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 $\{4, 1\}$

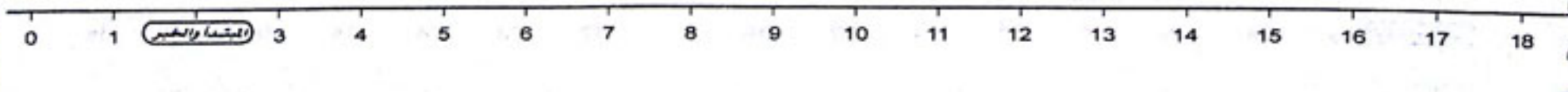
تمرين 3: أوجد حلول التطابق $6x \equiv 2 \pmod{9}$

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