كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

المادة : نظرية الاعداد

المحاضرة : الثالثة عشر /نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

المحاضرة الأخيرة
(نظري)

تذكره:

ملاحظة: نستخدم الرمز $\text{Ind}\ x$ بدلاً من $\text{Ind}_g\ x$ علماً أن g جذر أساسي بالنسبة للمقاس m

مبرهنة: ليكن m عدداً صحيحاً موجباً يملك جذر أساسي g وليكن $a, b \in \mathbb{Z}$ بحيث

$$\gcd(a, m) = \gcd(b, m) = 1$$

عندئذ:

1. إذا كان $a \equiv b(mod\ m)$ عندئذ $\text{Ind}\ (a) = \text{Ind}\ (b)$
2. $\text{Ind}(\ ab) \equiv \text{Ind}\ (a) + \text{Ind}\ (b)(mod\ \phi(m))$
3. $\text{Ind}\ (a^n) \equiv n\ \text{Ind}\ (a)(mod\ \phi(m))$ حيث n عدد صحيح موجب.
4. $\text{Ind}\ (g) = 1$
5. $\text{Ind}\ (1) = \phi(m)$

دراسة التطابقات من مراتب عليا $x^n \equiv a(mod\ m)$

تشمل

1. معرفة التطابق فيما إذا كان قابل للحلّ أم لا
2. إيجاد جميع الحلول المختلفة للتطابق $x^n \equiv a(mod\ m)$

❖ **ندرس في المبرهنة التالية شرط قابلية الحلّ للتطابق $x^n \equiv a(mod\ m)$**

مبرهنة أولر المعممة:

ليكن m عدداً صحيحاً موجباً يملك جذر أساسي g ولتكن $a, n \in \mathbb{Z}$ بحيث $n \geq 2$ وليكن

$$d = \gcd\big(n, \phi(m)\big)$$

عندئذٍ

التطابق $x^n \equiv a(mod\ m)$ قابل للحل إذا وفقط إذا كان

$$a^{\frac{\phi(m)}{d}} \equiv 1(mod\ m)$$

مثال:

بيّن فيما إذا كان التطابق $x^6 \equiv -9(mod\ 19)$ قابل للحلّ أم لا

الحلّ: التطابق المعطى هو: $x^6 \equiv -9(mod\ 19)$

لدينا $n = 6, a = -9, m = 19$

$$\phi(m) = 18, \qquad d = \gcd\big(n, \phi(m)\big) = 6$$

نلاحظ بأنّ

$$a^{\frac{\phi(m)}{d}} = (-9)^3 \not\equiv 1(mod\ 19)$$

بالتالي التطابق غير قابل للحلّ.

مثال:

بيّن فيما إذا كان التطابق $x^6 \equiv 5(mod\ 17)$ قابل للحلّ أم لا؟

الحل:

التطابق المعطى هو: $x^6 \equiv 5(mod\ 17)$

لدينا $n = 6, a = 5, m = 17$

$$\phi(m) = 16, \qquad d = \gcd(n, \phi(m)) = 2$$

نلاحظ بأنّ:

$$a^{\frac{\phi(m)}{d}} = 5^8 \not\equiv 1(mod\ 17)$$

بالتالي التطابق غير قابل للحلّ.

مثال:

بيّن فيما إذا كان التطابق $x^5 \equiv 11(mod\ 19)$ قابل للحلّ أم لا؟

الحلّ

التطابق المعطى هو: $x^5 \equiv 11(mod\ 19)$

لدينا $n = 5, a = 11, m = 19$

$$\phi(m) = 18, \qquad d = \gcd(n, \phi(m)) = 1$$

نلاحظ بأنّ

$$a^{\frac{\phi(m)}{d}} = (11)^{18} \equiv 1(mod\ 19)$$

بالتالي التطابق قابل للحلّ.

❖ ندرس الآن كيف نوجد الحلول المختلفة للتطابق $x^n \equiv a(mod\ m)$

1. نوجد جذر أساسي g بالنسبة للمقاس m.
2. نشكل جدول الأدلة بالنسبة للمقاس m علماً أنّ g جذر أساسي بالنسبة للمقاس m.
3. نطبق الدليل Ind لطرفي التطابق المعطى

$$x^n \equiv a(mod\ m)$$
$$\mathrm{Ind}(x^n) \equiv \mathrm{Ind}(a)\ (mod\ \boldsymbol{\phi}(\boldsymbol{m}))$$
$$n \times \mathrm{Ind}(x) \equiv \mathrm{Ind}(a)\ (mod\ \phi(m))$$

نحسب $\mathrm{Ind}(a)$ من جدول الأدلة ونفرض $\mathrm{Ind}x = y$ فنحصل على تطابق خطي من الدرجه الأولى فنقوم بإيجاد جميع حلوله المختلفة ومن ثم نستنتج من جدول الأدلة جميع قيم x التي تحقق التطابق المعطى $x^n \equiv a(mod\ m)$

مثال:

أوجد الحلول المختلفة للتطابق $x^{12} \equiv 16(mod\ 17)$ باستخدام نظرية الأدلة

الحلّ:

4. لدينا $g = 3$ جذر أساسي بالنسبة للمقاس 17 حسب اختبار لوكاس، ولنوجد جدول الأدلة بالنسبة للمقاس $m = 17$ علماً أنّ $g = 3$ جذر أساسي بالنسبة للمقاس 17.

1. نحسب 3^k حيث $1 \le k \le \phi(17) = 16$.

3^k	3^1	3^2	3^3	3^4	3^5	3^6	3^7	3^8	3^9	3^{10}	3^{11}	3^{12}	3^{13}	3^{14}	3^{15}	3^{16}
N	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
$\mathrm{Ind}N$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

N: هو باقي قسمة 3^k على العدد 17. $\mathrm{Ind}N$: دليل العدد N

$x^{12} \equiv 16(mod\ 17)$ نطبق نظرية الأدلة للطرفين نجد

$$12\ Indx \equiv Ind16(mod\ \phi(17))$$
$$12\ Indx \equiv 8(mod\ 16)$$

نفرض $Indx = y$

هذا التطابق$12\, y \equiv 8(mod\ 16)$ خطي يملك أربع حلول مختلفه بالنسبة للمقاس 16 هما

$$Indx = y \in \{2,6,10,14\}$$

بالتالي

$$Indx = 2 \Longrightarrow x = 9$$
$$Indx = 6 \Longrightarrow x = 15$$
$$Indx = 10 \Longrightarrow x = 8$$
$$Indx = 14 \Longrightarrow x = 2$$

بالتالي حلول التطابق $x^{12} \equiv 16(mod\ 17)$ هي $\{2,8,9,15\}$

مثال

أوجد الحلول المختلفة للتطابق $x^3 \equiv -1(mod\ 13)$ باستخدام نظرية الأدلة

الحلّ:

لدينا $g = 2$ جذر أساسي بالنسبة للمقاس 13، ولنوجد جدول الأدلة بالنسبة للمقاس $m = 13$ علماً أنّ $g = 2$ جذر أساسي بالنسبة للمقاس 13.

نحسب 2^k حيث $1 \le k \le \phi(13) = 12$.

2^k	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}
N	2	4	8	3	6	12	11	9	5	10	7	1
$IndN$	1	2	3	4	5	6	7	8	9	10	11	12

N: هو باقي قسمة 2^k على العدد 13. $IndN$: دليل العدد N

$x^3 \equiv -1(mod\ 13)$ تكافئ $x^3 \equiv 12(mod\ 13)$

$x^3 \equiv 12(mod\ 13)$ نطبق نظرية الأدلة للطرفين نجد

$$3\ Indx \equiv Ind12(mod\ \phi(13))$$
$$3\ Indx \equiv 6(mod\ 12)$$

نفرض $Indx = y$

هذا التطابق

$$3y \equiv 6(mod\ 12)$$

يملك ثلاث حلول مختلفة بالنسبة للمقاس 12 هي

$Indx = y \in \{2,6,10\}$ بالتالي

$$Indx = 2 \Longrightarrow x = 4$$
$$Indx = 6 \Longrightarrow x = 12$$
$$Indx = 10 \Longrightarrow x = 10$$

بالتالي حلول التطابق $x^3 \equiv 16(mod\ 13)$ هي $\{4,10,12\}$

بالتالي حلول التطابق $x^3 \equiv -1(mod\ 13)$ هي $\{4,10,12\}$

مثال

أوجد جدول الأدلة بالنسبة للمقاس 13 علماً أنّ $g = 2$ جذر أساسي بالنسبة للمقاس 13، ثم أوجد حلول التطابق $7x^3 \equiv 4\ (mod\ 13)$ باستخدام الأدلة.

الحلّ:

نحسب $2^k; 1 \le k \le \phi(13) = 12$ (2 جذر أساسي بالنسبة للمقاس 13).

2^k	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}
N	2	4	8	3	6	12	11	9	5	10	7	1
$IndN$	1	2	3	4	5	6	7	8	9	10	11	12

N: هو باقي قسمة 2^k على العدد 11. $IndN$: دليل العدد N

- المعكوس الضربي للعدد 7 بالنسبة للمقاس 13 هو العدد 2 أي أن
$7^{-1} = 2$

عندئذ حلول التطابق

$$7x^3 \equiv 4 \ (mod\ 13)$$

هي نفسها حلول التطابق

$$7^{-1} \times 7x^3 \equiv 7^{-1} \times 4 \ (mod\ 13)$$

أي $x^3 \equiv 2 \times 4 \ (mod\ 13)$ أي $x^3 \equiv 8 \ (mod\ 13)$

عندئذ

حلول التطابق

$$7x^3 \equiv 4 \ (mod\ 13)$$

هي نفسها حلول التطابق

$$x^3 \equiv 8 \ (mod\ 13)$$

نطبق نظرية الأدلة لطرفي التطابق $x^3 \equiv 8 \ (mod\ 13)$ نجد

$$3\ Indx \equiv Ind8 (mod\ \phi(13))$$
$$3\ Indx \equiv 3 (mod\ 12)$$

هذا التطابق يملك ثلاث حلول مختلفة هي $Indx \in \{1,5,9\}$ بالتالي

$$Indx = 1 \Longrightarrow x = 2$$
$$Indx = 5 \Longrightarrow x = 6$$
$$Indx = 9 \Longrightarrow x = 5$$

بالتالي حلول التطابق $7x^3 \equiv 4 \ (mod\ 13)$ هي

$$\{2,5,6\}$$

❖ **دراسة التطابق من النمط $ax^2 + bx + c \equiv 0 (mod\ p)$ حيث p عدد أولي فردي لا يقسم العدد a**

مبرهنة:

ليكن p عدداً أولياً فردياً لا يقسم العدد a عندئذ التطابق

$$ax^2 + bx + c \equiv 0 (mod\ p)$$

قابل للحل إذا وفقط إذا كان التطابق $y^2 \equiv d (mod\ p)$ قابلا للحل حيث $d = b^2 - 4ac$

ملاحظة:

إذا كان p عدداً أولياً فردياً و $a \in \mathbb{Z}$ بحيث $gcd(a,p) = 1$ عندئذ التطابق التربيعي $x^2 \equiv a (mod\ p)$ إما يملك حلين فقط أو ليس له حلول بالنسبة للمقاس p.

سؤال: إذا كان p عدداً أولياً فردياً و $a \in \mathbb{Z}$ بحيث $gcd(a,p) = 1$ والتطابق $ax^2 + bx + c \equiv 0 (mod\ p)$ قابل للحلّ عندئذ لإيجاد حلوله نقوم بالخطوات التالية:

- نوجد $d = b^2 - 4ac$

- نحلّ التطابق التالي $y^2 \equiv d(mod\ p)$ وليكن حلوله هي $y_0, y_1 = -y_0$ بالنسبة للمقاس p
- نحلّ التطابق الخطي $2ax \equiv y - b(mod\ p)$ وذلك من أجل كل حل y لـ $y^2 \equiv d(mod\ p)$

فنحصل على الحلين x_1 و x_2

بالتالي حلول التطابق $ax^2 + bx + c \equiv 0(mod\ p)$ هي $\{x_1, x_2\}$

مثال:

أوجد الحلين المختلفين للتطابق $5x^2 - 6x + 2 \equiv 0(mod\ 13)$.

لدينا $a = 5$ و $b = -6$ و $c = 2$ و $p = 13$

- نوجد $d = b^2 - 4ac = -4$
- نوجد حلول التطابق $y^2 \equiv d(mod\ p)$، أي لنوجد حلول التطابق $y^2 \equiv -4(mod\ 13)$

أي لنوجد حلول التطابق $y^2 \equiv 9(mod\ 13)$

وهي $\{-3, 3\}$

✓ من أجل $y_0 = 3$ نحل التطابق الخطي

$$2ax \equiv y_0 - b(mod\ 13)$$

فنجد

$$10x \equiv 9(mod\ 13) \Longrightarrow x \equiv 10(mod\ 13) \Longrightarrow x = 10$$

✓ من أجل $y_0 = -3$ نحل التطابق الخطي

$$2ax \equiv y_0 - b(mod\ 13)$$

فنجد

$$10x \equiv 3(mod\ 13) \Longrightarrow x \equiv 12(mod\ 13) \Longrightarrow x = 12$$

بالتالي حلول التطابق $5x^2 - 6x + 2 \equiv 0(mod\ 13)$ هي

$$\{10, 12\}$$

مثال:

أوجد الحلين المختلفين للتطابق $x^2 + 7x + 10 \equiv 0(mod\ 11)$.

لدينا $a = 1$ و $b = 7$ و $c = 10$ و $p = 11$

- نوجد $d = b^2 - 4ac = 9$
- نوجد حلول التطابق $y^2 \equiv d(mod\ p)$، أي لنوجد حلول التطابق $y^2 \equiv 9(mod\ 11)$

وهي $\{-3, 3\}$

✓ من أجل $y_0 = 3$ نحل التطابق الخطي

$$2ax \equiv y_0 - b(mod\ 11)$$

فنجد

$$2x \equiv -4(mod\ 11) \Longrightarrow x \equiv -2(mod\ 11) \Longrightarrow x \equiv 9(mod\ 11) \Longrightarrow x = 9$$

✓ من أجل $y_0 = -3$ نحل التطابق الخطي

$$2ax \equiv y_0 - b(mod\ 13)$$

فنجد

$$2x \equiv -3 - 7(mod\ 11) \Longrightarrow x \equiv 6(mod\ 11) \Longrightarrow x = 6$$

بالتالي حلول التطابق $x^2 + 7x + 10 \equiv 0(mod\ 11)$ هي

$$\{6, 9\}$$