كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

المادة : نظرية الاعداد

المحاضرة : **الثانية عشر/نظري/**

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

2025

كلية العلوم ، كلية الصيدلة ، الهندسة التقنية

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

ملاحظة:

• تعيين جذر أساسي بالنسبة للمقاس m :

1. $m=p$ حيث p عدد أولي فردي

نستخدم اختبار لوكاس لإيجاد جذر أساسي بالنسبة لـ $m=p$

2. $m=p^k$ حيث p عدد أولي فردي و $k \geq 2$ (عدد صحيح)

الطريقة

* نوجد جذر أساسي بالنسبة للمقاس p حسب اختبار لوكاس

وليكن g

* نوجد g^{p-1}

إذا كانت :

$$g^{p-1} \not\equiv 1 \pmod{p^2}$$

عندئذٍ g جذر أساسي بالنسبة للمقاس $m=p^k$

• إذا كانت :

$$g^{p-1} \equiv 1 \pmod{p^2}$$

عندئذٍ :

$$g' = g+p$$

جذر أساسي بالنسبة للمقاس $m=p^k$

3. $m = 2p^k$ حيث $k \geq 1$ (عدد صحيح)

* نعيّن جذر أساسي بالنسبة للمقاس p^k وليكن g

• اذا كان g فردي عندئذٍ g جذر أساسي بالنسبة للمقاس $m = 2p^k$

• اذا كان g زوجي عندئذٍ:

$$\acute{g} = g + p^k$$

جذر أساسي بالنسبة للمقاس $m = 2p^k$

مثال: ليكن $m = 5$

① أوجد جذر أساسي بالنسبة للمقاس m حسب اختيارك ثم استنتج جذر أساسي بالنسبة للمقاس 25 ثم جذر أساسي بالنسبة للمقاس 50

② أوجد عدد الجذور الأساسية بالنسبة للمقاس 25

③ أوجد جميع الجذور الأساسية بالنسبة للمقاس 5

④ أوجد جميع الأعداد الصحيحة الموجبة d الأقل من 25 والتي تحقق الشرط التالي:

$$O_{25}(a) = 4$$

⑤ أوجد $O_5(43)$

⑥ هل المجموعة

$$\{2^1, 2^2, 2^3, 2^4\}$$

نظام بواقي مختزل قياس 10

الحل:

*① $a \in Z_5^* = \{1, 2, 3, 4\}$

جذر أساسي بالنسبة للمقاس $m = 5$

TEL:0931497960 - Facebook Group: A to Z مكتبة

إذا تحقق الشرط:

$$a^{\frac{p-1}{q}} \not\equiv 1 \pmod 5$$

وذلك من أجل كل قاسم أولي q للعدد

$$p-1 = 4$$

$$\Rightarrow q = 2$$

- $a=1$: نلاحظ:

$$1^{\frac{4}{2}} = 1 \equiv 1 \pmod 5$$

$\Leftarrow a=1$ ليس جذراً أساسياً بالنسبة للقاس 5

- $a=2$:

$$2^{\frac{4}{2}} = 2^2 = 4 \not\equiv 1 \pmod 5$$

$\Leftarrow a=2$ جذراً أساسي بالنسبة للقاس 5 وذلك حسب اختبار لوكاس

* $25 = 5^2$ & 5 عدد أولي فردي

لدينا $g=2$ جذر أساسي بالنسبة للقاس 5

ثم نحسب:

$$g^{p-1} = 2^4$$

$$g^{p-1} = 2^4 \not\equiv 1 \pmod{5^2}$$

$\Leftarrow g=2$ جذر أساسي بالنسبة للقاس 25

TEL:0931497960 - Facebook Group: A to Z مكتبة

* $50 = 2 \times 5^2$

لدينا $g=2$ جذر أساسي بالنسبة لـ $25 = 5^2$

نلاحظ بأن g زوجي عندئذٍ:

$\acute{g} = g + 5^2 = 27$

جذر أساسي بالنسبة للمقاس 50

(2) عدد الجذور الأساسية بالنسبة للمقاس 25 هو:

$\phi(\phi(25)) = \phi(20)$

$= \phi(4 \times 5) = \phi(4) \times \phi(5)$

$= 2 \times 4 = 8$

(3) نشكل المجموعة التالية:

علماً بأن $g=2$ جذر أساسي بالنسبة للمقاس 5

$\{ 2^k ; 1 \le k \le \phi(5) \text{ & } gcd(k, \phi(5)) = 1 \}$

$= \{ 2^1, 2^3 \}$

نوجد بواقي القسمة:

$2^1 \equiv 2 \pmod 5$

$2^3 = 8 \equiv 3 \pmod 5$

نلاحظ بأن $\{2, 3\}$ هي الجذور الأساسية بالنسبة للمقاس 5

(4

$g = 2$ ، $O_{25}(a) = 4$

جذر أساسي بالنسبة للمقياس 25

$\gcd(a, 25) = 1$

$\Rightarrow a \equiv a^k \pmod{25}$ k

$\{$

$1 \leq k \leq \phi(25)$

$\Rightarrow O_{25}(a) = O_{25}(2^k)$

$\Rightarrow 4 = \dfrac{O_{25}(2)}{\gcd(k, O_{25}(2))}$

$= \dfrac{\phi(25)}{\gcd(k, \phi(25))}$

$= \dfrac{20}{\gcd(k, 20)}$

$\Rightarrow \gcd(k, 20) = 5$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$\Rightarrow k \in \{5, 15\}$

$2^k \in \{2^5, 2^{15}\}$

$2^5 \equiv 7 \pmod{25}$

$2^{15} \equiv 18 \pmod{25}$

بالتالي الأعداد الصحيحة الموجبة a الأقل من 25 و تحقق الشرط:

$O_{25}(a) = 4$

هي:

$\{7, 18\}$

(5) $43 \equiv 3 \pmod 5$

$O_5(43) = O_5(3) = \phi(5) = 4$

(6) $10 = 5 \times 2$

لدينا $g = 2$ جذر أساسي بالنسبة للمقاس 5 و $g = 2$ زوجي

عندئذ:

$\acute{g} = g + 5 = 7$

جذر أساسي بالنسبة للمقاس 10

- الجذور الأخرى بالنسبة للمقاس 10:

$\{7^k ; 1 \le k \le \phi(10) \ \& \ gcd(k, \phi(10)) = 1\}$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$7^1 \equiv 7 \pmod{10}$

$7^3 \equiv 3 \pmod{10}$

بالتالي الجذور الأساسية بالنسبة للمقاس 10 هي $\{3, 7\} \leftarrow 2$ ليس جذر أساسي بالنسبة للمقاس 10 بالتالي المجموعة

$\{2^1, 2^2, 2^3, 2^4\}$

ليست نظام بواقي مختزل بالنسبة للمقاس 10.

طريقة (2):

$\forall x \in A = \{2^1, 2^2, 2^3, 2^4\}$

$\gcd(x, 10) = 2 \neq 1$

* نظرية الأدلّة:

إذا كان g جذر أساسي بالنسبة للمقاس m عندئذٍ:

$\{g^1, g^2, \ldots, g^{\phi(m)}\}$

نظام بواقي مختزل قياس m.

$\forall a \in \mathbb{Z} ; \gcd(a, m) = 1 ; \exists$ (وحيد) $k \in \mathbb{Z}$

$1 \leq k \leq \phi(m)$

,

$a \equiv g^k \pmod{m}$

$g^k \equiv a \pmod{m}$

وهذا يقودنا إلى التعريف التالي:

● تعريف:

إذا كان $\gcd(a, m) = 1$ و g جذر أساسي بالنسبة

TEL:0931497960 - Facebook Group: A to Z مكتبة

للعدد m

نرمز للعدد k حيث $1 \leq k \leq \phi(m)$

الذي يحقق:

$$g^k \equiv a \pmod{m}$$

يسمى دليل العدد a بالنسبة للجذر الأساسي g وبالمقياس m

ونرمز لذلك بالرمز:

$Ind_g(a) = k$ واختصاراً $Ind(a)$

مثال:

ليكن $g=3$ جذر أساسي بالنسبة للمقياس 7 عندئذٍ المطلوب:

أوجد

$Ind_3(6), Ind_3(5), Ind_3(4), Ind_3(3), Ind_3(2), Ind_3(1)$

الحل:

نعلم أن $g^k = 3^k$ حيث

$1 \leq k \leq \phi(7)$

$1 \leq k \leq 6$

$3^1 \equiv 3 \pmod{7} \Rightarrow Ind_3(3) = 1$

$3^2 \equiv 2 \pmod{7} \Rightarrow Ind_3(2) = 2$

$3^3 \equiv 6 \pmod{7} \Rightarrow Ind_3(6) = 3$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$3^4 \equiv 4 \pmod 7 \Rightarrow Ind_3(4) = 4$

$3^5 \equiv 5 \pmod 7 \Rightarrow Ind_3(5) = 5$

$3^6 \equiv 1 \pmod 7 \Rightarrow Ind_3(1) = 6$

* جدول الأدلّة :

علماً أنّ $g=3$ جذر أساسي بالنسبة للقاس 7

$1 \leq k \leq \phi(m)$

3^k	3^1	3^2	3^3	3^4	3^5	3^6
N	3	2	6	4	5	1
Ind_N	1	2	3	4	5	6

مثال : مطلوب

ليكن $m=7$

1) أوجد جذر أساسي بالنسبة للقاس 98

2) أوجد جميع الأعداد الصحيحة الموجبة a الأقل من 98 والتي تحقق الشرط :

$O_{98}(a) = 6$

3) أثبت أن المجموعة

$\{3^1, 3^2, \ldots, 3^6\}$

نظام بواقي مختزل قياس 14

TEL:0931497960 - Facebook Group: A to Z مكتبة

مثال: ليكن $m = 11$

1) أوجد جذر أساسي بالنسبة للمقاس m

2) أوجد جميع الجذور الأساسية الأخرى بالنسبة للمقاس m .

3) أوجد جذر أساسي بالنسبة للمقاس 121

4) أوجد جميع الأعداد الصحيحة الموجبة a الأقل من 11 والتي تحقق الشرط:

$$O_{11}(a) = 5$$

5) أوجد جدول الأدلة بالنسبة للجذر الأساسي $g = 6$

الحل:

1) $a \in Z_p^* = \{1, 2, \ldots, 10\}$

جذر أساسي بالنسبة للمقاس $p = 11$ إذا تحقق الشرط:

$$a^{\frac{p-1}{q}} \not\equiv 1 \pmod{11}$$

وذلك من أجل كل قاسم أولي q للعدد

$$p - 1 = 10$$

$$q = \{2, 5\}$$ نلاحظ أن

★ $a = 1$ ليس جذر أساسي بالنسبة للمقاس 11

★ $a = 2$

$$2^{\frac{10}{q}}, \begin{cases} 2^5 \not\equiv 1 \pmod{11} \\ 2^3 \not\equiv 1 \pmod{11} \end{cases}$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

نلاحظ أن $a=2$ جذر أساسي $\Rightarrow$

مع اختبار لوكاس بالنسبة لـ 11

$g=2$ جذر أساسي بالنسبة لـ 11

(2) نكتب المجموعة التالية:

$$\{2^k ; 1 \leq k \leq \phi(11) \ \& \ \gcd(k, \phi(11)) = 1\}$$

$$= \{2^1, 2^3, 2^7, 2^9\}$$

$$2^1 \equiv 2 \pmod{11}$$
$$2^3 \equiv 8 \pmod{11}$$
$$2^7 \equiv 7 \pmod{11}$$
$$2^9 \equiv 6 \pmod{11}$$

بالتالي الجذور الأساسية بالنسبة للمقاس 11 هي:

$$\{2, 6, 7, 8\}$$

(3) $g=2$ جذر أساسي بالنسبة للمقاس 11

$$121 = 11^2$$

نوجد g^{P-1} نلاحظ:

$$g^{P-1} = 2^{10} \not\equiv 1 \pmod{121}$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$\Leftarrow$ $g=2$ جذر أساسي بالنسبة للقاسم 121

(4) $O_{11}(a) = 5$ & $\gcd(a, 11) = 1$

بما أنّ:

$\Rightarrow$ $g = 2$

جذر أساسي بالنسبة للقاسم 11

عندئذٍ فإن:

$$a \equiv 2^{k} \pmod{11}$$

حيث:

$$1 \leq k \leq \phi(11)$$

$$1 \leq k \leq 10$$

$$O_{11}(a) = O_{11}(2^{k}) = \frac{O_{11}(2)}{\gcd(k, O_{11}, 2)}$$

$$\Rightarrow 5 = \frac{\phi(11)}{\gcd(k, \phi(11))} = \frac{10}{\gcd(k, 10)}$$

$$\Rightarrow \gcd(k, 10) = \frac{10}{5} = 2$$

$$\Rightarrow k \in \{2, 4, 6, 8\}$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$\Rightarrow 2^k \in \{2^2, 2^4, 2^6, 2^8\}$

- نوجد بواقي القسمة:

$2^2 \equiv 4 \pmod{11}$

$2^4 \equiv 5 \pmod{11}$

$2^6 \equiv 9 \pmod{11}$

$2^8 \equiv 3 \pmod{11}$

الأعداد الصحيحة الموجبة المطلوبة هي:

$\{3, 4, 5, 9\}$

(5) $6 = 9$ جذر أحادي بالنسبة للمقاس 11

جدول الأدلة:

6^k	6^1	6^2	6^3	6^4	6^5	6^6	6^7	6^8	6^9	6^{10}
N	6	3	7	9	10	5	8	4	2	1
Ind N	1	2	3	4	5	6	7	8	9	10

انتهت

TEL:0931497960 - Facebook Group: A to Z مكتبة