كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : الثالثة عشر /نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

محاضرة النظري الأخيرة لمقرر نظرية الأعداد للعام الدراسي 2024-2025م

السنة الرابعة رياضيات

مدرس المقرر: د. احمد عيسى

ملاحظة: نستخدم الرمز $\mathrm{I}nd\ x$ بدلاً من $\mathrm{I}nd_g\ x$

مبرهنة: ليكن m عدد صحيح موجب 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 $\mathrm{I}nd\ a = \mathrm{I}nd\ b$
2. $\mathrm{I}nd(\ ab) \equiv \mathrm{I}nd\ a + \mathrm{I}nd\ b(mod\ \phi(m))$
3. $\mathrm{I}nd\ a^n \equiv n\ \mathrm{I}nd\ a(mod\ \phi(m))$ حيث n عدد صحيح موجب.
4. $\mathrm{I}nd\ g = 1$
5. $\mathrm{I}nd\ 1 = \phi(m)$

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 المعطى القابل للحلّ

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

مبرهنة أولر المعممة:

ليكن m عدد صحيح موجب 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 $x^6 \equiv 10(mod\ 19)$ قابل للحلّ أم لا؟

الحلّ: التطابق المعطى هو: $x^6 \equiv 10(mod\ 19)$

لدينا $n = 6, a = 10, m = 19$

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

نلاحظ بأنّ

$$a^{\frac{\phi(m)}{d}} = 10^3 \not\equiv 1(mod\ 19)$$

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 $n = 6, a = 5, m = 17$

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

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 $n = 5, a = 11, m = 19$

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

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 للجذر الأساسي g قياس m.
3. نطبق الدليل Ind لطرفي التطابق المعطى

$$x^n \equiv a(mod\ m)$$
$$\mathrm{I}ndx^n \equiv \mathrm{I}nda\ \big(mod\ \boldsymbol{\phi(m)}\big)$$
$$n\mathrm{I}ndx \equiv \mathrm{I}nda\ \big(mod\ \phi(m)\big)$$

نحسب $\mathrm{I}nda$ من جدول الأدلة ونفرض $Indx = y$ 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.

مثال:

أوجد الحلول المختلفة للتطابق $x^8 \equiv 16(mod\ 17)$.

الحلّ:

1. لدينا $g = 3$ جذر أساسي بالنسبة للمقاس 17 حسب اختبار لوكاس، ولنوجد جدول الأدلة بالنسبة للجذر الأساسي $g = 3$ قياس 17.

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
$\mathrm{I}ndN$	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. $\mathrm{I}ndN$: دليل العدد N

نطبق نظرية الأدلة للطرفين نجد $x^8 \equiv 16(mod\ 17)$

$$8\ \mathrm{I}ndx \equiv \mathrm{I}nd16(mod\ \phi(17))$$
$$8\ \mathrm{I}ndx \equiv 8(mod\ 16)$$

نفرض $\mathrm{I}ndx = y$

هذا التطابق

$$8\ y \equiv 8(mod\ 16)$$

يملك ثمان حلول مختلفه بالنسبة للمقاس 16 هما $\mathrm{I}ndx = y \in \{1,3,5,7,9,11,13,15\}$ بالتالي

$$\mathrm{I}ndx = 1 \Longrightarrow x = 3$$
$$\mathrm{I}ndx = 3 \Longrightarrow x = 10$$
$$\mathrm{I}ndx = 5 \Longrightarrow x = 5$$
$$\mathrm{I}ndx = 7 \Longrightarrow x = 11$$
$$\mathrm{I}ndx = 9 \Longrightarrow x = 14$$
$$\mathrm{I}ndx = 11 \Longrightarrow x = 7$$
$$\mathrm{I}ndx = 13 \Longrightarrow x = 12$$
$$\mathrm{I}ndx = 15 \Longrightarrow x = 6$$

بالتالي حلول التطابق هي $\{3,5,6,7,10,11,12,14\}$

السؤال الثاني:

أوجد الحلول المختلفة للتطابق $x^5 \equiv 11(mod\ 19)$.

الحلّ:

لدينا $g = 2$ جذر أساسي بالنسبة للمقاس 19، ولنوجد جدول الأدلة بالنسبة للجذر الأساسي $g = 2$ قياس 19.

نحسب 2^k حيث $1 \le k \le \phi(19) = 18$.

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}	2^{13}	2^{14}	2^{15}	2^{16}	2^{17}	2^{18}
N	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
$\mathrm{I}ndN$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

N: هو باقي قسمة 2^k على العدد 19. $\mathrm{I}ndN$: دليل العدد N

نطبق نظرية الأدلة للطرفين نجد $x^5 \equiv 11(mod\ 19)$

$$5\ \mathrm{I}ndx \equiv \mathrm{I}nd11(mod\ \phi(19))$$
$$5\ \mathrm{I}ndx \equiv 12(mod\ 18)$$

نفرض $\mathrm{I}ndx = y$

هذا التطابق

$$5y \equiv 12(mod\ 18)$$

يملك حل وحيد هو $\mathrm{I}ndx = 6$ بالتالي

$$\mathrm{I}ndx = 6 \Longrightarrow x = 7$$

بالتالي حلول التطابق هي $\{7\}$

السؤال الثالث:

أوجد جدول الأدلة بالنسبة للجذر الأساسي $g = 2$ قياس 11 ثم أوجد حلول التطابق $x^4 \equiv 4\ (mod\ 11)$ باستخدام الأدلة.

الحلّ:

نحسب $2^k; 1 \leq k \leq \phi(11) = 10$ (2 جذر أساسي بالنسبة للمقاس 11).

2^k	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
N	2	4	8	5	10	9	7	3	6	1
$\mathrm{I}ndN$	1	2	3	4	5	6	7	8	9	10

N: هو باقي قسمة 2^k على العدد 11. $\mathrm{I}ndN$: دليل العدد N

$x^4 \equiv 4\ (mod\ 11)$ نطبق نظرية الأدلة للطرفين نجد

$$4\ \mathrm{I}ndx \equiv \mathrm{I}nd4(mod\ \phi(11))$$
$$4\ \mathrm{I}ndx \equiv 2(mod\ 10)$$

هذا التطابق يملك حلين مختلفين هما $\mathrm{I}ndx \in \{3,8\}$ بالتالي

$$\mathrm{I}ndx = 3 \Longrightarrow x = 8$$
$$\mathrm{I}ndx = 8 \Longrightarrow x = 3$$

بالتالي حلول التطابق هي $\{3,8\}$

مكتبة

مكتبة A TO Z

فرع 1
تجمع الكليات(كلية العلوم)

فرع 2
الكورنيش الشرقي جانب MTN

طباعة محاضرات ـ قرطاسية

Mob:0931 497 960