الموضوع: المحاضرة الأولى | 2017/3/17

مبدأ الاستقراء الرياضي

مبدأ الترتيب الحسن:

لتكن A مجموعة جزئية من $\mathbb{Z}$ فإنه يوجد عنصر أصغري في المجموعة A وليكن a_0 أي يحقق $\forall a \in A \Rightarrow a_0 \leq a$

و العنصر الأصغري هو عنصر وحيد.

الاستقراء الرياضي:

لتكن S_n قضية رياضية والإثبات صحة القضية S_n من أجل $n \geq 1$ و $n \in \mathbb{N}$

مبدأ الاستقراء: لاثبات أن S_n صحيحة من أجل $n \geq 1$ نتبع الخطوات التالية:

خطوة البداية: نبرهن صحة S_n من أجل $n=1$

خطوة الاستقراء: نفرض صحة S_n من أجل $n=k$ و نبرهن أنها صحيحة من أجل $n=k+1$

مثال: لتكن S_n قضية تحقق: $\sum_{i=1}^{n} i^3 = 1^3+2^3+\cdots+n^3 = \left(\frac{n(n+1)}{2}\right)^2$

- لاثبات ذلك:

خطوة البداية: من أجل $n=1$

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

محققة

خطوة الاستقراء: نفرض $n=k$ القضية صحيحة أي: $\sum_{i=1}^{k} i^3 = \left[\frac{k(k+1)}{2}\right]^2$ صحيحة ونبرهن صحتها من أجل $n=k+1$

$$S_{k+1}: \sum_{i=1}^{k+1} i^3 = \sum_{i=1}^{k} i^3 + (k+1)^3$$

$$= \left[\frac{k(k+1)}{2}\right]^2 + (k+1)^3 = (k+1)^2\left[\frac{k^2}{4}+k+1\right]$$

$$S_{k+1}: \sum_{i=1}^{k+1} i^3 = (k+1)^2\,\frac{k^2+4k+4}{4} = \frac{(k+1)^2(k+2)^2}{4} = \left[\frac{(k+1)(k+2)}{2}\right]^2$$

و القضية صحيحة من أجل $n=k+1$

و بالتالي هي صحيحة من أجل $n \geq 1$

ملاحظة-1-: لدينا القضية S_n و لنثبت صحتها من أجل $n \geq n_0$

خطوة البداية: لنثبت صحتها من أجل $n=n_0$

خطوة الاستقراء: لنفرض صحتها من أجل $n=k \geq n_0$ ولنثبت صحتها من أجل $n=k+1$

ملاحظة-2- : لدينا القضية S_n ولنثبت ونثبت صحتها من أجل $n \geq n_0$

خطوة البداية: نثبت صحة S_n من أجل $n = n_0$

خطوة الاستقراء : نفرض صحة S_n من أجل كل قيمة $n_0 \leq k$

ونثبت صحة S_n من أجل $n = k+1$

مثال: اثبت صحة القضية S_n التالية:

$a_0 = 1 , a_1 = 2 , a_2 = 3$

$\forall n \geq 3 \quad a_n = a_{n-1} + a_{n-2} + a_{n-3}$

والمطلوب: إثبات صحة أن $a_n \leq 3^n$

من أجل $n \in \mathbb{N}$

* خطوة البداية: $n = 3$:

$a_3 = a_2 + a_1 + a_0 = 3 + 2 + 1 = 6$

$6 = a_3 \leq 3^3 = 27$ محققة

$a_4 = a_3 + a_2 + a_1 = 6 + 3 + 2 = 11$

$a_4 \leq 3^4 = 81$ محققة

خطوة الاستقراء: نفرض صحة S_k من أجل كل n محققة : $n \leq k$

$a_k \leq 3^k$

ونبرهن صحتها من أجل $n = k+1$

$a_{k+1} = a_k + a_{k-1} + a_{k-2}$

$a_{k+1} \leq 3^k + 3^{k-1} + 3^{k-2} < 3^k + 3^k + 3^k = 3^{k+1}$

القضية محققة من أجل $n = k+1$ فهي محققة من أجل $n \in \mathbb{N}$

مثال: إذا كانت S_1 صحيحة. "لم نتحقق من صحة S_k قد نصل لنتائج خاطئة"

$S_k = \sum_{i=1}^{k} i = 1 + 2 + \dots + k = \frac{k^2 + k + 2}{2}$

(نفرض أنها صحيحة من أجل $n = k$)

فإن S_{k+1} صحيحة من أجل $n = k+1$:

$\sum_{i=1}^{k+1} i = \frac{(k+1)^2 + k + 1 + 2}{2} = \frac{k^2 + 3k + 4}{2}$

لنثبت أنها صحيحة من أجل $n = k+1$

$\sum_{i=1}^{k+1} i = 1 + 2 + \dots + k + k + 1 = \frac{k^2 + 3k + 4}{2}$ محققة

لنناقش خطوة البداية ،

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

هل $\frac{k(k+1)}{2} \stackrel{?}{=} \frac{k^2+k+2}{2}$ محققة

ماهي قيمة n_0 التي تحقق هذه المساواة

$$\frac{n_0(n_0+1)}{2} = \frac{n_0^2+n_0+2}{2} \Rightarrow n_0^2+n_0 = n_0^2+n_0+2$$

$0 = 2$ مستحيل .

إذاً لا توجد قيمة n_0 تكون فيها المساواة محققة

إذاً لا يمكن أن نكتفي بخطوة البداية فقط أو خطوة الاستقراء فقط لاثبات أي قضية رياضية

تنويه: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

$$+\left(\begin{array}{l} \sum_{i=1}^{n} i = 1+2+3+\cdots+n-1+n \\ \sum_{i=1}^{n} i = n+n-1+\cdots+3+2+1 \end{array} \right.$$

$$2\sum_{i=1}^{n} i = \underbrace{n+1+\cdots+n+1}_{n \text{ مرة}} = n(n+1)$$

^^ اثبت بطريقة الاستقراء الرياضي :

[3] $\sum_{i=1}^{n} \frac{1}{i(i+1)} = 1 - \frac{1}{n+1}$

ثم احسب $\sum_{i=1}^{\infty} \frac{1}{i(i+1)}$

خطوة البداية :

$$\sum_{i=1}^{1} \frac{1}{i(i+1)} = \frac{1}{2} = 1 - \frac{1}{2} = \frac{1}{2}$$ محققة ✓

خطوة الاستقراء :

نفرض صحتها من أجل $n=k$

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

ولنبرهن صحتها من أجل $n=k+1$

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

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

وبالتالي القضية محققة من أجل $n=k+1$ بالتالي هي صحيحة من أجل كل $n \in \mathbb{N}$

وبالتالي :

$$\sum_{i=1}^{\infty} \frac{1}{i(i+1)} = \lim_{n\to\infty} \sum_{i=1}^{n} \frac{1}{i(i+1)} = 1$$

انتهت المحاضرة ^^

قابلية القسمة في $\mathbb{Z}$

تعريف : ليكن $a,b \in \mathbb{Z}$ و $a \neq 0$ نقول أن a يقسم b ونكتب $a \mid b$ إذا وجد عدد $c \in \mathbb{Z}$ بحيث يكون $b = a.c$

- b يقبل القسمة على a
- b مضاعف للعدد a

أما إذا كان a لا يقسم b نكتب $a \nmid b$

خواص قابلية القسمة :

1. العدد 1 يقسم جميع الأعداد الصحيحة والعدد 0 مضاعف لكل الأعداد الصحيحة
2. $a \mid b \Rightarrow -a \mid b$
3. $\forall k \in \mathbb{Z} : a \mid b \Rightarrow a \mid k.b$
4. $\forall a \in \mathbb{Z} : a \mid a$
5. $a \mid b \wedge b \mid c \Rightarrow a \mid c$
6. $a \mid b \wedge a \mid c \Rightarrow a \mid (bn+cm) \quad \forall n,m \in \mathbb{Z}$
7. $a \mid b_i : (i = 1,2,\dots,n) \Rightarrow a \mid (m_1 b_1 + m_2 b_2 + \dots + m_n b_n)$
8. $a \mid b \vee a \mid c \Rightarrow a \mid b.c$ ← العكس صحيح بس إذا a أولى
   مثال: $4 \mid 12 = 6.2$ ← $4 \mid 6 \wedge 4 \mid 2$ ولكن
9. $a \mid b \Rightarrow |a| \leq |b|$
10. $a \mid b \wedge b \mid a \Leftrightarrow |a| = |b|$

نتيجة : مجموعة القواسم الموجبة للعدد الصحيح $a \neq 0$ هي مجموعة منتهية من القواسم التي هي أصغر من $|a|$

مبرهنة إقليدس : إذا كان $a \neq 0$ و $a,b \in \mathbb{Z}$ فإنه يوجد عددين r,q وحيدين ويحققان العلاقة $b = aq + r$ حيث $0 \leq r < |a|$

البرهان : لتكن لدينا مجموعة الأعداد الصحيحة التالية :

$$S = \{x \geq 0 : x = b - at \quad ; t \in \mathbb{Z}\}$$

هي مجموعة مرتبة وغير خالية حسب مبدأ الترتيب الحسن يوجد عنصر أصغري هو r وقيمة t الموافقة له هي q : $0 \leq r = b - qa$

إذاً $b = aq + r$

لنثبت أن $r < |a|$

نفرض $r \geq |a| \Leftarrow r - |a| \geq 0$

إذا كان a موجبة $\Leftarrow$ $r - |a|$

تناقض. $r-|a| = r-a = b-qa-a = b-(q+1)a \in S$

إذا كان a سالب $\Leftarrow$ $r-|a| = r+a = b-qa+a = b-(q-1)a \in S$

بما أن $r-|a| \geq 0$ و ينتمي إلى S وهو أصغر من r هذا تناقض إذاً $r < |a|$

لنثبت أن q, r وحيدين نفرض أنه يوجد q_1, r_1 بحيث يكون

$$\left.\begin{array}{l} b = aq_1 + r_1 \\ b = aq + r \end{array}\right\} aq + r = aq_1 + r_1 \Rightarrow a(q_1 - q) = r - r_1$$

أي $r = r_1$ مضاعف لـ a و لكن $r < |a|$ وهذا يتحقق إذا كان $r - r_1 = 0$

أي $r = r_1$ كذلك نستنتج $q = q_1$

تمرين: اثبت أن مربع أي عدد فردي يقبل القسمة على مضاعفات العدد 8

$b^2 = 8M + 1 \overset{?}{\Longleftrightarrow}$ b عدد صحيح فردي

b عدد فردي $\Leftarrow b = 2n+1 \Leftarrow b^2 = 4n^2 + 4n + 1$

$b^2 = 4n(n+1) + 1$ حيث $n(n+1)$ جداء عددين متتاليين هو عدد زوجي "2M".

$\Rightarrow b^2 = 8M + 1$

مثال: اثبت أن $6 \mid f(m) = 5m^3 + 7m$ حيث $m \in \mathbb{N}$;

نستخدم الاستقراء الرياضي.

خطوة البداية: $m = 0$: محققة $6 \mid f(0) = 0$

كذلك: $6 \mid f(1) = 5 + 7 = 12$ محققة

خطوة الاستقراء: نفرض أن $6 \mid f(k)$ ولنبرهن أن $6 \mid f(k+1)$

$6 \mid f(x) = 5k^3 + 7k$

$$f(k+1) = 5(k+1)^3 + 7(k+1) = \underbrace{5k^3 + 7k}_{f(k)} + \underbrace{15k^2 + 15k}_{15(k+1)k} + 5 + 7$$

$$= f(k) + 15(k+1)k + 12 = f(k) + 30M + 12$$

حيث $2M = k(k+1)$.

إذاً كل حد في العلاقة السابقة يقبل القسمة على 6 بالتالي $6 \mid f(k+1)$ أي أن:

$6 \mid f(m) \; \forall m \in \mathbb{N}$

مثال: اثبت أن $14 \mid f(n) = 5^{2n+1} + 3^{4n+2}$ من أجل $n \geq 0$.

خطوة البداية: $n = 0 \Leftarrow 14 \mid f(0) = 5 + 9 = 14$

إذاً $14 \mid f(1) = 125 + 729 = 854 = 14 \times 61$

الموضوع : .....

خطوة الاستقراء: نفرض أن $14 \mid f(k)=5^{2k+1}+3^{4k+2}$

ولنبرهن صحتها من أجل $n=k+1$ أي $f(k+1)$:

$$f(k+1)=5^{2(k+1)+1}+3^{4(k+1)+2}$$

$$=5^2 \cdot 5^{2k+1}+3^{4k+2} \cdot 3^4$$

$$f(k+1)=5^2(5^{2k+1}+3^{4k+2})-5^2 \cdot 3^{4k+2}+3^{4k+2} \cdot 3^4$$

$$=5^2 \cdot f(k)-3^{4k+2}(-5^2+3^4)$$

$$=5^2 f(k)-3^{4k+2} \cdot 56 \qquad : 56=14 \times 4$$

$$=5^2 f(k)-14 \times 4 \times 3^{4k+2}$$

بما أن $14 \mid 14 \times 3 \times 3^{4k+2}$ ، $14 \mid 5^2 f(k)$ أي $14 \mid f(k+1)$ ومنه $14 \mid f(n)$ من أجل $n \geq 1$

القاسم المشترك الأعظم

تعريف: نقول عن d_1 إنه قاسم مشترك للعددين a,b غير صفريين معاً إذا كان

$$d_1 \mid a \wedge d_1 \mid b$$

كذلك يكون $-d_1 \mid a \wedge -d_1 \mid b$ أي $-d_1$ قاسم مشترك

يكون $|d_1| \leq |a|$ ، $|d_1| \leq |b|$ والقاسم المشترك d_1 لا يمكن أن يتجاوز العدد الأصغر بينهما

مجموعة القواسم الموجبة للعددين a,b غير الصفرين معاً هي تقاطع مجموع قواسم العدد a مع مجموعة قواسم العدد b وهي مجموعة منتهية

القاسم المشترك الأعظم. GCD, gcd : Greatest common Divisor

القاسم المشترك الأعظم للعددين a,b غير المعدومين معاً هو $d=(a,b)$

أو $d=gcd(a,b)$ تحقق ما يلي :

① $d>0$ ② $d \mid a \wedge d \mid b$

③ إذا كان العدد الصحيح c حيث $c \mid a \wedge c \mid b$ فإن $c \leq d$

مثال :

$$\{(-a,-b)=(a,-b)=(-a,b)=d\}$$

$d=(0,8)=8$

$d=(-2,15)=1$

$d=(-3,15)=3$

نتيجة : القاسم المشترك الأعظم لعددين غير معدومين موجود ووحيد

مبرهنة: ليكن لدينا العددين الصحيحين a,b غير المعدومين فإن القاسم المشترك الأعظم لهما يكتب كتركيب خطي للعددين $a,b\in\mathbb{Z}$ أي $a,b\in\mathbb{Z}$ و $d=(a,b)$
فإنه يوجد عددين صحيحين x_0, y_0 بحيث يكون $d=ax_0+by_0$

الإثبات: نأخذ مجموعة التراكيب الخطية للعددين a,b.

$$S=\{n=ax+by \;;\; x,y\in\mathbb{Z}\}$$

لأنه: من أجل $x=\mp 1$ ، $y=0$ $\leftarrow$ $n=\mp a\in S$
و $y=\mp 1$ ، $x=0$ $\leftarrow$ $n=\mp b\in S$

نعرف مجموعة $S_1=\{n>0 \;;\; n\in S\}$
$S_1\neq\emptyset$ و تحتوي على عنصر أصغري ولكن n_0.
أي $n_0=ax_0+by_0$ حيث $x_0, y_0\in\mathbb{Z}$
حسب مبرهنة إقليدس $n=n_0q+r$ حيث $0\leq r<n_0$

$$ax+by=q(ax_0+by_0)+r$$

ولدينا $0\leq r$:

$$r=a(x-qx_0)+b(y-y_0)$$

إذا كان $r=0$ نجد أن $n_0\backslash n$
أو $r>0$ أي $r\geq 0$ وهو أصغر من n_0 وهذا يناقض كون n_0 عدد أصغري في S_1
أي أن $n_0\backslash n$ أي أن n_0 تقسم جميع عناصر المجموعة S أي $n_0\backslash a$ و $n_0\backslash b$
أي أن $n_0\backslash d(a,b)$ $\leftarrow$ $n_0\leq d$
ومن جهة أخرى $d\backslash a \wedge d\backslash b$ أي $d\backslash n_0$
$d=n_0=ax_0+by_0 \leftarrow \{$

نتيجة: تمثيل القاسم المشترك الأعظمي للعددين a,b ليس وحيداً

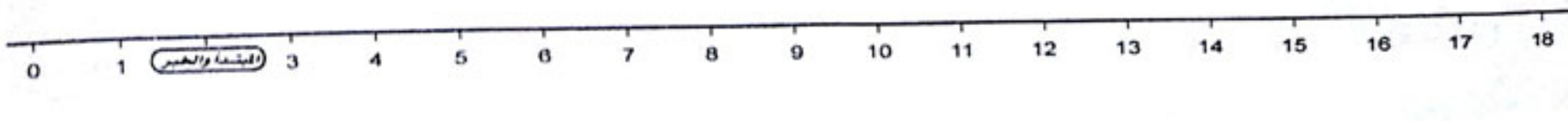
مثال: $d(15,24)=3$

$$3=(-3)15+(2)24=(5)15+(-3)24$$

تعريف: a,b عددين أوليين نسبياً $\leftarrow$ $d(a,b)=1$

مبرهنة: يكون العددين الصحيحين a, b غير المعدومين أوليين فيما بينهما نسبياً إذا وفقط إذا وجد عددان صحيحان x, y بحيث يكون $ax+by=1$

الإثبات: $\leftarrow$ $(a,b)=1=d$ نجد من المبرهنة السابقة $1=ax+by \;;\; x,y\in\mathbb{Z}$
$\rightarrow$ بالعكس: إذا كان $ax+by=1$ نفرض $d=(a,b)$ $\leftarrow$ $d\backslash a, d\backslash b$
أي $d\backslash 1$ $\leftarrow$ $d=1$



النتيجة : إذا كان $d=(a,b)$ ، $a=a_0 d$ ، $b=b_0 d$ فإن $(a_0,b_0)=1$

البرهان : $d>0$: $ax+by=d$

$\left(\frac{a}{d}\right)x+\left(\frac{b}{d}\right)y=1$ ... أي أن ... $\left(\frac{a}{d}=a_0, \frac{b}{d}=b_0\right)=1$

خواص

1. $d=(|a|,|b|)=(a,b)=(-a,b)=(a,-b)$
2. $(a,0)=|a| \wedge (1,a)=1$
3. $(a,m)=1 \wedge (b,m)=1 \Longrightarrow (a.b,m)=1$
4. $k \backslash a.b$, $(k,b)=1 \Rightarrow k \backslash a$

إذا كان $k \backslash a.b$ فقد تكون k تقسم أياً منهما a ، b

$4 \backslash 12=2.6$ ولكن $\rightarrow 4\times 2$ ، 4×6

5. إذا كان $(a,b)=1$ و $a \backslash n$ ، $b \backslash n \Rightarrow a.b \backslash n$

إذا لم يكن a ، b أوليان فيما بينهما فهذا ليس بالضرورة صحيح مثال: $12 \backslash 4$ ، $12 \backslash 4$ لكن $12 \backslash 4\times 4$

6. إذا كان $d=(a,b)$ فإن $D=(ma,mb)=md$

انتهت المحاضرة ٨ـ٨

الموضوع: المحاضرة الثالثة ٢٠١٧/٣/٢٨

مبرهنة: إذا كان $b=aq+r$; $0\leq r<a$ فإن $a,b>0$

$$d(a,b)=(a,r)$$

الإثبات: $d=(a,b)$ أي $d\mid a$, $d\mid b$ أي $d\mid b-aq$ $\Leftarrow d\mid r$

أي $d\mid a$ و $d\mid r$ $\Leftarrow$ d قاسم مشترك لـ a,r نفرض $c\mid a$ ∧ $c\mid r$

$\Leftarrow c\mid aq+r$ $\Leftarrow c\mid b$ وحسب $c\mid b$ و $c\mid a$ $\Leftarrow c\leq d$ أي $c\mid d$

ومنه $d=(a,r)$

خوارزمية إقليدس: تساعدنا في إيجاد القاسم المشترك الأعظم لـ a,b حيث $b>a>0$

$$b=aq_1+r_1 \quad , \quad 0\leq r_1<a$$

1- إذا كان $r_1=0$ $\Leftarrow$ b يقسم a $\Leftarrow d(a,b)=a$

2- إذا كان $r_1>0$

$$a=r_1q_2+r_2 \quad ; \quad 0\leq r_2<r_1$$

1- إذا كان $r_2=0$ $\Leftarrow r_1\mid a$ $\Leftarrow d=(a;b)=(a,r_1)=r_1$

2- $r_2>0$

$$r_1=r_2q_3+r_3 \quad ; \quad 0\leq r_3<r_2$$

نتابع حتى الخطوة t

$$r_t=r_{t+1}q_{t+2}+r_{t+2}$$

$$0\leq r_{t+2}<r_{t+1}$$

1- إذا كان $r_{t+2}=0$ $\Leftarrow r_{t+1}\mid r_t$

فالقاسم المشترك الأعظم $d=(a,b)=(a,r_1)=(r_1,r_2)=\dots=(r_t,r_{t+1})=r_{t+1}$

يمكننا الرجوع بالعلاقات مثل:

$$r_{t+2}=r_t-r_{t+1}q_{t+2}$$

نتابع حتى نصل إلى الصيغة $d=ax_0+by_0$

فنحصل على قيم x_0,y_0

مثال: أوجد القاسم المشترك الأعظم للعددين $d=(12378,3054)$

$$12378=4\cdot3054+162$$
$$3054=18\cdot162+138$$
$$162=1\cdot138+24$$

$138 = 5.24 + 18$.
$24 = 1.18 + 6$.
$18 = 3.6 + 0 \Rightarrow d = 6$
أوجد حل للمعادلة $d = 12378x + 3054y$.
$6 = 24 - 1.18 = 24.1(138 - 5.24)$
$= -1.(138) + 6.24 = -1.(138) + 6(162 - 1.138)$
$= 6.162 - 7.138 = 6.162 - 7(3054 - 18.162)$
$= (-7)(3054) + 132(12378 - 4.3054)$
$= 132(12378) - 535(3054)$
نجد أن $x = 132$ و $y = -535$.

القاسم المشترك الأعظم لعدة أعداد

تعريف: لتكن a_i أعداد صحيحة $i = 1, 2, \dots, n$ نقول عن $d = (a_1, \dots, a_n)$
أنه القاسم المشترك الأعظم لـ a_i : $i = 1, 2, \dots, n$
إذا تحقق مايلي:
1- $d > 0$
2- $d \mid a_i \quad i = 1, 2, \dots, n$
3- إذا كان $c \mid a_i$ $(i = 1, 2, \dots, n)$ فإن $c \leq d$

مبرهنة: إذا كان $d = gcd(a_1, a_2, \dots, a_n)$
$d = d_1 \Leftarrow \begin{cases} d = gcd(a_1, a_2, \dots, a_n) \\ d_1 = gcd(a_1, a_2, \dots, a_{n-2}, (a_{n-1}, a_n)) \end{cases}$

مثال: $d = gcd(256, (112, 72)) = gcd(256, 8) = 8$

تعريف: نقول عن الاعداد a_i إنها أولية نسبياً فيما بينها $i = 1, 2, \dots, n$
إذا كان: $d = gcd(a_1, a_2, \dots, a_n) = 1$
ونقول أن الاعداد الأولية a_i أولية نسبياً مثنى مثنى إذا كان:
$gcd(a_i, a_j) = 1$, $i, j = 1, 2, \dots, n$, $i \neq j$

نتيجة: إذا كانت الأعداد a_i أولية نسبياً مثنى مثنى فإنها أولية نسبياً فيما بينها
$\Rightarrow$ العكس غير صحيح بالضرورة مثال:
إن $d = gcd(24, 15, 7) = 1$ أولية نسبياً فيما بينها لكنها ليست أولية مثنى مثنى. $(24, 15, 40) = 1$ لكن $(24, 15) = 3$ $(15, 40) = 5$ $(24, 40) = 8$

الموضوع : .....

/ / 11

المضاعف المشترك الأصغر lcm

تعريف : لتكن a_i أعداد صحيحة $i=1,2,\dots,n$ غير صفرية إذا $a_i \backslash m$ فإن m مضاعف للأعداد a_i : $i=1,2,\dots,n$ ونقول $L=lcm(a_1,\dots,a_n)$ هو مضاعف مشترك الأصغر لهذه الأعداد إذا حقق مايلي :

1- $L>0$ 2- $a_i \backslash L$; $i=1,2,\dots,n$

3- إذا كان $a_i \backslash m$ فإن $L \leqslant m$; $i=1,2,\dots,n$

★ المضاعف المشترك الأصغر للاعداد صحيحة يقسم أي مضاعف مشترك لهذه الأعداد $L \backslash m$.

مبرهنة : إذا كان a و b عددان صحيحان موجبان و $d=(a,b)$ و $L=\frac{a.b}{d}$ فإن : $L=lcm$

البرهان : بما أن $d=(a,b) \Leftarrow \begin{cases} a=a_0 d \\ b=b_0 d \end{cases}$: $(a_0,b_0)=1$

$L=\frac{a.b}{d}=a_0 b=ab_0$

لتكن m مضاعف مشترك لـ a و b

$m=a_1.a=a_1.a_0 d \Leftarrow b \backslash m \Leftarrow bod \backslash a_1 a_0 d \Leftarrow b_0 \backslash a_1 a_0$

بما أن $(a_0,b_0)=1 \Leftarrow b_0 \backslash a_1 \Leftarrow ab_0 \backslash a.a_1$ (m)

$L \backslash m \longrightarrow L=lcm(a,b)$

مثال : احسب $L=lcm(21,6)=\frac{21.6}{3}=42$

تمارين : استخدم الاستقراء الرياضي لاثبات :

$48^2=2304 \backslash P(n)=7^{2n+2}-48n-49$ $n \geqslant 0$

خطوة البداية : $P(0) \backslash 2304 \longrightarrow P(1)=7^2-49=0$

$P(1)=7^4-48-49=7^2(7^2-1)-48=7^2.48-48=(7^2-1)48$

$=48^2 \Rightarrow 48^2 \backslash P(1)$

خطوة الاستقراء : نفرض $48^2 \backslash P(k)=7^{2k+2}-48k-49$

لنبرهن أن $48^2 \backslash P(k+1)$

$P(k+1)=7^{2k+4}-48(k+1)-49$

$=7^{2k+2}.7^2-48k-48-49.$

$= 7^2(7^{2k+2} - 48k - 49) + 7^2(48)k + 7^2(49) - 48k - 48 - 49$

$= 7^2 f(k) + 48k(7^2 - 1) + 7^2(49) - 48 - 49$

$= 7^2 f(k) + 48^2 k + f(1)$

بما أن كل حد يقبل القسمة على 48^2 أي أن $f(k+1)$ يقبل القسمة على 48^2 والعلاقة صحيحة من أجل n

2) اثبت أنه إذا كان $3x+2$ مضاعفاً لـ 7 فإن $49 \setminus 24x^2+4x+41 = f(x)$

$3x+2 = 7k$

$24x^2+4x+41 = (3x+2)(8x-4)+49$

$= (3x+2)[5(3x+2) - 7(x+2)] + 49$

$= 5(3x+2)^2 - 7(3x+2)(x+2) + 49$

$= 5(49k^2) - (49k)(x+2) + 49$ "49 كل حد يقبل القسمة على 49"

اثبت أن : $14 \setminus 15x^2 - 11x + 14$ إذا كان $3x+2 = 7k$

$f(x) = 15x^2 - 11x + 14 = (3x+2)(5x+7) - 2(14)$

نميز الحالتين : 1 إذا كان العدد x فردي.

$7x-5$ عدد زوجي يقبل القسمة على 2 $\Rightarrow f(x)$ يقبل القسمة على 14

$3x+2$ عدد فردي يقبل القسمة على 7

2 إذا كان العدد x زوجي :

$7x-5$ عدد فردي

$3x+2$ عدد زوجي يقبل القسمة على 2 و 7 $\Rightarrow (3x+2)$ يقبل القسمة على 14

$14 \setminus f(x)$

3. إذا كان $(a,b) = 1$ أوجد $d = (a+b, a-b)$

$(a,b) = 1 \iff ax + by = 1$

$d = (a+b, a-b) \iff d = (a+b)x + (a-b)y$

$= \underbrace{ax + b(-y)}_{=1} + \underbrace{bx + ay}_{=1} = 1+1 = 2$

أو

$d = a\underbrace{(x+y)} + b\underbrace{(x-y)}$

$a \underbrace{X}_{=1} + b\, Y = 1$

إذا أوجدت معادلات يكون فيها $d=1$

ومعادلات يكون فيها $d=2$

الموضوع : .....

/ / 3

الأعداد الأولية .

P عدد أولي : هو عدد يقبل القسمة على الواحد وعلى نفسه فقط ، $1<P$

n عدد مؤلف : هو عدد يمكن كتابته على شكل $n=a.b$: $1<a<n$ $1<b<n$

خواص

1- الأعداد الأولية P هي أعداد أولية نسبياً مثنى مثنى .

2- $P \nmid n \Longleftarrow gcd(P,n)=P$.

3- $P \mid a.b$ فإن P يقسم أحدهما على الأقل .

4- $P \mid a_1.a_2 \dots a_n$ فإن P يقسم أحدها على الأقل

5- $P \mid P_1.P_2 \dots P_n$ فإن P يساوي أحد هذه الأعداد

مبرهنة أساسية في الحساب : إذا كان $n>1$ فإن n عدد أولي أو n يكتب كجداء لأعداد أولية وهذا التمثيل وحيد

الإثبات : نستخدم الاستقراء الرياضي : 2 أولي ، 3 أولي و 4=2.2 ، 5 أولي

خطوة الاستقراء : نفرض أن k يكتب كجداء لأعداد أولية (عواملها الأولية)

إذا كان العدد $k>1$ يحقق المبرهنة

ونأخذ العدد $k+1$ إذا كان $k+1$ أولي فقد أثبتنا المطلوب

أما إذا كان $k+1$ غير أولي فإن $k+1=a.b$ حيث $\begin{cases}1<a<k+1\\1<b<k+1\end{cases}$

نجد أن $a<k+1$ يكتب كجداء لعواملها الأولية

و $b<k+1$ يكتب كجداء لعواملها الأولية

وبالتالي $k+1$ هو جداء العوامل أولية وبالتالي أياً كان n فإنه عدد أولي أو جداء الأعداد أولية لنفرض أن n يكتب بشكل غير وحيد أي :

$$n=P_1.P_2 \dots P_t = q_1.q_2 \dots q_s$$

$P_1 \mid q_1.q_2 \dots q_s$ إذاً P_1 يساوي أحد الأعداد الأولية q_i وليكن $P_1=q_1$

$a=P_2.P_3 \dots P_t = q_2.q_3 \dots q_s$ و $a<n$ (لدينا البرهان كذلك بالاستقراء) $\Longleftarrow$

$P_2 \mid q_2 q_3 \dots q_s$ فهو يساوي أحد الأعداد الأولية وليكن $P_2=q_2$

نتابع ... حتى نجد أن $t=s$

بالتالي يكتب n بشكل وحيد على شكل جداء عواملها الأولية .

* إن للعدد n عوامل متكررة فنكتبه بالشكل القانوني $n=P_1^{\alpha_1} P_2^{\alpha_2} \dots P_r^{\alpha_r}$

$P_1<P_2<\dots<P_r$ ، $\alpha_i \in \mathbb{Z}^+$:

مثل $360=2^3.3^2.5$

نتيجة (1): إذا كان $1<n$ فله عامل أولي P بحيث $P \mid n$

نتيجة (2): إذا كان $1<n$ فله عامل أولي P و $P \leq \sqrt{n}$

الإثبات: n عدد مؤلف : $n = a.b$

$$\left.\begin{matrix} 1<a<n \\ 1<b<n \end{matrix}\right\} \Rightarrow 1 < a \leq b < n$$

$$n = a.b \geq a^2 \Longrightarrow a \leq \sqrt{n}$$

$a>1 \leftarrow$ له عدد أولي P و $P \mid a$ و $P \leq a \leq \sqrt{n} \leftarrow P \leq \sqrt{n}$

نتيجة (3): إذا كان $n>1$ وليس له عامل أولي P بحيث $P \leq \sqrt{n}$

فإن n أولي .

مبرهنة: عدد الأعداد الأولية غير منته

الإثبات: نفرض أن عدد الأعداد الأولية منته وعددهم n

$P_1, P_2, \dots, P_n$ بحيث : $P_1 < P_2 < \dots < P_n$

نأخذ العدد $N = P_1 . P_2 \dots P_n + 1$ ($N > 1$) فله عامل أولي P

$P \mid N$ وهو أحد الأعداد الأولية $P_1, \dots, P_n \leftarrow P \mid P_1 . P_2 \dots P_n$

أي أن $P \mid N - P_1 . P_2 \dots P_n \leftarrow P \mid 1 \leftarrow P = 1$.

وهذا تناقض إذاً عدد الأعداد الأولية غير منته

صيغ تعطي أعداداً أولية "وربما غير أولية أيضاً"

هذه الصيغة تعطي أعداداً أولية $N = P_1 . P_2 \dots P_n + 1$

① $N = 2+1 = 3$ أولي

② $N = 2.3+1 = 7$ أولي

③ $N = 2.3.5+1 = 31$ أولي

④ $N = 2.3.5.7+1 = 211$ أولي

⑤ $N = 2.3.5.7.11+1 = 2311$ أولي

⑥ $N = 2.3.5.7.11.13+1 = 30031 = 59 \times 509$ غير أولي

إذاً لا توجد صيغة تعطي أعداداً أولية فقط

بعض الصيغ التي تعطي أعداداً أولية وغير أولية

$= x^2 - x + 41 \quad 0 \leq x \leq 40$

$= x^2 - 79x + 1601 \quad 0 \leq x \leq 79$

$= (a,b) = 1 \Longrightarrow ax + b$ تعطي أعداد أولية

$= F_n = 2^{2^n} + 1 \quad : F_1, F_2, F_3, F_4$ أعداد أولية (ولكن F_5 عدد مؤلف)

انتهت المحاضرة ^^

2017/4/4

المحاضرة الرابعة

التحليل إلى العوامل الأولية.

ليكن $n>1$ إذا كان n عدد زوجي نقسم على 2 حتى يصبح العدد فردي

نركز على تحليل الأعداد الفردية $n>1$

تمهيدية (1): إذا كان $n>1$ عدد فردي فيمكن كتابة n على شكل جداء عددين صحيحين a و b

أي $n=a.b$ إذا وفقط إذا أمكن كتابتها على شكل فرق مربعين

$$n=a.b \iff n=x^2-y^2$$

نكتب: إذا كان $n=a.b$

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

أما إذا كان $n=x^2-y^2$

$$n=(x+y)(x-y)=a.b$$

طريقة فيرما لتحليل العدد الفردي إلى جداء عاملين

نأخذ المعادلة $n=x^2-y^2$ نكتب $x^2-n=y^2$ لنبحث عن عدد k حقق $k^2>n$

لنوجد الأعداد k التي تحقق k^2-n يساوي مربع عدد.

أي نستمر بالتجريب $(k+1)^2-n$ - - - - - حتى نصل لـ $m^2-n=y^2$ حيث $m\geq\sqrt{n}$

وإذا لم نجد عدد m نتابع حتى نصل إلى $\left(\frac{n+1}{2}\right)^2-n=\left(\frac{n-1}{2}\right)^2$ أولي $n\leq n.1, n$

مثال: $n=202765281$ سنحتاج إلى الملاحظة

$n=44021\times46061$

مثال: $n=23449$ نلاحظ أن: $153^2<n<154^2$

$23409<n<23716$

$154^2-n=23716-23449=267$

$155^2-n=24025-23449=576=24^2$ $\Longrightarrow$ لنبحث بين الأعداد k $n=155^2-24^2$

$n=(155+24)(155-24)=179\times131$

أوليان

تمرين:

اثبت أن العدد الأولي الوحيد من الصيغة n^3-1 هو 7

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

وتحقق إذا كان $n=2$ وعندها $n^3-1=7$

إذا كان $n>2$ نحصل على عدد مؤلف.

2 اثبت أن الأولي الوحيد P الذي يحقق العلاقة $3P+1=n^2$ هو $P=5$

$3P+1=n^2 \Leftrightarrow 3P=n^2-1=(n-1)(n+1)$

ومنه إما $3 \backslash n-1$ وإما $3 \backslash n+1$

فإذا كان $n-1=3k$ يكون $3P=3k(3k+2)$ ومنه $P=k(3k+2)$

ولما كان P أولياً فإن $k=1$ ومنه $P=1\times(3+2)=5$

وإذا كان $n+1=3k$ يكون $3P=(3k-2)(3k)$ ومنه $P=k(3k-2)$

ولما كان P أولياً فإن $k=1 \Leftarrow P=1$ مرفوض لأنه ليس أولي

3 لدينا P عدد أولي و $P \backslash a^n$ اثبت أن $P^n \backslash a^n$ وأن $P \backslash a$

$a>1 \leftarrow a=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r} \leftarrow a^n=p_1^{\alpha_1 n}p_2^{\alpha_2 n}\dots p_r^{\alpha_r n}$

إذا كان $P \backslash p_1^{\alpha_1 n}p_2^{\alpha_2 n}\dots p_r^{\alpha_r n}$ يجب أن يكون P مساوياً لأحد الأوليات p_i ولنفرض $P=p_i \Longrightarrow P^{n'}=p_i^{n\alpha_i} \backslash a^n$

بما أن $a=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$ و $P=p_i$ فإن $P \backslash a$

4 إذا كان P عدداً أولياً فردياً و $P \neq 5$ اثبت أنه إما P^2+1 أو P^2+1 يقبل القسمة على 10

آحاد الأعداد الأولية هي 1، 3، 7، 9.

نأخذ مربعات الأعداد الأولية فنجد آحادها 1، 9، 9، 1

إذا أضفنا 1 إلى مربعات الأعداد الأولية التي آحادها 9 فيكون العدد يقبل القسمة على 10

وإذا طرحنا 1 من مربعات الأعداد التي آحادها 1 يكون العدد من مضاعفات 10

7 إذا كان P عدداً أولياً و $P \geq 5$ اثبت أن P^2+2 عدد مؤلف.

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

$=(P+1)(P-1)+3$

« P عدد أولي و $P \geq 5 \Leftarrow 3 \nmid P$ »

وبالتالي إما $3 \backslash (P+1)$ أو $3 \backslash (P-1)$

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

$b=aq+r$ ومنه نتيجة $(b,a)=(a,r)$

1- مالة $3 \backslash (P+1) \Longrightarrow (P+1,3)=3$

$\rightarrow (P^2+2, P+1)=(P+1,3)=3 \rightarrow$ ومنه P^2+2 مؤلف $3 \backslash P^2+2$

الموضوع: .....

1 1 3 17

مثالة $3 \setminus (P-1)$ $\leftarrow (P-1,3)=3$

$\rightarrow (P^2+2, P-1) = (P-1,3) = 3$

ففي كلا الحالتين $3 \setminus P^2+2$ إذاً $P+2$ عدد مؤلف.

8 $n>0$ ، اثبت أن $2^{4n+2}+1$ عدد مؤلف برهن أن $5 \setminus 2^{4n+2}+1$

بالاستقراء ← فإن العدد مؤلف.

9 977 عدد أولي .

$31^2 < 977 < 32^2$ .....

$n = 10541$

$102^2 < n = 10541 < 103^2$

$103^2 - n = 10609 - 10541 = 68$

$104^2 - n = 10816 - 10541 = 275$

$105^2 - n = 11025 - 10541 = 484 = 22^2$

$n = (105+22)(105-22) = 127 \times 83$

1 أوجد أعداداً صحيحة x, y, z تحقق العلاقة

$\gcd(198, 288, 512) = 198x + 288y + 512z$

معادلات ديوفانتس.

$ax+by=c$ حيث $a,b,c \in \mathbb{Z}$ نبحث عن x,y التي تحقق هذه المعادلة.

مثال: $2x+6y=7$ ليس لها حل لأن الطرف الأيسر عدد زوجي دائماً لا يساوي 7

مثال: $3x+6y=18$ حلولها: $(4,1)$ ، $(2,2)$ ، $(-6,6)$ ، ...

مبرهنة ^^ : إذا كانت المعادلة $ax+by=c$ ؛ $a,b,c \in \mathbb{Z}$ و a,b عددين غير صفريين معاً، يكون لهذه المعادلة حل إذا وفقط إذا كان $d=(a,b)$ يقسم العدد c $(d \setminus c)$

وإذا كان (x_0, y_0) حلاً خاصاً فإن جميع حلول المعادلة تعطى:

$x = x_0 + \frac{b}{d}t \quad , y = y_0 - \frac{a}{d}t \quad : t \in \mathbb{Z}$

البرهان ^^ : إذا كان $d=(a,b)$ ، $a=rd$ ، $b=sd$ $(r,s)=1$

إذا كان (x_0, y_0) حل للمعادلة فإن: $ax_0+by_0=c \rightarrow rdx_0+sdy_0=c$

$d(rx_0+sy_0)=c \rightarrow d \setminus c$

بالعكس إذا كان $d \setminus c$ ← بما أن $c=t.d$ فإن d يكتب $d=(a,b)$ كتركيب خطي لـ a,b

$d=an+bm \Longrightarrow t.d=c=a.tn+btm$

إذاً يوجد عدد $x_0=tn$, $y_0=tm$ بحيث يكون $c=ax_0+by_0$ للمعادلة

حل.

لنثبت العلاقات.

(x_0,y_0) حل للمعادلة أي $ax_0+by_0=c=ax+by$

$a(x-x_0)=b(y_0-y)$

$a=a_0d$, $b=b_0d$; $(a_0,b_0)=1$

$a_0d(x-x_0)=b_0d(y_0-y)$

$a_0(x-x_0)=b_0(y_0-y)$

بما أن $(a_0,b_0)=1$: $b_0 \mid (x-x_0)$

$\rightarrow x-x_0=t.b_0 \longrightarrow x=x_0+t\,b$

$y=y_0-\frac{a}{d}t \longleftarrow y_0-y=a_0t \longleftarrow a_0 \mid y_0-y$

مثال:

$172x+20y=1000$

$d(172,20)=4$

$172=8.20+12$

$20=1.12+8$

$12=1.8+4 \longrightarrow d=4$

$4=12-1.8=12-1.(20-1.12)$

$4=2.12-1.20=2(172-8.20)-1.20 \Rightarrow 4=2.172-17.$

$250\times4=1000=500(172)+(-4250)20$

$\longrightarrow x_0=500$, $y_0=-4250$

بالتالي جميع الحلول من الشكل:

$x=x_0+\frac{b}{d}t=500+5t$

$y=y_0-\frac{a}{d}t=-4250-43t$

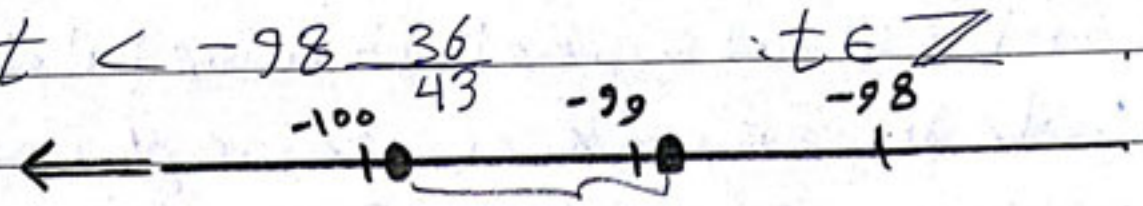
إذا طلب الحلول الموجبة فقط نكتب.

$500+5t>0 \longrightarrow t>-100$

$-4250-34>0 \Longrightarrow t<\frac{-4250}{43}=-98\frac{36}{43}$

$t \in \mathbb{Z}$: $-100 < t < -98\frac{36}{43}$

$t = -99$



$x = 500 - 99 \times 5 = 5$

$y = -4250 + 43 \times 99 = 7$

ثلاثيات فيثاغورث

نأخذ المعادلة $x^2 + y^2 = z^2$ حيث $x, y, z \in \mathbb{Z}^+$ إذا تحقق (x,y,z) المعادلة
نسميها ثلاثية فيثاغورث وإذا كان $\gcd(x,y,z) = 1$ نسميها ثلاثيات فيثاغورث
الأولية مثل $(3,4,5) = 1$

تمهيدية (1): إذا كانت $(x,y,z) = 1$ ثلاثية فيثاغورث أولية فإن x, y, z أولية مثنى مثنى
البرهان: نفرض أن $(x,y) = d > 1 \Leftarrow$ يوجد عدد أولي $p \mid d \Leftarrow p \mid x, p \mid y$
أي $p \mid x^2$, $p \mid y^2$ ومنه p يقسم أي تركيب خطي لهما أي
$p \mid x^2 + y^2 = z^2 \Leftarrow p \mid z$ ومنه يناقض كون $(x,y,z) = 1$
كذلك بنفس الطريقة نجد أن $(x,z) = 1$ و $(y,z) = 1$

تمهيدية (2): إذا كان $(x,y,z) = d$ و $x = x_0 d$, $y = y_0 d$, $z = z_0 d$
فإن $(x_0, y_0, z_0) = 1$

ملاحظة: إذا كان (x_0, y_0, z_0) ثلاثية فيثاغورث أولية فإن (kx_0, ky_0, kz_0) هي
ثلاثية فيثاغورث

تمهيدية (3): إذا كان $(x,y,z) = 1$ ثلاثية فيثاغورث أولية فإن العددين x, y أحدهما
فردي والآخر زوجي حيث $x^2 + y^2 = z^2$

البرهان: وجدنا أن $(x,y) = 1$ أي لا يمكن أن يكونا زوجيان
نفرض أن x, y فرديان فتعاقبان $x^2 = 8M_1 + 1$
$y^2 = 8M_2 + 1$
$x^2 + y^2 = 8(M_1 + M_2) + 2 = 8K + 2 = z^2$
وهذا غير ممكن لأنه إذا كان z فردي فإنه يكتب على الشكل $z = 8M + 1$
وإذا كان z زوجي فإن $z^2 = 4n^2$
بالتالي x, y أحدهما فردي والآخر زوجي

تمهيدية (4): إذا كان $a, b, c \in \mathbb{Z} : a \cdot b = c^n$ و $(a,b) = 1$ فإنه يوجد عددين a_1, b_1
بحيث يكون $a = a_1^n$, $b = b_1^n$

مبرهنة: إن جميع الحلول الصحيحة غير الصفرية للمعادلة فيثاغورث $x^2+y^2=z^2$ حيث y عدد زوجي و x عدد فردي بالإضافة لـ (x,y,z) تعطى بالعلاقة: $z=r^2+s^2$, $y=2rs$, $x=r^2-s^2$ حيث r,s أحدهما زوجي والآخر فردي، $(r,s)=1$

البرهان: y عدد زوجي أي $y=2y_1$ و x عدد فردي $\leftarrow z$ فردي نجد أن:

$$y^2=4y_1^2=z^2-x^2=(z+x)(z-x)$$

$$y_1^2=\left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right)$$

حسب التمهيدية (4) نجد بأن $\frac{z+x}{2}$, $\frac{z-x}{2}$ أوليان فيما بينهما نسبياً لأن إذا وجد d قاسم مشترك اعظم لهما فإنه يقسم مجموعهما z وتقسم فرقهما x بالتالي $d=1$

$$\frac{z+x}{2}=r^2 \quad , \quad \frac{z-x}{2}=s^2$$

ومنه

$$z=r^2+s^2$$

$$x=r^2-s^2$$

$$y_1^2=r^2.s^2 \rightarrow y=2.r.s$$

كذلك

$$x^2+y^2=(r^2-s^2)^2+4r^2s^2=r^4-2r^2s^2+s^4+4r^2s^2=r^4+2r^2s^2+s^4=(r^2+s^2)^2=z^2$$

مثال: اوجد ثلاثيات فيثاغورث الأولية من أجل $y=24$

$$y=24=2r.s \Rightarrow 12=r.s \rightarrow r=4, s=3$$

$$\rightarrow x=16-9=7 \quad , z=16+9=25 \rightarrow (7,24,25)$$ ثلاثية فيثاغورث أولية

أو $r=12$, $s=1$: $(12,1)=1$

$$x=12^2-1=143 \quad , z=12^2+1=145$$

$(143,24,145)$ ثلاثية فيثاغورث أولية.

انتهت المحاضرة

التطابقات

تعريف: ليكن $a,b\in\mathbb{Z}$ و $m\in\mathbb{Z}^+$ نقول إن العدد a يطابق b بالمقاس m ونكتب $a\equiv b\pmod m$ إذا كان $m\mid a-b$ وإذا كان $m\nmid a-b$ فإننا نقول إن a لا يطابق b بالمقاس m ونكتب $a\not\equiv b\pmod m$

مثال: $3^7\equiv 2\pmod 7$

صفوف البواقي: $m\in\mathbb{Z}^+$ و $n\in\mathbb{Z}$ فإنه يوجد عددان وحيدان r,q بحيث يكون: $n=mq+r$ ، $0\le r<m$ القيم التي يأخذها r هي:

$r_i=0,1,2,\dots,m-1$ عدد ها m لنضع جميع الأعداد الصحيحة التي باقي قسمتها على m يساوي أحد الأعداد r_i في صف واحد ونسميه صف الباقي r_i

نخصص بالتالي على m من هذه الصفوف ونلاحظ أنه إذا كان الفرق بين عددين صحيحين مضاعفاً لـ m فإنهما يقعان في صف واحد وأن الفرق بين أي عددين من صف واحد هو مضاعف لـ m نسمي هذه الصفوف صفوف البواقي للعدد m

مثال: $m=6$ ← صفوف البواقي هي $0,1,2,3,4,5$

صف الباقي $r=0$ هو $\{\dots,-12,-6,0,6,12,\dots\}$

صف الباقي $r=1$ هو $\{\dots,-11,-5,1,7,13,\dots\}$

صف الباقي $r=2$ هو $\{\dots,-10,-4,2,8,14,\dots\}$

صف الباقي $r=3$ هو $\{\dots,-9,-3,3,9,15,\dots\}$

صف الباقي $r=4$ هو $\{\dots,-8,-2,4,10,16,\dots\}$

صف الباقي $r=5$ هو $\{\dots,-7,-1,5,11,17,\dots\}$

مجموعة البواقي التامة:

تسمى مجموعة الأعداد الصحيحة A التي عندما نقسمها على m وكل عنصر فيها تنتمي إلى صف باقي واحد بالمقاس m، مجموعة البواقي بالمقاس m هي:

$A=\{0,1,2,\dots,m-1\}$

مثال: $m=5$ ← $A=\{0,1,2,3,4\}$

هل A_1 مجموعة بواقي تامة؟ $A_1=\{0,11,22,33,59\}$

الجواب: نعم، A_1 مجموعة بواقي تامة.

★ المجموعة $A=\{0,1,2,\dots,m-1\}$ نسميها مجموعة البواقي التامة الصغرى

مثال جانبي : $-500 \equiv 4 \pmod 6$ ← -500 ينتمي إلى صف الباقي 4 بالقاسم 6.
$500 \equiv 2 \pmod 6$ ← 500 ينتمي إلى صف الباقي 2 بالقاسم 6.

كنتيجة : إذا كان $a \equiv b \pmod n$ فإن a, b ينتميان إلى صف باقي واحد

إذا كان $r < n$: $n = mq + r \Leftarrow n \equiv r \pmod m$

$n - r = mq \Rightarrow m \mid n - r$

خواص التطابقات :

أ- التطابق (≡) علاقة تكافؤ أي :

1) $a \equiv a \pmod m$; $a \in \mathbb{Z}$ "انعكاسية"

2) $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ "تناظرية"

3) $a \equiv b \pmod m \wedge b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$ "متعدية"

ب- إذا كان $a \equiv b \pmod m$; $k \in \mathbb{Z}$

فإن : $k.a \equiv k.b \pmod m$

ج- إذا كان $a \equiv b \pmod m \wedge c \equiv d \pmod m$

فإن : $a \pm c \equiv b \pm d \pmod m$

د- إذا : 1) $a \equiv b \pmod m$

2) $c \equiv d \pmod m$ ← $a.c \equiv b.d \pmod m$

لأنه نضرب "c" في (1) ← $c.a \equiv c.b \pmod m$ ← حسب خاصية المتعديتين

من (2) $\xrightarrow{(\times b)}$ $a.c \equiv b.d \pmod m$ ← $c.b \equiv b.d \pmod m$

هـ- إذا كان $a \equiv b \pmod m$ فإن : $a^n \equiv b^n \pmod m$; $n \geq 1$

ز- إذا كان $a \equiv b \pmod m$ و الدالة $f(x) = \sum_{i=1}^{n} a_i x^i$ "كثيرة حدود"

فإن : $f(a) \equiv f(b) \pmod m$

ح- بما أن $a \equiv b \pmod m$ فإن $a^i \equiv b^i \pmod m$

و لنضرب الطرفين بقيمة عددية :

$(i = 1, \dots, n) : a_i a^i \equiv a_i b^i \pmod m$

$$\sum_{i=1}^{n} a_i a^i \equiv \sum_{i=1}^{n} a_i b^i \pmod m$$

$f(a) \equiv f(b) \pmod m$ ←

ع) إذا كان $(*)\ k.a \equiv k.b \pmod m$ و $(k,m)=d$ ،
فإنّ: $a \equiv b \pmod{\frac{m}{d}}$
لأنّ: بما أن $d=(k,m)$ فيمكن أن نكتب:
$k=k_0 d \ , \ m=m_0 d$
و $(k_0,m_0)=1$ ، وبما أن $k.a=k.b \pmod m$
فإن: $k(a-b)=Mm \Leftarrow k_0 d(a-b)=Mm_0 d$
أي أن $k_0(a-b)=Mm_0$ $\Leftarrow m_0 \mid k_0(a-b)$
ولما كان $(k_0,m_0)=1$ ينتج أن: $m_0 \mid a-b$
أي $a \equiv b \pmod{m_0}$ حيث $m_0=\frac{m}{d}$
// أما إذا كان $(k,m)=1 \Leftarrow a \equiv b \pmod m$
مثال: $10 \equiv 6 \pmod 4 \Leftarrow 5 \not\equiv 3 \pmod 4$
$(10,4)=2=d \Rightarrow 5 \equiv 3 \pmod 2$
صح) إذا كان $a \equiv b \pmod m$ و $n \mid m$ فإنّ: $a \equiv b \pmod n$ (سوف لم نكتب)
ك) المذاعون:
إذا كان $a,b \in \mathbb{Z}, m_i \in \mathbb{Z}^+ \ ; \ i=1,\dots,k$ ، $a \equiv b \pmod{m_i}$
فإن: $a \equiv b \pmod m$ ؛ $m=l.c.m(m_1,\dots,m_k)$
وإذا كان m_i أولية مثنى مثنى أي هي أولية فيما بينها فإنّ:
$m=m_1.m_2\dots m_k$
// نتيجة: إذا كان: $m=p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_r^{\alpha_r}$
فإن: $a \equiv b \pmod{p_i^{\alpha_i}} \Rightarrow a \equiv b \pmod m$ حيث $i=1,\dots,k$
ق) إذا كان $a \equiv b \pmod{p^r}$: $r \geq 1$ و p أولي
فإنّ: $a^{p^s} \equiv b^{p^s} \pmod{p^{r+s}}$ ؛ $s \geq 0$
الإثبات: بطريقة الاستقراء الرياضي
الخطوة الأساسية: من أجل $s=0 \Leftarrow a \equiv b \pmod{p^r}$ محققة
خطوة الاستقراء: لنفرض العلاقة صحيحة من أجل $s=k$
$\Leftarrow a^{p^k} \equiv b^{p^k} \pmod{p^{r+k}}$
و لنثبت صحتها من أجل $s=k+1$

الموضوع : .....

لدينا $a^{p^k} - b^{p^k} = M.p^{r+k}$

$a^{p^k} = b^{p^k} + M.p^{r+k}$

$(a^{p^k})^p = a^{p^k \cdot p} = a^{p^{k+1}} = (b^{p^r} + M p^{r+k})^p$

نفكر بطريقة ثنائي الحد نيوتن.

$= b^{p^{k+1}} + \frac{p}{1!}(b^{p^k})^{p-1}.(M.p^{r+k}) + \frac{p(p-1)}{2!}(b^{p^k})^{p-2}(M.p^{r+k})^2$

$+ \cdots + M^p (p^{r+k})^p$

نلاحظ أن قوى p ابتداءً من الحد الثاني هي :

$r+k+1$ ، $2r+2k+1$ ، ... وصغيرها أكبر من $r+k+1$ حتى $2r+2k$.

إذاً: جميع الحدود ابتداءً من الحد الثاني، يترك عزلاً بالمقاس p^{r+k+1}

$\Longrightarrow a^{p^{k+1}} \equiv b^{p^{k+1}} \pmod{p^{r+k+1}}$

وبالتالي صحة

أي العلاقة صحيحة من أجل $s \geq 0$

ملاحظة إضافية: يقبل العدد القسمة على 7 إذا كان مجموع أرقامه من مضاعفات الرقم 7

يقبل العدد $N = a+10b$ القسمة على 7 إذا قبل العدد $b-2a$ القسمة على 7

مثال: العدد $N=3741$ فإن $N = 1+10(374)$ ومنه

$b-2a = 374-2 = 372$ نطبق مرة أخرى

$372 = 2+10(37)$

$b-2a = 37-4 = 33$ وبما أن $7 \mid 33$ فإن $7 \mid N$ (N يقبل القسمة على 7)

مثال آخر: العدد 1470 فإن $N = 0+10(147)$

ومنه $b-2a = 147-0 = 147$ نطبق مرة أخرى.

$147 = 7+10(14)$

ومنه $b-2a = 14-14 = 0$ ومنه فإن $7 \mid N$

(N يقبل القسمة على 7)

تمرين (1) :

اثبت أن الفرقة بين أي عدد صحيح N بالنظام العشري ومجموع أرقامه يقبل القسمة على 9

$$N=\sum_{i=0}^{n} a_i 10^i = a_0 + a_1 \times 10 + \cdots + a_n \times 10^n$$

$$10 \equiv 1 \pmod 9$$

$$10^i \equiv 1 \pmod 9$$

$$a_i 10^i \equiv a_i \pmod 9 \qquad : i = 0, 1, \cdots, n$$

$$N \equiv \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i \pmod 9$$

$$N - \sum_{i=0}^{n} a_i \equiv \pmod 9$$

مثال :

$$N = 3741 = 1 + 4 \times 10 + 7 \times 10^2 + 3 \times 10^3$$

$$N = 3741 \equiv 1+4+7+3 \pmod 9 \rightarrow N = 3741 \equiv 15 \pmod 9$$

$$3741 - 15 = 3726 \equiv 0 \pmod 9$$

★ لمعرفة ميزان عدد: نحذف من مجموع أرقامه 9 أو مضاعفها مثلاً ميزان 3741 هو $15 - 9 = 6$

مثال : أوجد أصغر عدد صحيح موجب k يحقق العلاقة :

" أي $33(26)^2 \equiv k \pmod{31}$ " : $31 \backslash 33(26)^2 - k$

$$33 \equiv 2 \pmod{31}$$

$$26 \equiv -5 \pmod{31} \Rightarrow 26^2 \equiv 25 \pmod{31}$$

$$(33)(26)^2 \equiv 50 \pmod{31}$$

$$(33)(26) \equiv 19 \pmod{31} \Rightarrow k = 19$$

مثال : أوجد باقي قسمة $\sum_{i=1}^{1000} k!$ على 24

$$\sum_{k=1}^{1000} k! = 1! + 2! + 3! + \cdots + 1000!$$

$$4! = 24 \,, 5! = 24.5$$

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

حل تمارين الكتاب ص 46

5) هل العبارات التالية صحيحة أم خاطئة وإذا كانت صحيحة فاثبت صحتها وإن كانت خاطئة فأعط مثال يبين ذلك.

① إذا كان $a\backslash b$, $a\backslash c \Leftarrow a^2\backslash bc$

الحل: بما أن $a\backslash b \Leftarrow b=k_1.a \; ; k_1\in\mathbb{Z}$

و بما أن $a\backslash c \Leftarrow c=k_2.a \; ; k_2\in\mathbb{Z}$

$\Rightarrow b.c=k_1.k_2.a^2 \longrightarrow a^2\backslash b.c$ صحيحة ^^

② إذا كان $a\backslash b \longleftrightarrow ac\backslash b.c$ حيث $c\neq 0$ صحيحة دوما"

③ إذا كان $a\backslash b+c$ فإن إما $a\backslash b$ أو $a\backslash c$ خاطئة

مثال: $3\backslash 5+4$ و لكن: 3×5 , 3×4

④ إذا كان $a\backslash b^2+1$ فإن $a\backslash b^4+1$ خاطئة

مثال: $5\backslash 3^2+1$ و لكن $5\times 3^4+1=82$

⑤ إذا كان $a^2\backslash b^3$ فإن $a\backslash b$ خاطئة

$8^2\backslash 4^3$ و لكن 8×4

⑥ إذا كان $a^2\backslash n \wedge b^2\backslash n \wedge a^2\leq b^2 \Leftarrow a\backslash b$ خاطئة

$2^2\backslash 36 \wedge 3^2\backslash 36 \wedge 2^2\leq 3^2$, لكن $2\not\backslash 3$

إذا أن 2×3

⑨ $\gcd(198,288,512)=198x+288y+512z$

الحل:

$512=288\times 1+224$

$288=224\times 1+64$

$224=64\times 3+32$

$64=32\times 2+0 \longrightarrow \gcd(512,288)=32$

$198=6\cdot 32+6$

$32=6\times 5+2$

$6=3\times 2+0$

$\longrightarrow \gcd(198,288,512)=2$

$2=1\times 32-5.6$

$$2 = 1X32 - 5(198 - 6X32)$$
$$= -5.198 + 31X32$$
$$= -5X198 + 31(224 - 3X64)$$
$$= -5X198 + 31X224 - 93X64$$
$$= -5X198 + 31X224 - 93(288 - 1X224)$$
$$= -5X198 + 124X224 - 93X288$$
$$= -5X198 + 124(512 - 1X288) - 93X288$$
$$= \underbrace{-5}_{x} X198 - \underbrace{217}_{y} X288 + \underbrace{124}_{z} X512$$

$x = -5$ ، $y = -217$ ، $Z = 124$

أوجد الحلول الموجبة للمعادلات:

$$221x + 91y = 117$$

$$\left.\begin{aligned} 221 &= 2X91 + 39 \\ 91 &= 2X39 + 13 \\ 39 &= 3X13 + 0 \end{aligned}\right\} \rightarrow d = (221, 91) = 13$$

$13 \mid 117 = 13X9$

إذن للمعادلة حل

$$13 = 91 - 2X39$$
$$= 91 - 2(221 - 2X91)$$
$$13 = -2X221 + 5X91$$
$$117 = (-18)(221) + (45)(91)$$

بضرب الطرفين بـ 9:

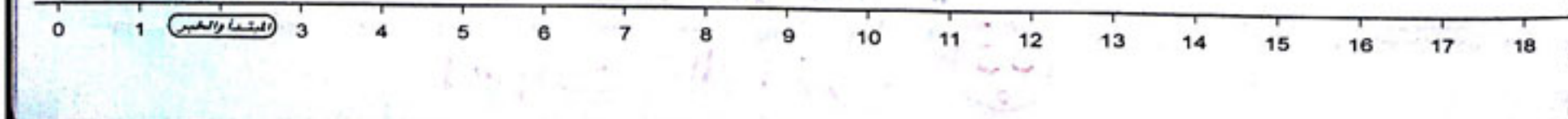
إذن إنّ: $(-18, 45)$ حل للمعادلة: $x_0 = -18$ ، $y_0 = 45$

وجميع الحلول تعطى بالعلاقات:

$$x = x_0 + \frac{b}{d}t = -18 + 7t$$
$$y = y_0 - \frac{a}{d}t = 45 - 17t$$

$$\left.\begin{aligned} -18 + 7t > 0 &\rightarrow t > \frac{18}{7} = 2\frac{4}{7} \\ 45 - 17t > 0 &\rightarrow t < \frac{45}{17} = 2\frac{11}{17} \end{aligned}\right\} \rightarrow 2\frac{4}{7} < t < 2\frac{11}{17}$$

إذن x تقبل حلول موجبة للمعادلة



الموضوع : .....

4) أوجد جميع ثلاثيات فيثاغورث من أجل $y=28$

$y=28=2(r.s) \longrightarrow r.s=14$

لدينا حالتين:

① $r=14$, $s=1$ $\longleftarrow$ $(r^2-s^2, 2rs, r^2+s^2)$

$(195, 28, 197)$

② $r=7$, $s=2$ $\longleftarrow$ $(45, 28, 53)$

إذا كان: $Z=125$ $\longleftarrow$ $Z=r^2+s^2=10^2+5^2$

$\Longrightarrow r=10$, $s=5$ مرفوضة

r و s أوليان فيما بينهما

$Z=(11)^2+(2)^2$; $r=11, s=2$ مقبولة

$x=r^2-s^2=121-4=117$

$y=2.r.s=2(11)(2)=44$

$(117, 44, 125)$

إذا كان: $x=21$

$x=r^2-s^2=21$

$r^2-s^2=(r+s)(r-s)=21$

① $r+s=7$, $r-s=3$

$2r=10 \longrightarrow r=5$

$2s=4 \longrightarrow s=2$

مقبولة إذاً:

الثلاثية $(21, 20, 29)$

② $r+s=21$, $r-s=1$

$2r=22 \longrightarrow r=11$

$2s=20 \longrightarrow s=10$

r و s أوليان فيما بينهما مقبولة ^_^

الثلاثية $(21, 220, 221)$

التطابقات الخطية $ax \equiv b \pmod m$ و المطلوب إيجاد قيمة x

نفرض أن التطابقة حل x_0 :

$ax_0 \equiv b \pmod m$

$ax_0 - b \equiv my_0 \Rightarrow ax_0 - my_0 = b$ وهي معادلة ديوفانتس

يؤول حل التطابق الخطي $ax \equiv b \pmod m$ إلى حل معادلة ديوفانتس $ax-my=b$

شرط $d=(a,m)$ يقسم b

انتهت المحاضرة

التطابقات الخطية:

هو معادلة من الشكل : $ax \equiv b \pmod m$ حيث أن : $x, m, a, b \in \mathbb{Z}$ و $m > 1$ و x مجهول
و m, a, b معاليم والمسألة تكون إيجاد قيم x التي تحقق هذه التطابقة.

يوجد حل x_0 للتطابقة إذا وفقط إذا كان:

$$ax_0 \equiv b \pmod m \iff ax_0 - b \equiv y_0 m \iff ax_0 - my_0 \equiv b$$
$$\iff d \mid b \quad ; \quad d = (a, m)$$

(وذلك لأن هذه التطابقة يمكن رده إلى شكل معادلة ديوفانتس ويكون لهذه المعادلة حل إذا تحقق التكافؤ أعلاه)

ملاحظة: نعتبر الحلول المتطابقة بالمقاس m هي حل واحد للتطابق الخطي أي أن الحلول المختلفة هي الحلول غير المتطابقة بالمقاس m

مبرهنة: يكون للتطابقة الخطي $ax \equiv b \pmod m$ حلاً إذا وفقط إذا كان $d \mid b$ حيث أن $d = (a, m)$ وإذا كان $d \mid b$ فإن للتطابقة الخطي d حلاً مختلفاً.

الإثبات: إن حل التطابقة يكافئ حل معادلة ديوفانتس الخطية وقد أثبتنا أن الشرط اللازم والكافي كي يكون للمعادلة حل هو أن يكون $d \mid b$ كما أثبتنا أنه إذا كان x_0, y_0 هو حل خاص لمعادلة ديوفانتس فإن الحل الكامل لها هو:

$$x = x_0 + \frac{m}{d} t \quad , \quad y = y_0 - \frac{m}{d} t \quad ; t \in \mathbb{Z}$$

لنأخذ الحلول المقابلة لقيم t التالية:

$$t = 0, 1, 2, \dots, d-1$$

أي لنكتب: $x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \dots, x_0 + \frac{(d-1)m}{d}$

ولنثبت أن هذه الحلول كلها غير متطابقة بالمقاس m إذ لو تطابقت مثلاً موافقتان للقيمتين t_1, t_2 لأمكن أن نكتب:

$$x_0 + \frac{m}{d} t_1 \equiv x_0 + \frac{m}{d} t_2 \pmod m \quad ; \quad 0 \le t_1 \le t_2 \le d-1$$

ومنه:
$$\frac{m}{d} t_1 \equiv \frac{m}{d} t_2 \pmod m$$

ولدينا: $\left(\frac{m}{d}, m\right) = \frac{m}{d}$ ومن خواص التطابقات يمكننا الاختصار $t_1 \equiv t_2 \pmod d$ وهذا تناقض

وذلك لأننا نقسم t أي الأعداد $t=0,1,2,\dots,d-1$ كلها غير متطابقة بالمقاس d.

لنثبت أخيراً أنه أي حل من الحلول $(x_0+\frac{m}{d}t)$ حيث $t\le d$ يطابقه بالمقاس m واحد من الحلول السابقة التي عددها يساوي d في الحقيقة بما أن $t\ge d$ فهي تكتب على الشكل $t=qd+r$ حيث $0\le r<d$

أي $0<r\le d-1$ نعوض في عبارة الحل نجد:

$$x_0+\frac{m}{d}t=x_0+\frac{m}{d}(qd+r)=x_0+mq+\frac{m}{d}r$$

ومنه:

$$x_0+\frac{m}{d}t\equiv(x_0+\frac{m}{d}r)\pmod m$$

و $x_0+\frac{m}{d}r$ هو أحد الحلول المذكورة وهو المطلوب

نتيجة: إذا كان $d=(a,m)$ فإن للتطابقة الخطية $ax\equiv b\pmod m$ حل وحيد.

وإذا كان المقاس عدداً أولياً P وكان $P\nmid a$ فإن للتطابقة $ax\equiv b\pmod m$ حل وحيد أيضاً.

تمرين (1): حل المعادلة (التطابقة) $9x\equiv 21\pmod{30}$

الحل: إن القاسم المشترك الأعظم $d(9,30)=(3^2,3\times5\times2)=3$

وبما أن $3\nmid 21$ فإن للمعادلة حل وهو يملك ثلاثة حلول مختلفة بالمقاس 30.

نكتب الحل على شكل معادلة ديوفانتس التالية $9x-30y=21$

لحل هذه المعادلة نحصل على حل (x_0,y_0) ونلاحظ أن $x_0=9$ هو حل لهذه المعادلة لأن: $9\cdot9-8\cdot9=21\pmod{30}$

وبالتالي الحلول المختلفة تعطى بالعلاقة:

$$x=x_0+\frac{30}{3}t=9+10t\ ;\ t=0,1,2$$

$$t=0\longrightarrow x_0=9\equiv39\pmod{30}\equiv-21\pmod{30}$$
$$t=1\longrightarrow x_1=-1\equiv29\pmod{30}\equiv59\pmod{30}$$

$t=2 \longrightarrow x_2 = -1 \equiv 19 \pmod{30} = 49 \pmod{30}$

أي أن الحلول الثلاثة المختلفة $\{29, 19, 9\}$

ملاحظة: نختصر طرفي التطابقة على 3 فنجد: $3x \equiv 7 \pmod{10}$

ولما كان $(3,10)=1$ فلهذا التطابقة حلول هي بالقاعدة 10

ونبتعويض x بأحد الأعداد من 0 إلى 9 نجد أن: $x=9$ يحقق التطابقة أي:

$9x = 21 \pmod{30}$ وهو يحقق التطابقة الأصلية $x_0 = 9 \pmod{10}$

ونحصل على الحلول الثلاثة بكتابة $x = x_0 + 10t$ حيث $t = 0, 1, 2$ و $x_0 = 9$

$x = 29 \pmod{30}$, $x = 19 \pmod{30}$ ← $x \equiv 9 \pmod{30}$

تمرين 2: حل التطابقة الخطية: $8x \equiv 2 \pmod{6}$

الحل: بما أن: $d = (8,6) = 2$ و $d \mid 2$ فإن التطابقة حل نكتب التطابقة على شكل معادلة ديوفانتس التالية: $8x - 6y' = 2 \longrightarrow 8x + 6y = 2 ; y = -y'$

نلاحظ أن $x = 1$ هي حل التطابقة لأن:

$8 \equiv 2 \pmod{6}$

لأو يمكن إيجاد الحل من حل معادلة ديوفانتس) وبالتالي:

نعطى الحلول المختلفة للمعادلة كما يلي: $x = x_0 + \frac{6}{d}t = 1 + 3t$; $t = 0, 1$

$t=0 \longrightarrow x_0 \equiv 1 \equiv 7 \pmod{6} \equiv -5 \pmod{6}$

$t=1 \longrightarrow x_1 \equiv 4 \equiv 10 \pmod{6} \equiv -2 \pmod{6}$

أي الحلان المختلفان للتطابقة هما $\{4, 1\}$

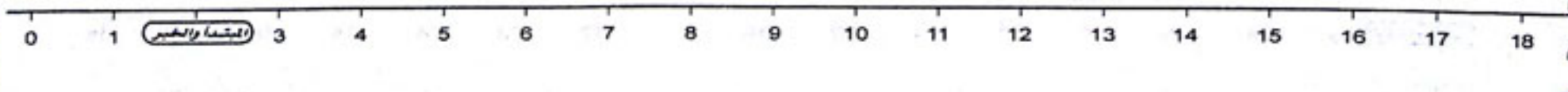
تمرين 3: أوجد حلول التطابق $6x \equiv 2 \pmod{9}$

الحل: نلاحظ أن $(6,9) = 3$ و $3 \nmid 2$ وليس للتطابقة أي حل

الكسور البسيطة المستمرة المنتهية:

إن إيجاد حلول التطابقات الخطية باستخدام خوارزمية قليدس أو بالتجريب تصبح طويلة أو متعذرة حين يكون المقاس عدداً كبيراً لذا نستخدم طريقة الكسور البسيطة المستمرة التي سنشرحها في هذه الفقرة لحل التطابقات الخطية وحل معادلات ديوفانتس الخطية

تعريف: الكسور البسيطة المستمرة المنتهية هي كسور تكتب كما يلي:



$$\frac{A}{B} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}}$$

بحيث أن $a_1 \in \mathbb{Z}$ و $a_2, a_3, \dots, a_n \in \mathbb{Z}^+$ ونكتبه لاختصار بالشكل:

$$\frac{A}{B} = \langle a_1, a_2 \dots, a_n \rangle$$

ويتم شرح طريقة كتابة هذا الكسر من خلال المثال التالي

$$\frac{-5}{4} = \frac{-8+3}{4} = -2 + \frac{3}{4} = -2 + \frac{1}{\frac{4}{3}} = -2 + \frac{1}{1+\frac{1}{3}}$$

$$\Rightarrow \frac{-5}{4} = \langle -2, 1, 3 \rangle$$

تمرين:

أكتب الكسر $\frac{32}{19}$ على شكل كسر بسيط منتهي ثم استنتج كتابة الكسر $\frac{19}{32}$

الحل:

$$\frac{32}{19} = 1 + \frac{13}{19} = 1 + \frac{1}{\frac{19}{13}} = 1 + \frac{1}{1 + \frac{1}{\frac{13}{6}}}$$

$$= 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{6}}} \Rightarrow \frac{32}{19} = \langle 1, 1, 2, 6 \rangle$$

$$\Rightarrow \frac{19}{32} = 0 + \frac{1}{\frac{32}{19}} \Rightarrow \frac{19}{32} = \langle 0, 1, 1, 2, 6 \rangle$$

مبرهنة: إذا كان لدينا الكسر المستمر المنتهي $\langle a_1, a_2, \dots, a_n \rangle$

ولنأخذ الرموز التالية: سأرمز لها بـ ♡ لأننا سنستخدمها فيما بعد

$q_1 = 1$ و $p_1 = a_1$ فيكون التقريب الأول هو $c_1 = \frac{p_1}{q_1} = a_1$

$P_2 = a_2 \times q_1 + 1$ و $q_2 = a_2$ فيكون التقريب الثاني هو: $c_2 = \frac{P_2}{q_2} = a_1 + \frac{1}{a_2}$

$P_3 = a_3 P_2 + P_1$ و $q_3 = a_3 q_2 + q_1$ فيكون التقريب الثالث هو: $c_3 = \frac{P_3}{q_3} = a_1 + \frac{1}{a_2 + \frac{1}{a_3}}$

وبفرض أن: $P_i = a_i P_{i-1} + P_{i-2}$ و $q_i = a_i q_{i-1} + q_{i-2}$

التقريب من المرتبة n للكسر البسيط هو: $C_n = \frac{P_n}{q_n} = \frac{A}{B}$

الاثبات:

نستخدم الاستقراء الرياضي

1- خطوة البداية: محققة من أجل $n=1$ لأن $c_1 = \frac{P_1}{q_1} = a_1$

محققة من أجل $n=2$ لأن: $c_2 = \frac{P_2}{q_2} = \frac{a_1 \cdot a_2 + 1}{a_2} = a_1 + \frac{1}{a_2}$

خطوة الاستقراء: نفرض صحة العلاقة من أجل $n=K$ أي:

$$c_k = \frac{P_k}{q_k} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\vdots + \cfrac{1}{a_{k-2} + \cfrac{1}{a_{k-1} + \frac{1}{a_k}}}}} = \frac{a_k P_{k-1} + P_{k-2}}{a_k q_{k-1} + q_{k-2}}$$

ونبرهن من أجل $n=k+1$ وبما أن C_{k+1} يختلف عن c_k بأن الحد الأخير هو $a_k + \frac{1}{a_{k+1}}$ بدلاً من a_k لذلك نعوض كل a_k في العبارة السابقة بـ $a_k + \frac{1}{a_{k+1}}$ فنحصل على C_{k+1} أي:

$$C_{k+1} = \frac{(a_k + \frac{1}{a_{k+1}})P_{k-1} + P_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}} = \frac{\{(a_k \cdot q_{k+1} + 1)P_{k-1} + q_{k+1} P_{k-2}\}/a_{k+1}}{\{(a_k q_{k+1} + 1)q_{k-1} + a_{k+1} q_{k-2}\}/a_{k+1}}$$

ومنه: $C_{k+1} = \frac{a_{k+1}(a_k P_{k-1} + P_{k-2}) + P_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1} P_k + P_{k-1}}{a_{k+1} q_k + q_{k-1}}$

$$\Rightarrow c_{k+1} = \frac{p_{k+1}}{q_{k+1}} = \frac{A}{B}$$

أي أن العلاقة محققة من أجل $n = k+1$ وبالتالي تكون محققة من أجل كل $n \geq 1$

مبرهنة = إذا كان $n \geq 2$ فإن: $p_n q_{n-1} - p_{n-1} q_n = (-1)^n$

الاثبات: يتم الإثبات بالاستقراء الرياضي على n

من أجل $n=2$ محققة لأن:

$$p_2 \cdot q_1 - p_1 q_2 = (a_2 \cdot a_1 + 1)(1) - a_1 \cdot a_2 = 1 = (-1)^2$$

خطوة الاستقراء:

نفرض أنها صحيحة من أجل $n=k$ أي: $p_k q_{k-1} - p_{k-1} q_k = (-1)^k$

ولنبرهن صحتها من أجل $n = k+1$

$$p_{k+1} q_k - p_k q_{k+1} = (a_{k+1} p_k + p_{k-1}) q_k - p_k (a_{k+1} q_k + q_{k-1})$$

$$= a_{k+1} p_k q_k + p_{k-1} q_k - a_{k+1} p_k q_k - p_k q_{k-1}$$

$$= p_{k-1} q_k - p_k q_{k-1} = -(p_k q_{k-1} - p_{k-1} q_k) = p_{k-1} q_k - p_k q_{k+1}$$

$$= -(-1)^k = (-1)^{k+1}$$

أي أن العلاقة محققة من أجل $n = k+1$

وبالتالي فهي محققة مهما كانت $n \geq 2$

سوف نستفيد من الكسور المنتهية في حل التطابقات الخطية باتباع مايلي:

1) $\frac{A}{B} = \langle q_1, \dots, q_n \rangle$

2) الرموز ♡ التي في البرهنة آخر صفحة 32

3) $p_n q_{n-1} - p_{n-1} q_n = (-1)^n$

تمرين: أوجد حل التطابق $79x \equiv 3 \pmod{103}$ باستخدام الكسور المستمرة

الحل: أولاً: نحول المعادلة الخطية (التطابق الخطي) إلى معادلة ديوفانتس

$$79x - 103y' = 3 \longrightarrow 79x + 103y$$

ومنه $y = -y'$

كما نلاحظ أن $d:(79,103)=1$ أي أن $d \backslash 3$
وبالتالي المعادلة تملك حلاً (قابل للحل)
ثانياً: نوجد الكسر البسيط المنتهي لـ $\frac{79}{103}$

$$\frac{79}{103}=0+\frac{1}{\frac{103}{79}}=0+\frac{1}{1+\frac{24}{79}}=0+\frac{1}{1+\frac{1}{\frac{79}{24}}}$$

$$=0+\frac{1}{1+\frac{1}{3+\frac{7}{24}}}=0+\frac{1}{1+\frac{1}{3+\frac{1}{\frac{24}{7}}}}=0+\frac{1}{1+\frac{1}{3+\frac{1}{3+\frac{1}{2+\frac{1}{3}}}}}$$

$$P_1=a_1=0,\ q_1=1 \Longrightarrow c_1=0$$
$$P_2=a_2.a_1+1=1,\ q_2=a_2=1 \longrightarrow c_2=1$$
$$c_3=\frac{a_3P_2+P_1}{a_3q_2+q_1}=\frac{3\times1+0}{3\times1+1}=\frac{3}{4} \Longrightarrow P_3=3,\ q_3=4$$
$$c_4=\frac{a_4P_3+P_2}{a_4q_3+q_2}=\frac{3(3)+1}{3(4)+1}=\frac{10}{13} \longrightarrow P_4=10,\ q_4=13$$
$$c_5=\frac{a_5P_4+P_3}{a_5q_4+q_4}=\frac{2(10)+3}{2(13)+4}=\frac{23}{30} \longrightarrow P_5=23,\ q_5=30$$
$$c_6=\frac{a_6P_5+P_4}{a_6q_5+q_4}=\frac{3(23)+10}{3(30)+13}=\frac{79}{103} \longrightarrow P_6=79,\ q_6=103$$

الآن حسب المبرهنة يكون لدينا: $P_6q_5-P_5q_6=(-1)^6=1$
$\Longrightarrow 79(30)-23(103)=1 \Longrightarrow 79(30)+103(-23)=1$
أي حصلنا على معادلة ديوفانتس $79x+103y=1$
ومتى نحصل على معادلة ديوفانتس التي لدينا، نضرب طرفي المعادلة بـ (3)
فنجد: $79(90)+103(-69)=3$
أي أن $(x_0,y_0)=(90,69)$ هو حل لمعادلة ديوفانتس المفروضة
وبالتالي فإن: $x_0=90$ هو حل التطابق الخطي المفروض وبما أن $d=1$ فإن التطابق لا يملك سوى حل واحد مختلف والحلول المتطابقة تعطى بالعلاقة: $x=90+103t$

للتأكد من الحل، نتحقق أن $3-(90)79\backslash 103$ أي أن $707\backslash 103$ وهذا محقق.

$C_n = \frac{P_n}{q_n}$ حيث P_n و q_n عددان أوليان نسبيًا فيما بينهما

تمرين 2 : أوجد مجموعة حلول التطابق: $187x \equiv 2 \pmod{503}$

الحل: معادلة ديوفانتس: $187x + 503y = 2$ نحل المعادلة:

$187x + 503y = 1$

$$\frac{503}{187} = 2 + \frac{1}{\frac{187}{129}} = 2 + \frac{1}{1 + \frac{1}{\frac{129}{58}}} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{\frac{58}{13}}}}$$

$$= 2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{\frac{13}{6}}}} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{4 + \frac{1}{2 + \frac{1}{3}}}}}$$

$$\frac{503}{187} = \langle 2, 1, 2, 4, 2, 6 \rangle \quad \text{: ومنه}$$

$$= \langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle$$

الموضوع : .....

/ / 37

محسب التقريبات :

$$c_1 = \frac{p_1}{q_1} = \frac{a_1}{1} = 2$$

$$c_2 = \frac{p_2}{q_2} = \frac{a_1 a_2 + 1}{a_2} = \frac{3}{1} = 3$$

$$c_3 = \frac{p_3}{q_3} = \frac{a_3 p_2 + p_1}{a_3 q_2 + q_1} = \frac{8}{3}$$

$$c_4 = \frac{p_4}{q_4} = \frac{a_4 p_3 + p_2}{a_4 q_3 + q_2} = \frac{35}{13}$$

$$c_5 = \frac{p_5}{q_5} = \frac{a_5 p_4 + p_3}{a_5 q_4 + q_3} = \frac{78}{29}$$

$$c_6 = \frac{p_6}{q_6} = \frac{a_6 p_5 + p_4}{a_6 p_5 + q_4} = \frac{503}{187}$$

$$p_6 q_5 - p_5 q_6 = (-1)^6 = 1$$

$$503(29) - 187(78) = 1$$

$$503(58) - 187(156) = 2$$

$$x \equiv -156 \pmod{503}$$

$$x \equiv 347 \pmod{503}$$

نعوض بـ $\boxed{n=6}$

نضرب بـ (2)

ومنه :

تمرين إضافي

أوجد حل التطابقة الخطية :

$$118x \equiv 3 \pmod{303}$$

وذلك باستخدام الكسور البسيطة.

الحل : أولاً لنحول هذه التطابقة لمعادلة ديوفانتس.

$118x - 303y' = 3 \longrightarrow$

$\Longrightarrow 118x + 303y = 3 \; ; \; y = -y'$

ونلاحظ أن $d = (118, 303) = 1$ أي أن $d \backslash 3$ وبالتالي المعادلة تملك حلاً (قابلة للحل) والآن لنوجد الكسر البسيط :

$$\frac{303}{118} = 2 + \frac{67}{118} = 2 + \frac{1}{\frac{118}{67}} = 2 + \frac{1}{1 + \frac{51}{67}} = 2 + \frac{1}{1 + \frac{1}{\frac{67}{51}}}$$

الموضوع: .....

$$= 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1+\frac{1}{3}}}}} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{5+\frac{1}{3}}}}}$$

$$\Rightarrow \frac{303}{118} = \langle 2,1,1,3,5,3 \rangle$$

$P_1 = a_1 = 2 \quad , q_1 = 1 \rightarrow c_1 = 2$

$P_2 = a_1 . a_2 + 1 = 3 \quad , q_2 = a_2 = 1 \Rightarrow c_2 = \frac{3}{1} = 3$

$c_3 = \frac{a_3 P_2 + P_1}{a_3 q_2 + q_1} = \frac{(1)(3)+(2)}{(1)(1)+(1)} = \frac{5}{2} \Rightarrow P_3 = 5, q_3 = 2$

$c_4 = \frac{a_4 P_3 + P_2}{a_4 q_3 + q_2} = \frac{(3)(5)+3}{(3)(2)+1} = \frac{18}{7} \Rightarrow P_4 = 18 , q_4 = 7$

$c_5 = \frac{a_5 P_4 + P_3}{a_5 q_4 + q_3} = \frac{(5)(18)+5}{(5)(7)+2} = \frac{95}{37} \Rightarrow P_5 = 95, q_3 = 37$

$c_6 = \frac{a_6 P_5 + P_4}{a_6 q_5 + q_4} = \frac{(3)(95)+18}{(3)(37)+7} = \frac{303}{118} \rightarrow P_6 = 303, q_6 = 118$

$P_6 q_5 - P_5 q_6 = (-1)^6 = 1$ ومن السهل هنا أن تكون:

$\rightarrow (303)(37) - (95)(118) = 1 \Rightarrow 118(-95) + 303(37) = 1$

ونضرب هذه المعادلة بـ (3) نجد:

$$118(-285) + 303(111) = 3$$

أي أن $(x_0, y_0) = (-285, 111)$ هو حل لمعادلة ديوفانتس

أي أن $x_0 = -285$ هو حل للتطابق الخطي المفروض وبما أن $d = 1$

فإن التطابق يملك حلاً واحداً ونعطي الحلول المتطابقة بالعلاقة:

$$x = -285 + 303t$$

$$t = 1 \longrightarrow x = 18$$

النظير الضربي: نقول عن العدد a^* إنه نظير ضربي للعدد a بالمقاس m إذا كان:

$$a^* . a \equiv 1 \pmod m$$

أي أن حل التطابق الخطي $ax \equiv 1 \pmod m$ حالة خاصة من التطابق $ax \equiv b \pmod m$

هو نظير ضربي للعدد a بالمقاس m

مبرهنة : يكون للعدد $a\in\mathbb{Z}$ نظير ضربي بالمقاس m إذا وفقط إذا كان $(a,m)=1$
أي $(a,m)=1 \iff ax\equiv 1 \pmod m$ لها حل

تمرين : أوجد النظير الضربي للعدد 17 بالمقاس 25

الحل : نحول السؤال إلى حل التطابق الخطي التالي :

$$17x\equiv 1 \pmod{25}$$

ولحل هذا التطابق يمكن أن نحله بتحويله إلى معادلة ديوفانتية أو باستخدام الكسور المستمرة المنتهية ، بالتجريب نجد أن $x_0=3$ هو حل لهذا التطابق وبما أن $d=(17,25)=1$ فإن هذا التطابق يملك حلاً وحيداً مختلفاً بالمقاس (25) أي أن $x=3+25t$ و $t\in\mathbb{Z}$ هي أيضاً حلول لهذا التطابق وبالتالي فإن (17) يملك عدد غير منته من النظائر الضربية المتساوية بالمقاس (25)

تمرين : أوجد نظير العدد 71 بالمقاس 55

الحل : أي لنوجد حل التطابق الخطي : $71x\equiv 1 \pmod{55}$ وبالتالي :

$$71x-55y'=1 \Rightarrow 71x+55y=1 \quad ; y=-y'$$

لحلها باستخدام الكسور المنتهية أو باستخدام القاسم المشترك الأعظم.

بما أن : $d=(71,55)=1$ فإن $d\mid 1$ أي يوجد للتطابق الخطي حل :

$$\frac{71}{55}=1+\frac{16}{55}=1+\frac{1}{\frac{55}{16}}=1+\frac{1}{3+\frac{7}{16}}$$

$$=1+\frac{1}{3+\frac{1}{\frac{16}{7}}}=1+\frac{1}{3+\frac{1}{2+\frac{2}{7}}}=1+\frac{1}{3+\frac{1}{2+\frac{1}{\frac{7}{2}}}}=1+\frac{1}{3+\frac{1}{2+\frac{1}{3+\frac{1}{2}}}}$$

$$\Rightarrow \frac{71}{55}=\langle 1,3,2,3,2\rangle \quad ; P_1=a_1=1,\ q_1=1,\ P_2=a_2a_1+1=4,\ q_2=a_2=3$$

$$C_3=\frac{a_3P_2+P_1}{a_3q_2+q_1}=\frac{(2)(4)+1}{(2)(3)+1}=\frac{9}{7} \Rightarrow P_3=9,\ q_3=7$$

$$C_4=\frac{a_4P_3+P_2}{a_4q_3+q_2}=\frac{(3)(9)+4}{(3)(7)+3}=\frac{31}{24} \Rightarrow P_4=31,\ q_4=24$$

$$C_5=\frac{a_5P_4+P_3}{a_5q_4+q_3}=\frac{(2)(31)+9}{(2)(24)+7}=\frac{71}{55} \Rightarrow P_5=71,\ q_5=55$$

الموضوع : .....

ونعلم أن (حسب مبرهنة) $P_5 q_4 - P_4 q_5 = (-1)^5 = -1$

$\Rightarrow (71)(24) - (31)(55) = -1 \longrightarrow 71|(-24) + 55(31) = 1$

إذاً فإن $(x_0, y_0) = (-24, 31)$ هو حل لتطابقة الخطي و يكون $x_0 = 24$ هو نظير ضربي للعدد 71 بالمقاس 55 كما أن كل قيمة t فيما يلي تعطي نظير ضربي: $x = -24 + 55t ; t \in \mathbb{Z}$ من أجل $t = 1$ فإن $x_1 = 31$ نظير ضربي لـ 71 بالمقاس 55

حل جملة التطابقات الخطية: لتكن لدينا جملة التطابقات التالية:

$$a_1 x \equiv b_1 \pmod{m_1}$$
$$a_2 x \equiv b_2 \pmod{m_2}$$
$$\vdots$$
$$a_n x \equiv b_n \pmod{m_n}$$

عندئذٍ نقول أن لجملة التطابقات السابقة حلاً مشتركاً x_0 إذا كان x_0 هو حل لجميع التطابقات: $a_i x \equiv b_i \pmod{m}$ حيث $i = 1, \dots, n$

مبرهنة البواقي الصينية: إذا كانت المقاسات $m_1, m_2, \dots, m_n$ أولية مثنى مثنى فإنه يوجد لجملة التطابقات $x = a_i \pmod{m_i}$ حيث $i = 1, \dots, n$ بالمقاس $m = m_1 \cdot m_2 \cdots m_n$

الإثبات: نكتب الأعداد التالية: $M_i = \frac{m}{m_i} = m_1 \cdot m_2 \cdots m_{i-1} \cdot m_{i+1} \cdots m_n$

حيث أن $i = 1, \dots, n$ وبالتالي يكون $(M_i, m_i) = 1$ "لأن m_i أولية مع مثنى مثنى"

وحسب المبرهنة السابقة فإن M_i يملك نظير ضربي بالمقاس m_i ولتكن m_i'

(نظير M_i ضربياً بالمقاس m_i) عندئذٍ تتحقق: $M_i m_i' \equiv 1 \pmod{m_i}$

لأجل كل $i = 1, \dots, n$

الآن نكتب x على الشكل التالي: $x = \sum_{i=1}^{n} a_i M_i m_i' = a_1 M_1 m_1' + \cdots + a_n M_n m_n'$

سنبرهن فيما يلي أن: x هو حل للجملة المعروضة وأنه وحيد بالمقاس m

$$\forall i \in \{1, \dots, n\} : x = \sum_{j=1}^{n} a_j M_j m_j' \pmod{m_i}$$

ولكن نلاحظ ما يلي: * إذا كان $j = i$ فإن $(M_j, m_i) = 1$ وبالتالي $a_j M_j m_j' \equiv a_i \pmod{m_i}$.

** إذا كان $j \neq i$ فإن m_i يقسم M_j وبالتالي $a_j M_j m_j' \equiv 0 \pmod{m_i}$ حسب ملاحظة سابقة:

« $\alpha_i \equiv B_i \pmod{m} \Longrightarrow \sum_{i=1}^{n} \alpha_i \equiv \sum_{i=1}^{n} B_i \pmod{m}$ »

وبالتالي فإن: $x = \sum_{j=1}^{n} a_j M_j m_j' = 0 + 0 + \cdots + a_i + 0 + \cdots + 0 \pmod{m_i}$

$\Rightarrow \forall i \in \{1,2,\cdots,n\} \quad : x \equiv a_i \pmod{m_i}$

و بالتالي فإن x هو حل لجملة التطابقات أيضاً عندئذٍ $\forall i \in \{1,2,\cdots,n\} : x' \equiv x \equiv a_i \pmod{m_i}$

$\Rightarrow x' - x \equiv 0 \pmod{m_i} \quad \forall i = 1,\cdots,n \Rightarrow m_i \mid x' - x \quad \forall i = 1,\cdots,n$

و بالتالي فإن $x - x'$ هو مضاعف مشترك لأعداد $m_1, \cdots, m_n$ وبما أن $m = lcm(m_1, \cdots, m_2)$ (لأنها أولية فيما بينها مثنى مثنى) فإن $m \mid x - x'$ و بالتالي $x' \equiv x \pmod{m}$ أي أن الحل x وحيد بالمقاس m

انتهت المحاضرة ""

المحاضرة السابعة 2017 / 4 / 25

مثال 17 أوجد أصغر عدد صحيح موجب باقي قسمته على 5 يساوي 5 وباقي قسمته على 12 يساوي 3 و باقي قسمته على 5 و يساوي 2

$x \equiv 5 \pmod{13}$

$x \equiv 3 \pmod{12}$

$x \equiv 2 \pmod{35}$

لنثبت أن m_i أولية مثنى مثنى $(12,13) = 1 , (13,35) = 1 , (12,35) = 1$

لنوجد $m = 12 \times 13 \times 35 = 5460$ لنشكل

$M_1 = 13 \times 35 = 455$

$M_2 = 12 \times 35 = 420$

$M_3 = 12 \times 13 = 156$

لنوجد النظائر M_i و $i = 1,2,3$

$M_1 m_1' \equiv 1 \pmod{12} \longrightarrow 455 m_1' \equiv 1 \pmod{12}$

$M_2 m_2' \equiv 1 \pmod{13} \longrightarrow 420 m_2' \equiv 1 \pmod{13}$

$M_3 m_3' \equiv 1 \pmod{35} \longrightarrow 156 m_3' \equiv 1 \pmod{35}$

$m_1' \equiv -1 \pmod{12}$

$m_2' \equiv -3 \pmod{13}$

$m_3' \equiv 11 \pmod{35}$

باستخدام النظائر المتوفرة

يكون لجملة التطابقات الخطية حل هو $x = \sum_{i=1}^{3} a_i M_i m_i' \pmod{5460}$,

$= 5 \times 455 \times (-1) + (3) \times 420 \times (-3) + 2 \times 156 \times 4 \equiv -4233 \equiv 1227 \pmod{5460}$

18 مثال: أوجد الحل المشترك لكل من جملة التطابقات التالية:

① $5x \equiv 2 \pmod{13}$
② $x \equiv 2 \pmod{35}$
③ $3x \equiv 13 \pmod{77}$
④ $x \equiv 7 \pmod{20}$

① $\Rightarrow x \equiv 3 \pmod{13}$
⑦ $x \equiv 2 \pmod{35}$
③ $\Rightarrow x \equiv 30 \pmod{77}$
④ $x \equiv 7 \pmod{20}$

② $\Rightarrow \begin{cases} x \equiv 2 \pmod 5 & ⑤ \\ x \equiv 2 \pmod 7 & ⑥ \end{cases}$

③ $\Rightarrow \begin{cases} x \equiv 30 \pmod 7 & ⑦ \\ x \equiv 30 \pmod{11} & ⑧ \equiv 8 \pmod{11} \end{cases}$

④ $\Rightarrow \begin{cases} x \equiv 7 \pmod 4 & ⑨ \equiv 3 \pmod 4 \\ x \equiv 7 \pmod 5 & ⑩ \end{cases}$

$x \equiv 2 \pmod 5 \leftarrow 7 \equiv 2 \pmod 5$ من ⑩ و ⑤.

$x \equiv 2 \pmod 7 \leftarrow 30 \equiv 2 \pmod 7$ من ⑥ و ⑦.

إذن الجملة المكافئة للجملة التالية:

$x \equiv 3 \pmod 4$
$x \equiv 2 \pmod 5$
$x \equiv 2 \pmod 7$
$x \equiv 8 \pmod{11}$
$x \equiv 3 \pmod{13}$

الأعداد (4, 5, 7, 11, 13) أولية فيما بينها مثنى مثنى.

$m = 4 \times 5 \times 7 \times 11 \times 13 = 2020$ فيكون للجملة حل:

$M_1 = \frac{m}{m_1} = 505$ "4 على m_1 تساوي" $\rightarrow 505 m_1' \equiv 1 \pmod 4$

$M_2 = \frac{m}{m_2} = 404 \rightarrow$ $\rightarrow 404 m_2' \equiv 1 \pmod 5$

$M_3 = \frac{m}{m_3} = 286 \rightarrow$ $\rightarrow 286 m_3' \equiv 1 \pmod 7$

$M_4 = \frac{m}{m_4} = 182 \rightarrow$ $\rightarrow 182 m_4' \equiv 1 \pmod{11}$

$M_5 = \frac{m}{m_5} = 154 \rightarrow$ $\rightarrow 154 m_5' \equiv 1 \pmod{13}$

$m_1' \equiv 1 \pmod 4$, $m_2' \equiv 1 \pmod 5$

$m_3' \equiv 2 \pmod 7$, $m_4' \equiv -2 \pmod{11}$, $m_5' \equiv -2 \pmod{13}$

$x \equiv \sum_{i=1}^{5} a_i m_i' M_i \pmod{2020}$ الحل هو

$x = 3 \times 505 \times 1 + 2 \times 404 \times (-1) + 2 \times (286) \times 2 + 8 \times 182 \times (-2) + 3 \times 154 \times (-2)$

$x \equiv 15015 - 8008 + 11440 - 29120 - 9240 = 26455 - 46368 = -19913$ بترتيب 20020

$x \equiv 107 \pmod{20020}$

مثال: أوجد حل التطابق $19x \equiv 1 \pmod{140}$ باستخدام برهنة البراهمي الهندية

$140 = 4 \times 5 \times 7$

$19x \equiv 1 \pmod 4 \Rightarrow x \equiv 3 \pmod 4$

$19x \equiv 1 \pmod 5 \Rightarrow x \equiv 4 \pmod 5$

$19x \equiv 1 \pmod 7 \Rightarrow x \equiv 3 \pmod 7$

4، 5، 7 أولية مثنى مثنى ← التطابقات حلها مشترك ← تمة الحل موجود في الكتاب

مبرهنة فيرما الصغرى: إذا كان P عدد أولي $P \nmid a$ فإن $a^{P-1} \equiv 1 \pmod P$

البرهان: نأخذ مجموعة مضاعفات العدد a:

$A = \{a, 2a, \dots, (P-1)a\}$

نبين أن هذه الأعداد غير متطابقة بالمقاس P لنفرض أنه يوجد تطابق بين العددين:

$1 \leq r < s \leq P-1$:

$r \cdot a \equiv s \cdot a \pmod P$

لدينا $(P, a) = 1$ إذن نختصر على a ← $r \equiv s \pmod P$ وهذا غير محقق كون:

$1 \leq r < s \leq P-1$ وهذه العناصر أولية تشبيا مع P

كل عنصر من المجموعة A يطابق عنصر من المجموعة A_1 حيث:

$A_1 = \{1, 2, \dots, (P-1)\}$

إذا جداء عناصر A يطابق جداء عناصر المجموعة A_1 بالمقاس P

$(1.2.3. \dots .P-1) \pmod P = 1.a.2a. \dots .(P-1)a$

$a^{P-1} (P-1)! \equiv (P-1)! \pmod P$

P أولي مع الأعداد $1, 2, \dots, P-1$ فهو أولي مع جداءهم $(P-1)!$

وبالتالي نختصر على $(P-1)!$ ← $a^{P-1} \equiv 1 \pmod P$ كذلك نجد $a^P \equiv a \pmod P$

مثال: اثبت أن $5^{38} \equiv 4 \pmod{11}$

$(5, 11) = 1$ ← $5^{10} \equiv 1 \pmod{11}$

$38 = 3 \times 10 + 8$

$5^{38} \equiv (5^{10})^3 . (5)^8 \pmod{11}$

$\equiv 5^8 \equiv (25)^4 \equiv 3^4 \equiv 81 \equiv 4 \pmod{11}$

$25 \equiv 3 \pmod{11}$

نتيجة: إذا كان P و q عددين أوليين وكان $a^q \equiv a \pmod q$ و $a^p \equiv a \pmod P$

فإن $a^{pq} \equiv a \pmod{P.q}$

الموضوع : .....

مثال : اثبت أن $2^{340} \equiv 1 \pmod{341}$

$341 = 11 \times 31$

$(2,11) = 1$ فيرما الصغرى $\leftarrow 2^{10} \equiv 1 \pmod{11}$

$2^{30} \equiv 1 \pmod{11}$

$2^{31} \equiv 2 \pmod{11}$

$2^{10} \equiv (2^5)^2 = (32)^2 \equiv 1 \pmod{31}$

$2^{11} \equiv 2 \pmod{31}$ ومنه:

$2^{341} \equiv 2 \pmod{341} \Leftarrow 2^{11 \times 31} \equiv 2 \pmod{31 \times 11}$ حسب النتيجة السابقة:

نقسم على 2 فنجد: $2^{340} \equiv 1 \pmod{341}$

ملاحظة: نقول إذا كان $a^n \equiv a \pmod{n}$ فليس من الضروري أن يكون n عدد أولي إذن عكس فيرما الصغرى ليس صحيح

تعريف: نسمي الأعداد n التي تحقق $2^n \equiv 2 \pmod{n}$ و $(n,2) = 1$ بالأعداد شبه الأولية مثل 341 ، 561 ، ... " يوجد أمثلة محلولة في الكتاب "

مبرهنة ويلسون: إذا كان P عدداً أولياً فإن: $P \mid (P-1)! + 1$

أو $(P-1)! \equiv -1 \pmod{P}$

الإثبات: إذا كان $P = 2$:

$2 \mid 1! + 1 = 2$

$P = 3$: $3 \mid 2! + 1 = 3$ محقق

إذا كان $P > 3$ ، نأخذ العدد a من المجموعة $A = \{2, 3, \dots, P-2\}$

بما أن $(a,P) = 1$ حسب مبرهنة سابقة يوجد نظير a^* للعدد a ينتمي إلى مجموعة البواقي التامة بالمقاس P وهي $a^* \in A_1 = \{0, 1, 2, \dots, P-2, P-1\}$

بما أن $a^* \neq 0 \pmod{P}$ لو تحقق ذلك لكان $a^* . a \equiv 0 \pmod{P}$ وهذا غير محقق

كذلك بما أن $a^* \neq +1 \pmod{P}$ إذن $a^* \neq P-1 \pmod{P}$ لأن $-1 \equiv P-1 \pmod{P}$

لو تحقق ذلك لكان: $a^* . a \equiv \mp a \equiv 1 \pmod{P} \rightarrow a \equiv \mp 1 \pmod{P}$

$$\rightarrow \begin{cases} a \equiv 1 \pmod{P} & , a = 1 \notin A \\ a \equiv -1 \equiv P-1 \pmod{P} & , P-1 \notin A \end{cases}$$

أي أن $a^* \in A$ ولدينا $a \in A$ ومنه العدد a ونظيره a^* من A

ويحققان $a^* . a \equiv 1 \pmod{P}$

عدد عناصر المجموعة A هو $P-3$ وهو عدد زوجي ويمكننا تقسيم المجموعة A إلى $\frac{P-3}{2}$ زوجاً

الموضوع : .....

جداء كل زوج يطابق الواحد بالقياس P

$2.3.\dots.P-2 \equiv 1 \pmod P$

$2.3.\dots.(P-2).(P-1) \equiv (P-1) \pmod P$

$(P-1)! \equiv P-1 \equiv -1 \pmod P$ و.ه.م

عكس مبرهنة ويلسون: إذا كان $n>2$ ويحقق $(n-1)! \equiv -1 \pmod n$ فإن n أولي

الاثبات: نفرض n ليس أولياً فله عامل أولي P: $P \setminus n$ ويحقق:

$1<P<n$ " $1<P \leq n-1$ "

يمكن أن يكون P أحد الأعداد من 1 إلى n-1 $\leftarrow P \setminus (n-1)!$

حسب الفرض $n \setminus (n-1)! + 1 \leftarrow P \setminus (n-1)! + 1 \leftarrow P \setminus 1$

$\leftarrow d = P-1$ وبالتالي n عدد أولي

مبرهنة ويلسون والعكس: يكون P عدداً أولياً إذا وفقط إذا تحقق:

$(P-1)! \equiv -1 \pmod P$

مثال: اثبت أن $18! \equiv -1 \pmod{437}$

$437 = 19 \times 23$ ، $18! = (19-1)! \equiv -1 \pmod{19}$

$18! \equiv -1 \pmod{19}$ ، $19 \setminus 18!+1$

$22! \equiv -1 \pmod{23}$

$22! = 22 \times 21 \times 20 \times 19 \times 18! \pmod{23}$

$22! \equiv 18! \pmod{23}$

$\Rightarrow 23 \setminus 18!+1$

$19 \setminus 18!+1$

$437 \setminus 18!+1$ أي $23 \times 19 \setminus 18!+1 \leftarrow (19,23)=1$

$18! \equiv -1 \pmod{437}$

تطبيق على مبرهنة ويلسون $P=13$

$A = \{2,3,4,5,6,7,8,9,10,11\}$

$2.7 \equiv 1 \pmod{13}$ ، $5.8 \equiv 1 \pmod{13}$

$3.9 \equiv 1 \pmod{13}$ $6.11 \equiv 1 \pmod{13}$

$4.10 \equiv 1 \pmod{13}$

تمارين 8

$17x \equiv 3 \pmod 2$
$17x \equiv 3 \pmod 3$
$17x \equiv 3 \pmod 5$
$17x \equiv 3 \pmod 7$

$\Longrightarrow$ $x \equiv 1 \pmod 2$
$x \equiv 3 \pmod 3$
$x \equiv 4 \pmod 5$
$x \equiv 1 \pmod 7$

2, 3, 5, 7 أولية مثنى مثنى

لحل التطابقات حل بالقاعدة $m = 5 \times 3 \times 7 \times 2 = 210$

إكمال الحل واجب و ستكون النتائج كمايلي :

$M_1 = 42 \longrightarrow m'_1 = -2$
$M_2 = 70 \longrightarrow m'_2 = 1$
$M_3 = 30 \longrightarrow m'_3 = -3$
$M_4 = 105 \longrightarrow m'_4 = 1$
$x = -111 \equiv 99 \pmod{210}$

انتهت المحاضرة

الدوال العددية

الدالة العددية هي دالة مجال تعريفها مجموعة الأعداد الصحيحة الموجبة

الدالة العددية الضربية: نقول عن دالة $f(n)$ إنها دالة ضربية إذا تحقق ما يلي

① الدالة f غير صفرية.

② إذا كان $a,b \in \mathbb{Z}^+$ ، $(a,b)=1$ فإن:

$$f(a.b)=f(a).f(b)$$

ونقول إن الدالة f ضربية تماماً إذا تحقق الشرط:

$$f(a.b)=f(a).f(b)$$

دون تحقق الشرط $(a,b)=1$

مثال: إذا كان $f_\alpha(n)=n^\alpha$

① $f(n)\neq 0$ إذا كان $n>0$

② $f_\alpha(a.b)=a^\alpha.b^\alpha=f_\alpha(a).f_\alpha(b)$

تحقق الشرط دون تحقق $(a,b)=1$

بالتالي الدالة f ضربية تماماً

مبرهنة: إذا كانت $f(n)$ دالة ضربية فإن:

$f(1)=1$ ① $\exists n,\ f(n)\neq 0$

بما أن: $n.1=n$; $(n,1)=1$

$$f(n)=f(n.1)=f(n).f(1) \Longrightarrow f(1)=1$$

تعريف الدالة الضربية يجب أن تحقق f الشرطين التاليين:

① $f(1)=1$

② $(a,b)=1$, $f(a.b)=f(a).f(b)$

نتيجة: إذا كانت f دالة ضربية و $n_1, n_2, \dots, n_k$ أعداد أولية مثنى مثنى فإن

$$f(n_1.n_2\cdots n_k)=f(n_1).f(n_2)\cdots f(n_k)$$

نتيجة: إذا كانت $n=p_1^{\alpha_1}.p_2^{\alpha_2}\cdots p_k^{\alpha_k}$

و f دالة ضربية فإن $f(n)=f(p_1^{\alpha_1}\cdots p_k^{\alpha_k})=f(p_1^{\alpha_1}).f(p_2^{\alpha_2})\cdots f(p_k^{\alpha_k})$

$p_i^{\alpha_i}$ أعداد أولية مثنى مثنى

تعريف: نعني بالمجموع $\sum_{d\mid n} f(d)$ المجموع بأخذ فقط على قواسم العدد n

$$\sum_{d\backslash 12} f(d) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)$$

(نتيجة) مبرهنة ①: إذا كانت f و g دالتين عدديتين فإن

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

الإثبات :

نفرض أن القواسم للعدد m ، هي $d_1, d_2, \dots, d_s$

والقواسم للعدد n ، هي $e_1, e_2, \dots, e_t$

$$\sum_{\substack{d\backslash m \\ e\backslash n}} f(d).g(e) = \sum_{\substack{i=1,2,\dots,s \\ j=1,2,\dots,t}} f(d_i)\,g(e_j)$$

$$= \sum_{i=1}^{s} f(d_i)\,g(e_1) + \sum_{i=1}^{s} f(d_i)\,g(e_2) + \cdots + \sum_{i=1}^{s} f(d_i)\,g(e_t)$$

$$= \left(\sum_{i=1}^{s} f(d_i)\right).\left(g(e_1)+g(e_2)+\cdots+g(e_t)\right) = \left(\sum_{d\backslash m} f(d)\right).\left(\sum_{e\backslash n} g(e)\right)$$

تمهيدية ② : إذا كان $n, m \in \mathbb{Z}^+$ حيث $(n,m)=1$ فإن أي قاسم d لـ $m.n$ يكتب بشكل وحيد كقاسم d_1 لـ m ضرب قاسم d_2 لـ n

$$d = d_1.d_2 \quad ; \quad (d_1,d_2)=1$$

مبرهنة : إذا كانت الدالة العددية f دالة ضربية وإذا عرفت الدالة العديدية F على النحو :

$$F(n) = \sum_{d\backslash n} f(d)$$

فإن F هي دالة ضربية

الإثبات : [1]

$$F(1) = \sum_{d\backslash 1} f(d) = f(1) = 1$$

[2] $n, m \in \mathbb{Z}^+$ ، $(n,m)=1$

$$F(n.m) = \sum_{d\backslash n.m} f(d)$$

حسب التمهيدية ② نجد أن $d = d_1.d_2$ حيث $d_1\backslash n$ و $d_2\backslash m$

$$F(n.m) = \sum_{\substack{d_1\backslash n \\ d_2\backslash m}} f(d_1.d_2)$$

$(d_1,d_2)=1$.

$$= \sum_{\substack{d_1\backslash n \\ d_2\backslash m}} f(d_1).f(d_2) \Leftarrow f \text{ ضربية}$$

$$F(n,m) = \left(\sum_{d_1\backslash n} f(d_1)\right)\left(\sum_{d_2\backslash m} f(d_2)\right)$$

حسب التمهيدية ①

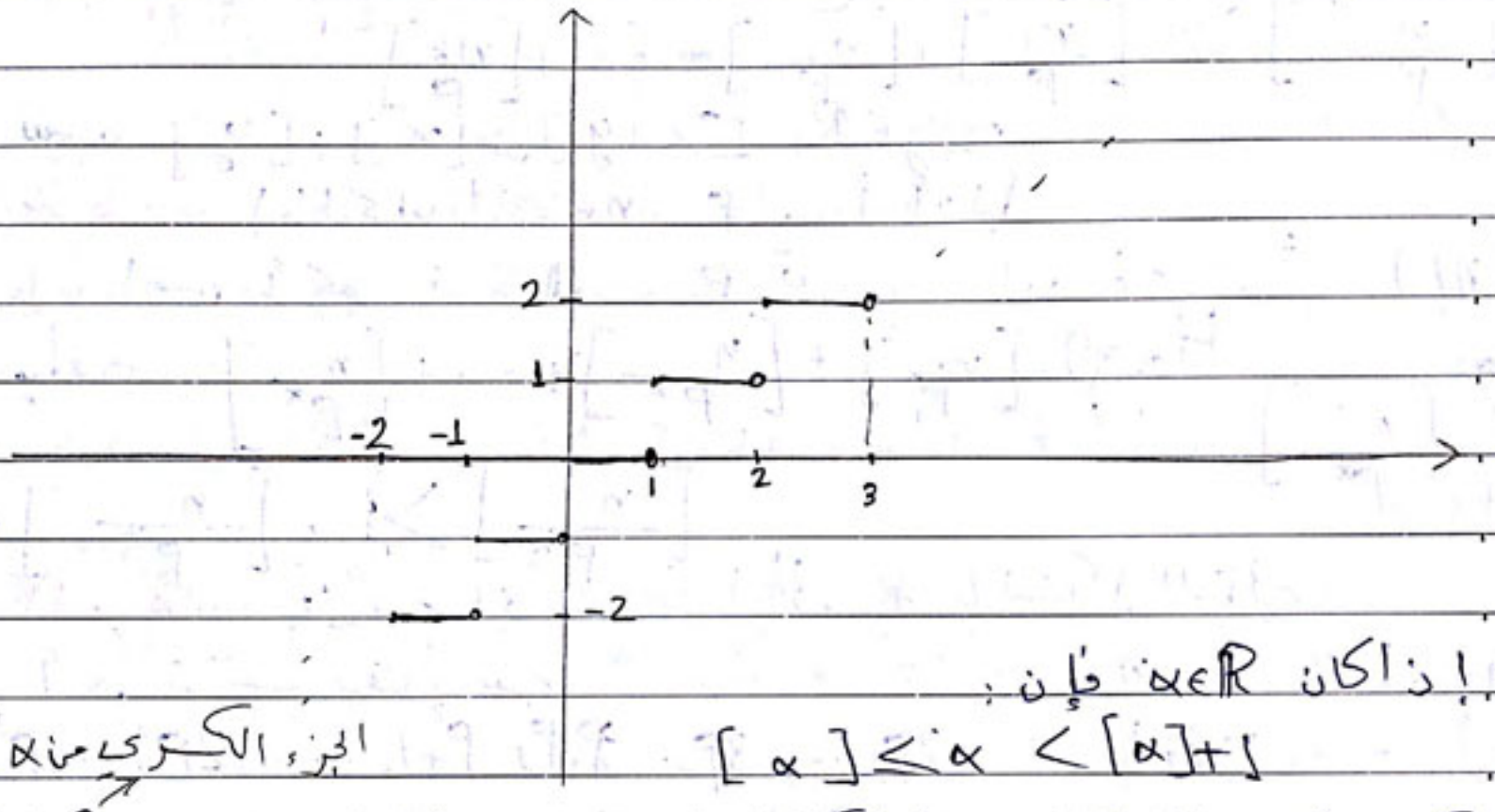
$= F(n).F(m)$ إذا F(n) دالة ضربية

1) دالة الجزء الصحيح $[x]$

تعريف : دالة الجزء الصحيح $[x]$ لعدد x هي أكبر عدد صحيح لا يتجاوز x

$[2,5]=2$, $[-\frac{10}{3}]=-4$, $[-2,5]=-3$

وهي دالة درجية :



إذا كان $\alpha \in \mathbb{R}$ فإن :

$[\alpha] \leq \alpha < [\alpha]+1$

* نكتب العدد الحقيقي α بالشكل التالي : $0 \leq \theta < 1$; $\alpha = [\alpha] + \theta$ ← الجزء الكسري من α

خواص : البرهان بسيط جدا في الكتاب ومطلوب :

1. $\alpha \in \mathbb{Z}, \alpha \in \mathbb{R}$; $[a+\alpha] = a + [\alpha]$

2. $n \in \mathbb{Z}^+, \alpha \in \mathbb{R}$; $\left[\frac{[\alpha]}{n}\right] = \left[\frac{\alpha}{n}\right]$

3. $a, b, n \in \mathbb{Z}^+$; $\left[\frac{a.b}{n}\right] \geq a\left[\frac{b}{n}\right]$

4. إذا كان $\alpha = \sum_{i=1}^{n} \alpha_i$; $\alpha_i \in \mathbb{R}$ فإن $[\alpha] \geq \sum_{i=1}^{n} [\alpha_i]$

الإثبات :

$\alpha_1 = [\alpha_1] + \theta_1 \quad 0 \leq \theta_1 < 1$

$\alpha_2 = [\alpha_2] + \theta_2 \quad 0 \leq \theta_2 < 1$

$\alpha_n = [\alpha_n] + \theta_n \quad 0 \leq \theta_n < 1$

$\alpha = \sum_{i=1}^{n} \alpha_i - \sum_{i=1}^{n} [\alpha_i] + \sum_{i=1}^{n} \theta_i \Longrightarrow [\alpha] = \sum_{i=1}^{n} [\alpha_i] + \left[\sum_{i=1}^{n} \theta_i\right]$

نعلم أن $\sum_{i=1}^{n}\theta_i$ مقدار موجب.

نبين أن $[\alpha] \geq \sum_{i=1}^{n}[\alpha_i]$

5- $\alpha \in \mathbb{R}$ ، $n \in \mathbb{Z}^+$ فإن $n>1$: $[\alpha] > \left[\frac{\alpha}{n}\right]$

نتيجة: $n = \sum_{i=1}^{k} n_i$ ، p عدد صحيح موجب حيث $n_i, n \in \mathbb{Z}^+$

$$\left[\frac{n}{p}\right] \geq \left[\frac{n_1}{p}\right] + \left[\frac{n_2}{p}\right] + \cdots + \left[\frac{n_k}{p}\right]$$

نتيجة: $x, y \in \mathbb{R}$; $[x+y] \geq [x] + [y]$

مبرهنة: إذا كان $n \in \mathbb{Z}^+$ ، p عدداً أولياً.

فإن أس أكبر قوة للعدد p تقسم $n!$ نرمز لها بـ $H_p(n!)$

بمساوي: $H_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^k}\right]$

$$= \sum_{i=1}^{\infty}\left[\frac{n}{p}\right]$$

$\left[\frac{n}{p^{k+1}}\right] = 0$ ، $\left[\frac{n}{p^k}\right] \geq 1$

البرهان: نرتب الأعداد من 1 إلى n بالشكل التالي:

$n! = 1, 2, \cdots, n$

أي ترتيب مضاريب.

$1, 2, \cdots, p, p+1, \cdots, 2p, \cdots, 3p, \cdots, p.p, p^2+1, \cdots, 2p^2, \cdots, p^3, \cdots, n$

فتكون الأعداد التي تقبل القسمة على p هي:

$p, 2p, \cdots, t_1 p$; $t_1 p \leq n$ هو أكبر عدد صحيح يحقق

$t_1 \leq \frac{n}{p} < t_1+1$ ($t_1 p \leq n < (t_1+1)p$) t_1 أكبر عدد صحيح أصغر من $\frac{n}{p}$

أي $t_1 = \left[\frac{n}{p}\right]$

إذاً عدد الأعداد التي تقبل القسمة على p هي $t_1 = \left[\frac{n}{p}\right]$

ثم الأعداد التي تقبل القسمة على p^2

$1p^2, 2p^2, \cdots, t_2 p^2$

بحيث يكون $t_2 p^2 \leq n$ ، t_2 أكبر عدد صحيح يحقق ذلك

بالتالي عدد الأعداد التي تقبل القسمة على p^2 هي $t_2 = \left[\frac{n}{p^2}\right]$

نتابع بنفس الفكرة فتجد عدد الأعداد التي تقبل القسمة على p^3 هي $t_n = \left[\frac{n}{p^3}\right]$

وهذه العملية منتهية. بالتالي يكون عدد الأعداد التي تقبل القسمة على p^k

تساوي $t_k = \left[\frac{n}{p^k}\right]$

فيكون عدد الأعداد التي تقبل قسمة $n!$ على p هي :

$$t_1 + t_2 + \cdots + t_n = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^k}\right]$$

فيكون:

$$H_p(n) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$$

إذا كان $n! = 19!$

و $p = 3$ لدينا $1, 2, 3, \cdots, 6, \cdots, 9, \cdots, 12, \cdots, 15, \cdots, 18, 19$

الأعداد التي تقبل القسمة على 3 هي $3, 6, 9, 12, 15, 18$

عددهم $6 = \left[\frac{n}{3}\right]$

الأعداد التي تقبل القسمة على 9 هي $\{9, 18\}$ وعددهم $2 = \left[\frac{19}{3^2}\right]$

$3^3 = 27 \nmid 19!$

$$H_3(19) = \left[\frac{19}{3}\right] + \left[\frac{19}{3^2}\right] + \left[\frac{19}{3^3}\right] = 6 + 2 + 0 = 8$$

فنجد أن $3^8 \mid 19!$ ، لكن $3^9 \nmid 19!$

مثال: $H_3(80!)$

أوجد أس أكبر قوة للعدد 3 تقسم $80!$

$$H_3(80!) = \left[\frac{80}{3}\right] + \left[\frac{80}{3^2}\right] + \left[\frac{80}{3^3}\right] + \left[\frac{80}{3^4}\right]$$

$$= 26 + 8 + 2 + 0 = 36$$

نجد أن $3^{36} \mid 80!$ وإن $3^{37} \nmid 80!$

مثال: ماهو عدد الأصفار في نهاية العدد $50!$

مطلوب حساب $H_{10}(50!)$

$10 = 2.5$ ، $(2,5) = 1$

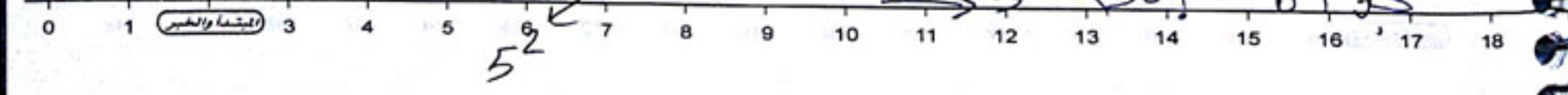
$$H_2(50!) = \left[\frac{50}{2}\right] + \left[\frac{50}{4}\right] + \left[\frac{50}{8}\right] + \left[\frac{50}{16}\right] + \left[\frac{50}{32}\right] + \left[\frac{50}{64}\right]$$

$$H_2(50!) = 25 + 12 + 6 + 3 + 1 = 47$$

نجد أن $2^{47} \mid 50!$ وإن $2^{48} \nmid 50!$

$$H_5(50!) = \left[\frac{50}{5}\right] + \left[\frac{50}{25}\right] + \left[\frac{50}{125}\right] = 10 + 2 = 12$$

نجد أن $5^{12} \mid 50!$



الموضوع : .....

$(10)^{12} = (2.5)^{12} \setminus 5^{12}$

يوجد 2 أصفار في العدد 10!

مبرهنة : إذا كتبت العدد الصحيح m بالنظام الذي أساسه العدد الأولي p فإن أس أكبر قوة للعدد p تقسم $m!$ تساوي $H_p(m!) = \frac{m - \sum_{i=0}^{r} a_i}{p-1}$ حيث $m = \sum_{i=0}^{r} a_i p^i$

$$m = \sum_{i=0}^{r} a_i p^i = a_r p^r + \cdots + a_1 p + a_0$$

الإثبات : حسب المبرهنة السابقة :

$$H_p(m!) = \left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \cdots + \left[\frac{m}{p^r}\right]$$

$$H_p(m!) = \underbrace{a_r p^{r-1} + a_{r-1} p^{r-2} + \cdots + a_2 p + a_1}_{\text{قسمنا على } p} + \underbrace{a_r p^{r-2} + a_{r-1} p^{r-3} + \cdots + a_2}_{\text{قسمنا على } p^2} + \cdots$$

$$\cdots + a_r p + a_{r-1} + a_r$$

$$= a_r (1 + p + p^2 + \cdots + p^{r-1}) + a_{r-1} (1 + p + \cdots + p^{r-2}) + \cdots + a_2 (1 + p) + a_1$$

$$= a_r \frac{1 - p^r}{1 - p} + a_{r-1} \frac{1 - p^{r-1}}{1 - p} + \cdots + a_2 \left(\frac{1 - p^2}{1 - p}\right) + a_1 \frac{1 - p}{1 - p}$$

$$H_p(m!) = \frac{a_r(p^r - 1) + \cdots + a_2(p^2 - 1) + a_1(p - 1) + a_0 - a_0}{p-1}$$

$$H_p(m!) = \frac{a_r p^r + a_{r-1} p^{r-1} + \cdots + a_2 p^2 + a_1 p^1 + a_0 - (a_r + a_{r-1} + \cdots + a_0)}{p-1}$$

$$= \frac{m - \sum_{i=0}^{r} a_i}{p-1}$$

مثال: اكتب العدد 347 بنظام العد الذي أساسه 7 ثم احسب $H_7(347!)$

$$347 = 1\cdot 7^3 + 0\cdot 7^2 + 0\cdot 7^1 + 4$$

$$\therefore H_7(347!) = \frac{347-5}{6} = \frac{347}{6} = 57$$

إذاً $7^{58} \nmid (347!)$, $7^{57} \mid (347!)$

تمرين: اثبت أن أس أكبر قوة للعدد 7 تقسم $(7^n-3)!$ هي $\frac{7^n-6n-1}{6}$

$n=1 \longrightarrow 7-3=4$

$n=2 \longrightarrow 7^2-3=46=6\cdot 7+4$

$n=3 \longrightarrow 7^3-3=346=6\cdot 7^2+6\cdot 7+4$

$n=n \longrightarrow 7^n-3=\underbrace{6\cdot 7^{n-1}+6\cdot 7^{n-2}+\dots+6\cdot 7^1}_{n-1}+4$

$$\sum_{i=0}^{n-1} a_i = 6\cdot(n-1)+4 = 6n-2$$

$$H_7((7^n-3)!) = \frac{n-\sum_{i=0}^{n-1} a_i}{7-1} = \frac{7^n-3-(6n-2)}{6}$$

$$= \frac{7^n-6n-1}{6}$$

تمارين:

1) اعط مثالاً تبين أنه إذا كان $a^2 \equiv b^2 \pmod n$ فليس من الضروري أن يكون $a \equiv b \pmod n$

$2^2 \equiv 3^2 \pmod 5$ ولكن $2 \not\equiv 3 \pmod 5$

2) اعطي مثالاً تبين أنه إذا كان $a^k \equiv b^k \pmod n$ و $k \equiv j \pmod n$ فليس من الضروري أن يكون $a^j \equiv b^j \pmod n$

$4^2 \equiv 5^2 \pmod 3$ و $2 \equiv 5 \pmod 3$

$\longrightarrow 4^5 \not\equiv 5^5 \pmod 3$ ($5^2 \equiv -1$ ، $5 \equiv -1$ ، $4^5 \equiv 1$ ، $4 \equiv 1 \pmod 3$)

3) اثبت أنه إذا كان $(a,n)=1$ فإن الأعداد $c, c+a, c+2a, \dots, c+(n-1)a$ تؤلف مجموعة بواقي تامة بالقياس n , $c \in \mathbb{Z}$

= بما أن عدد الأعداد n نفرض جدلاً أنه يوجد عددين متطابقين بالمقاس n.

$$c+ka \equiv ((c+ra) \bmod n) \quad ; \quad 0 \le k < r \le n-1$$

$ka \equiv ra \pmod n$ حسب الخواص:

$k \equiv r \pmod n$ لأن $(a,n)=1$

و منه تناقض كون k, r من مجموعة البواقي التامة بالقياس n

6- اثبت أنه إذا كان العدد الصحيح a لا يقبل القسمة على الأعداد: 2, 3, 5, 7 كان $840 \mid a^{12}-1$

$840 = 2^3 \times 3 \times 5 \times 7$

1) $(a,2)=1 \Rightarrow$ فرديا $\Rightarrow a^2 \equiv 1 \pmod 8$ حسب مبرهنة فيرما الصغرى

$(a^2)^6 \equiv 1 \pmod 8 \rightarrow 8 \mid a^{12}-1$ ①

2) $(a,3)=1 \rightarrow a^2 \equiv 1 \pmod 3$

$a^{12} \equiv 1 \pmod 3 \rightarrow 3 \mid a^{12}-1$ ②

3) $(a,5)=1 \rightarrow a^4 \equiv 1 \pmod 5$

$a^{12} \equiv 1 \pmod 5 \rightarrow 5 \mid a^{12}-1$ ③

4) $(a,7)=1 \rightarrow a^6 \equiv 1 \pmod 7$

$a^{12} \equiv 1 \pmod 7 \rightarrow 7 \mid a^{12}-1$ ④

بما أن 8, 3, 5, 7 أولية مثنى مثنى فإن

$8 \times 3 \times 5 \times 7 = 840 \mid a^{12}-1$

9- أوجد باقي قسمة 41^{65} على 7.

$41^{65} \equiv k \pmod 7$

بما أن $(41,7)=1$ فيرما $\Leftarrow 41^6 \equiv 1 \pmod 7$

$\left((41)^6\right)^{10} \cdot (41)^5 \equiv (-1)^5 = -1 \equiv 6 \pmod 7$

10- أوجد باقي قسمة المجموع $1^5+2^5+3^5+\cdots+99^5+100^5$ على العدد 4.

$2^5 \equiv 0 \pmod 4$

$4^5 \equiv 0 \pmod 4$

$100^5 \equiv 0 \pmod 4$

الأعداد الزوجية

نبين أن مجموع هذه الأعداد بالقياس 4 هو

$1^5 \equiv 1 \pmod 4$

$3^5 \equiv 3 \pmod 4$

$99^5 \equiv 99 \pmod 4$

$1^5+3^5+5^5+\cdots+99^5 \equiv 1+3+\cdots+99$

$\sum_{k=1}^{n}(2k-1) = 1+3+\cdots+(n-1) = n^2$ من الكتاب

$2n-1=99$

$2n=100$

$n=50$

$\Rightarrow 1+3+\cdots+99 = 50^2$

$1+3+\cdots+99 = 2500 \equiv 0 \pmod 4$

$\frac{119}{32} = \langle 3,1,2,1,1,4 \rangle$

$\frac{118}{303} = \langle 0,2,1,1,3,5,3 \rangle$

$\frac{-503}{187} = \frac{-561+58}{187} = \langle -3,3,4,2,6 \rangle$

$\frac{-125}{198} = \langle -1,2,1,2,2,10 \rangle$

انتهت المحاضرة ^^

٢٠١٦/٥/٩

المحاضرة التاسعة

مجموعة البواقي المختزلة

تعريف: لتكن المجموعة $A(m)=\{0,1,2,\dots,m-1\}$ مجموعة البواقي التامة بالمقاس m فتكون مجموعة البواقي المختزلة هي:

$$T(m)=\{a\in A \;;\; (a,m)=1\}$$

مثال: $m=6 \leftarrow A(6)=\{1,2,3,4,5,6\}$

$a\in A$, $(a,m)=1 \rightarrow T(6)=\{1,5\}$

القاسم المشترك لـ 6, 5 هو 1.

مثال: $m=12 \leftarrow A(12)=\{0,\pm1,\pm2,\pm3,\pm4,\pm5,6\}$

مجموعة البواقي المختزلة هي $\{\pm1,\pm5\}$

$$T(12)=\{1,5,7,11\}$$

دالة أولر: φ

هي دالة عددية قيمتها عند العدد m ; $\varphi(m)$ تساوي عدد الأعداد التي هي اصغر من m وأولية نسبياً مع m

$\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$

$\varphi(6)=2$, ...

مبرهنة: دالة أولر $\varphi(m)$ هي دالة ضربية. أي تحقق: ① $\varphi(1)=1$

② $\varphi(m.n)=\varphi(m).\varphi(n)$ حيث $m,n\in\mathbb{Z}^+$, $(n,m)=1$

مبرهنة: إذا كان P عدداً أولياً فإن $\varphi(P)=P-1$

مجموعة البواقي التامة $A(P)=\{0,1,2,\dots,P-1\}$

هي مجموعة البواقي المختزلة $T(P)=\{1,2,\dots,P-1\}$

أي $\varphi(P)=P-1$ عددها $P-1$

مبرهنة: إذا كان P عدداً أولياً فإن $\varphi(P^\alpha)=P^{\alpha-1}(P-1)$

الإثبات: مجموعة البواقي التامة بالمقاس P^α

عدد العناصر هو $m=P^\alpha$

$A=\{0,1,\dots,P^\alpha-1\}$

$=\{1,2,P,\dots,P^2,\dots,P.P^{\alpha-1}\}$

نجد العناصر التي لها عامل مشترك مع p^α في A هي :

$$p, 2p, 3p, \dots, p^{\alpha-1}.p$$

عدد هذه العناصر هو $p^{\alpha-1}$ فيكون عدد العناصر من المجموعة البواقي التامة التي هي أولية مع p^α هي :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$
$$= p^\alpha\left(1-\frac{1}{p}\right)$$
$$= p^{\alpha-1}(p-1)$$

مبرهنة : إذا كان $n = p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_r^{\alpha_r}$, p_i أوليات مختلفة فإن :

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)$$

الإثبات :

بما أن الدالة φ ضربية فإن :

$$\varphi(n) = \varphi(p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1}).\varphi(p_2^{\alpha_2})\dots\varphi(p_r^{\alpha_r})$$
$$= p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_r^{\alpha_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)$$
$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)$$

* $\varphi(360) = \varphi(2^3.3^2.5)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$
$= 2^3.3^2.5\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 96$

مبرهنة أويلر :

إذا كان $(a,m)=1$ فإن $a^{\varphi(m)} \equiv 1 \pmod m$

الإثبات : نأخذ مجموعة البواقي المختزلة بالقاس m وهي $T = \{a_1, a_2, \dots, a_{\varphi(m)}\}$

كذلك تكون المجموعة $T_1 = \{aa_1, aa_2, \dots, aa_{\varphi(m)}\}$

أيضاً مجموعة بواقي مختزلة بالمقاس m لذ أن عناصر T_1 أولية مع m وعناصر T_1 غير متطابقة بالمقاس m لنفرض عكس ذلك أي لوجد اعداد من T_1 متطابقة. $aa_i \equiv aa_j \pmod m$

بما أن $(a,m)=1 \Longleftarrow a_i \equiv a_j \pmod m$

$\{1 \le i < j \le \varphi(m)\}$ وهذا تناقض

بما أن كل عنصر من T يطابق عنصر من T_1 بالمقاس m ومنه جداء عناصر T يطابق جداء عناصر T_1 بالمقاس m

$a.a_1.a.a_2.\dots.a\varphi(m)\equiv a_1.a_2\dots a_{\varphi(m)}$

$a^{\varphi(m)}.a_1a_2\dots a_{\varphi(m)}\equiv a_1.a_2\dots a_{\varphi(m)} \pmod m$

بما أن $(a_1.a_2\dots a_{\varphi(m)}, m)=1$

نجد أنه $a^{\varphi(m)}\equiv 1 \pmod m$

* نجد أن مبرهنة فيرما الصغرى هي حالة خاصة عندما $m=p$ من مبرهنة أولر $a^{p-1}\equiv 1 \pmod p$

مثال: أوجد رقمي الآحاد والعشرات للعدد 3^{256} (رقمي الآحاد والعشرات في العدد 3^{256} هو باقي قسمته على 100)

$3^{\varphi(100)}\equiv 1 \pmod{100}$, $\varphi(100)=\varphi(2^2.5^2)$

$=2^2.5^2\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$

$=2^2.5^2\left(\frac{1}{2}\right)\left(\frac{4}{5}\right)=40$

$\Rightarrow 3^{40}\equiv 1 \pmod{100}$

$3^{256}=(3^{40})^6.3^{16}\equiv 3^{16}\equiv(81)^4\equiv(-19)^4\equiv(19)^4\equiv(361)^2\equiv(61)^2$

$\equiv(3721)\equiv 21 \pmod{100}$

مثال: حل المطابقة $6x\equiv 15 \pmod{21}$

$(6,21)=3 \nmid 15$ إذاً للمطابقة ثلاث حلول مختلفة بالقاسم m

$2x\equiv 5 \pmod 7$

$(2,7)=1$; $2^{\varphi(7)}\equiv 1 \pmod 7$, $2^6\equiv 1 \pmod 7$

$2^6x\equiv 5.2^6 \pmod 7$

$x\equiv 5.4 \pmod 7$

$\therefore x\equiv 6 \pmod 7 \Rightarrow x\equiv 6+7t \quad t=0,1,2$

$x\equiv 6,13,20 \pmod 7$

$x\equiv 6,13,20 \pmod{21}$

نتيجة: إذا أقسم القاسم d جميع قواسم العدد n فإن $\frac{n}{d}$ يقسم كذلك جميع قواسم العدد n

الموضوع : .....

$n=12$

$d=\{1,2,3,4,6,12\}$

$\frac{n}{d}=\{12,6,4,3,2,1\}$

$d_1=\frac{n}{d}$ ، $n=d.d_1$ ، $d \setminus n$ ، $d_1 \setminus n$

الدالة τ: هي الدالة العددية قيمتها عند العدد n تساوي عدد القواسم الموجبة للعدد n.

$$\tau(n)=\sum_{d \setminus n} 1$$

$\tau(1)=1$ ، $\tau(2)=2$ ، $\tau(3)=2$ ، $\tau(4)=3$ ، $\tau(5)=2$ ، $\tau(7)=2$

$\tau(11)=\tau(13)=2$

بشكل عام: p عدد أولي $\tau(p)=2$

$n=p^\alpha$ تكون قواسم العدد $n=p^\alpha$ هي $1, p, p^2, \dots, p^\alpha$

عددهم هو $\alpha+1$ أي $\tau(p^\alpha)=\alpha+1$

إذا كان $n>1$ الشكل القانوني لـ $n=p_1^{\alpha_1} \dots p_r^{\alpha_r}$

فإن $\tau(n)=\tau(p_1^{\alpha_1}) \dots \tau(p_r^{\alpha_r})$

كون τ دالة ضربية.

$$= (\alpha_1+1)(\alpha_2+1) \dots (\alpha_r+1)$$

* τ دالة ضربية لأنها تحقق:

* $\tau(1)=1$

كذلك $\tau(d_1.d_2) = \tau(d_1).\tau(d_2)$

عددية $\rightarrow$ $F(n)=\sum_{d \setminus n} f(d)$ $\rightarrow$ عددية

$f(d)=1 \Longleftarrow f(1)=1$

$f(d_1.d_2)=1$

$$f(d_1.d_2)=\sum_{d \setminus d_1.d_2} 1 = f(d_1).f(d_2)$$

ثم استنتج أن τ دالة ضربية.

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1)$$
$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

$$\tau(360) = \tau(2^3 \cdot 3^2 \cdot 5) = 4 \times 3 \times 2 = 24$$

الدالة $\sigma(n)$ هي دالة عددية تعطيها كل العدد n يساوي مجموع القواسم الموجبة للعدد n

$$\sigma(n) = \sum_{d \mid n} d$$

$\sigma(1) = 1$ ، $\sigma(2) = 3$ ، $\sigma(3) = 4$ ، $\sigma(4) = 7$ ، $\sigma(5) = 6$
$\sigma(6) = 12$ ، $\sigma(7) = 8$

مبرهنة: الدالة σ هي دالة ضربية:

1) $\sigma(1) = 1$

2) $\sigma(n.m) = \sigma(n)\sigma(m)$ ، $(n,m) = 1$

حسب الصيغة f دالة ضربية فإن $F(n) = \sum_{d \mid n} f(d)$ الدالة ضربية

$f(d) = d$ نثبت أن $f(d) = d$ دالة ضربية فإن $\sigma(n) = \sum_{d \mid n} d$ دالة ضربية.

1) $f(1) = 1$

2) $(d_1, d_2) = 1$; $f(d_1 d_2) = d_1 d_2 = f(d_1) \cdot f(d_2)$

$f(d) = d$ دالة ضربية ومنه $\sigma(n) = \sum_{d \mid n} d$ هي دالة ضربية.

إذا كان $n = p$ $\Leftarrow$ $\sigma(p) = p + 1$

إذا كان $n = p^\alpha$ $\Leftarrow$ قواسم العدد p^α هي: $1, p, p^2, \dots, p^\alpha$

$$\sigma(p^\alpha) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$$

إذا كان $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

$$\sigma(n) = \sigma(p_1^{\alpha_1} \cdots p_r^{\alpha_r})$$
$$= \sigma(p_1^{\alpha_1}) \cdot \sigma(p_2^{\alpha_2}) \cdots \sigma(p_r^{\alpha_r})$$
$$= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}$$
$$= \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

$$\sigma(360) = \sigma(2^3 \cdot 3^2 \cdot 5) \cdot \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1}$$

$$\sigma(360) = 15 \cdot 13 \cdot 6 = 1170$$

★ الدالتان τ ، σ ليستا ضربيتين تماماً.

$$\tau(20) = \tau(2^2 \cdot 5) = 6$$

$$\tau(2) \cdot \tau(10) = 2 \cdot 4 = 8 \qquad (2,10) = 2$$

ملاحظة:

$$\tau(20) = 6 \neq 8 = \tau(2) \cdot \tau(10)$$

τ ليست ضربية تماماً.

$$\sigma(20) = \sigma(2^2 \cdot 5) = \frac{2^3-1}{2-1} \cdot \frac{5^2-1}{5-1} = 7 \cdot 6 = 42$$

$$\sigma(2) \cdot \sigma(10) = 3 \cdot 18 = 54$$

$$\sigma(20) = 42 \neq \sigma(2) \cdot \sigma(10) = 54$$

σ ليست ضربية تماماً.

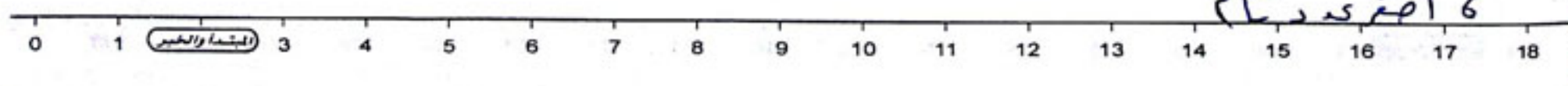
الأعداد التامة (الكاملة): تقول عن العدد n أنه تام (كامل) إذا كان $\sigma(n) = 2n$

ونقول أن العدد n هو عدد ناقص التام إذا كان: $\sigma(n) < 2n$

ويسمى فوق التام إذا كان: $\sigma(n) > 2n$

$$\sigma(6) = \sigma(2) \cdot \sigma(3) = 3 \cdot 4 = 2 \cdot 6 = 12$$

6 أصغر عدد تام



$\sigma(28) = \sigma(2^2 \cdot 7) = \frac{2^3-1}{2-1} \cdot \frac{7^2-1}{7-1} = 7 \cdot 8 = 56 = 2 \cdot 28$

28 هو عدد تام

مثال عن العدد الناقص (الغير التام):

$\sigma(8) = \sigma(2^3) = 15 < 2 \cdot 8 = 16$

وبكون 8 عدد ناقص.

مثال عن العدد فوق التام (زائد):

$\sigma(12) = \sigma(2^2 \cdot 3) = 7 \cdot 4 = 28 > 2 \cdot 12$

12 هو عدد زائد.

العددين التوأمين: هما عددين اوليان الفرق بينهما 2

$(3,5)$ ، $(5,7)$ ، $(11,13)$ ، $(17,19)$ ، ...

الأعداد المتحابة: نقول عن العددين انهما متحابان n و m.
إذا حققت مايلي:

$\sigma(n) - n = m$

$\sigma(m) - m = n$

بالرموز: $\sigma(n) = \sigma(m) = n+m$

مثال: $(220, 284)$

$\sigma(220) = \sigma(2^2 \cdot 5 \cdot 11) = 7 \cdot 6 \cdot 12 = 504$

$\sigma(220) - 220 = 504 - 220 = 284$

$\sigma(284) = \sigma(2^2 \times 71) = 7 \cdot 72 = 504$

$\sigma(284) - 284 = 504 - 284 = 220$

لا يوجد عدد تام فردي

الصيغة : $1 + 2 + 2^2 + \dots + 2^{k-1} = 2^k - 1 = p$

تعطي اعداد أولية واعداد غير اولية:

$k = 2 \Rightarrow 1 + 2 = 3$

$k = 3 \Rightarrow 1 + 2 + 2^2 = 7$

$k = 4 \Rightarrow 1 + 2 + 2^2 + 2^3 = 15$ غير أولي

خاصة: إذا كان العدد $2^k - 1$ اولياً , $k > 1$

فإن : $n = 2^{k-1}(2^k - 1)$

هو عدد تام (كامل) وكل عدد تام (كامل) زوجي هو من الشكل

الـــبات:

كذلك العدد الناقص هو : $A = 2^{k-2}(2^k - 1)$

والعدد الزائد هو: $B = 2^k(2^k - 1)$

امثلة:

1) $k = 2 \Rightarrow 2^k - 1 = 3$ اولي $\Rightarrow n = 2.3 = 6$

$k = 3 \Rightarrow 2^3 - 1 = 7$ اولي $\Rightarrow n = 4.7 = 28$

2) $k = 2 \Rightarrow 2^2 - 1 = 3$ اولي $\Rightarrow A = 3$ عدد ناقص

$k = 3 \Rightarrow 2^3 - 1 = 7$ اولي $\Rightarrow A = 27 = 14$ عدد ناقص

العدد الزائد: $B = 2^k(2^k - 1)$

$k = 2 \Rightarrow 2^2 - 1 = 3$ اولي $\Rightarrow B = 4.3 = 12$

$k = 3 \Rightarrow 2^3 - 1 = 7$ اولي $\Rightarrow B = 8.7 = 56$

الموضوع : .....

برهنة: إذا كان العدد $a^k - 1$ أولياً
$k \geq 2$ ، $a > 0$ فإن $a = 2$ و k عدد أولي
تسمى الأعداد $M_k = 2^k - 1$ ، $k \geq 2$
أعداد ميرسين

الأعداد $M_p = 2^p - 1$ هي أعداد أوليّة، سميت أعداد ميرسين الأوليّة.
وتكون أوليّة عندما p يأخذ القيم:
$p = 2, 3, 5, 7, 13, 17, 19, 31, 127, 257$.

دالة موبياس: نعرّف دالة موبياس μ قيمتها عند n تساوي:

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & p^2 \mid n \quad p \text{ أولي} \\ (-1)^r & n = p_1 \cdot p_2 \cdots p_r \end{cases}$$

$\mu(1) = 1$
$\mu(2) = \mu(3) = -1$
$\mu(4) = \mu(9) = 0$
$\mu(5) = -1$
$\mu(6) = 1$

* μ هي دالة ضربية
1) $\mu(1) = 1$
2) $\mu(n.m) = \mu(n).\mu(m)$
$(n, m) = 1$

صيغة موبياس للتعاكس: إذا كانت F ، f دالتين عدديتين
وكان $F(n) = \sum_{d \mid n} f(d)$

ملاحظة :

$$f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

تعريف : دالة ليوفيل

$$\lambda(n) = \begin{cases} 1 & n = 1 \\ (-1)^{\alpha_1+\alpha_2+\dots+\alpha_r} & ; \ n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \end{cases}$$

وهي دالة ضربية.

$\lambda(1) = 1$ ، $\lambda(2) = \lambda(3) = -1$

$\lambda(4) = 1$ ، ...

دالة ما نجولد : تعرف كالتالي :

$$\Lambda(n) = \begin{cases} \log p & n = p^k \text{ ، } p \text{ اولي} \\ & 1 \le k \\ 0 & \text{فيما عدا ذلك} \end{cases}$$

خواص :

1) $\sum_{d|n} \Lambda(d) = \log n$

2) $\Lambda(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log d$

الموضوع: المحاضرة العاشرة ١٦/١٦/٢٠١٧

المراتب والجذور الأولية والأدلة

مرتبة عدد a بالقاس m. هو أصغر عدد صحيح موجب e بحيث ما يلي:

$$a^e \equiv 1 \pmod m$$

e هو مرتبة العدد a بالقاس m

كذلك نسمي e دليل العدد a بالقاس m

كذلك نسمي e دليل العدد a بالقاس m

ونكتب $e = ind\, a \pmod m$ حيث $(a,m)=1$

مثال: $m=7$, $a=2$ $\Leftarrow$ $(2,7)=1$

$2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1 \pmod 7$

دليل 2 بالقاس 7 هو $e=3$

$5^2 \equiv 1 \pmod 6$

مرتبة العدد 5 بالقاس 6 هو 2

مثال: أوجد مرتبة العدد 3 بالقاس 14 هو

$3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv -1$

$3^4 \equiv -3 \equiv 11$, $3^5 \equiv -9 \equiv 5$

$3^6 \equiv 1 \pmod{14}$

مرتبة العدد 3 بالقاس 14 هو $e=6$

مبرهنة: إذا كانت مرتبة العدد a هي e بالقاس m فإن:

$a^k \equiv 1 \pmod m$, $k>0$

إذا وفقط إذا كان k | e

الإثبات:

إذا كان e | k $\quad k = e.q$

$a^k = (a^e)^q \equiv 1 \pmod m$

بالعكس: $a^k \equiv 1 \pmod m$

$k = eq + r \quad \dots \quad 0 \le r < e$

$1 \equiv a^k = (a^e)^q . a^r \equiv a^r \pmod m$

$\Rightarrow a^r \equiv 1 \pmod m \wedge 0 \leq r < e$

هذا الأمر محقق فقط إذا كان $r=0 \Leftarrow K = eq$

ومنه $e \setminus K$

حسب أولر لدينا $(a,m)=1 \Leftarrow a^{\varphi(m)} \equiv 1 \pmod m$

وإذا كانت مرتبة العدد a هي c بالمقاس m حسب المبرهنة السابقة $c \setminus \varphi(m)$ مرتبة العدد a وهي c تنتمي إلى مجموعة قواسم العدد $\varphi(m)$

مثال: إذا كانت $m=13$, $a=2$, $(2,13)=1$

مرتبة العدد 2 تنتمي إلى مجموعة قواسم $\varphi(13)=12$

مجموعة قواسم العدد 12 هي $c \in \{1,2,3,4,6,12\}$

$2^1 \equiv 2, 2^2 \equiv 4, 2^3 = 8, 2^4 \equiv 3, 2^6 = 12 \equiv -1, 2^{12} \equiv 1 \pmod{13}$

هل يوجد حلول للمعادلة $a^4 \equiv 1 \pmod{12}$ وتكون 4 مرتبة العدد a بالمقاس 12 ؟

$(a,12)=1$ أي أن a تنتمي إلى مجموعة البواقي المنزلة بالمقاس 12 وهي:

$\{1,5,7,11\}$

c هي المرتبة "4" ليست مرتبة العدد 5 بالمقاس 12 " $5^2 = 25 \equiv 1 \pmod{12}$

$7^2 \equiv 11^2 \equiv 1 \pmod{12}$

نجد أن $c=2$ مرتبة العدد 5, 7, 11 بالمقاس 12 وليس العدد 4

$(\varphi(12)=4)$

مبرهنة: إذا كانت c مرتبة العدد a بالمقاس m

فإن $a^t \equiv a^s \pmod m \iff t \equiv s \pmod c$

الإثبات: $a^t \equiv a^s \pmod m$, $(a,m)=1$

$a^{t-s} \equiv 1 \pmod m$, c هي المرتبة لـ a

$c \setminus t-s \Leftarrow t \equiv s \pmod c$

العكس: $t \equiv s \pmod c \Leftarrow t = eq+s$

$a^t = (a^e)^q . a^s = a^s \pmod m$

نتيجة: إذا كانت a مرتبتها c بالمقاس m فإن الأعداد $a, a^2, \dots, a^c$ غير متطابقة بالمقاس m $(a,m)=1$

مبرهنة : إذا كانت مرتبة العدد a هي e بالمقاس m فإن مرتبة العدد a^k $(k>0)$ بالمقاس m هي $\frac{e}{d}$ ، $d=(e,k)$

نبدأ البرهان :

$a^e \equiv 1 \pmod m \Leftarrow$ مرتبة a^k هي $\frac{e}{d}$ $d=(e,k)$

* إذا كان $d=(e,k)=1$ فإن مرتبة a^k هي نفس مرتبة العدد a

تمرين : عين مراتب الأعداد من 1 إلى 12 بالمقاس 13

a	1	2	3	4	5	6	7	8	9	10	11	12
مرتبة a	1	12	3	6	12		4	3		12	2	

$\varphi(13)=12$; أي $2^{12} \equiv 1 \pmod{13}$ ومنه نجد أن مرتبة العدد 2 بالمقاس 13 هي 12

$2^{2=k} = 4$, $d=(2,12)=2 \Rightarrow \frac{e}{d} = \frac{12}{2} = 6$

$2^{3=k} \equiv 8$ $d=(3,12)=3 \Rightarrow \frac{e}{d} = \frac{12}{3} = 4$

$2^4 \equiv 3$, $d=(4,12)=4 \Rightarrow \frac{e}{d} = \frac{12}{4} = 3$

$2^5 \equiv 6$, $d=(5,12)=1 \Rightarrow \frac{e}{d} = \frac{12}{1} = 12$

$2^6 \equiv 12$, $d=(6,12)=6 \Rightarrow \frac{e}{d} = \frac{12}{6} = 2$

$2^7 \equiv 11$, $d=(7,12)=1 \Rightarrow \frac{e}{d} = \frac{12}{1} = 12$

$2^8 \equiv 9$, $d=(8,12)=4 \Rightarrow \frac{e}{d} = \frac{12}{4} = 3$

$2^9 \equiv 5$, $d=(9,12) \Rightarrow \frac{e}{d} = \frac{12}{3} = 4$

$2^{10} \equiv 10$, $d=(10,12)=2 \Rightarrow \frac{e}{d} = \frac{12}{2} = 6$

$2^{11} \equiv 7$ $d=(11,12)=1 \Rightarrow \frac{e}{d} = \frac{12}{1} = 12$

مبرهنة: إذا كانت a مرتبة a بالمقاس m وكانت f=b بالمقاس m
فإن مرتبة a.b بالمقاس m هي e.f

مثال:
$2^3 \equiv 1 \pmod 7$
$6^2 \equiv 1 \pmod 7$
فإن مرتبة 2.6=12 هي 2.3
$12^{2.3} \equiv 1 \pmod 7$
و لن $12 \equiv 5 \pmod 7$
$12^6 = 5^6 = (25)^3 \equiv 4^3 \equiv 1 \pmod 7$

الجذور الأولية:
نقول ان a جذر أولي بالمقاس m إذا و فقط إذا كانت مرتبة العدد a بالمقاس m هي $\varphi(m)$

$a^{\varphi(m)} \equiv 1 \pmod m$ $\iff$ a جذر أولي بالمقاس m
$\varphi(m)$ هي أصغر عدد تحقق ذلك

إذا كان m=13 فإن جذور العدد 13 هي من الجدول السابق
m=13 أربع جذور أولية للعدد {2, 6, 7, 11}

مبرهنة: إذا كان (a,m)=1 و a جذراً أولياً بالمقاس m
فإن الاعداد $\{a, a^2, \dots, a^{\varphi(m)}\}$ هي مجموعة البواقي المختزلة بالمقاس m

مبرهنة: إذا كان a جذراً أولياً للعدد m حيث (a,m)=1 فإن للعدد m
$\varphi(\varphi(m))$ جذراً أولياً.

البرهان: a جذر أولياً للعدد m
(a,m)=1 أي a تنتمي إلى مجموعة البواقي المختزلة بالمقاس m وهي
$T_m = \{a, a^2, a^3, \dots, a^{\varphi(m)}\}$
a^k بالمقاس m تساوي مرتبة a بالمقاس m
إذا كان $(k, \varphi(m)) = 1$ حسب نتيجة سابقة
نبحث عن k بحيث تكون قيم k أولية مع $\varphi(m)$ وعدد هذه القيم هي
$\varphi(\varphi(m))$

مبرهنة :

يوجد للعدد m جذراً أولياً إذا كان $m=2$ أو $m=4$ أو $m=p^n$ أو $m=2p^n$, p عدد أولي $n \in \mathbb{Z}^+$

مثال : أوجد جذور العدد $m=10$ ، $m=2.5$

عدد الجذور الأولية للعدد 10 هي

$$\varphi(\varphi(10)) = \varphi(4) = 2$$

الجذر a ينتمي إلى مجموعة البواقي المختزلة بالقاس 10

$$T(10) = \{1, 3, 7, 9\}$$

$$3^2 \equiv 9 \equiv -1 \pmod{10}$$

$$3^4 \equiv 1 \pmod{10}$$

لنبحث عن الجذور من الشكل 3^k بحيث يكون $(k, \varphi(m)) = 1$

$$(k, 4) = 1$$

$$k \in \{1, 3\}$$

$$3^3 \equiv 7 \pmod{10}$$

7 هو الجذر الثاني

$$\varphi(16) = 2^4\left(1 - \frac{1}{2}\right)$$

$$7^2 \equiv 9$$

$$7^4 \equiv 1 \pmod{10}$$

3, 4 جذور أولية للعدد 10

$$3^{\varphi(16)} \equiv 1 \pmod{16}$$

/ / المحاضرة 19

قواعد قابلية القسمة :

كل عدد صحيح موجب يكتب بالشكل $N = a + 10b$

يقبل القسمة على العدد $M_1 = 1 + 10c$

M_1 مثل جميع الأعداد التي آحادها واحد

إذا قبل العدد $N = b - ac$ القسمة على M_1 وبالعكس

القواعد: يقبل العدد $N = a + 10.b$ القسمة على العدد

11: إذا قبل العدد $a - b$ القسمة على 11

21 " " " " $b - 2a$ " " " 21

31 " " " " $b - 3a$ " " " 31

41 إذا قبل العدد $b - 4a$ " " " 41

111 " " " $b - 11a$ " " " 111

2) يقبل العدد $N = a + 10b$ القسمة على العدد $M_3 = 3 + 10c$

إذا قبل العدد

$N_3 = b + (1 + 3c)a$

القسمة على M_3 وبالعكس.

القواعد: يقبل العدد $N = a + 10b$ القسمة على ,

13 إذا قبل العدد $b + 4a$ القسمة على 13

23 إذا قبل العدد $b + 7a$ " " 23

33 " " " $b + 10a$ " " " 33

/ /

تابع ص 93 إذا قبل العدد $a+28b$ العشرة ك 93

مثال: $13\overline{)7956}$

79	5	6
+	24	
81	9	
63		
11	7	
39		

39 ثقيل العشرة ك 13

أي العدد المفروض 7956

ثقيل العشرة ك 13

3) ثقيل العدد $N=a+10b$ العشرة ك

$M_7 = 7+10c$

إذا ثقيل العدد:

$N_7 = b-(2+3c)a$ العشرة ك M_7 وبالعكس

قواعد: ثقيل العدد $N=a+10b$ العشرة ك:

7 إذا قبل العدد $b-2a$ العشرة ك 7

17 إذا قبل العدد $b-5a$ " " 17

27 إذا قبل " $b-8a$ " " 27

107 " " " $b-32a$ " " 107

/ /

مثال / 7344 على 17

734	4	
-20		
71	4	
-20		
5	1	
-5		
0		

الصفر قبل القسمة

على 17 العدد

قبل القسمة 7344

17 على

نقبل العدد $N = a + 10b$ القسمة على العدد $9 + bc = M_9$

إذا قبل العدد

$$N_9 = b + (1+c)a$$

القسمة على M_9 والعكس

القواعد: نقبل العدد $N = a + 10b$ القسمة على

19 إذا قبل العدد $b + 2a$ القسمة على 19

29 " " " $b + 3a$ " " 29

39 " " " $b + 4a$ " " 39

/ /

اثبت أن

19 | 8209 | 9

+18

822 | 7
14

32 | 6
12

9 | 5
10

19

4) أثبت أن أس أكبر قوة للعدد 5 تقسم $(5^n - 4)!$

هي $\frac{5^n - 4n - 1}{4}$

$n = 1$

$$H_5((5^n-4)!) = \left[\frac{5^n-4}{5}\right] + \left[\frac{5^n-4}{5^2}\right]$$

$$+ \cdots + \left[\frac{5^n-4}{5^n}\right]$$

$$= 5^{n-1} + \left[\frac{-4}{5}\right] + 5^{n-2} + \left[\frac{-4}{5^2}\right] + \cdots + 1 + \left[\frac{-4}{5^n}\right]$$

$$= 5^{n-1} + 5^{n-2} + \cdots + 5 + 1 + \underbrace{[-1-1-\cdots-1]}_{\text{or } n}$$

$$= \frac{5^n - 1}{5-1} - n = \frac{5^n - 4n - 1}{4}$$

$$5^n - 4 = 4 \cdot 5^{n-1} + 4 \cdot 5^{n-2} + \cdots + 4 \cdot 5 + 1 \quad .2$$

كتبنا العدد $n-5^n$ بالنظام الذي أساسه 5

$$\sum_{i=0}^{n} a_i = 4(n-1)+1$$

$$H_5((5^n-4)) = \frac{n-\sum a_i}{5-1} = \frac{5^n-4-4(n-1)-1}{4}$$

$$= \frac{5^n-4n-1}{4}$$

$H_7(24001) = 396$ (6

7) إذا كان n عدداً صحيحاً موجباً فأثبت أن:

$$\mu(n)\,\mu(n+1)\,\mu(n+2)\,\mu(n+4) = 0$$

$$\mu(n) = \begin{cases} 1 & : n = 1 \\ 0 & p^2 \mid n \text{ يوجد } p \text{ أولي} \\ (-1)^r & n = p_1 p_2 \cdots p_r \end{cases}$$

حيث $n \in \mathbb{Z}^+$

$n \equiv 0 \pmod 4$ أو $n \equiv 1 \pmod 4$ أو $n \equiv 2 \pmod 4$ أو $n \equiv 3 \pmod 4$

$\Rightarrow$

$n \equiv 0 \pmod 4$

$n+1 \equiv 0 \pmod 4$

$n+2 \equiv 0 \pmod 4$

$n+3 \equiv 0 \pmod 4$

هوزاييك

/ /

$2^2 \equiv 4$

نجد انه اما ان يكون

$\mu(n) = 0$ أو

$\mu(n+1) = 0$ أو

$\mu(n+2) = 0$ أو

$\mu(n+3) = 0$ أو

بالتالي:

$$\mu(n).\mu(n+1).\mu(n+2)\mu(n+3) = 0$$

6) إذا كان $n = p_1^{q_1} \cdot p_2^{q_2} \cdots p_r^{q_r}$ حيث p_i اوليات مختلفة وإذا كانت f دالة ضربية فإثبت أن:

$$1) \sum_{d \mid n} \mu(d) f(d) = (1 - f(p_1)).(1 - f(p_2)) \cdots (1 - f(p_r))$$

الحل: إذا كان $n = p_1^{q_1}$ فإن قواسمه هي:

$$1, p_1, p_1^2, \cdots, p_1^{q_1}$$

$$\sum_{d \mid p_1^{q_1}} \mu(d) f(d) = \mu(1) f(1) + \mu(p_1) f(p_1) + \mu(p_1^2) \cdot f(p_1^2) + \cdots + \mu(p_1^{q_1}) f(p_1^{q_1})$$

$$\Rightarrow \sum_{d \mid p_1^{q_1}} \mu(d) f(d) = 1 - f(p_1)$$

وحيث $n = p_1^{q_1} \cdots p_r^{q_r}$ فإن

$$\sum_{d \mid \prod_{i=1}^{r} p_i^{\alpha_i}} \mu(d) f(d) = \prod_{i=1}^{r} \left(\sum_{d \mid p_i^{\alpha_i}} \mu(d) f(d) \right)$$

$$= \prod_{i=1}^{r} (1 - f(p_i))$$

2) $$\sum_{d \mid n} \mu(d) \tau(d) = (-1)^r$$

$f(d) = \tau(d)$ نضع (1) في

$$\sum_{d \mid n} \mu(d) \tau(d) = \prod_{i=1}^{r} (1 - \tau(p_i))$$

$$= \prod_{i=1}^{r} (1 - 2) = (-1)^r$$

$\tau(p_i) = 2$ لأن

3) $$\sum_{d \mid n} \mu(d) \sigma(d)$$

$f(d) = \sigma(d)$ نضع

$\sigma(p_i) = 1 + p_i$

11) إذا كان $(a, 30) = 1$ أثبت أن: $240 \mid a^4 - 1$

$240 = 2^4 \times 3 \times 5$

الحل: $(a, 2) = 1 \Leftarrow a$ فردي

$a^2 \equiv 1 \pmod{2^3}$ خاصة الشرط

$a^4 \equiv 1 \pmod{2^4} \Rightarrow 2^4 \mid a^4 - 1 \quad (1)$

$a^2 \equiv 1 \pmod{3}$ $\Leftarrow$ (مبرهنة) $(a,3) = 1$

$\Rightarrow a^4 \equiv 1 \pmod{3}$

$3 \mid a^4 - 1 \quad (2)$

$(a,5) = 1$

$a^4 \equiv 1 \pmod{5}$

$\Rightarrow 5 \mid a^4 - 1 \quad (3)$

$\Rightarrow 5 \cdot 2^4 \cdot 3 = 240 \mid a^4 - 1$

$\Rightarrow a^4 \equiv 1 \pmod{240}$

14) أثبت أن $\tau(n)$ يكون عدداً فردياً إذا كان n مربعاً كاملاً.

الحل:

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

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

إذا كان $\tau(n)$ فردياً فإن $\prod_{i=1}^{r}(\alpha_i+1)$ فردي $\Leftrightarrow$

(α_i+1) عدد فردي $\Leftrightarrow$ α_i عدد زوجي $\Leftrightarrow$

الخاصة السابقة:

$a \equiv b \pmod{p^r}$

$a^{p^s} \equiv b^{p^s} \pmod{p^{r+s}}$

/ /

$\alpha_i = 2\beta_i$ يوجد عدد k بحيث يكون $\Leftrightarrow$

$\Leftrightarrow$

$$n = p_1^{2\beta_1} \cdot p_2^{2\beta_2} \cdots p_r^{2\beta_r} = (p_1^{\beta_1} \cdots p_r^{\beta_r})^2$$

$$= m^2$$

22) إذا كان n عدداً كاملاً اثبت أن:

$$\sum_{d|n} \frac{1}{d} = 2$$

n عدد كامل $\Leftrightarrow \sigma(n) = 2n$

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} = 2n$$

$$\sum_{d|n} \frac{1}{\frac{n}{d}} = 2$$

25) استخدم أويلر لإثبات:

$$a^{13} \equiv a \pmod{2730}$$

$$(a, 2730) = 1$$

$$2730 = 2 \times 3 \times 5 \times 7 \times 13$$

/ /

$(a,2)=1 \Rightarrow a \equiv 1 \pmod 2$, $a^{12} \equiv 1 \pmod 2$

$a^{13} \equiv a \pmod 2$

$(a,3)=1 \Rightarrow a^2 \equiv 1 \pmod 3 \Rightarrow$

$a^{12} \equiv 1 \pmod 3$

$a^{13} \equiv a \pmod 3$

$(a,5)=1 \Rightarrow a^4 \equiv 1 \pmod 5 \Rightarrow a^{13} \equiv a \pmod 5$

$(a,7)=1 \Rightarrow a^6 \equiv 1 \pmod 7 \Rightarrow a^{13} \equiv a \pmod 7$

$(a,13)=1 \Rightarrow a^{12} \equiv 1 \pmod{13} \Rightarrow a^{13} \equiv a \pmod{13}$

اولية مش مش 13, 7, 5, 3, 2

$a^{13} \equiv a \pmod{2730}$

28. اثبت أن المجموعة:

$\{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$

هي مجموعة بواقي مختلفة بالمقياس 14

$\varepsilon(14) = 6$

لين هيك ان هذه الاعداد غير متطابقة بالمقياس 14

لنفرض انه يوجد تطابق بين هذه الاعداد

$$a^t \equiv a^s \pmod{14}$$

$$1 \le s < t \le 6$$

$$3^{t-s} \equiv 1 \pmod{14}$$

$$3^2 \equiv 9$$

$$3^3 \equiv -1$$

$$3^6 \equiv 1 \pmod{14}$$

$$3^6 \equiv 3^{\varphi(14)} \equiv 1 \pmod{14}$$

$$6 \mid t-s \implies t \equiv s \pmod 6$$

$$1 \le s < t \le 6$$

وهذا غير ممكن

وعدد عناصر هذه الزمرة هو $\varphi(14) = 6$

هذه الزمرة هي زمرة بواقي قابلة بالمقاس 14

او نبرهن ان 3 هو جذر للعدد 14

$$3^6 \equiv 1 \pmod{14} \quad : \quad 6 = \varphi(14)$$

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

$\varphi(m)$ هي مرتبة العدد a بالقياس m فإن a جذر أولي لـ m

تعريف الدليل :

ليكن r جذراً أولياً للعدد m وكان $(b,m)=1$ فإن أصغر عدد k تحقق $r^k \equiv b \pmod m$ حيث $1 \le k \le \varphi(m)$

يسمى دليل العدد b بالنسبة للأساس r والقياس m

ونرمز له بـ $k = \operatorname{Ind}_r b$ فنكتب $r^{\operatorname{Ind}_r b} \equiv b \pmod m$

خواص الأدلة :

ليكن $N, M \in \mathbb{Z}^+$

١ ، ٢ ، ٣

1, 2, 3

و r جذر أولي للعدد m

① إذا كان $M = N \pmod m \iff \operatorname{Ind}_r M \equiv \operatorname{Ind}_r N \pmod{\varphi(m)}$

الإثبات :

$$M = r^{\operatorname{Ind}_r M} \pmod m$$

$$\operatorname{Ind}_r M \equiv r^{\operatorname{Ind}_r N} \pmod m$$

$$\iff N = r^{\operatorname{Ind}_r N} \pmod m$$

$$r^{\operatorname{Ind}_r M} \equiv r^{\operatorname{Ind}_r N} \pmod m$$

$$[a^t \equiv a^s \pmod m \iff t \equiv s \pmod e \quad \text{عندما } a \text{ جذر}]$$

$$\operatorname{Ind}_r M \equiv \operatorname{Ind}_r N \pmod{\varphi(m)} \quad (1)$$

$$\operatorname{Ind}_r M.N \equiv \operatorname{Ind}_r M + \operatorname{Ind}_r N \pmod{\varphi(m)} \quad (2)$$

$$\operatorname{Ind}_r M^k \equiv k \operatorname{Ind}_r M \pmod{\varphi(m)} \quad (3)$$

$$\operatorname{Ind}_r N \equiv \operatorname{Ind}_s N \cdot \operatorname{Ind}_r S \pmod{\varphi(m)} \quad (4)$$

r ، s جذرين أوليين للعدد m

مثال : $m=13$ أوجد جدول الأدلة بالنسبة للأساس 2 والقياس 13

2 هو جذر أولي للعدد 13

$$2^{12} \equiv 1 \pmod{13} \qquad \varphi(13) = 12$$

0 1 (البداية والخير) 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

أخر يوم دوام

ذكرى farúza مع خالص محبتي وتقديري لك لزميلتي الغالية .

أمنيات الموضوع :

الآنسة : رزان سعيد . (27)

N	1	2	3	4	5	6	7	8	9	10	11	12
Ind N	12	1	4	2	9	5	11	3	8	10	7	6

$2^1 \equiv 2 \pmod{13}$

$2^2 \equiv 4$

$2^3 = 8$

$2^4 \equiv 3$

$2^5 \equiv 6$

$2^6 \equiv 12 \equiv -1$

$2^7 \equiv 11 \equiv -2$

$2^8 \equiv 9$

$2^9 \equiv 5$

$2^{10} \equiv 10$

$2^{11} \equiv 7$

$2^{12} \equiv 1$

$1 \leq k \leq 12$

$r^k \equiv b \pmod{m}$

$k = \text{Ind}_r\, b$

* اكتب جدول الأدلة للعدد 17 علماً أن 3 جذراً أولياً للعدد 17

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Ind N	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

$3^1 \equiv 3$

$3^2 \equiv 9$

$3^3 \equiv 10$

$3^4 \equiv 13 \equiv -4$

$3^5 \equiv 15 \equiv -2$

$3^6 \equiv 5$

$3^7 \equiv 11 \equiv -6$

$3^8 \equiv 16 \equiv -1$

$3^9 \equiv 14 \equiv -3$

$3^{10} \equiv 8$

$3^{11} \equiv 7$

$3^{12} \equiv 4$

$3^{13} \equiv 12 \equiv -5$

$3^{14} \equiv 2$

$3^{15} \equiv 6$

$3^{16} \equiv 1 \pmod{17}$

(17) أوجد الجذور الأولية للعدد 17 علماً أن 3 هو جذر أولي

مجموعة البواقي المختزلة للعدد 17 هي :

$T(17) = \{1, 2, 3, \ldots, 16\}$

لدينا ثمان جذور أولية مجموعة البواقي $\varphi(\varphi(17)) = \varphi(16) = 8$

المختزلة للعدد 16

$T(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$

ذكرى Sona

LOVE You

ذكرى رزان

1/5/201..

نبحث في الجذور الأولية من الشكل 3^k بحيث يكون
$(k,\varphi(m))=1$ ، $(k,16)=1$
القيم التي يأخذها k هي $k \in T(16)$
a^k ، a لهما نفس الرتبة إذا وفقط إذا كان $(k,16)=1$

$3^1=3 \Longrightarrow 3^{16}\equiv 1 \pmod{17}$
$3^5=5 \Longrightarrow 5^{16}\equiv 1 \pmod{17}$
$3^7=11 \Longrightarrow 11^{16}\equiv 1 \pmod{17}$
$3^3=10 \Longrightarrow 10^{16}\equiv 1 \pmod{17}$
$3^9=14 \Longrightarrow 14^{16}\equiv 1 \pmod{17}$
$3^{11}=7 \Longrightarrow 7^{16}\equiv 1 \pmod{17}$
$3^{13}=12 \Longrightarrow 12^{16}\equiv 1 \pmod{17}$
$3^{15}=6 \Longrightarrow 6^{16}\equiv 1 \pmod{17}$

نكتب جدول الأدلة لجذر العدد 11

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Ind,7	16	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

⑧ أوجد حلول التطابقات

① $3.x^3 \equiv 3 \pmod{13}$

باستخدام جدول الأدلة
2 جذر أولي للعدد 13 ، $\varphi(13)=12$ نأخذ دليل الطرفين
التطابقة بالنسبة للأساس 2

$\operatorname{Ind}_2 3+3\operatorname{Ind}_2 x \equiv \operatorname{Ind}_2 3 \pmod{12}$

نفرض $y=\operatorname{Ind}_2 x$ نأخذ القيم من الجدول:

$4+3y\equiv 4 \pmod{12}$
$3y\equiv 0 \pmod{12}$ $(3,12)=3 \mid 0$ التطابقة لها حلول
غير متطابقة

$y\equiv 0 \pmod 4$ $y=4+4t$ ، $t=0,1,2$

$y=4 \Rightarrow Ind_2 x \Rightarrow x \equiv 3 \pmod{13}$

$y=8 \Rightarrow x \equiv 9 \pmod{13}$

$y=12 \Rightarrow x \equiv 1 \pmod{13}$

2) $3x^6 \equiv 4 \pmod{13}$

2 جذر أولي لـ 13 $2^{12} \equiv 1 \pmod{13}$

$\varphi(13)=12$

نأخذ دليل طرفي التطابقة بالنسبة للأساس 2

$Ind_2 3 + 6\, Ind_2 x \equiv Ind_2 4 \pmod{12}$

$Ind_2 x \equiv y$ ونأخذ القيم من الجدول

$4+6y \equiv 2 \pmod{12}$

$6y \equiv -2 \pmod{12}$

$6y \equiv 10 \pmod{12} \Rightarrow (6,12) = 6 \nmid 10$

التطابقة ليس لها حل فالتطابقة المعطى ليس له حل

3) $x^8 \equiv 10 \pmod{13}$

$8y \equiv 10 \pmod{12}$

$(8,12) = 4 \nmid 10$ ليس للتطابقة حل

4) حل التطابقة غير الخطي

$9x^8 \equiv 8 \pmod{17}$

3 جذر أولي للعدد $\varphi(17)=16$

نأخذ دليل الطرفين

$Ind_3 9 + 8\, Ind_3 x \equiv Ind_3 8 \pmod{16}$

ونأخذ القيم من جدول 3^1 لأدلة العدد 17 $y = Ind_3 x$

$2+8y \equiv 10 \pmod{16}$

$8y = 8 \pmod{16}$, $(8,16) = 8 \nmid 8$

التطابقة 8 حلول غير متطابقة بالمقاس 16

$y \equiv 1 \pmod{2}$

الموضوع : .....

$y = 1 + 2t$

$t = 0, 1, 2, 3, 4, 5, 6, 7$

$y \equiv 1 \Longrightarrow x \equiv 3 \pmod{17}$

$y \equiv 3 \Longrightarrow x \equiv 10 \pmod{17}$

$y \equiv 5 \Longrightarrow x \equiv 5 \pmod{17}$

$y \equiv 7 \Longrightarrow x \equiv 11 \pmod{17}$

$y \equiv 9 \Longrightarrow x \equiv 14 \pmod{17}$

$y \equiv 11 \Longrightarrow x \equiv 7 \pmod{17}$

$y \equiv 13 \Longrightarrow x \equiv 12 \pmod{17}$

$y \equiv 15 \Longrightarrow x \equiv 6 \pmod{17}$