdots \\
0<r_n<r_{n-1} \quad &, \quad r_{n-2}=r_{n-1}q_n+r_n \\
r_{n+1}=0 \quad &, \quad r_{n-1}=r_nq_{n+1}+0
\end{aligned}$$

عندئذ ، $(a,b)=r_n$.

البرهان :

من الخوارزمية نلاحظ أن :

$$a>r_1>r_2>r_3>.....>r_n>r_{n+1}$$

وحيث أن الأعداد r_i صحيحة فلابد من وجود n بحيث $r_{n+1}=0$. ومن التمهيديتين السابقتين نجد أن :

$$(b,a)=(a,r_1)=(r_1,r_2)=.....=(r_n,r_{n+1})=(r_n,0)=r_n$$

ملحوظة :

بالإضافة إلى إيجاد القاسم المشترك الأعظم لعددين a,b فإن خوارزمية إقليدس تستخدم أيضاً لإيجاد x,y المرتبطين بالمساواة: (a,b)=ax+by

مثال :

احسب (6755,1587645) ، ثم جد عددين x,y بحيث :

(6755,1587645)= 6755 x+1587645 y

الحل :

$$1587645=235\times 6755+220$$
$$6755=30\times 220+155$$
$$220=1\times 155+65$$
$$155=2\times 65+25$$
$$65=2\times 25+15$$
$$25=1\times 15+10$$
$$15=1\times 10+5$$
$$10=2\times 5+0$$

وعليه فإن : 5=(6755,1587645).

من الخطوة قبل الأخيرة أعلاه وبالمرور على خطوات الخوارزمية بصورة عكسية نحصل على :

$$
\begin{aligned}
5 &= 15 - 1\times 10 \\
&= 15\text{-}1\times(25 - 1\times 15) \\
&= \text{-}25 + 2\times 15 \\
&= \text{-}25+2(65 - 2\times 25) \\
&= 2\times 65 - 5(155 - 2\times 65) = 2\times 65 - 5\times 25 \\
&= \text{-}5\times 155+12\times 65 \\
&= \text{-}5\times 155+12(220 - 1\times 155) \\
&= 12\times 220 - 17(6755 - 30\times 220) \\
&= \text{-}17\times 6755 + 522(1587645 - 235\times 6755) \\
&= 6755(-122687) + 1587645(522)
\end{aligned}
$$

ومنه نجد :

$y=522$ و $x=-122687$

مبرهنة :

إذا كان a,b عددين صحيحين ليس كلاهما صفراً فإن $(a,b)=1$ إذا وفقط إذا وجد عددان صحيحان x,y بحيث ان $ax+by=1$.

تعريف :

يسمى العددان a,b اللذان قاسمهما المشترك الأعظم 1 عددين أوليين نسبياً (relatively prime) .

مثال :

العددان 15 و 32 أوليان نسبياً ، أما العددان 15 و18 فإنهما ليسا أوليين نسبياً .

نتيجة :

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

نتيجة :

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

ملحوظة :

لا يمكن الإستغناء عن الشرط $(a,b)=1$ فمثلا :

$48|8$ و $48|12$ ولكن $8\times12\not|48$.

نتيجة :

إذا كان $a|bc$ وكان $(a,b)=1$ فإن $a|c$.

ملحوظة :

لا يمكن الإستغناء عن الشرط $(a,b)=1$ فمثلا :

$$8\times9\,|\,12 \quad \text{ولكن} \quad 9\not|12 \quad , \quad 8\not|12.$$

مثال :

جد $(256,112,72)$.

الحل :

$$(256,112,72)=(256,(112,72))=(256,8)=8$$

تعريف:

توصف الأعداد $a_1,a_2,...,a_n$ بأنها اولية تبادليا (mutually prime) إذا كان $(a_1,a_2,...,a_n)=1$ وتوصف بأنها أولية نسبيا مثنى مثنى (relatively prime in pairs) إذا كان $(a_i,a_j)=1$ لكل $1\le i\ne j\le n$.

ملحوظة :

الأعداد الأولية نسبيا مثنى مثنى هي اعداد أولية تبادليا ولكن العكس غير صحيح .

مثال توضيحي :

الاعداد 15 ,21,35 اولية تبادلياً لأن :

$$(15,21,35)=(15,(21,35))=(15,7)=1$$

ولكنها ليست اعداد أولية نسبيا مثنى مثنى لأن :

$$(21,35)=7 \quad , \quad (15,35)=5 \quad , \quad (15,21)=3.$$

تعريف :

إذا كان كل من a,b عدداً صحيحاً فإننا نقول m هو المضاعف المشترك الأصغر(least common multiple) للعددين a,b ونكتب $m=[a,b]$ إذا تحقق ما يلي :

(1) $m>0$.

(2) $a|m$ و $b|m$.

(3) إذا كان $a|c$ و $b|c$ ، $c>0$ فإن $m \le c$.

مثال :

$[5,15]=15$, $[6,15]=30$, $[9,8]=72$.

إذا عُلم القاسم المشترك الاعظم فبالإمكان حساب المضاعف المشترك الأصغر من خلال المبرهنة التالية :

مبرهنة :

إذا كان $a>0$ و$b>0$ فإن $[a,b](a,b)=ab$.

البرهان :

بافتراض ان $d=(a,b)$ وان $m=\frac{ab}{d}$. فإنه يوجد عددان صحيحان r,s بحيث ان

$a=dr$, $b=ds$. وبالتالي فإن $m=as=rb$.

إذا كان $a|c$ و$b|c$ ،فإنه يوجد عددان صحيحان t,u بحيث أن $c=au=bt$

وبما ان $d=(a,b)$ فإنه يوجد عددان x,y بحيث أن

$$d=ax+by$$

وعليه فإن :

$$\frac{c}{m}=\frac{cd}{ab}=\frac{c(ax+by)}{ab}=\frac{c}{b}x+\frac{c}{a}y=tx+uy$$

ومنه نجد أن $m|c$ ، أي أن $m \le c$.

وبذلك نكون برهنا على أن $m=[a,b]$.

ملحوظة :

هذه العلاقة $[a,b](a,b)=ab$ غير صحيحة لأكثر من عددين .

مثال توضيحي:

بما أن :

$(6,10,15)=1$, $[6,10,15]=30$ فإن : $[6,10,15](6,10,15)=30\neq 900=6\times 10\times 15$

التمارين

السؤال الاول :

اثبت صحة أو خطأ العبارات التالية :

(1) إذا كان $a|b$ و$a|c$ فإن $a^2 \mid bc$.

(2) $a|b$ إذا وفقط إذا كان $ac|bc$ ، حيث إن $c \neq 0$.

(3) إذا كان $a|(b+c)$ فإنه إما أن يكون $a|b$ أو يكون $a|c$.

(4) إذا كان $a|c$ و $b|c$ فإن $[a,b]|c$.

السؤال الثاني :

اثبت أن $5^{2n+1} + 3^{4n+2}$ يقبل القسمة على 14 لكل $n \geq 1$.

السؤال الثالث :

جد (123456789,987654321) ثم جد x,y بحيث يكون :

(123456789,987654321)= 123456789x+987654321y

الأعداد الأولية والمبرهنة الأساسية في الحساب

Prime Numbers and The Fundamental Theorem of Arithmetic

تعريف :

نقول إن العدد الصحيح p عدد أولي (prime number) ، إذا كان $p>1$ وكان لا يقبل القسمة إلا على نفسه والعدد 1 . نسمي العدد الصحيح الموجب غير الأولي الذي لا يساوي 1 عدد مؤلفاً (composite number) .

إذن فالعدد المؤلف n يمكن أن نكتبه كما يلي :

$n=ab$ حيث إن $1<b<n$ و $1<a<n$.

مبرهنة :

إن أي عدد صحيح $n>1$ إما أن يكون أولياً ، أو أن يكون حاصل ضرب عدد منته من الأعداد الأولية .

البرهان :

بواسطة المبدأ الثاني للأستقراء الرياضي .

الخطوة الأساسية :

العدد 2 عدد أولي .

خطوة الأستقراء :

نفرض أن أي عدد m بحيث إن $2 \le m \le k$ هو حاصل ضرب عدد منته من الأعداد الأولية .

سنبرهن على أن k+1 هو حاصل ضرب عدد منته من الأعداد الأولية .

إذا كان k+1 عدد أولي فتتحقق المبرهنة .

إذا كان k+1 عدد مؤلف فإن k+1=ab حيث إن $2 \le a, b \le k$. فبإستخدام فرضية الاستقراء الرياضي نستطيع كتابة كل من a,b كحاصل ضرب عدد منته من الأعداد الأولية ،

وبالتالي فإننا نستطيع كتابة k+1 كحاصل ضرب عدد منته من الأعداد الأولية .

نتيجة :

كل عدد صحيح n>1 يكون له قاسم أولي .

البرهان :

إذا كان n عدداً أولياً فالعبارة صحيحة لأن $n|n$. أما إذا كان n عدداً مؤلفاً فإننا نحصل على القاسم الأولي لأنه عبارة عن حاصل ضرب عدد منته من الأعداد الأولية (وذلك من المبرهنة السابقة).

نتيجة :

إذا كان n عدد مؤلف فإنه يوجد قاسم أولي p للعدد n بحيث أن $p \le \sqrt{n}$.

البرهان :

بما ان n عدد مؤلف فإن n=ab و $1 < a \le b < n$. ولذا فإن $n = ab \ge a^2$ ومنه نجد $a \le \sqrt{n}$.
وبالتالي فإنه يوجد عدد أولي p بحيث $p|a$. ومنه نجد أن $p|n$ و $p \le a$. وبالتالي فإن $p \le \sqrt{n}$.

نتيجة :

إذا كان n>1 عدداً لا يوجد له أي قاسم أولي أقل من $\sqrt{n}$ أو يساويه فإن n يجب أن يكون عدداً أولياً .

البرهان:

بفرض العكس إذا كان n عدداً مؤلفاً فإنه يجب أن يكون له قاسم أولي أقل من $\sqrt{n}$ أو يساويه وهذا تناقض.

مبرهنة :

يوجد عدد غير منته من الأعداد الأولية .

البرهان :

بوضع $Q_n = n!+1$ حيث $n \geq 1$. نجد أن Q_n له على الأقل عامل أولي واحد وليكن q_n . إذا كان $q_n \leq n$ فإن $q_n \mid n!$. ومنه نجد أن $q_n \mid (Q_n - n!)$. أي أن $q_n \mid 1$ وهذا مستحيل . أي أن $q_n > n$. إذن نكون قد برهنا على أنه يوجد لكل عدد صحيح موجب n عدد أولي أكبر من n ، وبالتالي يكون عدد الأعداد الأولية غير منته لأن مجموعة الأعداد الصحيحة الموجبة غير منتهية .

مبرهنة :

لكل عدد صحيح موجب n يوجد على الأقل n من الأعداد الصحيحة المؤلفة المتتالية الموجبة .

البرهان :

الأعداد الصحيحة التالية:

$$(n+1)!+2\ ,(n+1)!+3,\ .....\ ,\ (n+1)!+(n+1)$$

عددها n وهي جميعها مؤلفة وذلك لأن $k \mid (n+1)!$ لكل k

حيث إن $2 \leq k \leq n+1$ ومنه نجد أن $k \mid (k+1)!+k$ لكل k

حيث إن $2 \leq k \leq n+1$.

إحدى المبرهنات المهمة في نظرية الأعداد تعرف بالمبرهنة الأساسية للحساب وقبل تقديمها سنمهد لها بالتمهيدية التالية :

تمهيدية :

(أ) إذا كان p عدداً أولياً حيث إن $p \mid ab$ فإن $p \mid a$ أو $p \mid b$.

(ب) إذا كان $p \mid a_1 a_2 .... a_n$ حيث إن p عدد أولي فلابد للعدد p أن يقسم عدداً واحداً على الأقل بين الأعداد $a_1 a_2 .... a_n$.

البرهان :

(أ) بفرض أن $p \nmid a$. بما أن p عدد أولي فإنه يجب أن يكون (p,a)=1 ، وبما أن $p \mid ab$ فبإستخدام تمهيدية إقليدس نجد أن $p \mid b$.

(ب) بواسطة الأستقراء الرياضي .

الخطوة الأساسية :

إذا كان n=1 فإن العبارة صحيحة .

خطوة الإستقراء :

نفرض أن العبارة صحيحة لجميع الأعداد 1,2,3,...,n وليكن $p|(a_1a_2....a_na_{n+1})$. ومنه نجد أن $p|(a_1a_2.... a_n)a_{n+1}$ ومن (أ) نجد أنه إما أن $p|a_1a_2....a_n$ أو أن $p|a_{n+1}$.

إذا كان $p|a_1a_2....a_n$ فإنه بإستخدام الاستقراء الرياضي يوجد a_i حيث $p|a_i$. وبهذا يكون قد تم البرهان .

مبرهنة :[المبرهنة الأساسية في الحساب] The Fundamental theorem of arithmetic

أي عدد صحيح n>1 يمكن كتابته بشكل وحيد كحاصل ضرب عدد منته من الأعداد الأولية .

ملحوظات :

(1) من الممكن أن يتكرر عدد أولي معين عند تحليل العدد n إلى عوامله الأولية ، فإذا كانت العوامل الأولية المختلفة للعدد n هي $p_1,p_2,...,p_k$ وعدد تكرار p_i هو a_i لكل i و $1\le i\le k$ فإننا نستطيع كتابة العدد n على الصورة :

$$n=p_1^{a_1}p_2^{a_2}\ ....\ p_k^{a_k}$$

ويسمى التحليل السابق بالصورة القياسية لتحليل n .

(2) إذا كان كل من n,m عدد صحيح موجب فإننا نحتاج أحيانا إلى تحليل كل من n,m إلى عوامل أولية بحيث تكون جميع الأوليات في تحليل n هي الأوليات نفسها في تحليل m ، ويمكن الحصول على ذلك بإدخال عوامل أولية مرفوعة إلى القوة 0 كما في المثال التالي :

$$30=2\times3\times5\times7^0$$
$$14=2\times3^0\times5^0\times7$$

(3)إن أهمية المبرهنة الأساسية للحساب ترجع إلى أن تحليل العدد إلى حاصل ضرب أعداد أولية هو تحليل وحيد ، وهناك مجموعات كثيرة من الأعداد لا تتحقق فيها هذه الخاصية الهامة ،

على سبيل المثال :

لو أخذنا الأعداد الزوجية ورمزنا لهذه المجموعة بالرمز E واتفقنا أن نقول أن العدد الزوجي يكون عدد أولي في المجموعة E إذا لم نستطع كتابته كحاصل ضرب عددين في المجموعة E.

وعليه فإن الأعداد 14,10,6,2 جميعها أعداد أولية في المجموعة E ، بينما الأعداد 16,12,8,4 ليست أولية في المجموعة E .
من السهل الآن أن نرى أنه يمكن كتابة العدد 60 بطريقتين مختلفتين كحاصل ضرب أعداد أولية في المجموعة E . في الحقيقية :

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

مبرهنة :

إذا كان a,b عددين صحيحين موجبين وكان (a,b)=1 وكان أيضاً $ab = c^n$ فإنه يوجد عددان صحيحان e,d بحيث إن :

$$a=d^n \quad , \quad b = e^n$$

مبرهنة :

ليكن n,m عددين صحيحين أوليين نسبياً . إذا كان d عاملا موجباً للعدد mn فإنه يوجد عددان صحيحان موجبان وحيدان d_1, d_2 بحيث إن

$$d = d_1 d_2 \text{ ، } (d_1, d_2) = 1 \text{ ، } d_1 \mid m, d_2 \mid n .$$

مبرهنة :

إذا كانت : $f(x) = x^n + c_{n-1}x^{n-1} + ... + c_1 x + c_0$ كثيرة حدود واحدية حيث c_i و $0 \le i \le n-1$ أعداد صحيحة وكان α جذراً للمعادلة f(x)=0 فإنه إما أن يكون α عدد غير نسبي أو عدد صحيح .

البرهان :

بفرض أن α عدد نسبي . فإنه يمكن كتابة :

$$\alpha = \frac{a}{b} \quad , \quad a,b \in Z \quad , \quad b \neq 0 \quad , \quad (a,b) = 1 .$$

بما أن α جذر للمعادلة f(x)=0 فإنه يكون :

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

وبضرب طرفي المعادلة بالعدد b^n نحصل على المساواة :

$$a^n=b\left(-c_{n-1}a^{n-1}-.....-c_1ab^{n-2}-c_0b^{n-1}\right)$$

ومنه نجد أن $b\mid a^n$ ندعي أن $b=\pm1$. إذا كان $b\neq\pm1$ فإنه يوجد عدد أولي p ، $p\mid b$ وبما أن $b\mid a^n$ فإن $p\mid a^n$. ومنه نجد أن $p\mid a$. أي أن (a,b) >1 وهذا تناقض . إذن ، $b=\pm1$. ومنه فإن $\alpha=\pm a$. أي أن α عدد صحيح .

نتيجة :

إذا كان n,a عددين صحيحين موجبين وكان $\sqrt[n]{a}$ عدداً نسبياً فإن $\sqrt[n]{a}$ عدد صحيح .

البرهان :

لاحظ أن $\sqrt[n]{a}$ جذر للمعادلة : $x^n-a=0$. وبما أنه عدد نسبي فيجب أن يكون عدداً صحيحاً .

مثال :

برهن على أن العدد $\sqrt{2}$ غير نسبي .

الحل :

بما أن $1<\sqrt{2}<2$ فإن $\sqrt{2}$ عدد غير صحيح وهو جذراً للمعادلة $x^2-2=0$. وعليه فإنه يجب أن يكون غير نسبي .

مثال :

أثبت أن العدد $\sqrt[3]{10}$ غير نسبي .

الحل :

لاحظ أن $\sqrt[3]{10}$ جذر للمعادلة $x^3-10=0$. وبما أن $2<\sqrt[3]{10}<3$ فإنه غير صحيح .وبالتالي فإنه غير نسبي .

مثال :

أثبت أن العدد $\log_{10}2$ غير نسبي .

الحل :

إذا كان $\log_{10} 2$ عدداً نسبياً فإن $\log_{10} 2 = \frac{a}{b}$ حيث إن $a,b \in Z \quad , \quad b \neq 0$. ومنه نجد أن $10^a = 2^b$ أي أن .

$$2^a 5^a = 2^b$$

وهذا يناقض الوحدانية في المبرهنة الأساسية للحساب .

تمـارين

السؤال الأول :

جد جميع الأعداد الأولية التي تكون على الصورة $m^3 - 1$.

السؤال الثاني :

أثبت أن $8^n + 1$ عدد مؤلف لكل $n \geq 1$.

السؤال الثالث :

برهن أن $p^2 + 2$ عدد مؤلف حيث p عدد أولي أكبر من العدد 5 أو يساويه .

السؤال الرابع :

إذا كان $n>2$ فبرهن على أنه لابد من وجود عدد أولي يحقق $n<p<n!$.

أعداد فيرما وطريقة فيرما للتحليل

Fermat Numbers and Fermat Method of Factorization

تعريف :

تسمى الأعداد التي يمكن كتابتها على الصورة $2^{2^n} + 1$ حيث إن $n \geq 0$ بأعداد فيرما Fermats numbers) ويرمز لها بالرمز F_n . وتسمى بأعداد فيرما الأولية إذا كان F_n عدداً أوليا.

مبرهنة :

إذا كان $p = 2^m + 1$ عدداً أولياً فإن $m = 2^n$. أي أن $p = F_n$.

البرهان :

سنبرهن المكافئ العكسي ، أي أنه إذا كان $m \neq 2^n$ لكل $n \geq 0$ فإن p ليس أولياً .

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 $2^m + 1$. وبالتالي فإن $p = 2^m + 1$ ليس أولياً .

إن أحد الخواص المهمة لأعداد فيرما هي أنها أولية نسبياً مثنى مثنى والتي سنمهد لها بالتمهيدية التالية :

تمهيدية :

ليكن $F_n = 2^{2^n} + 1$ عدد فيرما من الرتبة n ، $n \geq 0$. لكل $m \geq 1$ تتحقق المساواة التالية :

$$F_0 \; F_1 \; F_2 \; \ldots \; F_{m-1} = F_m - 2$$

مبرهنة :

$\left(F_m, F_n\right) = 1$ لكل $m, n \geq 0$ ، $m \neq n$.

البرهان:

لنفرض أن m<n . ومن التمهيدية السابقة نجد أن :

$$F_0 \; F_1 \; F_2 \; \ldots F_m \; F_{m+1} \; \ldots F_{n-1} = F_n - 2$$

إذا كان $\left(F_m, F_n\right) = d$ فإن $d \mid F_m, d \mid F_n$. وعليه فإن

$$d \mid \left(F_n - F_0 \; F_1 \; F_2 \; \ldots F_m \; F_{m+1} \; \ldots F_{n-1}\right)$$

، أي أن d|2 ، ومنه نجد أن d=1 أو d=2 ، وبما أن أعداد فيرما هي أعداد فردية فإن $d \neq 2$. مما يجعل d=1 .

نتيجة :

يوجد عدد غير منته من الأوليات .

البرهان :

بما أن $F_m > 1$ فإنه يوجد عدد أولي p_m يقسم F_m . إذن ، لكل F_m يوجد عدد أولي يقسمه . بما أن $\left(F_m, F_n\right) = 1$ فإننا نستنتج أن $p_m \neq p_n$ لكل $m \neq n$ ، مما يدل على وجود عدد غير منته من الأعداد الأولية .

مبرهنة :

كل قاسم أولي لعدد فيرما F_n يكتب على الصورة :

$$2^{n+1}k+1 \text{ حيث إن } k \in Z^+ .$$

مثال :

اثبت أن $F_3 = 257$ عدد أولي .

الحل :

إذا كان $p \mid F_3$ فإن $p = 2^4k+1$. إن أصغرعدد أولي على هذه الصورة هو 17 وهو أكبر من $\sqrt{257}$.

إذن ، F_3 عدد أولي .

مثال :

اثبت أن العدد F_5 مؤلف.

الحل :

إذا كان p عدداً أولياً يقسم F_5 فإن $p = 2^6k+1$ وأن $p \le \sqrt{F_5} < 65537$.

وحيث أن العدد الأولي $641 = 2^6 \times 10 + 1$ يقسم العدد F_5 .

ولذا فإن F_5مؤلف .

تمهيدية :

يكون العدد الفردي n>1 مؤلفاً إذا وفقط إذا وجد عددان صحيحان a,b حيث

$n = a^2 - b^2$ و a-b>1.

البرهان :

نفرض أولاً أن n=rs حيث $r \ge s > 1$. عندئذ ،

$$n = \left(\frac{r+s}{2}\right)^2 - \left(\frac{r-s}{2}\right)^2 .$$

وبما أن n فردي إذاً كلاً من r,s فردي ومن ثم فإن كلاً من r+s و r-s زوجي .

أما برهان العكس فهو واضح لأن

$$n = a^2 - b^2 = (a-b)(a+b)$$

عدد مؤلف.

مثال :

استخدم طريقة فيرما لتحليل العدد n=119143 .

الحل :

بما أن $\sqrt{119143} < 346$

فإننا نبحث عن مربع كامل في المتتالية :

$$(346)^2 - n = 573$$
$$(347)^2 - n = 1266$$
$$(348)^2 - n = 1961$$
$$(349)^2 - n = 2658$$
$$(350)^2 - n = 3357$$
$$(351)^2 - n = 4058$$
$$(352)^2 - n = 4761 = (69)^2$$

ولذا فإن

$$n = 119143 = (352-69)(352+69) = 283 \times 421$$

وهذا هو تحليل nلأن كلا العددين 421 و 283 أولي .

ملحوظة :

لاحظ أنه إذا كان n=ab حيث a-b صغير نسبياً فإن طريقة فيرما لتحليل العدد n تكون فعالة حيث نستطيع إيجاد العاملين a,b بسرعة ، **على سبيل المثال:**

إذا كان n=23360947609 فإن $\sqrt{n} < 152843$ ونجد في المحاولة الثالثة أن $(152845)^2 - n = (804)^2$.

ولذا فإن $n = 152041 \times 153649$.

أما إذا كان الفرق a-b كبيراً جداً فإن طريقة فيرما لتحليل n تكون في العادة غير فعالة .

مثال :

استخدم طريقة فيرما لتحليل العدد n=14152 .

الحل :

لاحظ أولاً أن $n = 2^3 \times 1769$. وبما أن 42<1769<43 فإننا نبحث عن مربع كامل في المتتالية :

$$(43)^2 - 1769 = 80$$
$$(44)^2 - 1769 = 167$$
$$(45)^2 - 1769 = 256 = (16)^2$$

ولذا فإن

$$1769 = (45-16)(45+16) = 29 \times 61 .$$

وبالتالي فإن $14152 = 2^3 \times 29 \times 61$.

التمارين

السؤال الأول :

استخدم طريقة فيرما لتحليل :

326072228 , 977

السؤال الثاني :

أثبت أن العدد F_4 أولي .

السؤال الثالث :

أثبت أن $F_{n+1} = F_n^2 - 2F_n + 2$ لكل $n \geq 0$.

السؤال الرابع :

أثبت أن العدد F_7 مؤلف.

المعادلات الديوفنتية الخطية

Linear Diophantine Equations

مبرهنة :

يوجد حل للمعادلة الديفونتية الخطية ax+by= c إذا وفقط إذا كان (a,b)=d يقسم العدد c .

البرهان :

ليكن d|c . عندئذ توجد أعداد صحيحة n,m,k بحيث إن c=kd وإن d=am+bn ، وبضرب طرفي المعادلة الأخيرة بالعدد k نجد :

$$a(mk)+b(nk)=dk=c$$

وبالتالي فإن x=m k و y=nk حل للمعادلة ax+by=c .

ولبرهان العكس نفرض أن x_0 , y_0 حل للمعادلة . وهذا يؤدي إلى أن :

$$ax_0 + by_0 = c .$$

وبما أن d|a و d|b فإن $d \mid (ax_0 + by_0)$ أي أن d|c.

ملحوظة :

إن المبرهنة السابقة بالإضافة إلى خوارزمية إقليدس تزودنا بطريقة عملية لإيجاد حل للمعادلة ax+by=c ، وبالتحديد فإننا نلجأ إلى إيجاد (a,b) أولاً ثم نكتبه كتركيب خطي للعددين a,b ثم نضرب بعدد مناسب .

مثال توضيحي :

جد حلاً للمعادلة الديوفنتية :

. 56x+72y=40

الحل :

نبحث عن (56,72) بواسطة خوارزمية القسمة فنجد :

$$72 = 1 \times 56 + 16$$

$$56 = 3 \times 16 + 8$$

$$16 = 2 \times 8 + 0$$

ومنه فإن (56,72)=8 يقسم العدد 40 .

الآن ، نضع 8 على صورة تركيب خطي للعددين 56,72 فنجد :

$$\begin{aligned} 8 &= 56-3\times 16 \\ &= 56-3\left(72-1\times 56\right) \\ &= 4\times 56+\left(-3\right)72 \end{aligned}$$

وبضرب طرفي المعادلة بالعدد 5 نجد :

56(20)+72(-15)=40

وبالتالي فإن $x_0 = 20 \ , \ y_0 = -15$ حل للمعادلة .

مبرهنة :

ليكن (a,b)=d وليكن d|c . إذا كان x_0 , y_0 حلاً للمعادلة الديوفنتية ax+by=c

فإن الحل العام للمعادلة يكون على الصورة :

$$y = y_0 - k\left(a/d\right) \quad , \quad x = x_0 + k\left(b/d\right)$$

حيث إن $k \in Z$.

البرهان :

سنبرهن أولاً على أن $y_0 - k\left(a/d\right) \quad , x_0 + k\left(b/d\right)$ حل للمعادلة لكل قيم k الصحيحة . بالتعويض المباشر في المعادلة نحصل على المساواة :

$$\begin{aligned} ax+by &= a\left(x_0 + k\left(b/d\right)\right) + b\left(y_0 - k\left(a/d\right)\right) \\ &= ax_0 + by_0 + k\left(ab/d\right) - k\left(ab/d\right) \\ &= ax_0 + by_0 = c \end{aligned}$$

وسنبرهن الآن على أن أي حل للمعادلة يكون على الصورة المطلوبة إذا كان x_1 , y_1 حلاً آخر للمعادلة فإن :

$$ax_1 + by_1 = c = ax_0 + by_0$$

ومنه

$$a\left(x_1-x_0\right)=-b\left(y_1-y_0\right).$$

وبما أن (a,b)=d فإننا نستطيع أن نجد عددين صحيحين أوليين نسبياً r,s بحيث أن b=sd, a=rd .
وبالتعويض في المعادلة الأخيرة وقسمة طرفيها على العدد d نجد :

$$r\left(x_1-x_0\right)=-s\left(y_1-y_0\right)$$

ومنه نجد $s\mid r\left(x_1-x_0\right)$.

وبما أن (r,s)=1 فإننا نستنتج $s\mid\left(x_1-x_0\right)$.

أي أن

$$x_1-x_0=ks$$

حيث أن $k\in Z$.

وبالتعويض في المعادلة (1) نحصل على المساواة

$$y_1-y_0=-kr$$

وبالتالي فإن :

$$x_1=x_0+ks=x_0+k\left(b/d\right)$$
$$y_1=y_0-kr=y_0-k\left(a/d\right)$$

حيث إن $k\in Z$. وبهذا يتم برهان المبرهنة .

مثال :

جد الحل العام للمعادلة الديوفنتية :

56x+72y=40 .

الحل :

لقد وجدنا في المثال التوضيحي السابق أن $y_0=-15\ ,\ x_0=20$ حل للمعادلة .

بإستخدام المبرهنة االسابقة نجد أن الحل العام :

X=20+(72/8)k=20+9k

y=-15-(56/8)k=-15-7k

حيث إن $k \in Z$.

مثال :

جد جميع الحلول الصحيحة الموجبة للمعادلة الديوفنتية :

54x+21y=906

الحل :

نستخدم خوارزمية إقليدس لإيجاد (54,21) فنجد على التوالي :

$$54 = 2 \times 21 + 12$$
$$21 = 1 \times 12 + 9$$
$$12 = 1 \times 9 + 3$$
$$9 = 3 \times 3 + 0$$

ومنه نجد أن 3=(54,21) يقسم العدد 906 .

وإذا وضعنا العدد 3 على صورة تركيب خطي للعددين 54,21 فنجد :

$$3 = 54 \times 2 + 21(-5) .$$

وبضرب طرفي المعادلة الأخيرة بالعدد 302 نحصل على المساواة :

906=54(604)+21(-1510) .

ومنه نستنتج أن $x_0 = 604 \ , \ y_0 = -1510$ حل للمعادلة .

وبالتالي فإن جميع الحلول يجب أن تكون على الصورة :

x=604+7k

y=-1510-18k

حيث إن $k \in Z$. ولإيجاد الحلول الموجبة نضع :

-1510-18k >0 , 604+7k >0 .

وبحل المتباينتين نجد أن :

$$k < -83\frac{8}{9} \quad , \quad k > -86\frac{2}{7}$$

أي أن

$$-86\frac{2}{7} < k < -83\frac{8}{9}$$

ومنه نجد أن k يأخذ القيم -84,-85,-86 .

وهذه القيم سوف تعطينا جميع الحلول الموجبة وهي : (2,38),(9,20),(16,2).

تمهيدية :

توجد أعداد صحيحة $y_1, y_2, ..., y_n$ بحيث إن :

$$(a_1, a_2, ..., a_n) = a_1y_1 + a_2y_2 + ... + a_ny_n$$

حيث إن $n \geq 2$.

مبرهنة :

يوجد حل للمعادلة الديوفنتية : $a_1x_1 + a_2x_2 + ... + a_kx_k = c$

حيث إن $k \geq 2$ إذا وفقط إذا كان $(a_1, a_2, ..., a_k) \mid c$.

البرهان :

ليكن $d = (a_1, a_2, ..., a_k)$. إذا كان $d \mid c$ فإنه يوجد $k \in Z$ بحيث إن $c=dr$. واستنادا إلى التمهيدية يوجد أعداد $y_1, y_2, ..., y_k$ بحيث إن :

$$a_1y_1 + a_2y_2 + ... + a_ky_k = d$$

. وبالتالي فإننا نستنتج أن

$$x_1 = ry_1 \quad , \quad x_2 = ry_2 \quad , ..., \quad x_k = ry_k$$

حل للمعادلة .

ولإثبات العكس ، نفرض أن $y_1, y_2, ..., y_k$ حل للمعادلة . بالتالي فإنه يحقق المعادلة ، أي أن :

$$a_1y_1 + a_2y_2 + ... + a_ky_k = c.$$

وبما أن : $d \mid a_i$ لكل i , $1 \le i \le k$ فإن $d \mid (a_1y_1 + a_2y_2 + ... + a_ky_k)$. $d \mid c$ أي أن .

ملحوظة:

إن إيجاد الحل العام للمعادلة الديوفنتية التي تحتوي على أكثر من مجهولين يتم بإختزالها إلى معادلة بمجهولين فقط . ولكننا هنا بدلاً من ذلك سنوجد الحل العام بطريقة أويلر (Eulers method).

وتعتمد هذه الطريقة على أن عمليتي الجمع والطرح على الأعداد الصحيحة مغلقتان . وسنبدأ بحالة المعادلة ذات المتغيرين أي : $a_1x_1 + a_2x_2 = c$ ، حيث إن $c \mid (a_1, a_2)$ لضمان وجود حل لهذه المعادلة .

مثال :

جد جميع حلول المعادلة :

$$-15x_1 + 21x_2 = 66.$$

الحل :

لاحظ أولا أن 66|3=(-15,21) ، وعليه فإن للمعادلة حلاً .

لأجل إيجاد جميع الحلول نتبع الخطوات التالية ولكن قبل ذلك نقسم طرفي المعادلة على القاسم المشترك الأعظم 3 ،

فنحصل على المعادلة المكافئة :

$$-5x_1 + 7x_2 = 22$$

(1) نختار المجهول الذي قيمة معامله المطلقة هي الصغرى . في هذه الحالة نختار x_1 لأن |-7|>|5| .

(2) نبقي الحد الذي فيه المجهول المختار في الخطوة (1) في الطرف الأيسر وننقل بقية الحدود إلى الطرف الأيمن فنحصل على المعادلة :

$$-5x_1 = 22 - 7x_2$$

(3) نقسم طرفي المعادلة في الخطوة (2) على -5 فنحصل على المعادلة :

$$x_1 = x_2 + \frac{2}{5}x_2 - 4 - \frac{2}{5}$$

لاحظ أن المقدار $\frac{2}{5}x_2 - \frac{2}{5}$ يجب أن يكون عدداً صحيحاً

كي يكون للمعادلة حل .

(4) نفرض أن $t_1 = \frac{2}{5}x_2 - \frac{2}{5}$. أي أن $2x_2 - 5t_1 = 2$.

(5) نطبق الخطوات (1) و(2)و(3) على المعادلة التي حصلنا عليها في الخطوة (4) فنحصل على :

$$x_2 = 2t_1 + \frac{1}{2}t_1 + 1 .$$

(6) نطبق الخطوة (4) على المعادلة في الخطوة (5) فنجعل $\frac{1}{2}t_1 = t_2$ أي أن

$$t_1 = 2t_2 .$$

نتوقف هنا لأن أصغر معامل لمتغير أصبح يساوي 1 وهو معامل t_1 .نعوض في المعادلة في الخطوة (5) لنحصل على

$$x_2 = 4t_2 + t_2 + 1 = 5t_2 + 1 .$$

ومن المعادلة في الخطوة (3) نحصل بالتعويض على :

$$x_1 = 5t_2 + 1 - 4 + 2t_2 = 7t_2 - 3$$

إنه ليس هناك قيد على t_2 ما دام أنه عدد صحيح ، كما أنه من الواضح أن جميع الحلول للمعادلة على الصورة أعلاه .

مثال :

جد جميع حلول المعادلة : $7x+3y-20z=23$.

الحل :

لاحظ أن 23|1=(7,3,20) .لذا فإن للمعادلة حلاً .

نتبع نفس خطوات الحل في المثال السابق.

(1) لاحظ أن أصغر قيمة مطلقة للمعاملات هي 3 معامل y فنكتب المعادلة المكافئة :

$$3y=23-7x+20z$$

(2) نقسم طرفي المعادلة على 3 فنحصل على المعادلة :

$$y = 7 + \frac{2}{3} - 2x - \frac{1}{3}x + 6z + \frac{2}{3}z$$

(3) نجعل الجزء الكسري يساوي t_1 : $t_1 = \frac{2}{3} - \frac{1}{3}x + \frac{2}{3}z$. أي أن

$$x + 3t_1 - 2z = 2 .$$

نتوقف عند هذه الخطوة لأن أصغر معامل هو 1 ومنها نجد أن :

$$x = 2 - 3t_1 + 2z$$

ومن المعادلة في الخطوة (2) نحصل على :

$$y = 7 + t_1 - 2x + 6z$$
$$= 3 + 7t_1 + 2z$$
$$z = t_2$$

حيث أن t_1, t_2 تأخذ جميع القيم الصحيحة في z .

مثال : جد قيمة (91,35,112).

الحل :

لاحظ أن (35,91,112) =(91,35,112)

$$91 = 2 \times 35 + 21$$
$$112 = 3 \times 35 + 7$$

إذن ،(7,21,35)= (35,21,7)= (35,91,112)

$$21 = 3 \times 7 + 0$$

$$35 = 5 \times 7 + 0$$

إذن ، 7=(7,0,0)=(7,21,35)

وعليه يكون 7=(91,35,112).

التمارين :

السؤال الأول :

بين ما إذا كان للمعادلة الديوفنتية حل وإذا كان للمعادلة حل فجد جميع الحلول :

2x+5y=11 (1).

60x+18y=97 (2)

السؤال الثاني :

جد جميع الحلول الصحيحة الموجبة للمعادلة : 62x+11y=788

السؤال الثالث :

جد جميع الحلول للمعادلة الديوفنتية : 15x+12y+30z=24

الخواص الأساسية للتطابقات

Basic Properties of Congruences

تعريف :

ليكن $a,b \in Z \quad , \quad n \in Z^+$. نقول إن a يطابق b قياس n

(a Congruences to b modulo n) ونرمز لذلك بالرمز :

$$a \equiv b \pmod{n}$$

إذا كان $n \mid (a-b)$. وإذا كان $n \nmid (a-b)$ فإننا نقول إن a لا يطابق b قياس n ونكتب

$$a \not\equiv b \pmod{n}.$$

مثال :

لاحظ أن $32 \equiv 5 \pmod 9$ وأن $3 \equiv -15 \pmod 9$ ولكن $22 \not\equiv 5 \pmod 9$.

مبرهنة :

إذا كان $a,b \in Z$ فإن $a \equiv b \pmod n$ إذا وفقط إذا وجد عدد صحيح k بحيث إن a=b+kn .

البرهان :

إذا كان $a \equiv b \pmod n$ فإن $n \mid (a-b)$ وبالتالي يوجد عدد صحيح k حيث إن a-b=kn ، أي أن

. a=b+kn

وبالعكس إذا فرضنا وجود عدد صحيح k حيث إن a=b+kn فإن a-b=k n ومنه نجد أن $n \mid (a-b)$ أي أن

$$. \ a \equiv b \pmod n$$

ملحوظة :

إن أي عدد صحيح a يطابق باقي قسمته على n قياس العدد n وذلك لأن :

$$0 \le r < n \quad , a=nq+r$$

حسب خوارزمية القسمة مما يجعل $a \equiv r \pmod n$.

مبرهنة :

إذا كان $a,b,c \in Z \quad , \quad n \in Z^+$ فإن :

(1) $. \ a \equiv a \pmod n$

(2) إذا كان $a \equiv b \pmod n$، فإن $b \equiv a \pmod n$.

(3) إذا كان $a \equiv b \pmod n$ ، وكان $b \equiv c \pmod n$ فإن $a \equiv c \pmod n$.

البرهان :

(1) بما أن $n \mid (a-a) = 0$ فإن $a \equiv a \pmod{n}$.

(2) بما أن $a \equiv b \pmod{n}$ فإننا نستطيع إيجاد عدد صحيح k بحيث أن :

a-b=kn ،

أي أن b-a=(-k)n .

ومنه نجد أن :

$$b \equiv a \pmod{n} .$$

(3) بما أن $a \equiv b \pmod{n}$ وأن $b \equiv c \pmod{n}$. فإنه يوجد عددان صحيحان k و j بحيث إن kn=a-b وإن jn=b-c .وبناء على ذلك نجد أن :

$$a\text{-}c = (a-b)+(b-c) = kn + jn = (k+j)n .$$

أي أن $n \mid (a-c)$.

ومنه نجد أن :

$$a \equiv c \pmod{n} .$$

مبرهنة :

إذا كانت d,c,b,a أعداد صحيحة وكان n عدد صحيح موجب بحيث إن: $a \equiv b \pmod{n}$ وإن $c \equiv d \pmod{n}$ فإن :

(1) $a+c \equiv b+d \pmod{n}$.

(2) $a\text{-}c \equiv b\text{-}d \pmod{n}$.

(3) $ac \equiv bd \pmod{n}$.

البرهان :

بما أن $a \equiv b \pmod{n}$ وأن $c \equiv d \pmod{n}$ فإنه يوجد عددان صحيحان k و j بحيث إن kn=a-b وإن jn=c-d.

للبرهنة على (1) نلاحظ أن :

$$(a+c)-(b+d)=(a-b)+(c-d)=kn+jn=(k+j)n.$$

ومنه نجد :

$a+c=(b+d)+(k+j)n$، أي أن :

$$a+c\equiv b+d\pmod{n}.$$

و للبرهنة على (2) نلاحظ أن :

$$(a-c)-(b-d)=(a-b)-(c-d)=kn-jn=(k-j)n.$$

ومنه نجد :

$$a-c=(b-d)+(k-j)n$$

،أي أن :

$$a-c\equiv b-d\pmod{n}.$$

و للبرهنة على (3) نلاحظ أن :

$$ac-bd=ac-bc+bc-bd=c(a-b)+b(c-d)=(ck+bj)n.$$

ومنه نجد :

$$ac=bd+(ck+bj)n$$

، أي أن :

$$ac\equiv bd\pmod{n}.$$

نتيجة :

إذا كان $n\in Z^{+}$ وكان $a_i\equiv b_i\pmod{n}$ لكل i حيث إن $1\le i\le k$ فإن :

$$a_1+a_2+\ldots+a_k\equiv b_1+b_2+\ldots+b_k\pmod{n}\quad(1).$$

$$a_1a_2...a_k \equiv b_1b_2...b_k \pmod{n} \quad (2)$$.

نتيجة :

إذا كان $a \equiv b \pmod{n}$ فإن $a^k \equiv b^k \pmod{n}$ وأن $ka \equiv kb \pmod{n}$ لكل $k \geq 1$.

ملحوظة :

عكس النتيجة السابقة غير صحيح أي أنه إذا كان $ka \equiv kb \pmod{n}$ حيث إن k أي عدد صحيح فإنه ليس بالضرورة أن تكون $a \equiv b \pmod{n}$ علاقة متحققة .

مثال توضيحي :

$7 \times 2 \equiv 4 \times 2 = 2 \pmod{6}$ ولكن $7 \not\equiv 4 \pmod{6}$.

مبرهنة :

إذا كان c,b,a أعداد صحيحة وكان n عدداً صحيحاً موجباً فإن :

$ac \equiv bc \pmod{n}$ ، إذا وفقط إذا كان $a \equiv b \pmod{n/d}$ حيث إن d=(c,n) .

البرهان :

الإتجاه الأول :

نفرض أولاً أن $ac \equiv bc \pmod{n}$ ،

فإنه يوجد عدد صحيح k بحيث

$$ac - bc = kn$$

ومنه نجد أن: c(a-b)=kn .

وبقسمة طرفي المعادلة الأخيرة على d نحصل على المعادلة :

.(c/d)(a-b)=k(n/d)

وبما أن d=(c,n) فإن

.1=(c/d,n/d)

و بإستخدام تمهيدية إقليدس نجد أن

$$(n/d)|(a-b)$$

أي أن

$$a \equiv b \pmod{n/d}.$$

برهان الإتجاه الثاني مباشر.

ملحوظة :

من المبرهنة السابقة نستنتج الحالتين التاليتين اللتين سكون لهما استخدامات كثيرة :

(1) إذا كانت c,b,a أعداد صحيحة وكان n عدداً صحيحاً موجباً بحيث إن $ac \equiv bc \pmod{n}$ وإن $(c,n)=1$ فإن $a \equiv b \pmod{n}$.

(2) إذا كان $ac \equiv bc \pmod{p}$ حيث إن p عدد أولي لا يقسم c فإن $a \equiv b \pmod{p}$

مبرهنة :

إذا كان $a \equiv b \pmod{n}$ وكان $m|n$ فإن $a \equiv b \pmod{m}$.

البرهان :

بما أن $a \equiv b \pmod{n}$ فإن $n|(a-b)$. وبما أن $m|n$ فإن $m|(a-b)$. وبالتالي فإن $a \equiv b \pmod{m}$.

تعريف :

ليكن a عدداً صحيحاً . نقول إن العدد b هو النظير الضربي للعدد a قياس n إذا كان $ab \equiv 1 \pmod{n}$.

ملحوظة :

النظير الضربي للعدد الصحيح هو المرادف لمقلوب العدد . وفي الحقيقة المتطابقة $ab \equiv 1 \pmod{n}$ هي المرادف للمعادلة $a.\frac{1}{a} = 1$. ونلاحظ أيضا أنه **ليس بالضرورة** أن يكون لكل عدد صحيح نظير ضربي قياس n . أما في حالة وجوده فهو وحيد وسنرمز له بالرمز a^{-1} .

مثال توضيحي :

لاحظ أن $2 \times 0 \equiv 0 \pmod{4}$ ، $2 \times 1 \equiv 2 \pmod{4}$ ، $2 \times 2 \equiv 0 \pmod{4}$ ، و $2 \times 3 \equiv 2 \pmod{4}$. إذن العدد 2 ليس له نظير ضربي قياس 4 .

مبرهنة :

يوجد للعدد الصحيح a نظيراً ضربياً قياس n إذا وفقط إذا كان (a,n)=1 .

البرهان :

لنفرض أولا أن (a,n)=1 .

عندها يوجد عددان صحيحان x,y بحيث إن :

$$ax+ny=1$$

، أي أن $ax-1=n(-y)$ وبالتالي فإن :

$$n|(ax-1)$$

ومنه نجد أن

$$ax \equiv 1 \pmod{n} .$$

وبالتالي فإن $x = a^{-1}$.

وللبرهان على العكس بفرض أن a^{-1} نظير ضربي للعدد a قياس n .

بناء على ذلك فإن

$$aa^{-1} \equiv 1 \pmod{n}$$

، ومنه $n \mid \left(aa^{-1} - 1\right)$.

أي أن

$$aa^{-1} - kn = 1$$

حيث إن $k \in Z$ ، وبالتالي فإن (a,n)=1 .

مثال :

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 وبالتالي فإن 17^{-1} قياس 25 موجود . ولإيجاد 17^{-1} نضع 1 كتركيب خطي للعددين 17,25 فنجد :

$$1 = 17 - 2 \times 8$$
$$\rightarrow 1 = 17 - 2(25 - 1 \times 17)$$
$$\rightarrow 1 = 3 \times 17 - 2 \times 25$$
$$\rightarrow 3 \times 17 - 1 = 2 \times 25$$
$$\rightarrow 25 \mid 3 \times 17 - 1$$
$$\rightarrow 3 \times 17 \equiv 1 (\mathrm{mod}\ 25)$$

. وبالتالي نجد أن 3 هو النظير الضربي للعدد 17 قياس 25 .

مبرهنة :

ليكن a,b عددين صحيحين ولتكن $n_1, n_2, \ldots, n_k$ أعداداً صحيحة موجبة . إذا كان $a \equiv b (\mathrm{mod}\ n_i)$ لكل i ، $1 \le i \le k$ فإن $a \equiv b (\mathrm{mod}\ n)$ حيث $n = [n_1, n_2, \ldots, n_k]$.

نتيجة :

إذا كان $a \equiv b \pmod{n_i}$ و $1 \le i \le k$ وكانت n_i أعداداً موجبة أولية نسبياً مثنى مثنى فإن :

$a \equiv b \pmod{n_1, n_2, ..., n_k}$.

نتيجة :

إذا كان $n = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$ هو تحليل n إلى قوى عوامله الأولية المختلفة وكان

$a \equiv b \pmod{p_i^{r_i}}$ فإن $a \equiv b \pmod{n}$.

مثال :

أثبت أن : $F_5 = 2^{32} + 1 \equiv 0 \pmod{641}$

الحل :

$$2^4 \equiv 16 \pmod{641}$$

$$2^8 \equiv 256 \pmod{641}$$

$$2^{16} \equiv 154 \pmod{641}$$

$$2^{32} \equiv 640 \pmod{641}$$

إذن

$$F_5 = 2^{32} + 1 \equiv 0 \pmod{641}$$

مثال :

جد باقي قسمة العدد $\sum_{k=1}^{1000} k!$ على 24 .

الحل :

لاحظ ان $4! = 24 \equiv 0 \pmod{24}$،

ومنه نجد أن: $k! \equiv 0 \pmod{24}$ لكل $k \ge 4$.

وبالتالي فإن :

$$\sum_{k=1}^{1000} k! = 1+2+6+\sum_{k=4}^{1000} k! = 9+0 \equiv 9 \pmod{24}$$

اختبارات خاصة لقابلية القسمة

(Divisibility Tests)

تمهيدية :

(1) $10^n \equiv 0 \pmod{2^k}$ لكل عدد صحيح موجب n بحيث إن $n \geq k$.

(2) $10^n \equiv 0 \pmod{5^k}$ لكل عدد صحيح موجب n بحيث إن $n \geq k$.

البرهان :

لاحظ أن $10 = 2 \times 5$ ومنه $10^k = 2^k \times 5^k$ لكل $k \geq 1$.

أي أن

$2^k \mid 10^k$ وأن $5^k \mid 10^k$ لكل $k \geq 1$.

ومنه نجد

$2^k \mid 10^n$ وأن $5^k \mid 10^n$ لكل $n \geq k$

وبالتالي فإن $10^n \equiv 0 \pmod{2^k}$ وإن

$$10^n \equiv 0 \pmod{5^k} \text{ لكل } 1 \leq k \leq n.$$

مبرهنة :

لنفرض أن العدد N له التمثيل العشري التالي :

$$N = (a_m a_{m-1} \ldots a_1 a_0)_{10}$$

، حيث إن $0 \leq a_k < 10$ لكل k ، $0 \leq k \leq m$،

ولنفرض أن $S=\sum_{k=0}^{m} a_k$ وأن $T=\sum_{k=0}^{m}(-1)^k a_k$ وأن $N_k=(a_{k-1}...a_1a_0)_{10}$.

عندئذ :

(1) $2^k \mid N$ إذا وفقط إذا كان $2^k \mid N_K$.

(2) $5^k \mid N$ إذا وفقط إذا كان $5^k \mid N_K$.

(3) $3 \mid N$ إذا وفقط إذا كان $3 \mid S$.

(4) $9 \mid N$ إذا وفقط إذا كان $9 \mid S$.

(5) $11 \mid N$ إذا وفقط إذا كان $11 \mid T$.

مثال :

جد أعلى قوة K للعدد 2 بحيث إن العدد N=4157892348 يقبل القسمة على 2^k .

الحل :

بما أن $4 \mid 48$ فإن $2^2 = 4 \mid N$. وبما أن $2^3 \nmid 348$ فإن $2^3 \nmid N$. إذن أعلى قوة هي K=2 .

مثال :

جد 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 :

اختبر قابيلة قسمة العدد N=894325734 على كل من 9 و 11 .

الحل :

بما أن :

S=4+3+7+5+2+3+4+9+8

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 .

مبرهنة :

ليكن r(n),q(n) خارج القسمة والباقي اللذان نحصل عليهما عند قسمة العدد n على العدد 1000 . فإذا كان c=7,11,13 فإن : c|n إذا وفقط إذا كان c|((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|n إذا وفقط إذا كان

$$c|(1001q(n)-n)$$

،أي إذا وفقط إذا كان (c|(q(n)-r(n) .

مثال :

اختبر قابيلة 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 :

$$14823358 = 1000\times14823 + 358$$

ومنه :

$$q(n_1)-r(n_1) = 14823 - 358 = 14465$$

وبقسمة العدد $n_2 = 14465$ على 1000 مرة أخرى نجد :

$$14465 = 1000 \times 14 + 465$$

ومنه :

$$q(n_2) - r(n_2) = 14 - 465 = -451$$

بما أن $11 \mid -451$ وأن $7 \nmid -451$ وأن $13 \nmid -451$ فإننا نجد $11 \mid n$ ولكن $7 \nmid n$ و $13 \nmid n$.

التمارين

السؤال الأول :

إذا كان $ab \equiv cd \pmod{n}$ وكان $b \equiv d \pmod{n}$ ، حيث إن (b,n)=1 فاثبت أن $a \equiv c \pmod{n}$.

السؤال الثاني :

اثبت أن علاقة التطابق : $6^n \equiv 1 + 5n \pmod{25}$ صحيحة لكل عدد صحيح موجب n .

السؤال الثالث:

إذا كان a عدد زوجي فأثبت أن $a^2 \equiv 0 \pmod{4}$. وإذا كان a عدد فردي فأثبت أن $a^2 \equiv 1 \pmod{4}$.

السؤال الرابع :

إذا كان $a^2 \equiv b^2 \pmod{p}$ حيث p عدد أولي ، فأثبت أن $a \equiv \pm b \pmod{p}$.

السؤال الخامس :

إذا كان $n \equiv 3 \pmod{4}$ فأثبت أنه لا يمكن كتابة n كحاصل جمع مربعين كاملين .

أنظمة الرواسب

Residue Systems

تمهيدية :

أي عدد صحيح يجب أن يكون مطابقاً لعدد واحد فقط من بين الأعداد 0,1,2,....,n-1 قياس n .

البرهان:

لنفرض أن x عدد صحيح . بإستخدام خوارزمية القسمة نستطيع كتابة العدد x على الصورة :

$$x = qn+r \quad , \quad 0 \le r \le n-1 .$$

ومن تعريف التطابق نجد أن : $x \equiv r \pmod{n}$.

ولو فرضنا أيضاً أن $x \equiv r' \pmod{n}$ حيث إن $0 \le r' \le n-1$ فإن

$$x = q'n+r' \quad , \quad q' \in Z .$$

أي أن : $x = q'n+r' = qn + r$.

وبإستخدام الوحدانية في خوارزمية القسمة نجد أن : $r = r'$.

تعريف :

نقول إن الأعداد $r_1, r_2, \ldots, r_n$ تمثل نظام رواسب تام (complete residue system) قياس n ، إذا كان كل عدد صحيح يطابق عدداً واحداً فقط من الأعداد $r_1, r_2, \ldots, r_n$ قياس n .

ملحوظات :

(1) لاحظ أن 0,1,2,....,n-1 نظام رواسب تام قياس n .

(2) لكي نبرهن أن n من الأعداد الصحيحة تمثل نظام رواسب تام قياس n ، يكفي أن نثبت أن كل عدد صحيح من الأعداد المعطاة يطابق عدداً واحداً فقط من الأعداد 0,1,2,....,n-1 قياس n

مثال :

أثبت أن المجموعة $\{0, \pm 1, \pm 2\}$ تمثل نظام رواسب تام قياس 5 .

الحل :

لاحظ أن :

$$-2 \equiv 3 \pmod 5 \quad , \quad -1 \equiv 4 \pmod 5$$
$$0 \equiv 0 \pmod 5 \quad , \quad 1 \equiv 1 \pmod 5$$
$$2 \equiv 2 \pmod 5$$

ولذا بإستخدام الملحوظة (2) نجد أن المجموعة هي نظام رواسب تام قياس 5 .

مبرهنة :

الأعداد $a_1, a_2, \ldots, a_n$ تمثل نظام رواسب تام قياس n إذا وفقط إذا كان $a_i \not\equiv a_j \pmod n$ لكل $i \neq j \quad , \quad j \leq n \quad , \quad 1 \leq i$.

نتيجة :

أي n من الأعداد الصحيحة المتتالية تمثل نظام رواسب تام قياس n .

البرهان :

لتكن b,b+1,b+2,....,b+n-1 أعداد متتالية عددها n .

ولنفرض أن

$$k \neq j \text{ ، } b + j \equiv b + k \pmod n$$

ومنه نجد أن

$$j \equiv k \pmod n$$

وهذا تناقض لأن 0,1,2,....,n-1 نظام رواسب تام .

نتيجة :

إذا كان $r_1, r_2, \ldots, r_n$ نظام رواسب تام قياس n وكان (a,n)=1 حيث إن $a \in Z$ فإن :

$ar_1 + b, ar_2 + b, \ldots, ar_n + b$ نظام رواسب تام قياس n لكل عدد صحيح b .

البرهان :

يكفي أن نبرهن على أن :

$ar_i + b \not\equiv ar_j + b \pmod{n}$ لكل $1 \le i \ne j \le n$.

لنفرض أن : $ar_i + b \equiv ar_j + b \pmod{n}$. عندئذ فإن

$$ar_i \equiv ar_j \pmod{n}$$

وبما أن (a,n)=1 فإن $r_i \equiv r_j \pmod{n}$ وهذا مستحيل إلا إذا كان i=j .

تعريف :

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 :

إذا كان n=12 ، وأخذنا {0,1,2,....,11} كنظام رواسب تام قياس 12 فإن

{1,5,7,11} تكوّن نظام رواسب مختزل قياس 12 .

وإذا أخذنا المجموعة $\{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, 6\}$ كنظام رواسب تام قياس 12 فعندئذ يكون

$\{\pm 1, \pm 5\}$ نظام رواسب مختزل قياس 12 .

تمهيدية :

ليكن $T = \{a_1, a_2, \ldots, a_k\}$ نظام رواسب مختزل قياس n .

إذا كان (a,n)=1 ، فإن

a يكون متطابقاً مع عدد واحد فقط من المجموعة T قياس n .

مبرهنة :

جميع أنظمة الرواسب المختزلة قياس n تحتوي على العدد نفسه من العناصر .

تعريف :

إذا كان عدد عدد صحيح موجب فإننا نعرف دالة أويلر (Eulers function) ونرمز لها بالرمز $\varphi(n)$ بأنها عدد العناصر التي يحتويها أي نظام رواسب مختزل قياس n .

ملحوظة :

من تعريف نظام رواسب المختزل قياس n نجد أن عناصره هي الأعداد الأولية نسبياً مع n والتي هي أقل من n أو تساويه ، ومن ثم فإنه يكون واضحاً لدينا أن $\varphi(n)$ هو عدد الأعداد الأولية نسبيا مع n والتي لا تزيد عن n .

مثال :

$\varphi(9)=6$ لأن عدد الأعداد الأولية نسبياً مع 9 والتي هي أقل من 9 أو تساويه هي :

. 1,2,4,5,7,8

أما $\varphi(12)=4$ لأن الأعداد الأولية نسبياً مع 12 والتي هي أقل من 12 أو تساويه هي :

. 1,5,7,11

ملاحظة :

$\varphi(n)\le n-1$ لكل عدد صحيح موجب n. وهذه المتباينه تصبح مساواة إذا كان العدد n أولي لأن الأعداد التي هي أقل من العدد الأولي p أو تساويه جميعها أولية نسبياً مع p وعددها p-1 .

مبرهنة :

لنفرض أن

$$S=\{a_1,a_2,...,a_n\}$$

نظام رواسب تام قياس n ولنفرض أن المجموعة الجزئية $T\subseteq S$ ،

$$T=\{r_1,r_{2,}....,r_{\varphi(n)}\}$$

هي نظام رواسب مختزل قياس n .

إذا كان (a,n)=1 ، $a \in Z^+$ فإن :

$$T' = \left\{ ar_1, ar_2, ..., ar_{\varphi(n)} \right\}$$

نظام رواسب مختزل قياس n .

التمارين

السؤال الأول :

جد نظام رواسب تام قياس 13 جميع عناصره قوى للعدد 3 ؟

السؤال الثاني :

جد نظام رواسب مختزل قياس 13 جميع عناصره قوى للعدد 3 ؟

التطابقات الخطية

Linear Congruences

مبرهنة :

إذا كان (a,n)=d ، فإن للتطابق الخطي $ax \equiv b \pmod{n}$ حلاً إذا وإذا فقط كان d|b . وإذا كان d|b وكان x_0 حلاً للتطابق فإن جميع الحلول غير المتطابقة قياس n هي :

$$0 \le k \le d-1 \quad , \quad x = x_0 + \frac{kn}{d}$$

البرهان :

بما أن التطابق

$$ax \equiv b \pmod{n}$$

يكافئ المعادلة الديوفنتية الخطية ax-ny=b .

فإننا نجد أن للمعادلة الأخيرة حلاً إذا وفقط إذا كان d|b (من مبرهنة سابقة). وبالتالي فإن للمعادلة $ax \equiv b \pmod{n}$ حلاً إذا وفقط إذا كان d|b .

ونجد أنه إذا كان x_0, y_0 حلاً للمعادلة الديوفنتية ax-ny=b فإن جميع الحلول تكتب على الصورة :

$$x = x_0 + \frac{n}{d}k \quad , \quad y = y_0 + \frac{a}{d}k$$ حيث $k \in Z$.

نأخذ من بين جميع الأعداد الصحيحة التي تحقق المعادلة الأولى الأعداد التي تكون قيم k عندها 0,1,2,....,d-1 وهذه القيم هي :

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, ..., x_0 + \frac{(d-1)n}{d}$$

نبرهن الآن أن جميع هذه الأعداد غير متطابقة قياس n وأن أي حل آخر يجب أن يكون متطابقاً مع أحد هذه الأعداد قياس n .

نفرض أن (لغرض التناقض)

$$x_0 + \frac{n}{d}k_1 \equiv x_0 + \frac{n}{d}k_2 \pmod{n}$$

حيث أن $0 \le k_1 < k_2 \le d-1$. ومنه نجد أن

$$\frac{n}{d}k_1 \equiv \frac{n}{d}k_2 \pmod{n} .$$

وبما أن $\left(\frac{n}{d}, n\right) = \frac{n}{d}$ نجد أن :

$$k_1 \equiv k_2 \pmod{n}$$

أي أن $d \mid (k_2 - k_1)$ وهذا مستحيل لأن $0 < k_2 - k_1 < d$.

نفرض الآن أن $x_0 + \frac{n}{d}k$ حل للتطابق . بإستخدام خوارزمية القسمة نستطيع كتابة k على الصورة :

$$k = qd + r \quad , \quad 0 \le r \le d-1$$

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 .

ملحوظة :

لاحظ أنه لو كان (a,n)=1 فإنه يوجد حل وحيد للتطابق

$ax \equiv b \pmod{n}$ وهو

$$x \equiv a^{-1}b \pmod{n} .$$

مثال :

جد جميع الحلول غير المتطابقة قياس 15 للمعادلة :

$$27x \equiv 3 \pmod{15} .$$

الحل :

بما أن 3|3=(27,15) فإن للمعادلة 3 حلول غير متطابقة قياس 15 . ولإيجاد أحد هذه الحلول إما أن نكتب المعادلة الخطية المكافئة لها ونستخدم خوارزمية إقليدس لإيجاد أحد الحلول ،

أو نستخدم التجريب بالتعويض عن x بعناصر أحد أنظمة الرواسب التامة قياس 15 .

بإستخدام نظام الرواسب التام {0,1,...,14} نجد أن العدد 4 يحقق المعادلة لأن

$$27 \times 4 = 108 \equiv 3 \pmod{15} .$$

وبالتالي نجد أن جميع الحلول غير المتطابقة قياس 15 :

K=0,1,2 , x=4+5k

مثال :

استخدم التطابق لحل المعادلة : 7x+5y=3 .

الحل :

المعادلة : 7x+5y=3 تكافئ $7x \equiv 3 \pmod 5$.

أي أن

$$2x \equiv 3 \pmod 5.$$

بما أن 3|1=(2,5) فإن للتطابق حلاً وحيداً وهو :

$$x \equiv -1 \pmod 5.$$

وهذا يعني أن : x=-1+5k .

وبالتعويض في المعادلة الأصلية نجد أن : y=2-7k حيث إن $k \in Z$.

مثال:

جد جميع الحلول للتطابق :

$$36x \equiv 8 \pmod{102}.$$

الحل :

بما أن $8 \not| 6 = (36,102)$.

بالتالي فإن التطابق المعطى ليس له حل .

التمارين

السؤال الأول :

جد جميع الحلول لكل من المتطابقات التالية:

$$(1)\ 65x \equiv 15 \pmod{29}$$
$$(2) 128x \equiv 833 \pmod{1001}$$
$$(3) 66x \equiv 121 \pmod{737}$$

السؤال الثاني:

إذا كان p عدد أولي فردي وكان k عدد صحيح موجب فأثبت أن للمعادلة $x^2 \equiv 1 \pmod{p^k}$ حلين غير متطابقين .

أنظمة التطابقات الخطية بمتغير واحد

Systems of Linear Congruences in one Variable

تمهيدية :

ليكن لدينا النظام التالي :

$$\left.\begin{aligned} a_1x &\equiv c_1 \pmod{m_1} \\ a_2x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ a_kx &\equiv c_k \pmod{m_k} \end{aligned}\right\} \quad .....(1)$$

وليكن $(a_i, m_i) = d_i$ ، $1 \le i \le k$ وليكن x_i حلاً للتطابق $a_ix \equiv c_i \pmod{m_i}$ و $1 \le i \le k$.

عندئذ x حل للنظام (1) إذا وفقط إذا كان x حلاً للنظام :

$$x \equiv x_1 \left(\mod \frac{m_1}{d_1}\right)$$

$$x \equiv x_2 \left(\mod \frac{m_2}{d_2}\right)$$

$$\vdots$$

$$x \equiv x_k \left(\mod \frac{m_k}{d_k}\right)$$

ملحوظة:

إذا كانت إحدى التطابقات في نظام ما من التطابقات غير قابلة للحل فإن النظام غير قابل للحل ، ولكن العكس غير صحيح .

مثال توضيحي :

إذا كان لدينا النظام :

$$\left.\begin{aligned} 6x &\equiv 4 \pmod 8 \\ 9x &\equiv 3 \pmod{12} \end{aligned}\right\} \ldots(1)$$

بما أن $4|2=(8,6)$ وأن $3|3=(9,12)$ فإنه يوجد حل لكل تطابق من التطابقين . ومنه نجد أن :

$$x \equiv 2 \pmod 4$$

حل للتطابق الأول وأن $x \equiv 3 \pmod 4$ حل للتطابق الثاني . وهذا تناقض إذن ليس له حل.

وبالتالي فإنه يكون للنظام (1) حل إذا وفقط إذا كان للنظام :

$$\left.\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 3 \pmod 4 \end{aligned}\right\} \quad \ldots(2)$$

حل . ولكن من الواضح أنه ليس هناك حل للنظام (2) . وعليه فإنه لا يوجد حل للنظام (1) .

المبرهنة التالية تعرف بمبرهنة الباقي الصينية

(the Chinese remainder theorem) وهي تضمن لنا وجود حل لبعض الأنظمة .

مبرهنة :

إذا كانت الأعداد $m_1, m_2, \ldots, m_k$ أعداد أولية نسبيا مثنى مثنى فإنه يوجد للنظام :

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}$$

حل وحيد قياس العدد $M = m_1 m_2 \ldots m_k$.

البرهان :

لإيجاد حل للنظام نفرض أن :

$$M_r = \frac{M}{m_r} = m_1 m_2 \dots m_{r-1} m_{r+1} \dots m_k$$

لكل $r = 1, 2, \dots, k$.

بما أن $(m_r, m_s) = 1$ عندما $r \neq s$ فإننا نجد أن $(M_r, m_r) = 1$.ومنه نجد أن للعدد M_r نظيرا ضربيا قياس m_r وليكن y_r ، وهذا يعني أن $M_r y_r \equiv 1 (\text{mod } m_r)$. لنبرهن الآن على أن العدد x حيث أن :

$$x = c_1 M_1 y_1 + c_2 M_2 y_2 + \dots + c_k M_k y_k$$

هو حل للنظام ، للبرهنة على ذلك يجب أن نثبت أن : $x \equiv c_r (\text{mod } m_r)$ لكل r حيث إن $1 \leq r \leq k$.

بما أن $m_r \mid M_s$ عندما $r \neq s$ فإن : $M_s \equiv 0 (\text{mod } m_r)$ ومنه :

$$x \equiv c_r M_r y_r \equiv c_r (\text{mod } m_r)$$

ولبرهان الوحدانية نفرض أن x_0, x_1 حلان للنظام . من تعريف الحل نجد أن

$x_0 \equiv x_1 \equiv c_r (\text{mod } m_r)$ لكل r ، $1 \leq r \leq k$.

ومنه نجد أن $m_r \mid (x_0 - x_1)$.

وبالتالي نجد أن $M \mid (x_0 - x_1)$ أي أن

$$x_0 \equiv x_1 (\text{mod } M).$$

مثال :

جد أصغر عدد صحيح موجب بحيث إذا قسم على 3 بقي 1 وإذا قسم على 4 بقي 2 وإذا قسم على 5 بقي 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

$$M_3 = 12 \quad , \quad M_2 = 15 \quad , \quad M_1 = 20 \quad , \quad M = (3)(4)(5) = 60$$

لإيجاد y_1, y_2, y_3 يجب أن نجد حلاً لكل من المعادلات :

$$12y_3 \equiv 1(\text{mod } 5) \quad , \quad 5y_2 \equiv 1(\text{mod } 4) \quad , \quad 20y_1 \equiv 1(\text{mod } 3)$$

من التطابق الأول نجد أن $y_1 = 2$

ومن الثاني $y_2 = 3$

ومن التطابق الثالث $y_3 = 3$.

وبتطبيق المبرهنة نجد أن :

$$x \equiv (1)(20)(2) + (2)(15)(3) + (3)(12)(3) \equiv 238 \equiv 58(\text{mod } 60)$$

ملحوظة :

يمكن حل المثال بطريقة أخرى وهي :

من التطابق (1) يوجد k_1 بحيث إن $x = 1 + 3k_1$.

بالتعويض في (2) 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 (3) نحصل على :

$$10 + 12k_2 \equiv 3 \pmod 5$$

أي أن $2k_1 \equiv 3 \pmod 5$.

وبالضرب في 3 نحصل على

$$k_2 \equiv 9 \equiv 4 \pmod 5.$$

إذن يوجد k_3 بحيث إن $k_2 = 4 + 5k_3$.

ومنه فإن :

$$x = 10 + 12(4 + 5k_3) = 58 + 60k_3 \equiv 58 \pmod{60}$$

إذن العدد المطلوب هو 58.

مثال :

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 :

$$M_1 = 35 \quad , \quad M_2 = 28 \quad , \quad M_3 = 20 .$$

بحل المعادلة $35y_1 \equiv 1 \pmod 4$ نجد أن : $y_1 = 3$.

ومن المعادلة $28y_2 \equiv 1 \pmod 5$ نجد أن : $y_2 = 2$.

ومن المعادلة $20y_3 \equiv 1 \pmod 7$ نجد أن $y_3 = 6$.

مما سبق نجد أن :

$$x \equiv (35)(3)(3) + (28)(2)(4) + (20)(6)(3) \equiv 899 \equiv 59 \pmod{140}$$

تعريف :

لنفرض أن لدينا النظام التالي :

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv c_k \pmod{m_k}$$

ولنفرض أن $(m_i, m_j) = d_{ij}$ لكل $1 \le i \ne j \le k$.

نقول إن النظام منسجم (compatible system) إذا كان :

$c_i \equiv c_j \pmod{d_{ij}}$ لكل $1 \le i \ne j \le k$.

مثال :

النظام

$$x \equiv 5 \pmod{12}$$
$$x \equiv 7 \pmod{9}$$

غير منسجم لأن 3=(12,9) ولكن $5 \not\equiv 7 \pmod{3}$.

أما النظام

$$x \equiv 4 \pmod{21}$$
$$x \equiv 18 \pmod{35}$$
$$x \equiv 13 \pmod{15}$$

فهو نظام منسجم لأن :

$$4 \equiv 18 \pmod{7} \quad , \quad (21,35) = 7$$
$$4 \equiv 13 \pmod{3} \quad , \quad (21,15) = 3$$
$$18 \equiv 13 \pmod{5} \quad , \quad (35,15) = 5$$

ملحوظة :

لاحظ أن انسجام أي نظام من التطابقات يعتمد على إنسجام كل زوج من التطابقات في النظام .

إن انسجام نظام التطابقات هو شرط لازم وكافي لوجود حل للنظام .

مبرهنة :

إذا وجد حل للنظام :

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv c_k \pmod{m_k}$$

فيجب أن يكون هذا النظام منسجماً .

البرهان:

لنفرض أن x حل للنظام . ولنفرض أن

$$\left(m_i, m_j\right) = d_{ij} \text{ لكل } 1 \le i \ne j \le k .$$

بما أن x حل للنظام فإننا نجد :

$$x \equiv c_i \left(\text{mod } m_i\right) \text{ لكل } 1 \le i \le k .$$

وبما أن $d_{ij} \mid m_i$ فإننا نجد أن $x \equiv c_i \left(\text{mod } d_{ij}\right)$.

وبالطريقة نفسها نستطيع أن نبرهن على أن $x \equiv c_j \left(\text{mod } d_{ij}\right)$. وبالتالي فإن $c_i \equiv x \equiv c_j \left(\text{mod } d_{ij}\right)$، أي أن النظام منسجم .

مثال :

أثبت أنه لا يوجد حل لنظام التطابقات :

$$x \equiv 4\left(\text{mod } 21\right)$$
$$x \equiv 18\left(\text{mod } 35\right)$$
$$x \equiv 8\left(\text{mod } 15\right)$$

الحل :

النظام غير منسجم لأن (21,15)=3 ولكن $4 \not\equiv 8\left(\text{mod } 3\right)$. وبالتالي فإنه ليس هناك حل للنظام .

مبرهنة :

ليكن $m_1, m_2, \ldots, m_k \in Z^+$ وليكن $c_1, c_2, \ldots, c_k \in Z$ و ليكن

$$x \equiv c_1 \left(\text{mod } m_1\right)$$
$$x \equiv c_2 \left(\text{mod } m_2\right)$$
$$\vdots$$
$$x \equiv c_k \left(\text{mod } m_k\right)$$

إذا كان منسجماً فإنه يوجد له حل وحيد قياس

$$m = \left[m_1, m_2, \ldots, m_k\right] .$$

مثال :

حل نظام التطابقات :

$$x \equiv 11 \pmod{36}$$
$$x \equiv 7 \pmod{40}$$
$$x \equiv 32 \pmod{75}$$

الحل :

لاحظ أولاً أن

$$m_3 = 75 \quad , \quad m_2 = 40 \quad , \quad m_1 = 36$$

، وأن

$$d_{1\,2} = (36,40) = 4 \ , d_{1\,3} = (36,75) = 3 \ , d_{2\,3} = (40,75) = 5$$

وأن

$$c_1 - c_2 = 4 \quad , \quad c_1 - c_3 = -12 \quad , \quad c_2 - c_3 = -25 .$$

ولذا فإن $d_{ij} \mid (c_i - c_j)$. ومن ثم فإن للنظام حل وحيد قياس

$$m = [36,40,75] = 1800 = 2^3 \times 3^2 \times 5^2 .$$

ولإيجاد هذا الحل ، لاحظ أن النظام يكافئ :

$$x \equiv 11 \pmod{2^2}$$
$$x \equiv 11 \pmod{3^2}$$
$$x \equiv 7 \pmod{2^3}$$
$$x \equiv 7 \pmod{5}$$
$$x \equiv 32 \pmod{3}$$
$$x \equiv 32 \pmod{5^2}$$

وهذا النظام يكافئ بدوره النظام :

$$x \equiv 7\left(\mathrm{mod}\ 2^3\right) \equiv 7(\mathrm{mod}\ 8)$$

$$x \equiv 11\left(\mathrm{mod}\ 3^2\right) \equiv 2(\mathrm{mod}\ 9)$$

$$x \equiv 32\left(\mathrm{mod}\ 5^2\right) \equiv 7(\mathrm{mod}\ 25)$$

وبحل هذا النظام بإستخدام مبرهنة الباقي الصينية نجد أن الحل الوحيد هو

$$.x \equiv 407(\mathrm{mod}\ 1800)$$

ملحوظة :

لاحظ أنه بالإمكان حل النظام (بعد التأكد من من إنسجامه) بحل كل من التطابقات على حده والتعويض المتتالي في التطابقات .

حل المثال السابق بطريقة التعويض المتتالي :

من التطابق الأول نجد أن

$$.k_1 \in Z \text{ حيث } x = 11 + 36k_1$$

وبالتعويض في التطابق الثاني والإختصار نحصل على

$$. k_1 \equiv 1(\mathrm{mod}\ 40)$$

$$. k_2 \in Z \text{ حيث } k_1 = 1 + 40k_2 \text{ أي أن}$$

ولذا فإن

$$.x = 11 + 36k_1 = 47 + 1440k_2$$

وبالتعويض عن x في التطابق الثالث والإختصار نجد أن

$$.k_2 \equiv -1 \equiv 74(\mathrm{mod}\ 75)$$

$$.k_3 \in Z \text{ حيث } k_2 = 74 + 75k_3 \text{ أي أن}$$

وبالتالي فإن حل النظام هو :

$$x = 47 + 1440(74 + 75k_3) = 106607 + 108000k_3$$

$$.x \equiv 106607(\mathrm{mod}\ 108000) \text{ أي أن}$$

ومنه فإن $x \equiv 106607 \equiv 407 \pmod{1800}$.

التمارين

السؤال الأول :

حل نظام التطابقات المعطى :

$$(1)\ x \equiv 5 \pmod{11}\ ,\ x \equiv 14 \pmod{29}\ ,\ x \equiv 15 \pmod{31}$$
$$(2)\ 3x \equiv 6 \pmod{12}\ ,\ 2x \equiv 5 \pmod{7}\ ,\ 3x \equiv 1 \pmod{5}$$
$$(3)\ x \equiv 2 \pmod{9}\ ,\ x \equiv 8 \pmod{15}\ ,\ x \equiv 10 \pmod{25}$$

السؤال الثاني :

جد أصغر عدد صحيح موجب بحيث يكون باقي قسمته على كل من 17,13,10 هو 15,11,3 .

بعض التطابقات الخاصة

Special Congruences

مبرهنة أويلر :

ليكن n عدداً صحيحا موجباً . إذا كان (a,n)=1 فإن

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

حيث إن $\varphi(n)$ ترمز لدالة أويلر.

البرهان :

لنفرض أن الأعداد $r_1, r_2, \ldots, r_{\varphi(n)}$ نظام رواسب مختزل قياس n . بما أن (a,n)=1 فإننا نجد أن:

$ar_1, ar_2, \ldots, ar_{\varphi(n)}$ نظام رواسب مختزل قياس n .

وبالتالي نجد أن كل r_i يجب أن يطابق عدداً وحيداً ar_j قياس n . وعليه فإن :

$$(ar_1)(ar_2)\ldots(ar_{\varphi(n)}) \equiv r_1, r_2, \ldots, r_{\varphi(n)} \pmod{n}$$

أي أن :

$$a^{\varphi(n)} r_1, r_2, \ldots, r_{\varphi(n)} \equiv r_1, r_2, \ldots, r_{\varphi(n)} \pmod{n}$$

وبما أن : $(r_1, r_2, \ldots, r_{\varphi(n)}, n) = 1$ فإن :

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

ملحوظة :

لاحظ أن عكس مبرهنة أويلر صحيح أيضاً وذلك لأنه لو كان

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

فإنه يوجد $k \in Z$ حيث $a^{\varphi(n)} + nk = 1$.

ومنه فإن $aa^{\varphi(n)-1} + nk = 1$ وبالتالي فإن (a,n)=1 .

نتيجة :(مبرهنة فيرما الصغرى)

إذا كان p عدداً أولياً حيث إن $p \nmid a$ فإن :

$$a^{p-1} \equiv 1 \pmod{p}.$$

البرهان :

بما أن $p \nmid a$ فإن (a,p)=1 وأن $\varphi(p) = p - 1$.وبالتالي نجد بإستخدام مبرهنة أويلر أن :

$$a^{p-1} \equiv 1 \pmod{p}.$$

نتيجة :

إذا كان p عدداً أولياً فإن $a^p \equiv a \pmod{p}$ لكل عدد صحيح a .

البرهان :

إذا كان $p|a$ ، فإن $a \equiv 0 \pmod{p}$ ومنه نجد أن :

$$a^p \equiv 0 \pmod{p}.$$

أي أن $a^p \equiv a \pmod{p}$.

أما إذا كان $p \nmid a$، فبإستخدام النتيجة السابقة نجد أن

$$a^{p-1} \equiv 1 \pmod{p}.$$

أي أن $a^p \equiv a \pmod{p}$.

نتيجة :

إذا كان (a,n)=1 فإن $a^{\varphi(n)-1}$ نظير ضربي للعدد a قياس n .

البرهان :

بإستخدام مبرهنة أويلر نجد أن :

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

وبالتالي فإن :

$$aa^{\varphi(n)-1} \equiv 1 \pmod{n}.$$

نتيجة :

إذا كان (a,n)=1 فإن الحل الوحيد للتطابق :

$$ax \equiv b \pmod{n}$$

هو $x \equiv a^{\varphi(n)-1}b \pmod{n}$.

البرهان :

بما أن $ax \equiv b \pmod{n}$ وأن (a,n)=1 فإن الحل الوحيد للتطابق هو

$$x \equiv a^{-1}b \pmod{n}.$$

ولكن بإستخدام النتيجة السابقة نعلم أن

$$a^{-1} \equiv a^{\varphi(n)-1} \pmod{n}.$$

وبالتالي فإن $x \equiv a^{\varphi(n)-1} b \pmod{n}$.

مثال : جد 2^{-1} قياس 9 .

الحل :

بما أن (2,9)=1 فإن $2^{\varphi(9)-1}$ هو نظير العدد الضربي قياس 9 .

لكن $\varphi(9)-1=5$ وعليه فإن :

$$2^5 \equiv 32 \equiv 5 \pmod{9} .$$

وبالتالي فإن 5 هو النظير الضربي للعدد 2 قياس 9 .

مثال :

حل التطابق : $3x \equiv 7 \pmod{10}$.

الحل :

بما أن (3,10)=1 فإن :

$$x \equiv 3^{\varphi(10)-1} \times 7 \equiv 3^3 \times 7 \equiv 9 \pmod{10} .$$

مثال : جد باقي قسمة العدد 5^{38} على العدد 11 .

الحل :

بإستخدام مبرهنة فيرما الصغرى نجد أن :

$$5^{10} \equiv 1 \pmod{11}$$

ومنه نجد أن :

$$5^{38} \equiv \left(5^{10}\right)^3 \left(5^2\right)^4 \equiv (1)(3)^4 \equiv 81 \equiv 4 \pmod{11}$$

إذن باقي القسمة هو العدد 4 .

مثال : جد مرتبتي الآحاد والعشرات للعدد 3^{256} .

الحل :

نجد باقي قسمة العدد 3^{256} على العدد 100 .

بما أن (3,100) =1 وأن $\varphi(100)=40$

فإننا نجد بإستخدام مبرهنة أويلر أن :

$$3^{40}\equiv 1(\mathrm{mod}\ 100)$$

. ومنه نجد :

$$3^{256}=(3^{40})^{6}(3^{16})\equiv(1)(3^{16})=(81)^{4}\equiv(-19)^{4}\equiv(61)^{2}\equiv 21(\mathrm{mod}\ 100)$$

أي أن باقي القسمة هو 21 .

إذن ، مرتبة الآحاد هى 1 والعشرات هي 2 .

مثال : استخدم مبرهنة فيرما الصغرى لإثبات أن العدد 117 مؤلف .

الحل :

نريد أن نجد عدداً صحيحاً a بحيث يكون :

$$.a^{117}\not\equiv a(\mathrm{mod}\ 117)$$

إذا اخترنا a=2 فإن :

$$2^{117}=(2^{7})^{16}(2^{5})\equiv 11^{16}\times 2^{5}\equiv 121^{8}\times 2^{5}\equiv 4^{8}\times 2^{5}\equiv 2^{21}\equiv(2^{7})^{3}$$
$$\equiv 11^{3}\equiv 4\times 11\equiv 44\not\equiv 2(\mathrm{mod}\ 117)$$

وبالتالي فإن 117 مؤلف .

تعريف :

ليكن n,b عددين صحيحين موجبين بحيث يكون n مؤلفاً .

نقول إن العدد n عدد شبه أولي (pseudoprime) للأساس b إذا كان

$$.b^{n}\equiv b(\mathrm{mod}\ n)$$

مثال : أثبت أن العدد 341 شبه أولي للأساس 2 .

الحل :

لاحظ أن 341=31×11 . بإستخدام مبرهنة فيرما الصغرى نجد أن :

$$2^{10} \equiv 1(\mathrm{mod}\ 11) \text{ وأن } 2^{30} \equiv 1(\mathrm{mod}\ 31).$$

لدينا الآن :

$$2^{340} = \left(2^{10}\right)^{34} \equiv 1(\mathrm{mod}\ 11)$$

وأيضاً :

$$2^{340} = \left(2^{30}\right)^{11} 2^{10} \equiv (1)(1) \equiv 1(\mathrm{mod}\ 31)$$

مما سبق نجد أن :

$$2^{340} = 1(\mathrm{mod}\ 11\times 31) \equiv 1(\mathrm{mod}\ 341)$$

أي أن :

$$2^{340} = 2(\mathrm{mod}\ 341)$$

ملاحظة :

عكس مبرهنة فيرما الصغرى غير صحيح .

تعريف :

نسمي العدد المؤلف n بعدد كارمايكل (Carmichael number) إذا كان

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

لكل عدد صحيح a حيث إن (a,n)=1.

مثال : أثبت أن العدد 561 عدد كارمايكل .

الحل :

لاحظ أن $561 = 3\times 11\times 17$. لنفرض أن $a \in Z$ وأن (a,561)=1 ومنه نجد :

(a,3)=(a,11)=(a,17)=1 .

و بإستخدام مبرهنة فيرما الصغرى نجد أن :

$$a^{10} \equiv 1(\text{mod } 11), a^{2} \equiv 1(\text{mod } 3)$$

وأن

$$.a^{16} \equiv 1(\text{mod } 17)$$

لدينا الآن :

$$a^{560} \equiv \left(a^{10}\right)^{56} \equiv 1(\text{mod } 11)$$

$$a^{560} \equiv \left(a^{16}\right)^{35} \equiv 1(\text{mod } 17)$$

$$a^{560} \equiv \left(a^{2}\right)^{280} \equiv 1(\text{mod } 3)$$

وبالتالي فإن :

$$.a^{560} \equiv 1(\text{mod } 561)$$

مبرهنة ويلسن: (Wilsons theorem)

إذا كان p عدداً أولياً فإن

$$.(p-1)! \equiv -1(\text{mod } p)$$

البرهان :

إذا كان p=2 فإن

$$.(p-1)! \equiv 1 \equiv -1(\text{mod } 2)$$

لنفرض إذن أن p>2 . بما أن (a,p)=1 لكل a ،

$1 \le a \le p-1$ فإنه يوجد نظير ضربي a^{-1} للعدد a قياس p بحيث إن :

$$.1 \le a^{-1} \le p-1$$

ولكن من السهل أن نرى أن $a^{2} \equiv 1(\text{mod } p)$ إذا وفقط إذا كان $a \equiv \pm 1(\text{mod } p)$.

إذن ، نستطيع أن نستنتج أن:

الأعداد التي تقل عن p وتساوي نظيرها الضربي قياس p هي : 1 , p-1 .

وعليه يكون بإستطاعتنا تكوين

$\frac{p-3}{2}$ زوجاً من الأعداد بين 2 و p-2

بحيث يكون حاصل ضرب كل زوج منها يطابق 1 قياس p . ومنه نجد أن :

$$2\times 3\times \ldots \times (p-3)(p-2)\equiv 1(\mathrm{mod}\ p)$$

ولذا فإن :

$$1\times 2\times 3\times \ldots \times (p-3)(p-2)(p-1)\equiv 1\times (p-1)\equiv -1(\mathrm{mod}\ p)$$

أي أن :

$$(p-1)!\equiv -1(\mathrm{mod}\ p).$$

مبرهنة (عكس مبرهنة ويلسن):

إذا كان $n\in Z^{+}$ وكان $(n-1)!\equiv -1(\mathrm{mod}\ n)$ فإن n عدد أولي .

البرهان :

لنفرض أن n عدد مؤلف . وعليه فإن

$1<a,b<n$ ، $n=ab$.

بما أن a<n فإن a|(n-1)!.

وبما أن

$$(n-1)!\equiv -1(\mathrm{mod}\ n)$$

فإن n|[(n-1)!+1].

ومنه نجد أن : a|[(n-1)!+1] .

وبالتالي فإننا نخلص إلى أن a|1 وهذا مستحيل .

ملحوظة :

إن مبرهنة ويلسن وعكسها تزودنا بإختبار لأولية العدد n . لكن هذا الأختبار عديم الفائدة من الناحية العلمية وذلك لكبر العدد

(n-1)! خصوصاً إذا كان العدد n كبيراً.

بعض التطبيقات المهمة على مبرهنتي فيرما الصغرى وويلسن .

مبرهنة :

إذا كان p عدداً أولياً فردياً فإنه 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 $x = \left(\frac{p-1}{2}\right)!$

حل للتطابق .

البرهان :

لنفرض أولاً أنه يوجد عدد x بحيث يكون : $x^2 \equiv -1 \pmod{p}$. لدينا الآن :

$$x^{p-1} = \left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

ومن ناحية أخرى لدينا من مبرهنة فيرما الصغرى :

$$x^{p-1} \equiv 1 \pmod{p}$$

مما سبق نستنتج أن :

$$. 1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

أي أن : $p \mid 1-(-1)^{\frac{p-1}{2}}$.

ولكن العدد $1-(-1)^{\frac{p-1}{2}}$ إما يساوي صفراً أو يساوي 2.

إذا كان لا يساوي صفراً فإن $p|2$ وهذا مستحيل لأن p فردي . وبالتالي فإن

$$1-(-1)^{\frac{p-1}{2}}=0$$

وهذا يلزم أن يكون $\frac{p-1}{2}$ زوجياً .

أي أن

$$\frac{p-1}{2}=2k \quad \text{و} \quad k \in Z .$$

وبالتالي فإن $p \equiv 1 \pmod 4$.

وللبرهنة على العكس:

لنفرض أن $p \equiv 1 \pmod 4$.

لدينا الآن :

$$\begin{aligned}(p-1)! &= \left(1\times 2\times \ldots \times \frac{p-1}{2}\right).\left(\frac{p+1}{2}\ldots(p-2)(p-1)\right) \\ &\equiv 1\times 2\times \ldots \times \frac{p-1}{2}.\left(-\frac{p-1}{2}\right)\ldots(-2)(-1)\pmod p \\ &\equiv (-1)^{\frac{p-1}{2}}\left(1\times 2\times \ldots \times \frac{p-1}{2}\right)^2 \pmod p \\ &\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p\end{aligned}$$

لأن $\frac{p-1}{2}$ زوجي حسب الفرض .

ولكن بإستخدام مبرهنة ويلسن لدينا

$$(p-1)!\equiv -1(\mathrm{mod}\ p).$$

وبالتالي فإن العدد $\left(\frac{p-1}{2}\right)!$ يجب أن يكون حلاً للتطابق :

$$x^2\equiv -1(\mathrm{mod}\ p).$$

مثال :

بما أن $p=17\equiv 1(\mathrm{mod}\ 4)$ فإن للتطابق $x^2\equiv -1(\mathrm{mod}\ 17)$ حلاً .

أحد الحلول هو

$$\left(\frac{17-1}{2}\right)!=8!.$$

ولكن $8!\equiv 13(\mathrm{mod}\ 17)$. إذن x=13 هو أحد الحلول و $x=-13\equiv 4(\mathrm{mod}\ 17)$ هو حل آخر .

نتيجة :

يوجد عدد غير منته من الأعداد الأولية على الصورة : 4n+1 ، $n\in Z^+$.

البرهان:

لنفرض أن عدد الأعداد الأولية التي على الصورة 4n+1 منته ولتكن هذه الأعداد :
$p_1<p_2<\ldots<p_k$. لنفرض ان العدد N معطى بالمساواة :

$$N=(2p_1p_2\ldots p_k)^2+1$$

بما أن N >1 فردي . إذن يوجد عدد أولي P>2 بحيث يكون P|N . أي أن $N\equiv 0(\mathrm{mod}\ p)$.

ومنه فإن :

$$.\left(2p_1p_2...p_k\right)^2 \equiv -1\left(\mathrm{mod}\ p\right)$$

ونجد أن p يجب أن يكون على الصورة 4n+1 .

وبما أن $p_1, p_2, ..., p_k$ هي جميع الأعداد الأولية التي تكون على الصورة 4n+1 فإن $p = p_i$ حيث إن $1 \le i \le k$.

وبما أن p|N وكذلك $p \mid \left(2p_1p_2...p_k\right)^2$ فإن p|1 وهذا مستحيل .

تعريف :

ليكن $n \in Z^+$ و $a \in Z$ حيث (a,n)=1 نقول إن k هو رتبة العدد a قياس n (order of a modulo n) ونكتب

$$\mathrm{ord}_n\left(a\right) = k$$

إذا كان k هو أصغر عدد صحيح موجب يحقق

$$.a^k \equiv 1\left(\mathrm{mod}\ n\right)$$

مثال : احسب $\mathrm{ord}_{14}\left(5\right)$.

الحل :

لاحظ أن

$$5^2 \equiv 11\left(\mathrm{mod}\ 14\right)$$
$$5^3 \equiv 13\left(\mathrm{mod}\ 14\right)$$
$$5^4 \equiv 9\left(\mathrm{mod}\ 14\right)$$
$$5^5 \equiv 3\left(\mathrm{mod}\ 14\right)$$
$$5^6 \equiv 1\left(\mathrm{mod}\ 14\right)$$

ولذا فإن $\mathrm{ord}_{14}\left(5\right) = 6$.

مبرهنة (الخصائص الأساسية لرتبة العدد):

ليكن $n \in Z^+$ و $a \in Z$ حيث (a,n)=1 و $\mathrm{ord}_n(a) = k$ عندئذ:

(1) $a^m \equiv 1 \pmod{n}$ إذا وفقط إذا كان k|m.

(2) $k \mid \varphi(n)$.

(3) $a^r \equiv a^s \pmod{n}$ إذا وفقط إذا كان

$r \equiv s \pmod{k}$.

(4) جميع الأعداد $a, a^2, a^3, \ldots, a^k$ غير متطابقة قياس n .

(5) إذا كان $m \in Z^+$ فإن $\mathrm{ord}_n(a^m) = \dfrac{k}{(k,m)}$.

(6) $\mathrm{ord}_n(a^m) = k$ إذا وفقط إذا كان (k,m)=1 .

البرهان :

(1) لنفرض أن $a^m \equiv 1 \pmod{n}$. عندئذ ، باستخدام خوارزمية القسمة نجد أن m=kq+r: حيث $0 \le r < k$. ولذا فإن :

$$1 \equiv a^m = (a^k)^q a^r \equiv a^r \pmod{n}$$

ولذا نجد من تعريف k أن r=0 . وبالتالي k|m .

ولبرهان العكس ،

نفرض ان k|m . عندئذ ، m=kt حيث $t \in Z$. ومنه فإن :

$$a^m = a^k = (a^k)^t \equiv (1)^t \equiv 1 \pmod{n}$$

(2) بما أن (a,n)=1 فإننا نجد بإستخدام مبرهنة أويلر أن $a^{\varphi(n)} \equiv 1 \pmod{n}$. ولذا فباستخدام الفقرة (1) نجد أن $k \mid \varphi(n)$.

(3) لنفرض أن r<s . بما أن (a,n)=1 فإننا نجد أن $a^r \equiv a^s \pmod{n}$ إذا وفقط إذا كان

$$a^{s-r} \equiv 1 \pmod{n}.$$

ولكن نجد باستخدام الفقرة (1) أن $a^{s-r} \equiv 1 \pmod{n}$ إذا وفقط إذا كان k|(s-r).

وبالتالي فإننا نخلص إلى أن $a^r \equiv a^s \pmod{n}$ إذا وفقط إذا كان $s \equiv r \pmod{k}$.

(4) إذا كان $1 \le i \ne j < k$ حيث

$$a^i \equiv a^j \pmod{n}$$

فإننا نجد بإستخدام الفقرة (3) أن $i \equiv j \pmod{k}$ وهذا مستحيل .

(5) لنفرض أن $d=(k,m)$. عندئذ ، $k=rd$, $m=sd$ و $(s,r)=1$.

ولذا فإن :

$$\left(a^m\right)^{\frac{k}{d}} = \left(a^m\right)^{\frac{rd}{d}} = \left(a^m\right)^r = a^{srd} = a^{sk} = \left(a^k\right)^s \equiv 1 \pmod{n}$$

ومنه فإن : $t = \operatorname{ord}_n\left(a^m\right) \mid \frac{k}{d}$.

ومن ناحية أخرى ،

بما أن

$$a^{mt} = \left(a^m\right)^t \equiv 1 \pmod{n}$$

فإن k|mt. أي أن rd|sdt . ومنه فإن r|st .

ولكن (r,s)=1 . ولذا فإن r|t . أي أن $\frac{k}{d} \mid t$.

وبما أن t و $\frac{k}{d}$ موجبان فإن $t = \frac{k}{d}$.

(6) لنفرض أولاً أن $\operatorname{ord}_n\left(a^m\right) = k$. عندئذ ، بإستخدام الفقرة (5) نجد أن

$$k = \frac{k}{(k,m)}.$$

ومنه فإن (k,m)=1. وبالعكس ،

إذا كان (k,m)=1 فإن

$$\text{ord}_n\left(a^m\right)=\frac{k}{(k,m)}.$$

مثال : احسب $\text{ord}_{40}\left(3\right)$.

الحل :

بما أن $\varphi(40)=16$ فإن $\text{ord}_{40}\left(3\right)$ هو أحد قواسم العدد 16 وهي 16,8,4,2,1 . والآن :

$$3^1\equiv 3(\text{mod } 40)$$

$$3^2\equiv 9(\text{mod } 40)$$

$$3^4\equiv 1(\text{mod } 40)$$

وبالتالي فإن $\text{ord}_{40}\left(3\right)=4$.

مبرهنة :

ليكن (a,n)=(b,n)=1 وليكن

$$\text{ord}_n\left(a\right)=h \text{ و } \text{ord}_n\left(b\right)=k.$$

إذا كان (h,k)=1 فإن

$$\text{ord}_n\left(ab\right)=hk.$$

البرهان :

بما أن

$$(ab)^{hk}=a^{hk}b^{hk}=\left(a^h\right)^k\left(b^k\right)^h\equiv 1\times 1\equiv 1(\text{mod } n)$$

فإننا نجد أن $\text{ord}_n\left(ab\right)=hk$.

وبما أن (h,k)=1 فإنه لابد وأن يكون

$$\mathrm{ord}_n(ab) = rs$$

حيث $r|h$, $s|k$. أي أن $k=sx$, $h=rw$.

سنبرهن الأن أن $x=w=1$. الآن ، لدينا :

$$a^{rs}b^{rs} = (ab)^{rs} \equiv 1 (\mathrm{mod}\ n)$$

$$\left(a^{rs}b^{rs}\right)^{w} \equiv 1^{w} \equiv 1 (\mathrm{mod}\ n)$$

$$\left(a^{rw}\right)^{s}\left(b^{rw}\right)^{s} \equiv 1 (\mathrm{mod}\ n)$$

ولكن $a^{rw} = a^{h} \equiv 1 (\mathrm{mod}\ n)$. ولذا فإن

$$b^{hs} = \left(b^{h}\right)^{s} = \left(b^{rw}\right)^{s} \equiv 1 (\mathrm{mod}\ n).$$

ولذا نجد أن

$$\mathrm{ord}_n(b) = k \mid hs$$

وبما أن $(h,k)=1$ فإن $k|s$. ولكن $s|k$.

وبالتالي فإن $s=k$. وبالمثل $r=h$. إذن ،

$$\mathrm{ord}_n(ab) = hk .$$

مثال : احسب $\mathrm{ord}_{11}(30)$.

الحل :

لاحظ أن $30=10\times3$ وأن $(3,10)=1$. ولذا فإن

$$\mathrm{ord}_{11}(30) = \mathrm{ord}_{11}(3)\times\mathrm{ord}_{11}(10) = 5\times2 = 10$$

مبرهنة (اختبار لوقا)(Lucas test):

إذا كان $n \in Z^+$ وإذا وجد $a \in Z$ بحيث يتحقق :

$$a^{n-1} \equiv 1 \pmod{n} \quad (1)$$

$$a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n} \quad (2)$$

لكل عدد أولي p يقسم n-1 .

فإن n عدد أولي .

البرهان :

بما أن $a^{n-1} \equiv 1 \pmod{n}$ فإن (a,n)=1 .

ولذا فإننا نجد أن

$$k = \text{ord}_n(a) \mid (n-1).$$

سنبرهن الآن أن k=n-1.

لنفرض لغرض التناقض أن $k \neq n-1$ وبما أن k|(n-1) فإنه يوجد t>1 حيث n-1=kt .

لنفرض أن q قاسما أولياً للعدد t . عندئذ ،

$$a^{\frac{n-1}{q}} = a^{\frac{kt}{q}} = \left(a^k\right)^{\frac{t}{q}} \equiv 1 \pmod{n}$$

مما يتناقض مع الفقرة (2) من الفرض .

إذن ، k=n-1.

ولكن

$$\text{ord}_n(a) = k \leq \varphi(n)$$ وأن $\varphi(n) \leq n-1$.

ولذا فإن $\varphi(n) = n-1$.وبالتالي فإن هذا يجعل n أولياً .

ملحوظة :

لاحظ ان اختبار لوكا مثل اختبار ويلسن عديم الفائدة من الناحية العلمية لأنه قبل تطبيقه يجب معرفة تحليل العدد n-1 وهذا أصعب من أختبار أولية العدد بصورة عامة ،

ولكن إذا كان تحليل العدد n-1 سهلاً كما هو لبعض الأعداد الخاصة مثل أعداد فيرما F_n وبعض أعداد ميرسين وهي على الصورة $2^n - 1$ فإنه من الممكن الأستفادة علمياً من اختبار لوكا .

مثال : استخدم اختبار لوكا لإثبات أن $F_3 = 2^{2^3} + 1 = 257$ **عدداً اولياً .**

الحل :

$F_3 - 1 = 256 = 2^7$. ولذا فإن القاسم الأولي الوحيد للعدد $F_3 - 1$ هو 2 .

الآن :

$$3^2 \equiv 9 \pmod{257}$$
$$3^4 \equiv 81 \pmod{257}$$
$$3^8 \equiv 136 \pmod{257}$$
$$3^{16} \equiv 259 \equiv -8 \pmod{257}$$
$$3^{32} \equiv 64 \pmod{257}$$
$$3^{64} \equiv 241 \equiv -16 \pmod{257}$$
$$3^{128} \equiv 256 \equiv -1 \pmod{257}$$
$$3^{256} \equiv 1 \pmod{257}$$

ولذا فإن

$$3^{F_3 - 1} \equiv 1 \pmod{257}$$

ولكن

$$3^{\frac{F_3 - 1}{2}} \not\equiv 1 \pmod{257}.$$

وبالتالي فإن F_3 عدد أولي .

التمارين

السؤال الأول :

إذا كان $n \mid \left(2^n + 1\right)$ حيث إن n عدد أولي فأثبت أن n=3 .

السؤال الثاني :

إذا كان p,q عددين أوليين مختلفين بحيث إن :

$$a^q \equiv a\left(\text{mod } p\right) \text{ و } a^p \equiv a\left(\text{mod } q\right)$$

فأثبت أن : $a^{pq} \equiv a\left(\text{mod } pq\right)$.

الدوال العددية

NUMBER THEORETIC FUNCTIONS

تعريف :

تسمى الدالة التي مجالها الأعداد الصحيحة الموجبة ، ومجالها المقابل الأعداد الحقيقية أو المركبة بالدالة العددية .

تعريف :

نقول إن الدالة العددية f غير الصفرية دالة ضربية (multiplicative function) إذا كان

$$f\left(mn\right) = f\left(m\right)f\left(n\right)$$

لكل $m,n \in Z^+$ حيث $\left(m,n\right) = 1$.

كما نقول إن f دالة ضربية تماماً إذا كان :

$$f\left(mn\right) = f\left(m\right)f\left(n\right)$$ لكل $m,n \in Z^+$.

مثال :

لنفرض أن $\alpha \in R$. الدالة المعرفة بالقاعدة : $f_\alpha\left(n\right) = n^\alpha$ لكل $n \in Z^+$

دالة ضربية تماماً ، لأن :

$$f_\alpha(m\ n)=(m\ n)^\alpha=m^\alpha n^\alpha=f_\alpha(m)f_\alpha(n)$$

لكل $m,n\in Z^+$.

مثال :

الدالة التالية تعرف بدالة (Mangoldt) وتعرف على النحو التالي:

$$\Lambda(n)=\begin{cases}\ln(p) & ,\ n=p^m\\ 0 & ,\ n\neq p^m\end{cases}$$

دالة غير ضربية لأن :

$$\Lambda(2\times5)=\Lambda(10)=0\neq\Lambda(2)\times\Lambda(5)=\ln(2)\ln(5).$$

مبرهنة :

إذا كانت f دالة ضربية فإن f(1)=1 .

البرهان :

بما أن f دالة غير صفرية فإنه فإنه يوجد عدد صحيح موجب n بحيث إن $f(n)\neq0$. وبما أن $(n,1)=1$ فإن

$$f(2)=f(n\times1)=f(n)f(1).$$

وبالتالي فإن $f(1)=1$.

ملحوظة :

بإستخدام المبرهنة السابقة وملاحظة أن $\Lambda(1)=0\neq1$ نجد أن دالة غير ضربية .

تعريف :

لنفرض أن n عدد صحيح موجب . نرمز لعدد قواسم $\tau(n)$ الموجبة بالرمز ولمجموع هذه القواسم بالرمز $\sigma(n)$.

أي أن :

$$\tau(n)=\sum_{d|n}1 \quad \text{و} \quad \sigma(n)=\sum_{d|n}d$$

حيث إن $\sum_{d|n}$ تعني أن المجموع مأخوذ على جميع قواسم العدد n الموجبة .

مثال : احسب :

$$\sigma(10),\sigma(8),\sigma(4),\sigma(2)$$
$$,\tau(10),\tau(8),\tau(4),\tau(2)$$

الحل :

قواسم العدد 2 الموجبة هي : 2,1.

ومنه فإن :

$$.\sigma(2)=3 \ , \ \tau(2)=2$$

قواسم العدد 4 الموجبة هي : 4,2,1.

ومنه فإن :

$$.\ \sigma(4)=7 \ , \ \tau(4)=3$$

قواسم العدد 8 الموجبة هي : 8,4,2,1.

ومنه فإن :

$$.\sigma(8)=15 \ , \ \tau(8)=4$$

وأخيراً قواسم العدد 10 الموجبة هي : 10,5,2,1 .

ومنه فإن :

$$.\sigma(10)=18 \ , \ \tau(10)=4$$

ملحوظة :

لاحظ أن الدالتين σ,τ دالتان غير ضربيتين تماماً لأنه على سبيل المثال :

$$4 = \tau(8) \neq \tau(2)\tau(4) = (2)(3) = 6$$

كما أن :

$$.15 = \sigma(8) \neq \sigma(2)\sigma(4) = (3)(7) = 21$$

بعض خواص الدوال العددية :

تمهيدية :

إذا كانت f,g دالتين عدديتين 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

$$e_1, e_2, ..., e_t \quad \text{و} \quad d_1, d_2, ..., d_s$$

هي جميع قواسم العددين n,m الموجبة على الترتيب .

لدينا الآن :

$$\sum_{\substack{d|m \\ e|n}} f(d)g(e) = \sum_{\substack{j=1,...,s \\ k=1,...,t}} f(d_j)g(e_k)$$

$$= \sum_{j=1,...,s} f(d_j)g(e_1) + ...+ = \sum_{j=1,...,s} f(d_j)g(e_t)$$

(خاصية توزيع الضرب على الجمع)

$$= \left(\sum_{j=1}^{s} f(d_j)\right)\left(\sum_{k=1}^{t} g(e_k)\right)$$

$$= \left(\sum_{d|m} f(d)\right)\left(\sum_{e|n} g(e)\right)$$

مبرهنة :

إذا كانت g دالة ضربية فإن الدالة $f(n)=\sum_{d|n} g(d)$ دالة ضربية أيضاً .

البرهان :

لنفرض أن $m,n \in Z^+$ حيث إن (m,n)=1 .

الآن $f(mn)=\sum_{d|mn} g(d)$.

وبالتالي فإنه يوجد عددان صحيحان وحيدان d_1,d_2 بحيث إن :

$$d_1 d_2 = d \ , \ (d_1,d_2)=1 \ , \ d_2 \mid n \ , \ d_1 \mid m$$

وعليه فإن :

$$f(mn)=\sum_{\substack{d_1|m \\ d_2|n}} g(d_1 d_2)$$

$$=\sum_{\substack{d_1|m \\ d_2|n}} g(d_1)g(d_2)$$

(لأن g دالة ضربية)

$$=\sum_{d_1|m} g(d_1)\sum_{d_2|n} g(d_2)$$

$$=f(m)f(n)$$

إذن ، f دالة ضربية .

نتيجة :

الدالتان σ,τ ضربيتان .

البرهان :

من الواضح أن f(n)=1 , g(n)=n دالتان ضربيتان .

وبما أن $\tau(n)=\sum_{d|n} f(d)=\sum_{d|n} 1$

وأن

$$\sigma(n)=\sum_{d|n} g(d)=\sum_{d|n} d \ .$$

وبالتالي نجد أن σ,τ ضربيتان .

مبرهنة :

إذا كانت f دالة ضربية وكانت $n_1,n_2,...,n_r$ أعداد صحيحة موجبة أولية نسبياً مثنى مثنى فإن :

$$f(n_1n_2...n_r)=f(n_1)f(n_2)....f(n_r)$$

البرهان :

باستخدام الاستقراء الرياضي على r .

الخطوة الأساسية :

بما أن f دالة ضربية وأن $(n_1,n_2)=1$ فإن

$$.f(n_1n_2)=f(n_1)f(n_2)$$

إذن ، العبارة صحيحة عند r=2 .

خطوة الأستقراء :

لنفرض أن العبارة صحيحة عندما يكون r=k . والمطلوب هو إثبات صحة العبارة عندما يكون r=k+1 .
بما أن

$$(n_1n_2...n_k,n_{k+1})=1$$

فإن :

$$f(n_1n_2...n_kn_{k+1})=f(n_1n_2...n_k)f(n_{k+1})$$

وباستخدام فرضية الاستقراء لدينا :

$$f(n_1n_2...n_k)=f(n_1)f(n_2)....f(n_k)$$

إذن ،

$$f\left(n_1 n_2 ... n_k n_{k+1}\right) = f\left(n_1\right) f\left(n_2\right) .... f\left(n_k\right) f\left(n_{k+1}\right) .$$

أي أن العبارة صحيحة عندما r=k+1 .

نتيجة :

إذا كانت f دالة ضربية وكان $n = p_1^{k_1} p_2^{k_2} .... p_t^{k_t}$ فإن

$$f\left(n\right) = f\left(p_1^{k_1}\right) f\left(p_2^{k_2}\right) .... f\left(p_t^{k_t}\right)$$

البرهان :

بما أن الأعداد $p_1^{k_1} p_2^{k_2} .... p_t^{k_t}$ أولية نسبياً مثنى مثنى فإننا نحصل على النتيجة المطلوبة بتطبيق المبرهنة السابقة.

مبرهنة :

إذا كان $n = p_1^{k_1} p_2^{k_2} .... p_t^{k_t}$ فإن :

(أ) $\tau\left(n\right) = \left(k_1 + 1\right)\left(k_2 + 1\right)...\left(k_t + 1\right)$.

(ب) $\sigma\left(n\right) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} ... \frac{p_t^{k_1+1} - 1}{p_t - 1}$.

البرهان :

لاحظ أن جميع قواسم العدد $p_i^{k_i}$ الموجبة هي :

$$1, p_i, p_i^2, ..., p_i^{k_i - 1}, p_i^{k_i}$$

وعدد هذه القواسم هو $\left(k_i + 1\right)$ ،

أما مجموعها فهو :

$$1 + p_i + p_i^2 + ... + p_i^{k_i}$$

وهذا المجموع عبارة عن مجموع متتالية هندسية حدها الأول 1 وحدها الأخير $p_i^{k_i}$ ونسبتها p_i ،

وعليه فإن مجموعها يساوي :

$$\frac{p_i^{k_i+1}-1}{p_i-1}.$$

ولذا فإن :

$$\tau\left(p_i^{k_i}\right)=\left(k_i+1\right)$$

وأن

$$\sigma\left(p_i^{k_i}\right)=\frac{p_i^{k_i+1}-1}{p_i-1} \quad \text{لكل } 1\le i\le t.$$

وبما أن σ,τ دالتان ضربيتان فمن النتيجة السابقة نحصل على الصيغة المطلوبة لكل من $\sigma(n),\tau(n)$.

مثال : إذا كان $n=200=2^3\times5^2$ فإن :

$$\tau(n)=(3+1)(2+1)=12$$

وإن

$$\sigma(n)=\frac{2^4-1}{2-1}\times\frac{5^3-1}{5-1}=465 .$$

التمارين

السؤال الأول : جد n بحيث أن $\tau(10n)=10$.

السؤال الثاني : جد جميع الأعداد الصحيحة الموجبة n التي تحقق كل مما يلي :

$$(1)\ \sigma(n)=12$$
$$(2)\ \sigma(n)=18$$
$$(3)\ \sigma(n)=52$$

الأعداد التامة

Perfect Numbers

تعريف :

ليكن n عدداً صحيحاً موجباً نقول إن n عدد تام (perfect number) إذا كان

$$\sigma(n) = 2n$$

، ونقول إن n عدد زائد (abundant number) إذا كان

$$\sigma(n) > 2n$$

ونقول إن n عدد ناقص (deficient number) إذا كان

$$\sigma(n) < 2n \text{ .}$$

مثال :

العدد 12 عدد زائد لأن :

$$\sigma(12) = \sigma(2^2 \times 3) = \frac{2^3 - 1}{2 - 1} \times \frac{3^2 - 1}{3 - 1} = 28 > 2(12)$$

مثال:

العدد 14 عدد ناقص لأن :

$$\sigma(14) = \sigma(2 \times 7) = \frac{2^2 - 1}{2 - 1} \times \frac{7^2 - 1}{7 - 1} = 24 < 2(14)$$

مثال:

العددان 6,28 تامان لأن :

$$\sigma(6) = \sigma(2 \times 3) = \sigma(2)\sigma(3) = 3 \times 4 = 2 \times 6$$

$$\sigma(28) = \sigma(4 \times 7) = \sigma(4)\sigma(7) = 7 \times 8 = 2 \times 28$$

مبرهنة :

ليكن m عدداً زوجياً . عندئذ ، m عدد تام إذا وفقط إذا كان

$$m = 2^n \left(2^{n+1} - 1\right)$$

حيث إن $2^{n+1} - 1$ عدد أولي .

البرهان :

نفرض أولاً أن $m = 2^n \left(2^{n+1} - 1\right)$ حيث إن $p = 2^{n+1} - 1$ عدد أولي .

لدينا الآن :

$$\sigma(m) = \sigma\left(2^n p\right) = \sigma\left(2^n\right)\sigma(p) = \left(2^{n+1} - 1\right)(p+1) = \left(2^{n+1} - 1\right)2^{n+1} = 22^n\left(2^{n+1} - 1\right) = 2m$$

وبالتالي فإن m عدد تام .

وللبرهان على العكس :

نفرض أن m عدد زوجي تام . بما أن m عدد زوجي فإننا نستطيع كتابته على الصورة : $m = 2^n b$
حيث إن n>0 ، b عدد فردي . وبما أن m عدد تام فإن :

$$2^{n+1} b = 2m = \sigma\left(2^n\right)\sigma(b) = \left(2^{n+1} - 1\right)\sigma(b)$$

ومنه فإن 2^{n+1} يقسم $\left(2^{n+1} - 1\right)\sigma(b)$.

وحيث أن

$$\left(2^{n+1} - 1, 2^{n+1}\right) = 1$$

فإننا نستنتج من تمهيدية أقليدس أن :

$$2^{n+1} \mid \sigma(b)$$

إذن ، يوجد عدد صحيح c بحيث يكون :

$$\sigma(b) = 2^{n+1} c .$$

ولذا فإن :

$$2^{n+1}b=\left(2^{n+1}-1\right)2^{n+1}c$$

. أي أن:

$$b=\left(2^{n+1}-1\right)c$$

. ومنه فإن: $m=2^n b=2^n\left(2^{n+1}-1\right)c$.

سنبرهن الآن على أن c =1 .

إذا كان c >1 فإن للعدد b ثلاث قواسم على الأقل وهي b,c,1 وهذا يؤدي إلى أن :

$$\sigma(b)\geq b+c+1=\left(2^{n+1}-1\right)c+c+1=2^{n+1}c+1>2^{n+1}c=\sigma(b)$$

وهذا تناقض . إذن c =1 .

وبالتالي فإن :

$$.m=2^n b=2^n\left(2^{n+1}-1\right)$$

وإن :

$$.\sigma\left(2^{n+1}-1\right)=2^{n+1}$$

سنبرهن أخيراً على أن $2^{n+1}-1$ عدد أولي .

إذا فرضنا أن $2^{n+1}-1$ عدد مؤلف فإننا نستطيع إيجاد عدد k بحيث إن :

$$1<k<2^{n+1}-1\quad,\quad k\left|\left(2^{n+1}-1\right)\right.$$

ومنه فإن :

$$2^{n+1}=\sigma\left(2^{n+1}-1\right)\geq 2^{n+1}-1+k+1>2^{n+1}$$

وهذا تناقض . وبالتالي فإن :

$$m=2^n\left(2^{n+1}-1\right)$$

حيث إن $2^{n+1}-1$ أولي .

تعريف :

إذا كان k عدداً صحيحاً موجباً فإننا نسمي العدد 2^k-1 بعدد مرسين (Mersenne number) ونرمز له بالرمز M_k.

مبرهنة :

إذا كان p أولياً فردياً فإن أي قاسم أولي لعدد مرسين M_k يكون على الصورة $2kp+1$ حيث إن $k \geq 1$.

البرهان :

لنفرض أن q عدد أولي بحيث إن $q \mid M_k$. بإستخدام مبرهنة فيرما الصغرى لدينا : $q \mid 2^{q-1}-1$

وبما أن $q \mid 2^p-1$ فإن :

$$\left(2^p-1, 2^{q-1}-1\right) > 1.$$

ولكن $\left(2^p-1, 2^{q-1}-1\right) = 2^{(p,q-1)}-1$

إذن $2^{(p,q-1)}-1 > 1$. أي أن :

$$\left(p, q-1\right) > 1$$

وعليه فإن $\left(p, q-1\right) = p$ ومنه $p \mid \left(q-1\right)$.

إذن يوجد عدد صحيح m بحيث يكون q=mp+1 .

وبما أن q فردي فيجب أن يكون m زوجياً .

أي أن m=2k ، $k \geq 1$.

وبالتالي فإن : q=2kp+1 ، $k \geq 1$.

مثال :

أثبت أن العدد $M_{13} = 8191$ عدد أولي .

الحل :

بما أن $91 < \sqrt{8191}$ فإنه يكفي أن نختبر الأعداد الأولية التي هي أقل من 91 والتي تكتب على الصورة : 26k+1 . وهذه الأعداد هي : 79,53 . ولكن $M_{13} \nmid 79$, $M_{13} \nmid 53$ ، وبالتالي فإن M_{13} أولي .

التمارين

السؤال الأول :

إذا كان p,q عددين أوليين بحيث إن $pq \neq 6$ فأثبت أن pq عدد ناقص .

السؤال الثاني :

جد قيم k التي تجعل العدد $3 \times 5^k \times 7$ زائداً.

دالة أويلر

Eulers Function

سبق أن قدمنا دالة أويلر ورمزنا لها بالرمز φ وكذلك عرفنا $\varphi(n)$ على أنه عدد أعداد أي نظام رواسب مختزل قياس n . وهذا يساوي أيضاً عدد الأعداد التي هي أقل من n أو تساويه وأولية نسبياً مع n .

تمهيدية :

$\varphi(n) = n - 1$ إذا وفقط إذا كان n عدداً أولياً .

البرهان :

لنفرض أن n عدد أولي . إن جميع الأعداد 1,2,....,n-1 أولية نسبياً مع n وبالتالي فإن $\varphi(n) = n - 1$.

وبالعكس

إذا فرضنا أن $\varphi(n) = n - 1$ وأن n عدد مؤلف فإنه يوجد قاسم d للعدد n بحيث إن 1< d <n ، (n,d)=d . ومنه نستطيع أن نستنتج أنه يوجد على الأقل عدد من بين الأعداد 1,2,..., n-1 ليس أولياً نسبياً مع n وبالتالي فإن $\varphi(n) \leq n - 2$ وهذا تناقض .

تمهيدية :

إذا كان p عدداً أولياً وكان k عدداً صحيحاً موجباً فإن :

$$\varphi\left(p^k\right)=p^k-p^{k-1}.$$

البرهان :

لنفرض أن $A=\left\{1,2,...,p^k\right\}$ عندئذ ،

$$\varphi\left(p^k\right)=\left|\left\{t\in A:(t,p)=1\right\}\right|.$$

لاحظ أن $\left(t,p^k\right)>1$ إذا وفقط إذا كان $p\mid t$.

ولذا فإن

$$\varphi\left(p^k\right)=p^k-\left|\left\{t\in A:p^k\mid 1\right\}\right|.$$

لكن إذا كان $p\mid t$ فإن $t=pn$ وحيث إن $1\le t\le p^k$

فهذا يعني أن $1\le n\le p^{k-1}$.

إذن ، $\left|\left\{t\in A:p\mid t\right\}\right|=p^{k-1}$ وبالتالي :

$$\varphi\left(p^k\right)=p^k-p^{k-1}$$

مثال :

احسب $\varphi(125)$.

الحل :

$$\varphi(125)=\varphi\left(5^3\right)=5^3-5^2$$

$$=125\text{-}25=100$$

تمهيدية :

إذا كان n,m عددين أوليين نسبياً فإن

$$\varphi(mn)=\varphi(m)\varphi(n).$$

أي أن φ ضربية .

البرهان :

ليكن

$$A=\{a_1,a_2,...,a_{\varphi(m)}\}$$

$$B=\{b_1,b_2,...,b_{\varphi(n)}\}$$

نظامي رواسب مختزلين قياس n,m على الترتيب وليكن

$$C=\{c_1,c_2,...,c_{\varphi(mn)}\}$$

نظام رواسب مختزل قياس mn .

سنبرهن على أن $|A\times B|=|C|$.

وذلك بتعريف دالة $f:A\times B\to C$ وإثبات أنها تقابل .

ليكن (a_i,b_j) عنصراً ينتمي إلى $A\times B$. حسب مبرهنة الباقي الصينية يوجد عدد x_0 يحقق النظام :

$$x_0\equiv a_i\pmod m$$
$$x_0\equiv b_j\pmod n$$

لاحظ أن

$$(x_0,m)=1$$
$$(x_0,n)=1$$

ومن ثم فإن $(x_0, mn) = 1$. وبالتالي نجد أن x_0 يطابق عدداً وحيداً قياس mn من المجموعة C وليكن c_t.

نعرف الآن :

$$f(a_i, b_j) = c_t$$

للبرهان على أن f أحادية نفرض أن

$$f[(a_r, b_s)] = f[(a_i, b_j)] = c_t \quad .$$

عندئذ ،

$$a_r \equiv c_t \pmod{m}$$
$$a_i \equiv c_t \pmod{m}$$

ولذا فإن $a_i \equiv a_r \pmod{m}$.

وبما أن A مجموعة جزئية من نظام رواسب تام قياس m فإن $a_i = a_r$. وبالمثل ، يمكن إثبات أن $b_j = b_s$.

وبالتالي فإن $(a_i, b_j) = (a_r, b_s)$.

أي أن f أحادية .

بقي أن نثبت أن f شاملة ولهذا الغرض نفرض أن $c_s \in C$.

بما أن $(c_s, mn) = 1$ فإن

$$(c_s, m) = 1 \ , \ (c_s, n) = 1.$$

وبالتالي فإنه يوجد عنصران وحيدان

$$b_j \in B \ , \ a_i \in A$$

بحيث إن :

$$a_i \equiv c_s \pmod{m}$$
$$a_j \equiv c_s \pmod{n}$$

إذن ، $f\left[\left(a_i, b_j\right)\right] = c_s$. وبالتالي فإن f شاملة.

ومن ثم فإن f تقابل . ونخلص إلى أن $|A \times B| = |C|$.

أي أن :

$$\varphi(mn) = \varphi(m)\varphi(n).$$

مبرهنة :

ليكن n عدداً صحيحاً أكبر من 2 وليكن $n = p_1^{k_1} p_2^{k_2} \ldots . p_t^{k_t}$.

هو تحليل n إلى قوى عوامله الأولية . عندئذ ،

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right).....\left(1-\frac{1}{p_t}\right)$$

البرهان:

نجد أنه لكل i=1,2,...,t لدينا

$$\varphi\left(p_i^{k_i}\right) = p_i^{k_i} - p_i^{k_{i-1}} = p_i^{k_i}\left(1-\frac{1}{p_i}\right)$$

وبما أن φ دالة ضربية فإن :

$$\varphi(n) = \varphi\left(p_1^{k_1}\right)\varphi\left(p_2^{k_2}\right)....\varphi\left(p_t^{k_t}\right)$$
$$= p_1^{k_1}\left(1-\frac{1}{p_1}\right)p_2^{k_2}\left(1-\frac{1}{p_2}\right).....p_t^{k_t}\left(1-\frac{1}{p_t}\right)$$
$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right).....\left(1-\frac{1}{p_t}\right)$$

وهو ما نود برهانه .

مثال:

احسب $\varphi(360)$.

الحل :

$$\varphi(360)=\varphi\left(2^3\ 3^2\ 5\right)=360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=96$$

مثال :

احسب $\varphi(151200)$.

الحل:

$$\varphi(151200)=\varphi\left(2^5\ 3^3\ 5^2\ 7^1\right)$$

$$=151200\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)$$

$$=34560$$

مبرهنة :

$n=\sum_{d|n}\varphi(d)$ لكل $n\geq 1$.

البرهان:

سأقدم برهانين لهذه المبرهنة .

البرهان الأول:

لنفرض أن S={1,2,...,n} . لكل قاسم d من قواسم n دع :

$$A(d)=\left\{k:(k,n)=d\ ,\ 0<k\leq n\right\}$$

. من الواضح أن {A(d)} تجزئ للمجموعة S ومنه نجد أن

$$\sum_{d|n}\left|A(d)\right| = n .$$

الآن : (k,n)=d إذا وفقط إذا كان $\left(\frac{k}{d},\frac{n}{d}\right) = 1$.

وكذلك :

$0 < k \le n$ إذا وفقط إذا كان $0 < \frac{k}{d} \le \frac{n}{d}$.

وبناء على ذلك إذا وضعنا $q = \frac{k}{d}$ فإننا نجد تقابلاً بين عناصر A(d) وبين الأعداد الصحيحة q التي تحقق : $0 < q \le \frac{n}{d}$, $\left(q,\frac{n}{d}\right) = 1$.

ولكن عدد هذه الأعداد q هو $\varphi\left(\frac{n}{d}\right)$ وعليه فإن

$$\left|A(d)\right| = \varphi\left(\frac{n}{d}\right) .$$

وبالتالي فإن :

$$\sum_{d|n}\varphi(d) = \sum_{d|n}\varphi\left(\frac{n}{d}\right) = n .$$

البرهان الثاني :

لنفرض أن $f(n) = \sum_{d|n}\varphi(d)$. وبما أن φ دالة ضربية فإن f دالة ضربية أيضاً .لنفرض الآن ان $n = p_1^{k_1} p_2^{k_2} \ldots p_t^{k_t}$ هو تحليل n إلى قوى عوامله الأولية .

الآن :

$$f\left(p_i^{k_i}\right)=\sum_{d|p_i^{k_i}}\varphi(d)=\varphi(1)+\varphi\left(p_i\right)+\varphi\left(p_i^2\right)+....+\varphi\left(p_i^{k_i}\right)$$

$$=1+\left(p_i-1\right)+\left(p_i^2-p_i\right)+\left(p_i^3-p_i^2\right)+....+\left(p_i^{k_i}-p_i^{k_i-1}\right)=p_i^{k_i}$$

وبالتالي فإن :

$$\cdot\sum_{d|n}\varphi(d)=f(n)=f\left(p_1^{k_1}\right)f\left(p_2^{k_2}\right)....f\left(p_t^{k_t}\right)=p_1^{k_1}p_2^{k_2}....p_t^{k_t}=n$$

مثال يوضح البرهان الأول :

لنأخذ n=14 .

لدينا المجموعات التالية :

$$A(1)=\{1,3,5,9,11,13\}$$
$$A(2)=\{2,4,6,8,10,12\}$$
$$A(7)=\{7\}$$
$$A(14)=\{14\}$$

وعدد عناصر هذه المجموعات :

$$\left|A(1)\right|=\varphi(14)=6$$
$$\left|A(2)\right|=\varphi(7)=6$$
$$\left|A(7)\right|=\varphi(2)=1$$
$$\left|A(14)\right|=\varphi(1)=1$$

. وبالتالي فإن :

$$.\sum_{d|n}\varphi(d)=\varphi(1)+\varphi(2)+\varphi(7)+\varphi(14)=14$$

مبرهنة :

إذا كان $n>1$ عدداً صحيحاً وكان $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$ نظام رواسب مختزل قياس n فإن:

$$\sum_{k=1}^{\varphi(n)} a_k \equiv \frac{1}{2} n\ \varphi(n) \pmod{n} .$$

البرهان :

لكل $1 \le i \le \varphi(n)$ يوجد عدد $1 \le b_i < n$ بحيث يكون

$$a_i \equiv b_i \pmod{n}$$

وبما أن $(a_i, n) = 1$ نجد أن $(b_i, n) = 1$. كذلك لاحظ أن $(b_i, n) = 1$ إذا وفقط إذا كان $(n - b_i, n) = 1$.

إذن ،

$$\sum_{i=1}^{\varphi(n)} b_i = \sum_{i=1}^{\varphi(n)} (n - b_i) = \varphi(n) n - \sum_{i=1}^{\varphi(n)} b_i$$

وهذا يقتضي :

$$\sum_{i=1}^{\varphi(n)} b_i = \frac{n\ \varphi(n)}{2} .$$

ولكن

$$\sum_{i=1}^{\varphi(n)} b_i = \sum_{i=1}^{\varphi(n)} a_i \pmod{n} .$$

ومن ثم فإن

$$\sum_{i=1}^{\varphi(n)} a_i \equiv \frac{n\ \varphi(n)}{2} \pmod{n} .$$

التمارين

السؤال الأول :

أثبت أن $\varphi(2n)=\varphi(n)$ إذا كان n فردياً ، وأن $\varphi(2n)=2\varphi(n)$ إذا كان n زوجياً .

السؤال الثاني :

جد جميع قيم n التي تحقق $\varphi(n)=16$.

السؤال الثالث :

جد جميع قيم x بحيث يكون 4 لا يقسم $\varphi(x)$.