كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

المادة : نظرية الاعداد

المحاضرة : السادسة/نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

2025

يمكنكم طلب المحاضرات برسالة نصية (SMS) أو عبر (What's app-Telegram) على الرقم 0931497960

* التطبيقات الخطية:

• تعريف:

يدعى التطابق من الشكل:

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

حيث $a, b, m \in \mathbb{Z}$

&

$m \geq 2$

&

$a \not\equiv 0 \pmod{m}$

تطابقاً خطياً بالمجهول x

• مثال:

$$3x \equiv \pmod{5}$$

★ $x_0 = 3$ حل للتطابق لأن:

$$3 \times 3 = 9 \equiv 4 \pmod{5}$$

★ $x_0 = 2$ ليس حلاً لأن:

$$6 \not\equiv 4 \pmod{5}$$

* دراسة التطابق الخطّي بالنسبة لمقاس m تتضمّن النقاط التالية:

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

2- إذا كان التطابق الخطّي $ax \equiv b \pmod m$ قابل للحل فما هي جميع حلوله الأخرى

ملاحظة

إذا كان x_0 حلاً للتطابق

$ax \equiv b \pmod m$

عندئذٍ:

$(x_0 + qm) \; ; \; q \in \mathbb{Z}$

هي حلّ للتطابق:

$ax \equiv b \pmod m$

التعليل:

لدينا x_0 حلّ للتطابق $ax \equiv b \pmod m$

$\Rightarrow ax_0 \equiv b \pmod m$

$a(x_0 + qm) = ax_0 + aqm$

$\equiv ax_0 \pmod m$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$\equiv b \pmod m$

بالتالي:

$x_0 + qm$ هي حلّ التطابق

$ax \equiv b \pmod m$

ملاحظة

إذا كان x حلاً لـ $ax \equiv b \pmod m$

عندئذٍ:

$(x_0 + qm)$; $q \in \mathbb{Z}$ هي حلول التطابق

$ax \equiv b \pmod m$

وهذه الحلول متطابقة بالنسبة للقاسم m

• تعريف:

إذا كان x_0 حلاً للتطابق

$ax \equiv b \pmod m$

عندئذٍ نقول بأنّ x_0 حل وحيد للتطابق

$ax \equiv b \pmod m$

إذا تحقق الشرط التالي:

أيّاً كان x^* حلاً للتطابق المفروض

فإنّ:

$x^* \equiv x_0 \pmod m$

TEL:0931497960 - Facebook Group: A to Z مكتبة

- نتيجة :

الحلول المختلفة للتطابق الخطي :

$$ax \equiv b \pmod m$$

هي الحلول لهذا التطابق والغير متطابقة بالنسبة للمقياس m

- ملاحظة :

الحلول المختلفة للتطابق :

$$ax \equiv b \pmod m$$

هي العناصر من :

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

- ملاحظة :

لاختبار قابلية حل تطابق خطي

$$ax \equiv b \pmod m$$

كفي أن نبحث عن الحلول في المجموعة

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

فإذا لم يوجد حل في هذه المجموعة يكون التطابق غير قابل للحل.

- مثال (1) :

التطابق الخطي

$$2x \equiv 1 \pmod 5$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

بملك حل وحيد هو $x_0 = 3$

لأن:

$Z_5 = \{0, 1, 2, 3, 4\}$

$2X0 \not\equiv 1 \pmod 5$

$2X1 \not\equiv 1 \pmod 5$

$2X2 = 4 \not\equiv 1 \pmod 5$

$2X3 = 6 \equiv 1 \pmod 5 \Rightarrow x_0 = 3$

$2X4 = 8 \not\equiv 1 \pmod 5$

مثال (2):

التطابق $4x \equiv 2 \pmod 6$

يملك حلين $x_1 = 2$

$x_2 = 5$

لأن:

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

$4X0 \not\equiv 2 \pmod 6$

$4X1 = 4 \not\equiv 2 \pmod 6$

$4X2 = 8 \equiv 2 \pmod 6 \Rightarrow x_1 = 2$

$4X3 = 12 \not\equiv 2 \pmod 6$

$4X4 = 16 \not\equiv 2 \pmod 6$

$4X5 = 20 \equiv 2 \pmod 6 \Rightarrow x_2 = 5$

مثال (3):

التطابق $4x \equiv 2 \pmod 8$

غير قابل للحل.

- نستنتج من الأمثلة السابقة بأن التطابق الخطي

$$dx \equiv b \pmod m$$

إما يقبل الحل أو قابل للحل

فإذا كان قابل للحل فقد يملك حلاً وحيداً أو يملك أكثر من حل

ملاحظة

التطابق $dx \equiv b \pmod m$

حيث $\gcd(d, m) = 1$

يملك حلاً وحيداً بالنسبة للمقاس m

الإثبات:

$$1 = \gcd(d, m)$$

$$= dd_0 + mm_0 \quad ; \quad d_0, m_0 \in \mathbb{Z}$$

نضرب الطرفين بـ b:

$$\Rightarrow d(d_0 b) + mm_0 b = b$$

$$d(d_0 b) \equiv b \pmod m$$

$\Leftarrow$ التطابق

$$dx \equiv b \pmod m$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

قابل للحل:

ليكن x_0 حل معين للتطابق

$$ax \equiv b \pmod m$$

وليكن x^* حل آخر للتطابق

$$ax \equiv b \pmod m$$

بما أن: x_0 حل $\Leftarrow$

$$ax_0 \equiv b \pmod m$$

و x^* حل $\Leftarrow$

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

$$\Rightarrow ax^* \equiv ax_0 \pmod m$$

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

$\Leftarrow$ التطابق يملك حل وحيد بالنسبة للمقاس m

• برهنة (1):

شرط قابلية الحل

ليكن $a, b, m \in \mathbb{Z}$ ، $m \geq 2$

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

عندئذ التطابق الخطي:

$$ax \equiv b \pmod m$$

قابل الحل إذا وفقط إذا كان $d \mid b$

TEL:0931497960 - Facebook Group: A to Z مكتبة

- الإثبات:

$\Leftarrow$ - التطابق $dx \equiv b \pmod{m}$

قابل الحل، ولكن x_0 حلاً لـ

$$dx_0 \equiv b \pmod{m}$$

$$dx_0 = b + qm \quad \star$$

- لدينا $d = gcd(a, m) \Rightarrow a = a_0 d$

$$m = m_0 d$$

نعوض في $\star$ نجد:

$$da_0 x_0 = b + qm_0 d$$

$$\Rightarrow da_0 x_0 - qm_0 d = b$$

$$\Rightarrow d(a_0 x_0 - qm_0) = b$$

$$\Rightarrow d \mid b$$

$\Rightarrow$ لدينا فرضاً $d \mid b$ ولنثبت أن التطابق

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

قابلاً الحل

- بما أن

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

$$\exists a_0, m_0 \in \mathbb{Z} : \quad d = a_0 d + m_0 m \quad (1)$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

برهان: $d \mid b$ عندئذٍ:

$b = b_0 d \quad ; \quad b_0 \in \mathbb{Z}$

نضرب (1) بـ b_0 نجد:

$b_0 d = a_0 b_0 d + m_0 b_0 m$

$\Rightarrow b = a(a_0 b_0) + m_0 b_0 m$

$\Rightarrow a(a_0 b_0) \equiv b \pmod{m}$

$\Leftarrow x_0 = a_0 b_0$ حل للتطابق

$dx \equiv b \pmod{m}$

(التطابق قابل للحل.)

ومنه المبرهنة حيث شرط قابلية الحل للتطابق الخطي

$dx \equiv b \pmod{m}$

في مجموعة الأعداد الصحيحة.

- سندرس في المبرهنة التالية جميع حلول التطابق الخطي

$dx \equiv b \pmod{m}$

إذا كان قابلاً للحل في مجموعة الأعداد الصحيحة.

TEL:0931497960 - Facebook Group: A to Z مكتبة

برهنة (2):

ليكن $a, b, m \in \mathbb{Z}$ ، $m \geq 2$

$d = gcd(a, m)$

عندئذٍ إذا كان $d \mid b$ عندئذٍ

التطابق الخطي

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

يقبل بالضبط d حلاً مختلفاً بالقياس للعدد m

وهذه الحلول هي:

$$\left\{ x_0 + k\frac{m}{d} \; ; \; 0 \leq k \leq d-1 \right\}$$

$$= \left\{ x_0 + k m_1 \; ; \; m_1 = \frac{m}{d} \; \wedge \; 0 \leq k \leq d-1 \right\}$$

$$= \{ x_0, x_0 + m_1, x_0 + 2m_1, \ldots\ldots, x_0 + (d-1)m_1 \}$$

حيث x_0 حل التطابق:

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

- الإثبات:

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

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

$$; \; a = a_0 d$$

$$m = m_1 d$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$d \mid b \Rightarrow b = b_0 d \quad ; b_0 \in \mathbb{Z}$

- نثبت أن أي حل للتطابق

هو حل للتطابق $dx \equiv b \pmod{m}$

$d_0 x \equiv b_0 \pmod{m_1}$

والعكس صحيح

$\Leftarrow$ لدينا فرضاً x_0 حلاً لـ

$dx \equiv b \pmod{m}$

$\Rightarrow d_0 d x_0 \equiv b_0 d \pmod{m_1 d}$

$\Rightarrow$ نقسم الطرفين على d

$\Rightarrow d_0 x_0 \equiv b \pmod{m_1}$

$\Leftarrow$ x_0 حلاً لـ $d_0 x \equiv b_0 \pmod{m_1}$

$\Rightarrow$ لنكن x_0 حلاً لـ $d_0 x \equiv b_0 \pmod{m_1}$

$\Rightarrow d_0 x \equiv b_0 \pmod{m_1}$

$\Rightarrow d_0 x_0 = b_0 + q m_1$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$d_0 d x_0 = b_0 d + q m_1 d$

$d x_0 = b + q m$

$\Rightarrow d x_0 \equiv b \pmod m$

$\Leftarrow x_0$ حلاً للتطابق

$dx \equiv b \pmod m$

- نلاحظ بأنّ التطابق الخطّي:

$d_0 x \equiv b_0 \pmod{m_1}$

يملك حل وحيد

لأنّ:

$gcd(d_0, m_1) = 1$

نستنتج بأنّ حلول التطابق

$dx \equiv b \pmod m$

هي:

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

وجميع هذه الحلول متطابقة بالنسبة للمقاس m_1

- لنأخذ:

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

TEL:0931497960 - Facebook Group: A to Z مكتبة

ولنثبت أنّ:

① جميع عناصر H غير متطابقة بالنسبة للمقاس m

② أي عنصر من H يطابق أحد عناصر H بالنسبة للمقاس m

إثبات ①

نفرض جدلاً أنّ:

$$x_0 + i m_1 \equiv x_0 + j m_1 \pmod{m}$$

حيث $i \neq j$

$$0 \leq j < i \leq d-1$$

عندئذٍ:

$$m \mid (i-j)\, m_1$$
$$\Rightarrow m_1 d \mid (i-j)\, m_1$$
$$\Rightarrow d \mid (i-j) \; ; \; 0 < i-j < d$$

وهذا مرفوض

← الفرض الجدلي خاطئ

← $x_0 + i m_1 \not\equiv x_0 + j m_1 \pmod{m}$

← عناصر H غير متطابقة بالنسبة للمقاس m

إثبات ②

$$\forall\, y \in H \; : \; y = x_0 + t m_1$$

(بتطبيق القسمة الإقليدية نجد:
$t = qd + r$)

TEL:0931497960 - Facebook Group: A to Z مكتبة

حيث:

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

$$\Rightarrow y = x_0 + t m_1$$

$$= x_0 + (qd + r) m_1$$

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

$$= x_0 + qm + r m_1$$

$$\Rightarrow y \equiv x_0 + r m_1 \pmod{m}$$

(أمثلة):

1- أوجد حلول التطابق

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

$a = 6$ ، $b = 8$ ، $m = 10$

$$d = \gcd(a, m) = 2$$

$2 \mid b$ ⟸ التطابق قابل للحل

ويملك حلول مختلفان بالنسبة للقاس 10.

$$\{ x_0 + k m_1 \; ; \; 0 \leq k \leq 1 \;\; \& \;\; m_1 = \frac{m}{d} = 5 \}$$

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

TEL:0931497960 - Facebook Group: A to Z مكتبة

لنوجد x_0 :

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

$$3x \equiv 4 \pmod{5}$$

$$6x \equiv 8 \pmod{5}$$

$$x \equiv 3 \pmod{5}$$

$$\Rightarrow \boxed{x_0 = 3}$$

$\Leftarrow$ الحلول هي $\{3, 8\}$

2- $9x \equiv 21 \pmod{30}$

$a = 9 \quad , \quad b = 21 \quad , \quad m = 30$

$d = \gcd(a, m) = 3$

$3 \mid b \Leftarrow$ التطابق يملك ثلاث حلول مختلفة بالبنية للقاسم 30 هي :

$$\{x_0 + k m_1 \; ; \; 0 \le k \le 2 \;\&\; m_1 = \frac{m}{d} = 10\}$$

$$= \{x_0, x_0 + 10, x_0 + 20\}$$

ولنوجد x_0 :

$$9x \equiv 21 \pmod{30}$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$$3x \equiv 7 \pmod{10}$$
$$9x \equiv 21 \pmod{10}$$
$$-x \equiv 1 \pmod{10}$$
$$x \equiv -1 \pmod{10}$$
$$\Rightarrow x \equiv 9 \pmod{10}$$

$x_0 = 9$ ⟸

⟸ الحلول هي $\{9, 19, 29\}$

-3

$$8x \equiv 16 \pmod{20}$$

$a = 8$ ، $b = 16$ ، $m = 20$

$d = \gcd(a, m) = 4$

$4 \mid b$ ⟸ التطابق يملك أربعة حلول مختلفة بالنسبة للقاس 20 مثلاً:

$$\{x_0 + k m_1 ; \ 0 \le k \le 3 \ \text{و} \ m_1 = \frac{m}{d}\}$$

$$= \{x_0, x_0 + m_1, x_0 + 2m_1, x_0 + 3m_1\}$$
$$= \{x_0, x_0 + 5, x_0 + 10, x_0 + 15\}$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

ولنوجد x_0 :

$$8x \equiv 16 \pmod{20}$$
$$2x \equiv 4 \pmod{5}$$
$$6x \equiv 12 \pmod{5}$$
$$x \equiv 2 \pmod{5}$$
$$\Rightarrow x_0 = 2$$

الحلول هي $\Leftarrow$ $\{2, 7, 12, 17\}$

انتهت المحاضرة

TEL:0931497960 - Facebook Group: A to Z مكتبة