كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : الخامسة /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

تعريف: يُدعى التطابق $ax \equiv b \pmod m$ حيث $a, b, m \in \mathbb{Z}$ و $m \neq 0, 1$ تطابقاً خطياً بمتحوّل واحد x.

يُدعى x_0 حلاً للتطابق الخطي $ax \equiv b \pmod m$ إذا كان: $ax_0 \equiv b \pmod m$

مثال: ليكن لدينا التطابق الخطي $3x \equiv 4 \pmod 5$ إنّ:

- $x_0 = 3$ حلاً للتطابق لأنّ: $3 \times 3 = 9 \equiv 4 \pmod 5$
- $x_0 = 2$ ليس حلاً للتطابق لأنّ $3 \times 2 = 6 \not\equiv 4 \pmod 5$

إنّ دراسة التطابق الخطي بالنسبة لمقاس m يشمل مايلي:

1- معرفة فيما إذا كان التطابق الخطي $ax \equiv b \pmod m$ قابل للحل أم لا في مجموعة الأعداد الصحيحة $\mathbb{Z}$.

2- إذا كان التطابق الخطي $ax \equiv b \pmod m$ قابلاً للحل في $\mathbb{Z}$ فما هي جميع حلوله.

ملاحظة (1): إذا كان x_0 حلاً للتطابق $ax \equiv b \pmod m$ وكان $x^* \equiv x_0 \pmod m$ فإنّ x^* حل للتطابق $ax \equiv b \pmod m$ بالتالي

ملاحظة (2): إذا كان x_0 حلاً للتطابق الخطي $ax \equiv b \pmod m$ عندئذٍ $q \in \mathbb{Z}$ ؛ $x_0 + q.m$ هي حلول للتطابق الخطي وتكون جميع هذه الحلول متطابقة بالنسبة للمقاس m.

تعريف: إذا كان x_0 حلاً للتطابق الخطي $ax \equiv b \pmod m$ فإنّ x_0 يدعى حل وحيد لـ $ax \equiv b \pmod m$ إذا تحقق الشرط:

أياً كانت x^* حلاً للتطابق المفروض فإنّ $x^* \equiv x_0 \pmod m$ أي:

$$x^* = x_0 + q.m$$

نتيجة: الحلول المختلفة للتطابق الخطي $ax \equiv b \pmod m$ هي الحلول لهذا التطابق والغير متطابقة بالنسبة للمقاس m.

ملاحظة: الحلول المختلفة للتطابق $ax \equiv b \pmod m$ هي عناصر من

$$Z_m = \{0, 1, 2, \dots, m-1\}$$

ملاحظة: لاختبار قابلية حل تطابق خطي $ax \equiv b \pmod m$ يكفي أن نبحث عن الحلول في عناصر المجموعة $Z_m = \{0, 1, \dots, m-1\}$ فإذا لم يوجد حل في هذه المجموعة يكون التطابق غير قابل للحل.

مثال (1): التطابق الخطي $2x \equiv 1 \pmod 5$.

$a = 2, \ b = 1, \ m = 5$ حيث $Z_5 = \{0, 1, 2, 3, 4\}$

$2(0) = 0 \not\equiv 1 \pmod 5 \Rightarrow$ الصفر ليس حل للتطابق

$2(1) = 2 \not\equiv 1 \pmod 5 \Rightarrow$ الواحد ليس حل للتطابق

$2(2) = 4 \not\equiv 1 \pmod 5 \Rightarrow$ 2 ليس حل للتطابق

$2(3) = 6 \equiv 1 \pmod 5 \Rightarrow$ 3 هو حل للتطابق

$2(4) = 8 \not\equiv 1 \pmod 5 \Rightarrow$ 4 ليس حل

نلاحظ بأنّ التطابق يملك حل وحيد هو $x_0 = 3$

مثال (2): $4x \equiv 2 \pmod 6$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$4(0) = 0 \not\equiv 2 \pmod 6$

$4(1) = 4 \not\equiv 2 \pmod 6$

$4(2) = 8 \equiv 2 \pmod 6 \Rightarrow \boxed{x_1 = 2}$ حل للتطابق

$4(3) = 12 \not\equiv 2 \pmod 6$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$4(4) = 16 \not\equiv 2 \pmod 6$

$4(5) = 20 \equiv 2 \pmod 6 \Rightarrow \boxed{x_2 = 5}$ حل للتطابق

نلاحظ أنّ $x_1 \not\equiv x_2 \pmod 6$ إذاً التطابق الخطي

$4x \equiv 2 \pmod 6$ يملك حلان

مثال (3): ليكن التطابق الخطي $4x = 2 \pmod 8$

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$4(0) \not\equiv 2 \pmod 8$ $\quad 4(1) \not\equiv 2 \pmod 8$

$4(2) = 8 \not\equiv 2 \pmod 8$ $\quad 4(3) = 12 \not\equiv 2 \pmod 8$

$4(4) = 16 \not\equiv 2 \pmod 8$ $\quad 4(5) = 20 \not\equiv 2 \pmod 8$

$4(6) = 24 \not\equiv 2 \pmod 8$ $\quad 4(7) = 28 \not\equiv 2 \pmod 8$

نستنتج أنّ هذا التطابق غير قابل للحل

- نستنتج من الأمثلة السّابقة أنّ التطابق الخطي $ax \equiv b \pmod m$ إما أن يستحيل الحل أو قابل للحل فإذا كان قابل للحل فقد يملك حلّاً وحيداً أو يملك أكثر من حل.
- نقدّم الآن مبرهنة تعطينا شرطاً لازماً وكافياً لقابلية حل التطابق الخطي $ax \equiv b \pmod m$:

مبرهنة: ليكن $a, b, m \in \mathbb{Z}$ و $m \neq 0$ و $d = \gcd(a, m)$

عندئذٍ التطابق الخطي $ax \equiv b \pmod m$ قابلاً للحل إذا وفقط إذا كان $d \mid b$ ؛

الإثبات: $\Leftarrow$ لدينا فرضاً التطابق الخطي $ax \equiv b \pmod m$ قابلاً للحل وليكن x_0 حلّاً له

$ax_0 \equiv b \pmod m$

$\Rightarrow ax_0 = b + q.m \quad ; q \in \mathbb{Z}$

$\Rightarrow \boxed{ax_0 - q.m = b} \quad (*)$

TEL:0931497960 - Facebook Group: A to Z مكتبة

لدينا $d=gcd(a,m) \Leftarrow d\mid a \;\&\; d\mid m$

$d\mid a \Rightarrow \exists a_1 \in \mathbb{Z} \;;\; a=a_1 \cdot d$

$d\mid m \Rightarrow \exists m_1 \in \mathbb{Z} \;;\; m=m_1 \cdot d$

نعوّض في (*) فنجد أنّ $(a_1 x_0)\cdot d-(q\cdot m_1)\cdot d=b$

$d(a_1 x_0 - q\cdot m_1)=b \Rightarrow d\mid b$

وهو المطلوب.

$\Rightarrow$ لدينا فرضاً $d\mid b$ بالتالي $b=b_1 d$ ① حيث $b_1 \in \mathbb{Z}$

ولدينا $d=gcd(a,m)$ بالتالي يوجد $q_0, m_0 \in \mathbb{Z}$ بحيث $d=q_0 a+m_0 m$ ②

نعوض ② في ① :

$b_1(q_0 a+m_0 m)=b$

$a(q_0 b_1)+m_0 b_1 m=b$

$\Rightarrow a(q_0 b_1)\equiv b \pmod m$

نضع $x_0=q_0\cdot b_1$ بالتالي $ax_0\equiv b \pmod m$ بالتالي

التطابق $ax\equiv b \pmod m$ قابل للحل

ملاحظة: التطابق الخطي $ax\equiv b \pmod m$ حيث $gcd(a,m)=1$

قابل للحل دوماً وهو يملك حل وحيد

الإثبات:

$gcd(a,m)=1 \Rightarrow \exists q_0, m_0 \in \mathbb{Z} \;;\; q_0 a+m_0 m=1$

نضرب الطرفين بـ b نجد: $aq_0 b+m_0 mb=b$

$aq_0 b\equiv b \pmod m$

التطابق قابل للحل $\Rightarrow ax_0\equiv b \pmod n \;;\; \exists x_0=q_0 b$

ليكن x_0 حلّ التطابق بالتالي $ax_0\equiv b \pmod m$ حيث $gcd(a,m)=1$ وليكن x^* حل آخر للتطابق الخطي:

TEL:0931497960 - Facebook Group: A to Z مكتبة

$ax \equiv b \pmod m$ بالتالي $ax^* \equiv b \pmod m$ بالتالي:

$ax^* \equiv ax_0 \pmod m$; $\gcd(a,m) = 1$

$\Rightarrow x^* \equiv x_0 \pmod m$ $\Rightarrow$ حل وحيد x_0

• نقدم الآن مبرهنة تعطينا جميع الحلول المختلفة للتطابق الخطي

$ax \equiv b \pmod m$ إذا كان قابلاً للحل:

مبرهنة: ليكن $a,b,m \in \mathbb{Z}$ و $m \geq 2$ و $d = \gcd(a,m)$ عندئذٍ

إذا كان $d \mid b$ بالتالي التطابق الخطي $ax \equiv b \pmod m$

يقبل بالضبط d حلاً مختلفاً بالقياس للعدد m ومنه الحلول هي:

$$\{x_0 + km_1 \; ; \; m_1 = \frac{m}{d} \;\&\; 0 \leq k \leq d-1\}$$

حيث x_0 حل ما للتطابق $ax \equiv b \pmod m$.

الإثبات:

• سنثبت أولاً بأنّ أي حل للتطابق $ax \equiv b \pmod m$ هو

حل للتطابق $a_0 x \equiv b_0 \pmod{m_1}$ وبالعكس حيث:

$a = a_0 d$ و $b = b_0 d$ و $m = m_1 d$ و $\gcd(a_0, m_1) = 1$

ليكن x_0 حلاً للتطابق $ax \equiv b \pmod m$ ولدينا:

$d = \gcd(a,m)$;

$\exists a_0, m_1 \in \mathbb{Z}$; $\gcd(a_0, m_1) = 1$, $a = a_0 d$, $m = m_1 d$

وبما أنّ $d \mid b$ $\Leftarrow$ $b = b_0 d$ $\Leftarrow$ $ax_0 \equiv b \pmod m$

$\gcd(d, m_1 d) = d$; $a_0 d x_0 \equiv b_0 d \pmod{m_1 d}$

x_0 حل للتطابق $a_0 x_0 \equiv b_0 \pmod{m_1}$ $\Rightarrow$

$a_0 x \equiv b_0 \pmod{m_1}$

• ليكن x_0 حلاً لـ $a_0 x \equiv b_0 \pmod{m_1}$

$\Rightarrow a_0 x_0 \equiv b_0 \pmod{m_1}$ $\Rightarrow a_0 x_0 = b_0 + q \cdot m_1$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$\Rightarrow a_0 . d . x_0 = b_0 . d + q_1 . m_1 . d$

$\Rightarrow a x_0 = b + q . m$

$\Rightarrow a x_0 \equiv b \pmod{m} \Rightarrow$ x_0 حل للتطابق

$ax \equiv b \pmod{m}$

نلاحظ أنّ $a_0 x \equiv b_0 \pmod{m}$ يملك حل وحيد كون $\gcd(a, m_1) = 1$

نستنتج مما سبق بأنّ حلول التطابق $ax \equiv b \pmod{m}$

$H = \{ x_0 + t . m_1 \; ; \; t \in \mathbb{Z} \;\; \& \;\; m_1 = \frac{m}{d} \}$

جميع هذه الحلول متطابقة بالنسبة للمقاس m_1.

نأخذ: $H' = \{ x_0 + k . m_1 \; ; \; 0 \leq k \leq d-1 \}$

سنثبت مايلي:

1- جميع عناصر H' مختلفة مثنى مثنى (غير متطابقة بالنسبة للمقاس m)

2- أي عنصر من H يطابق أحد عناصر H'.

اثبات ①: نفرض جدلاً أنّ:

$x_0 + i m_1 \equiv x_0 + j m_1 \pmod{m} \; ; \; i \neq j \;\; و \;\; 0 \leq j < i \leq d-1$

$m \mid (i-j) . m_1$

$\Rightarrow m_1 . d \mid (i-j) . m_1 \Rightarrow d \mid (i-j)$

وهذا مرفوض لأنّ $0 < i-j < d$ بالتالي الفرض الجدلي خاطئ.

اثبات ②: $\forall y \in H \Rightarrow y = x_0 + t m_1 \; ; \; t \in \mathbb{Z}$

حسب القسمة الاقليدية:

$t = q . d + r \; ; \; 0 \leq r \leq d-1$

$\Rightarrow y = x_0 + (q . d + r) . m_1$

$= x_0 + q . d . m_1 + r . m_1$

$= x_0 + q . m + r . m_1$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$\Rightarrow y = x_0 + r.m_1 \pmod m \in H'$

مثال: أوجد الحلول المختلفة للتطابق $6x \equiv 8 \pmod{10}$ ؟

الحل:

$a = 6 \quad b = 8 \quad m = 10$

$\gcd(a, m) = 2 \; ; \; d \mid b$

التطابق قابل للحل ويملك حلين مختلفين

$\{x_0 + k.m \; ; \; m_1 = \frac{m}{d} \; \& \; 0 \leq k \leq 1\}$

$= \{x_0, x_0 + m_1\} = \{x_0, x_0 + 5\}$

إيجاد x_0 :

$6x \equiv 8 \pmod{10}$

$2 \times 3x \equiv 2 \times 4 \pmod{10}$

$3x \equiv 4 \pmod 5$

نضرب الطرفين بـ 2 فنجد :

$6x \equiv 8 \pmod 5$

$x = 3 \pmod 5$

$\Rightarrow \boxed{x_0 = 3}$

الحلول المختلفة للتطابق هي $\{3, 8\}$

انتهت المحاضرة

TEL:0931497960 - Facebook Group: A to Z مكتبة