الأربعاء: 15/4/2015

المحاضرة العاشرة:

الفصل الثاني:

- التطابقات الخطية -

تعريف:

التطابقة الخطي هو معادلة من الشكل:

$$ax \equiv b \pmod{m} \quad ; \quad a, b \in \mathbb{Z}$$

$m \geq 1$ ، x عدد صحيح مجهول.

وحل التطابقة الخطي هو إيجاد قيمة العدد الصحيح x الذي يحقق المعادلة

$$ax_0 \equiv b \pmod{m}$$

ومن تعريف التطابقة نعلم أنّ:

$$m \mid ax_0 - b \iff ax_0 - b = my$$

أي أنّ مسألة حل تطابقة خطي تؤول إلى مسألة إيجاد الحلول الكاملة لمعادلة ديوفانتس الخطية $ax_0 - my = b$

ومعادلة ديوفانتس لها حل إذا كان $d = (a, m)$ و $d \mid b$

مثال:

$$3x \equiv 9 \pmod{12}$$

بشكل تجريبي: $x \equiv -1$ ، $x \equiv 11$ ، $x \equiv 7$

$x \equiv 23$ ، $x \equiv 15$

ومنه نجد أن:

$x = 23$ ، $x \equiv 11$ ، $x \equiv -1$ حلاً واحداً بالمقاس 12

$x \equiv -1 \neq 15 \pmod{12}$ ، $x \equiv -1 \neq 7 \pmod{12}$

حل المطابقة $ax \equiv b \pmod{m}$ هي حلول غير المتطابقة بالمقاس m.

مبرهنة:

يكون للمتطابقة الخطية $ax \equiv b \pmod{m}$ حلاً إذا وفقط إذا كانت

$d = (a, m)$ حيث $d \mid b$

وإذا كان $d \mid b$ يكون للمتطابقة d حلاً مختلفاً بالمقاس m.

(غير متطابقاً)

الإثبات:

حل المتطابقة $ax \equiv b \pmod{m}$ يكافئ حل معادلة ديوفانتس $ax - my = b$

والشرط اللازم والكافي كي يكون للمعادلة حل هو أن يكون:

$d = (a, m)$; $d \mid b$ (أساسي)

وحل معادلة ديوفانتس هو:

$$x = x_0 + \frac{m}{d}t \quad , \quad y = y_0 - \frac{a}{d}t$$

حيث x_0, y_0 حلاً خاصاً، و $t \in \mathbb{Z}$ وبأخذ القيم $t = 0, 1, 2, \dots, d-1$

حل المتطابقة هو:

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

لنثبت أن هذه الحلول كلها غير متطابقة بالمقاس m، لنفرض عكس ذلك:

أي لنفرض أنه يوجد حلان متطابقان بالمقاس m وهما:

$$x_0 + t_1 \frac{m}{d} \equiv x_0 + t_2 \frac{m}{d} \pmod{m}$$

$$0 \leq t_1 < t_2 \leq d-1 \quad ;$$

حسب خواص التطابقة:

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

ولدينا: $\left(\frac{m}{d}, m\right) = \frac{m}{d}$

وحسب الخاصة (٦) من خواص التطابقات:

$$t_1 \equiv t_2 \pmod{d} \quad ; \quad 0 \leq t_1 < t_2 \leq d-1$$

t_1, t_2 تنتمي إلى مجموعة البواقي المختزلة بالقاس d أي:

$$t_1 \not\equiv t_2 \pmod{d}$$

وهذا يناقض كون:

$$t \equiv t \pmod{d}$$

ومنه مجموعة الحلول غير متطابقة بالقاس m.

لنثبت أن أي حل من الحلول $\left(x_0 + \frac{m}{d}t\right)$ يطابق بالقاس m واحداً من الحلول السابقة.

لنفرض أن: $d < t$ حيث

$$t = qd + r$$

$$0 \leq r \leq d-1 \quad ;$$

نعوض في عبارة الحل:

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

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

$$r < d \quad ;$$

وبالتالي وجدنا أن: $x_0 + t\frac{m}{d}$ ، $t > d$

بطابقة الحل من l حل غير المطابقة بالمقاس m . (أحد الحلول المذكورة)

مثال:
أوجد حلول المطابقة $9x \equiv 21 \pmod{30}$
الحل:
لدينا $(9,30) = 3 \mid 21$ لدينا 3 حلول
نختصر غرض المطابقة على 3

$$3x \equiv 7 \pmod{10}$$

$$\Rightarrow (3,10) = 1 \mid 7$$

$x \equiv 9 \pmod{10}$ حل المطابقة

نحصل على الحلول الثلاثة $x = x_0 + mt \quad ; \quad t = 0, 1, 2$

$$x = 9 + 10t$$

$$x_1 \equiv 9 \pmod{30} \quad , \quad x_2 = 19 \pmod{30} \quad , \quad x_3 \equiv 29 \pmod{30}$$

الحل بطريقة ثانية: حسب ديوفانتس.

$$9x - 30y \equiv 21 \iff 9x \equiv 21 \pmod{30}$$

نحل $9x - 30y = 21$ حسب خوارزمية القسمة

$$30 = 9 \times 3 + 3$$

$$9 = 3 \times 3 + 0$$

$$\Rightarrow d = 3 \qquad (9,30) = 3 \mid 21$$

المطابقة ثلاثة حلول مختلفة بالمقاس 30

$$3 = 30 - 3 \times 9$$

$$3 = 9 \times (-3) + 30 \times (1)$$

نضرب الطرفين بـ 7

$$21 = 9 \times (-21) + 30 \times (7)$$

$\Leftarrow x_0 = -21$ والحل هو:

$$x = -21 + 10t \quad ; \quad t = 0, 1, 2$$

$$x_1 \equiv -21 \pmod{30} \equiv 9 \pmod{30}$$
$$x_2 \equiv -11 \pmod{30} \equiv 19 \pmod{30}$$
$$x_3 \equiv -1 \pmod{30} \equiv 29 \pmod{30}$$

الكسور البسيطة المستمرة المنتهية:

إنَّ إيجاد حلول المعادلات الخطية باستخدام خوارزمية إقليدس أو التقريب تصبح طويلة أو متعذرة حين يكون المقام عدداً كبيراً لذلك سنستخدم طريقة الكسور البسيطة المستمرة.

تعريف:

الكسر البسيط المستمر المنتهي هو كسر يكتب على الشكل:

$$\frac{A}{B} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\cdots\cdots + \cfrac{1}{a_k}}}}}$$

$$\frac{A}{B} = \langle a_1, a_2, \cdots, a_k \rangle \quad ; \quad a_1 \in \mathbb{Z}$$
$$a_2, a_3, \cdots, a_k \in \mathbb{Z}^+$$ حيث:

مثال:

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

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

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

$= 1 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{6}}} = \langle 1, 1, 2, 6 \rangle$

ليكن العدد a_k النسبة الجزئية من المرتبة k إذا كتب كسرا مختصرا بالكسر عند النسبة الجزئية فإننا نحصل على التقريب من المرتبة k: c_k ونكتب

$$c_1 = a_1 \quad , \quad c_2 = a_1 + \frac{1}{a_2} \quad , \quad \cdots \quad , \quad c_k = a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_k}}$$

في المثال السابق:

$$c_1 = 1 \quad , \quad c_2 = 1 + \frac{1}{1} = 2 \quad , \quad c_3 = 1 + \frac{1}{1+\frac{1}{2}} = \frac{5}{3}$$

$$c_4 = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{6}}} = \frac{32}{19}$$

مبرهنة:

إذا كان لدينا الكسر المستمر المنتهي $<a_1, a_2, \dots, a_n>$
وأدخلنا الرموز التالية:

$$p_1 = a_1 \quad , \quad q_1 = 1$$

$$p_2 = a_1 a_2 + 1 \qquad q_2 = a_2$$

$$p_3 = a_3 p_2 + p_1 \qquad q_3 = a_3 q_2 + q_1$$

$$\dots \qquad \dots$$

$$p_k = a_k p_{k-1} + p_{k-2} \qquad q_k = a_k q_{k-1} + q_{k-2}$$

فإن التقريب من المرتبة n هو:

$$c_n = \frac{p_n}{q_n} \quad ; \quad \text{عندما } 1 \le n$$

البرهان:

بطريقة الاستقراء الرياضي:

1- الخطوة الأساسية:

عندما $n=1$

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

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

2- خطوة الاستقراء:

نفرض أن $c = \frac{p_n}{q_n}$ محققة من أجل $n=k$ ونثبت أنها محققة من أجل $n=k+1$

$$c_k = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}$$

$$c_{k+1} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_k + \cfrac{1}{a_{k+1}}}}}$$

لنثبت أنّ

$$\boxed{c_{k+1} = \frac{p_{k+1}}{q_{k+1}}}$$

إن c_{k+1} تختلف عن c_k بأن الحد الأخير في الكسر هو $a_k + \frac{1}{a_{k+1}}$ بدلاً عن a_k، لذلك نضع بدل a_k القيمة:

$$a_k + \frac{1}{a_{k+1}}$$

في العلاقة:

$$c_{k+1} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}} = \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(q_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}}$$

نوحد المقامات:

$$= \frac{a_k a_{k+1} p_{k-1} + p_{k-1} + a_{k+1} p_{k-2}}{a_k \cdot a_{k+1} q_{k-1} + q_{k-1} + a_{k+1} q_{k-2}}$$

$$= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}}$$

$$C_{k+1} = \frac{q_{k+1} P_k + P_{k-1}}{q_{k+1} q_k + q_{k-1}} = \frac{P_{k+1}}{q_{k+1}}$$

العلاقة محققة من أجل $n = k+1$ وبالتالي هي محققة من أجل $n \geq 1$

ملاحظة:
من أجل $n \geq 2$ فإن:

$$P_n q_{n-1} - P_{n-1} q_n = (-1)^n$$

البرهان:
بالاستقراء الرياضي: 1- الخطوة الأساسية:

$$n = 2 \Rightarrow P_2 q_1 - P_1 q_2 \stackrel{?}{=} (-1)^2 = 1$$

$$(a_2 q_1 + 1) \times 1 - q_1 q_2 = 1$$

2- خطوة الاستقراء: نفرض أن العلاقة محققة من أجل $n = k$ ونثبت صحتها من أجل $n = k+1$

$$P_k q_{k-1} - P_{k-1} q_k = (-1)^k$$

$$P_{k+1} q_k - P_k q_{k+1} = (a_{k+1} P_k + P_{k-1}) q_k - P_k (a_{k+1} q_k + q_{k-1})$$

$$= -(P_k q_{k-1} - P_{k-1} q_k) = -(-1)^k = (-1)^{k+1}$$

محققة من أجل $n = k+1$ وبالتالي من أجل $n \geq 1$

نتيجة: إن P_n و q_n أوليان نسبياً.

انتهت المحاضرة..