الأربعاء: 2015/4/29

المحاضرة الحادية عشرة:

نتيجة:
إنّ P_n و q_n أوليان نسبياً.

الإثبات:
نفرض $d = (P_n, q_n) > 1$ وعنه d يقسم التركيب الخطي P_n, q_n أي:

$d \mid P_n q_{n-1} - P_{n-1} q_n$ وإنه لا يصح إلا إذا كان $d \mid 1$ وبالتالي $d = 1$

وعنه P_n و q_n أوليان نسبياً.

الاستفادة من الكسور البسيطة في إيجاد حلول التطابقات الخطية.

مثال:
أوجد حل التطابقة $79x \equiv 2 \pmod{153}$ بطريقة الكسور المستمرة.

الحل:

$(79, 153) = 1$

$$\frac{153}{79} = 1 + \cfrac{1}{1 + \cfrac{1}{14 + \cfrac{4}{5}}} = 1 + \cfrac{1}{1 + \cfrac{1}{14 + \cfrac{1}{1 + \cfrac{1}{4}}}}$$

$$\frac{153}{79} = \langle \overset{q_1}{1}, \overset{q_2}{1}, \overset{q_3}{14}, \overset{q_4}{1}, \overset{q_5}{4} \rangle$$

$P_1 = 1 \qquad q_1 = 1$

$P_2 = 2$ $\quad q_2 = q_2 = 1$

$C_1 = \frac{P_1}{q_1} = \frac{1}{1}$, $C_2 = \frac{P_2}{q_2} = \frac{2}{1}$

$C_3 = \frac{29}{15}$

$C_4 = \frac{31}{16}$

$C_5 = \frac{153}{79}$

نعوض في المعادلة:

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

$$P_5 q_4 - P_4 q_5 = (-1)^5 = -1$$

$153 \times 16 - 31 \times 79 = -1$ (-2) نضرب الطرفين بـ

$(62) \times 79 - (32) \times 153 = 2$

$\Rightarrow x \equiv 62 \pmod{153}$

نتأكد أن الحل صحيح

$$62 \times 79 \overset{?}{\equiv} 2 \pmod{153}$$

$153 \mid 4896 = 62 \times 79 - 2 = 32 \times 153$

النظير الضربي:

تعريف:

نقول عن a^* إنه نظير ضربي للعدد الصحيح a بالمقاس m إذا وفقط إذا تحقق:

$$a^* a \equiv 1 \pmod{m}$$

وكان $(a, m) = 1$ -151

مثال:

$2x \equiv 1 \pmod 4$ $\qquad 1 + 2 = (2,4)$

لا يوجد نظير ضربي لأي عدد زوجي إذا كان المقياس زوجياً.

مبرهنة:

يكون العدد a نظير ضربي بالمقياس m إذا وفقط إذا كان $(a,m) = 1$

مثال:(1)

حل المطابقة $17x \equiv 1 \pmod{25}$

نجد أن 3 نظير ضربي للعدد 17 بالمقياس 25 ، $x = 3$

مثال(2):

أوجد النظير الضربي للعدد 71 بالمقياس 55

الحل:

لنوجد حل المطابقة $71x \equiv 1 \pmod{55}$ بطريقة الكسور البسيطة المستمرة

$$\frac{71}{55} = 1 + \frac{1}{\frac{55}{16}} = 1 + \frac{1}{3 + \frac{1}{\frac{16}{7}}} = 1 + \frac{1}{3 + \frac{1}{2 + \frac{1}{3 + \frac{1}{2}}}}$$

$\frac{71}{55} = \langle 1, 3, 2, 3, 2 \rangle$ $\qquad n = 5$

$P_1 = 1$, $q_1 = 1$

$P_2 = a_2 a_1 + 1 = 4$, $q_2 = a_2 = 3$

$$C_1 = \frac{P_1}{q_1} = \frac{1}{1}\ , \qquad C_2 = \frac{P_2}{q_2} = \frac{4}{3}\ , \quad C_3 = \frac{P_3}{q_3} = \frac{9}{7}$$

$$C_4 = \frac{P_4}{q_4} = \frac{31}{24}\ , \qquad C_5 = \frac{P_5}{q_5} = \frac{71}{55}$$

نعوض في المعادلة من أجل $n = 5$

$$P_5 q_4 - P_4 q_5 = (-1)^5 = -1$$

$$71 \times 24 - 31 \times 55 = -1$$
$$(-24) \times 71 + (31) \times 55 = 1$$

ومنه:

$$x \equiv -24 (mod\ 55) \equiv 31 (mod\ 55)$$

وبالتالي $x = 31$ هو النظير الضربي

مثال:

لتكن لدينا:

$$x \equiv 1 (mod\ 3)$$
$$x \equiv 1 (mod\ 9)$$

أوجد الحل المشترك للتطابقين.

الحل:

مجموعة حلول المعادلة الأولى $\{\ldots, 1, 4, 7, 10, 13, 16, 19, 21, \ldots\}$

مجموعة حلول التطابقة للمعادلة الثانية:

$\{\ldots, 1, 10, 19, 28, 37, \ldots\}$

مجموعة الحلول المشتركة هي:

$\{\ldots, 1, 10, 19, \ldots\}$

وهي مجموعة حلول المعادلة الثانية أي:

$$x \equiv 1 (mod\ 9)$$

نأخذ التطابقة الذي mod له أكبر

حل جملة المعادلات الخطية:

لتكن لدينا جملة المعادلات:

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

نلاحظ مايلي:

1. يمكن أن يكون لكل تطابقة حل ولكن ليس بالضرورة أن يكون لجملة التطابقات حل مشترك.
2. إذا كان لا يوجد لأي تطابقة حل فإنه لا يوجد حل مشترك للجملة.

مبرهنة الباقي الصيني:

هي وسيلة لحل مسألة إيجاد عدد صحيح علمت بواقي قسمته على عدة أعداد معلومة.

نص المبرهنة:

إذا كانت المقاسات $m_1, m_2, \dots, m_k$ أولية نسبياً مثنى مثنى فإنه يوجد لجملة التطابقات الخطية:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\text{- - - - - -} \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

حل وحيد بالمقاسات:

$$m = m_1 \cdot m_2 \cdots m_k$$

البرهان:

نأخذ الأعداد: $M_i = \frac{m}{m_i}$; $i = 1, 2, \ldots, k$

$$M_1 = \frac{m}{m_1} = m_2 \cdot m_3 \cdots m_k$$

$$M_2 = m_1 \cdot m_3 \cdots m_k$$

$$M_k = m_1 \cdot m_2 \cdots m_{k-1}$$

بما أنّ: $(M_i, m_i) = 1$; $i = 1, \ldots, k$

نكتب:

$$M_i \cdot m_i' \equiv 1 \pmod{m_i}$$ العنزي

حيث m_i' هي النظير للعدد M_i بالمقاس m_i

نكتب العدد x على الشكل:

$$x = a_1 m_1' M_1 + a_2 m_2' M_2 + \cdots + a_k m_k' M_k$$

$$= \sum_{i=1}^{k} a_i m_i' M_i$$

بما أنّ x هو حل لكل تطابقة من الجملة بالمقاس m.

لدينا: $m_i \mid M_j$ شرط $i \neq j$

$$M_j \equiv 0 \pmod{m_i}$$ شرط $i \neq j$

$$M_j \not\equiv 0 \pmod{m_i}$$ $i = j$

$$x \equiv a_i m_i' M_i \pmod{m_i} \qquad i=1$$

$$x \equiv a_2 m_2' M_2 \pmod{m_2}$$

$$x \equiv a_i m_i' M_i \pmod{m}$$

بالتالي:

$$x \equiv \sum a_i m_i' M_i \pmod{m}$$

هو الحل المشترك لجملة التطابقات الخطية بالمقاس m.
لنثبت أنّ الحل وحيد ولذا:
نفرض أنّ x' ، x حلان مختلفان لجملة التطابقات أي أنّ:

$$x \equiv x' \equiv a_i \pmod{m_i} \quad ; \quad 1 \le i \le k$$

x ، x' حلان للجملة:

$$x - x' \equiv 0 \pmod{m_i}$$

$m_i \mid x - x'$ ، m مضاعف مشترك أصغر للأعداد m_i

$$m \mid x - x' \Leftarrow x \equiv x' \pmod{m}$$

انتهت المحاضرة...