المحاضرة الثالثة عشر

مبرهنة الباقي الصينية

المبرهنة الاتية تستخدم لإيجاد حل مشترك وحيد معيار n.

مبرهنة (31): (مبرهنة البواقي الصينية)

اذا كان $m_1, m_2, \dots, m_k$ اعداد موجبة اولية فيما بينها مثنى مثنى، وكان $\mathrm{d}(m_i, m_j) = 1$

لكل قيم $i \neq j$ ، فان للنظام من التطابقات الخطية

$$x \equiv a_i \ (mod\ m), for\ 1 \leq i \leq k$$

يملك حل وحيد للمتطابقة $m = \prod_{i=1}^{k} m_i$.

مثال:

1- استخدم مبرهنة البواقي الصينية لحل النظام، وايجاد النظام التطابقي

$$\boldsymbol{x \equiv 2\ (mod\ 3)}$$

$$\boldsymbol{x \equiv 3 (mod\ 5)}$$

$$\boldsymbol{x \equiv 2\ (mod\ 7)}$$

Let $m = 3 \cdot 5 \cdot 7 = 105$, then

$$m_1 = 3, \quad m_2 = 5, \quad m_3 = 7,$$
$$a_1 = 2, \quad a_2 = 3, \quad a_3 = 2,$$
$$M_1 = 35, \quad M_2 = 21, \quad M_3 = 15.$$

Solve the following congruences for b_i, for $i = 1, 2$, and 3.

$$35b_1 \equiv 1 \pmod 3, \quad 21b_2 \equiv 1 \pmod 5, \quad 15b_3 \equiv 1 \pmod 7,$$
$$2b_1 \equiv 1 \pmod 3, \quad b_2 \equiv 1 \pmod 5, \quad b_3 \equiv 1 \pmod 7,$$
$$b_1 \equiv 2 \pmod 3, \quad b_2 \equiv 1 \pmod 5.$$

Therefore, $x \equiv \sum_{i=1}^{3} M_i b_i a_i = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 \equiv 233 \equiv 23 \pmod{105}$.

2- استخدم مبرهنة الباقي الصينية لحل التطابق $19x\equiv 1 \pmod{140}$.

التطابق يكافئ النظام

$19x\equiv 1 \pmod 4$

$19x\equiv 1 \pmod 5$

$19x\equiv 1 \pmod 7$.

وهذا بدوره يكافئ النظام

$x\equiv 3 \pmod 4$

$x\equiv 4 \pmod 5$

$x\equiv 3 \pmod 7$.

Let m=4.5.7=140, $M_1 = 35, M_2 = 28, M_3 = 20$

بحل المعادلات

$35b_1\equiv 1 \pmod 4 \Rightarrow b_1 = -1$

$28b_2\equiv 1 \pmod 5 \Rightarrow b_2 = 2$

$20b_3\equiv 1 \pmod 7 \Rightarrow b_3 = -1$

$x = \sum_{i=1}^{3} M_i\, b_i a_i = (35)(-1)(3) + (28)(2)(4) + (20)(-1)(3)$

$= 59\ (mod\ 140)$.

مبرهنة (32): ليكن d= (a, n)

$ax \equiv b\ (mod\ n)$ (3)

فانه يوجد للتطابق الخطي (3) حل اذا وفقط اذا كان $d \setminus b$.

البرهان:

(أ) نفرض أن x حل للتطابق الخطي (3) . إذاً $n \setminus ax - b$. لكـــن $d \setminus n$ و $d \setminus a$ إذاً $d \setminus b$. ولإثبات العكس لاحظ أن

$$ax \equiv b(\text{mod } n) \Leftrightarrow \frac{a}{d}x \equiv \frac{b}{d} \bmod (\frac{n}{d})$$

لكن كل من a,b,n يقبل القسمة علـــى d . إذاً $\frac{a}{d}, \frac{b}{d}, \frac{n}{d} \in Z$ ، وحيـــث أن

$\left(\frac{a}{d}, \frac{n}{d}\right) = 1$ حسب النتيجة المبرهنة إذا (a, n) =1، فأن للتطابق الخطي

$ax \equiv (b\ (mod\ n)$.

وعليه يوجد حل للتطابق الخطي $ax \equiv (b\ (mod\ n)$.

مبرهنتي أويلر & فيرما Eular & Fermat Theorem

يعرف الصينيون قبل أكثر من 2000 سنة بأن $(2^p - 2)$ يقبل القسمة على p لأي عدد أولي p ، وقد عمم فيرما تلك الحقيقة بدون إثبات عام ١٦٤٠م إلى ما يسمى مبرهنة فيرما الصغيرة "Fermat's Little Theorem" والتي تنص على أن " **إذا كان a عدداً صحيحاً لا يقبل القسمة على العدد الأولي p** ، فإن $(a^{p-1} - 1)$ **يقبل القسمة على p** " .

وقد حصل الألماني ليبنز (١٦٤٦-١٧١٦) على نفس النتيجة وأثبتها بالأستقراء الرياضي سنة ١٦٨٣م "ولم ينشر البرهان". أما أول إثبات منشور لتلك المبرهنة فقد كان لأويلر سنة ١٧٣٦م ، ثم عمم أويلر تلك المبرهنة سنة ١٧٦٠م .

مبرهنة أويلر (33) Euler's Theorem

ليكن n عدداً صحيحًا موجبًا . إذا كان $(a\ ,\ n) = 1$ فإن $a^{\varphi(n)} \equiv 1\ (\text{mod } n)$ حيث إن $\varphi(n)$ ترمز لدالة أويلر .

تعريف: دالة اويلر $\varphi(n)$ هي الاعداد الصحيحة الموجبة الأقل من او تساوي n والاولية نسبيا مع n. أي أن $\varphi(n) = |\{m \in Z | 1 \leq m \leq n, (m,n) = 1\}|$

امثلة:

$$\phi(3) = |\{1,2\}| = 2 \ ، \ \phi(4) = |\{1,3\}| = 2$$

$$\phi(9) = |\{1,2,4,5,7,8\}| = 6 \ ، \ \phi(8) = |\{1,35,7\}| = 4$$

مبرهنة(34) : اذا كان p عدد اولي، وكانت $k > 0$ ، فان

$$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right).$$

مثال: احسب القيم التالية:

1- $\varphi(1) = 1 - 1^0 = 1.$

2- $\varphi(9) = \varphi(3^2) = 3^2 - 3 = 9 - 3 = 6.$

3- $\varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 16 - 8 = 8.$

4- $\varphi(10) = \varphi(2.5) = 10\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 10\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 4.$

5- $\varphi(360) = \varphi(2^3.3^2.5) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$

$= 360.\left(\frac{1}{2}\right).\left(\frac{2}{3}\right).\left(\frac{4}{5}\right) = 96.$

مثال:

1- لاحظ ان $3^4 = 81 \equiv 1\ (mod\ 5)$،

2- كذلك $2^{\varphi(9)} = 2^6 = 64 \equiv 1\ (mod\ 9)$.

3- أثبت أن: $2^{12} \equiv 1\ (mod\ 21)$

بما ان n=21 و a=2 نوجد $\varphi(21)$

$$2^{\varphi(21)} \equiv 1 (\text{mod } 21)$$

$$2^{12} \equiv 1 (\text{mod } 21)$$

ملاحظة:

لاحظ أن عكس مبرهنة أويلر صحيح أيضاً وذلك لأنه لو كان $a^{\varphi(n)} \equiv 1 \pmod n$ فإنه يوجد $k \in \mathbb{Z}$ حيث $a^{\varphi(n)} + nk = 1$. ومنه فإن $a a^{\varphi(n)-1} + nk = 1$. وبالتالي فإن $(a, n) = 1$.
