كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : السادسة /نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

يمكنكم طلب المحاضرات برسالة نصية (SMS) أو عبر (What's app-Telegram) على الرقم 0931497960

بعد أن درسنا التطابقات الخطية سندرس مع جملة تطابقات خطية لكن قبل ذلك سنحتاج إلى بعض المفاهيم والمعلومات

تعريف: الدالة العددية: هي الدالة المعرّفة على مجموعة الأعداد الصحيحة الموجبة أو مجموعة جزئية منها ومجموعة قيمها أعداد مركبة (عقدية).

الدالة العددية المضربية: يُقال بأنّ الدالة العددية f أنّها مضربيّة إذا تحقّق الشرط: $\gcd(a,b)=1$ و $\forall a,b \in \mathbb{Z}^+$ فإنّ $f(ab)=f(a).f(b)$

الدالة العددية المضربية تماماً:

يُقال عن الدالة f أنّها دالة مضربيّة تماماً إذا تحقّق الشرط:

$$\forall a,b \in \mathbb{Z}^+ \quad ; \quad f(ab)=f(a).f(b)$$

مثال: إذا أخذنا: $n,k \in \mathbb{Z}^+$ حيث $f(n)=n^k$

$$f(n_1.n_2)=(n_1.n_2)^k=n_1^k.n_2^k=f(n_1).f(n_2)$$

$\Leftarrow$ f دالة مضربيّة تماماً

دالة أولر:

$$\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$$

$$\phi(n)=|\{m \; ; \; 1 \le m \le n \;\&\; \gcd(m,n)=1\}|$$

أي أنّ $\phi(n)$ هو عدد الأعداد الصحيحة الموجبة m الأصغر أو تساوي n والأولية مع العدد n

قدرة المجموعة ولي قيمة مطلقة

$$\phi(1)=|\{m \; ; \; 1 \le m \le 1 \;\&\; \gcd(m,1)=1\}|=1$$

$$\phi(4)=|\{m \; ; \; 1 \le m \le 4 \;\&\; \gcd(m,4)=1\}|=|\{1,3\}|=2$$

$$\phi(8)=|\{m \; ; \; 1 \le m \le 8 \;\&\; \gcd(m,8)=1\}|=4$$

• خواص دالة أولر:

1. ϕ دالة ضربية $\forall n,m \in \mathbb{Z}^+ ; \gcd(n,m)=1$
$\Rightarrow \phi(n,m)=\phi(n).\phi(m)$

• ϕ ليست دالة ضربية تماماً يكفي أن نعطي مثال:
$\phi(4)=2$ لكن $\phi(2).\phi(2)=1$ نلاحظ بأنّ:
$\phi(4)=\phi(2\times 2)\neq \phi(2).\phi(2)$

2. إذا كانت p عدد أولي عندئذٍ $\phi(p)=p-1$.

3. $t\in\mathbb{Z}^+$ و p عدد أولي حيث $\phi(p^t)=p^{t-1}.(p-1)$

مثال: $\phi(9)=\phi(3^2)=3^{2-1}.(3-1)=3\times 2=6$
$\phi(8)=\phi(2^3)=2^{3-1}.(2-1)=2^2\times 1=4$

4. إذا كان n عدداً صحيحاً موجباً و $n=p_1^{t_1}.p_2^{t_2}.\dots.p_r^{t_r}$ حيث: $p_r,\dots,p_2,p_1$ أعداد مختلفة أولية فإنّ:
$$\phi(n)=n.\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$$

مثال (1):
$360=2^3\times 3^2\times 5$
$\phi(360)=\phi(2^3).\phi(3^2).\phi(5)=4\times 6\times 4=96$
أو $\phi(360)=360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=360\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)=96$

مثال (2):
$\phi(100)=\phi(2^2\times 5^2)=\phi(2^2).\phi(5^2)=$
$2\times 20=40$

5. مبرهنة أولر: $\forall a\in\mathbb{Z} ; \gcd(a,m)=1$ عندئذٍ:
$a^{\phi(m)}\equiv 1 \pmod m$

تعريف: ليكن a عدداً صحيحاً بحيث $\gcd(a,m)=1$ عندئذٍ:
إنّ العدد الصحيح b الذي يجعل $ab\equiv 1 \pmod m$ يُدعى بالمعكوس الضربي للعدد a بالنّسبة للمقاس m ونكتب عندئذٍ $a^{-1}=b$ أو $\bar{a}=b$

TEL:0931497960 - Facebook Group: A to Z مكتبة

أي معكوس العدد a هو العدد b

ملاحظة: إذا كان $\gcd(a,m) \neq 1$ عندئذٍ لا يوجد معكوس ضربي للعدد a بالنسبة للمقاس m لأنّ التطابق $ax \equiv 1 \pmod m$ قابل للحل إذا وفقط إذا كان $\gcd(a,m) = 1$

مثال: هل يملك العدد 2 معكوس ضربي بالنسبة للمقاس $m=6$ ؟

الحل: لدينا $\gcd(a,m) = \gcd(2,6) = 2 \neq 1$

بالتالي ليس للعدد 2 معكوس ضربي بالنّسبة للمقاس 6

ملاحظة: إذا كان $\gcd(a,m) = 1$ عندئذٍ لإيجاد المعكوس الضربي للعدد a بالنّسبة للمقاس m نقوم بما يلي:

1. نوجد $\phi(m)$ حيث ϕ دالة أويلر
2. نوجد $(a)^{\phi(m)-1}$
3. نوجد باقي قسمة $(a)^{\phi(m)-1}$ على العدد m

مثال: أوجد المعكوس الضربي للعدد $a=2$ بالنسبة للمقاس 5 ؟

الحل:

$m=5$

$\Rightarrow \gcd(a,m) = 1$

① لدينا $\phi(m) = \phi(5) = 4$

② $a^{\phi(m)-1} = 2^3 = 8$

③ نوجد باقي قسمة العدد 8 على العدد $m=5$ أي:

$8 \equiv 3 \pmod 5 \Leftarrow$ المعكوس الضربي للعدد 2 بالنّسبة للمقاس 5 هو العدد 3.

يمكن استخدام المعكوس الضربي لعددٍ ما بالنّسبة لمقاس ما في حل بعض التطابقات الخطية

مثال: أوجد الحل الوحيد للتطابق الخطي: $4x \equiv 2 \pmod 5$ ؟

TEL:0931497960 - Facebook Group: A to Z مكتبة

نوجد أولاً المعكوس الضربي للعدد $a=4$ بالنسبة للمقاس $m=4$

$a^{\phi(m)-1} = 4^3 \equiv 4 \pmod 5 \Rightarrow 4^{-1} = 4$

نضرب طرفي التطابق بالعدد $4^{-1} = 4$ نجد:

$4 \times 4x \equiv 8 \pmod 5 \Rightarrow x \equiv 3 \pmod 5$

$\Rightarrow \boxed{x_0 = 3}$

دراسة على جملة تطابقات خطية:

تعريف: كل جملة تطابقات خطية من الشكل:

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_k x \equiv b_k \pmod{m_k} \end{cases}$$

حيث a_i, b_i, m_i أعداد صحيحة و $m_i > 1$ $\forall\, 1 \le i \le K$

تكتب الجملة بشكل مختصر على الشكل $a_i x \equiv b_i \pmod{m_i}$; $1 \le i \le K$

دراسة الجملة $a_i x \equiv b_i \pmod{m_i}$ حيث $1 \le i \le K$ في الحالة:

$d_i = \gcd(a_i, m_i) = 1$

وذلك $d_{ij} = \gcd(m_i, m_j) = 1$ $\forall\, 1 \le i,j \le K$ & $i \ne j$

برهنة البواقي الصينية:

جملة التطابقات الخطية $a_i x \equiv b_i \pmod{m_i}$; $\forall\, 1 \le i \le K$

حيث $d_i = \gcd(a_i, m_i) = 1$ وذلك $\forall\, 1 \le i \le K$ و

$d_{ij} = \gcd(m_i, m_j) = 1$ وذلك $\forall\, 1 \le i,j \le K$ & $i \ne j$

تملك حل مشترك وحيد بالنسبة للمقاس m حيث:

$m = m_1 \cdot m_2 \cdots m_K$ يعطى هذا الحل بالصيغة التالية:

$$x^* = x_1 \cdot m_1' \cdot N_1 + x_2 \cdot m_2' \cdot N_2 + \cdots + x_K \cdot m_K' \cdot N_K$$

حيث: $m_i' = \dfrac{m}{m_i} = m_1 \cdot m_2 \cdots m_{i-1} \cdot m_{i+1} \cdots m_K$

TEL:0931497960 - Facebook Group: A to Z مكتبة

x_i و هو حل التطابق $a_i x_i \equiv b_i \pmod{m_i}$ حيث

N_i هو المعكوس الضربي للعدد m_i' بالنسبة للمقاس m_i

مثال: حل جملة التطابقات الخطية التالية:

$$\begin{cases} 2x \equiv 1 \pmod 3 \\ 4x \equiv 2 \pmod 5 \\ 5x \equiv 3 \pmod 8 \end{cases}$$

الحل:

$a_1 = 2$	$b_1 = 1$	$m_1 = 3$
$a_2 = 4$	$b_2 = 2$	$m_2 = 5$
$a_3 = 5$	$b_3 = 3$	$m_3 = 8$

$d_i = \gcd(a_i, m_i) = 1 \quad \forall\ 1 \le i \le 3$

$d_{ij} = \gcd(m_i, m_j) = 1$ و $1 \le j, i \le 3$

بالتالي الجملة تملك حل مشترك وحيد x^* بالنسبة للمقاس m حيث

$m = m_1 . m_2 . m_3 = 120$ والحل هو:

$$x^* = x_1 . m_1' . N_1 + x_2 . m_2' . N_2 + x_3 . m_3' . N_3$$

- إيجاد x_1:

$$2x_1 \equiv 1 \pmod 3$$

$$\Rightarrow 2x \equiv 1 \pmod 3$$

نضرب بـ 2

$$4x \equiv 2 \pmod 3$$

$$x \equiv 2 \pmod 3 \Rightarrow \boxed{x_1 = 2}$$

- إيجاد x_2: $4x \equiv 2 \pmod 5$ نعلم أنّ المعكوس الضربي للعدد 4 بالنسبة للمقاس 5 هو 4 $\Leftarrow$ نضرب طرفي التطابق بـ 4

$$16x \equiv 8 \pmod 5 \Rightarrow x \equiv 3 \pmod 5$$

$$\Rightarrow \boxed{x_2 = 3}$$

- إيجاد x_3: $5x \equiv 3 \pmod 8$ لنوجد 5^{-1} (المعكوس الضربي)

TEL:0931497960 - Facebook Group: A to Z مكتبة

للعدد 5 بالنسبة للمقاس 8

$5^{\phi(m)-1} = 5^{3} \equiv 5 \pmod 8 \Rightarrow$

نضرب طرفي التطابق بالعدد 5 فنجد: $5x \equiv 3 \pmod 8$

$25x \equiv 15 \pmod 8 \Rightarrow x \equiv 7 \pmod 8 \Rightarrow \boxed{x_3 = 7}$

$m_1' = \frac{m}{m_1} = \frac{m_1 \cdot m_2 \cdot m_3}{m_1} = m_2 \cdot m_3 = 5 \times 8 = 40$

$m_2' = \frac{m}{m_2} = 3 \times 8 = 24$

$m_3' = \frac{m}{m_3} = 3 \times 5 = 15$

إيجاد N_1: حيث N_1 هو المعكوس الضربي للعدد m_1' بالنسبة للمقاس m_1 أي:

$m_1' \cdot N_1 \equiv 1 \pmod{m_1}$

$m_1' \cdot N_1 \equiv 1 \pmod{m_1}$ طريقة (1):

$5 \times 8 \, N_1 \equiv 1 \pmod 3$

$40 N_1 \equiv 1 \pmod 3$

$N_1 \equiv 1 \pmod 3 \Rightarrow \boxed{N_1 = 1}$

$(m_1')^{\phi(m_1)-1} = 40 \equiv 1 \pmod 3$ طريقة (2):

نستنتج أنّ $N_1 = 1$

إيجاد N_2: هو المعكوس الضربي للعدد m_2' بالنسبة للمقاس $m_2 = 5$:

$(m_2')^{\phi(m_2)-1} = (24)^{\phi(5)-1} = (24)^{3} \equiv 4 \pmod 5$

$\Rightarrow \boxed{N_2 = 4}$

إيجاد N_3: هو المعكوس الضربي للعدد m_3' بالنسبة للمقاس $m_3 = 8$:

$(m_3')^{\phi(m_3)-1} = (15)^{\phi(8)-1} = 15^{3} \equiv 7 \pmod 8 \Rightarrow \boxed{N_3 = 7}$

بالتالي:

$x^* = x_1 \cdot m_1' \cdot N_1 + x_2 \cdot m_2' \cdot N_2 + x_3 \cdot m_3' \cdot N_3$

$= 1103 \equiv 23 \pmod{120}$

TEL:0931497960 - Facebook Group: A to Z مكتبة

بالتالي 23 هو حل الجملة كاملة.

نتيجة: إذا كانت لدينا الجملة $x \equiv b_i \pmod{m_i}$ حيث $\forall\ 1 \le i \le k$ $\gcd(m_i, m_j) = 1$ فالجملة تقبل حلاً وحيداً x^* يُعطى بالعلاقة:

$$x^* = b_1 . m_1' . N_1 + \dots + b_k m_k' N_k$$

ملاحظة: إنّ النتيجة الأخيرة تفيد في تعيين عدد عُرِفَ باقي قسمته على أعداد معينة وهي مسألة قديمة تُدعى مسألة اللغز الصيني وسنوضح ذلك بمثال.

مثال: أوجد أصغر عدد صحيح موجب باقي قسمته على العدد 6 هو 2 وباقي قسمته على العدد 5 هو 3 وباقي قسمته على العدد 11 هو 7 ؟

الحل:

إنّ العدد المطلوب هو الحل المشترك للجملة:

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 3 \pmod 5 \\ x \equiv 7 \pmod{11} \end{cases}$$

$d_i = \gcd(a_i, m_i) = 1$

$d_{ij} = \gcd(m_i, m_j) = 1$

$\forall\ 1 \le i, j \le 3 \quad \& \quad i \ne j$

تمتلك الجملة حل مشترك وحيد x^* بالنسبة للمقاس m حيث $m = m_1 . m_2 . m_3 = 330$ وهذا الحل هو:

$$x^* = x_1 . m_1' . N_1 + x_2 . m_2' . N_2 + x_3 . m_3' N_3$$

نلاحظ بسهولة أنّ

$$x_1 = 2 \quad , \quad x_2 = 3 \quad , \quad x_3 = 7$$

$$m_1' = 5 \times 11 = 55$$

$$m_2' = 6 \times 11 = 66$$

$$m_3' = 6 \times 5 = 30$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

N_1 هو المعكوس الضربي لـ $m_1' = 55$ بالنسبة للمقياس $m_1 = 6$

$$(m_1')^{\phi(m_1)-1} = (55)^1 = 55 \equiv 1 \pmod 6$$

$$\Rightarrow \boxed{N_1 = 1}$$

أو بطريقة أخرى:

$$m_1' \cdot N_1 \equiv 1 \pmod{m_1}$$

$$5 \times 11\, N_1 \equiv 1 \pmod 6$$

$$(-1)(-1)\, N_1 \equiv 1 \pmod 6$$

$$N_1 \equiv 1 \pmod 6 \Rightarrow N_1 = 1$$

وبسهولة يمكن حساب N_2 و N_3 فنجد:

$$\boxed{N_2 = 1} \quad \& \quad \boxed{N_3 = 7}$$

نستنتج مما سبق أن:

$$x^* = 1778 \equiv 128 \pmod{330}$$

انتهت المحاضرة

TEL:0931497960 - Facebook Group: A to Z مكتبة

مكتبة A to Z