كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

المادة : نظرية الاعداد

المحاضرة : الحادية عشر /نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

كلية العلوم ، كلية الصيدلة ، الهندسة التقنية

4

2026

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

ملاحظة: تعيين جذر أساسي بالنسبة لمقاس m:

نميز الحالات التالية:

1- $m=p$ عدد أولي فردي: نستخدم اختبار لوكاس في إيجاد جذر أساسي بالنسبة للمقاس p

2- $m=p^k$ حيث p عدد أولي فردي و $k\in\mathbb{Z}^+$ حيث $k\geq 2$ عندئذٍ نقوم بالخطوات التالية:

1- نعيّن جذر أساسي بالنسبة للمقاس p وليكن g

2- نوجد g^{p-1} عندئذٍ:

• إذا كان $g^{p-1}\neq 1 \pmod{p^2}$ عندئذٍ g جذر أساسي بالنسبة للمقاس p^k

• إذا كان $g^{p-1}\equiv 1 \pmod{p^2}$ عندئذٍ يكون $g'=g+p$ جذر أساسي بالنسبة للمقاس p^k

3- $m=2p^k$ حيث $k\in\mathbb{Z}^+$ و p عدد أولي فردي عندئذٍ:

1- نعيّن جذر أساسي بالنسبة للمقاس p^k كما ورد معنا سابقاً وليكن g

2- إذا كان g عدد فردي فإنّ g جذر أساسي بالنسبة للمقاس $m=2p^k$

إذا كان g عدد زوجي فإنّ $g'=g+p^k$ هو جذر أساسي بالنسبة للمقاس $m=2p^k$

تمرين (1): ليكن $m=5$

1- أوجد جذر أساسي بالنسبة للمقاس m ؟

2- أوجد جذر أساسي بالنسبة للمقاس m^2 ثمّ استنتج جذر أساسي بالنسبة للمقاس $2m^2$ ؟

3- أوجد عدد الجذور الأساسية بالنسبة للمقاس $m^2=25$ ؟

4- أوجد جميع الجذور الأساسية بالنسبة للمقاس 5 ؟

الحل:

① $m=5$ عدد أولي فردي ، نطبق اختبار لوكاس:

$a \in \mathbb{Z}_5^* = \{1,2,3,4\}$ جذر أساسي بالنسبة للمقاس 5 إذا كان:

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

لكل قاسم أولي q لـ $5-1=4$

من أجل $q=2$ و $a=1$ لدينا $(1)^{\frac{4}{2}} \equiv 1 \pmod 5$

بالتالي $a=1$ ليس جذر أساسي بالنسبة للمقاس m

لدينا $a=2$ $(2)^{\frac{4}{2}} \not\equiv 1 \pmod 5$

نستنتج أنّ $a=2$ جذر أساسي بالنسبة للمقاس $m=5$ عندئذٍ نضع $g=2$.

② $m^2=5^2$ عدد أولي فردي مرفوع للقوة 2

لدينا من الطلب السابق $g=2$ جذر أساسي بالنسبة للمقاس 5

$$g^{p-1}=2^4=16 \not\equiv 1 \pmod{25}$$

بالتالي $g=2$ جذر أساسي بالنسبة للمقاس $m^2=25$.

لدينا $g=2$ جذر أساسي بالنسبة للمقاس $m^2=25$ ونلاحظ أنّ $g=2$ عدد زوجي عندئذٍ: $g'=g+5^2=27$ جذر أساسي بالنسبة للمقاس $2m^2$.

TEL:0931497960 - Facebook Group: A to Z مكتبة

③ عدد الجذور هو: $\phi(\phi(m^2)) = \phi(\phi(25)) = \phi(20) = 8$

بالتالي لدينا 8 جذور أساسية بالنسبة للمقاس $m^2 = 25$.

④ عدد الجذور الأساسية بالنسبة للمقاس 5 هو:

$\phi(\phi(5)) = \phi(4) = 2$

• نشكل المجموعة التالية علماً أنّ $g = 2$ جذر أساسي بالنسبة للمقاس $m = 5$:

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

$= \{2^k, 1 \le k \le 4 \ \& \ \gcd(k, 4) = 1\}$

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

• نوجد بواقي قسمة عناصر المجموعة السابقة على العدد $m = 5$

$2 \equiv 2 \pmod 5$ ، $2^3 \equiv 3 \pmod 5$

بالتالي الجذور هي $\{2, 3\}$.

تمرين (2): ليكن $p = 7$.

1- أوجد جذر أساسي بالنسبة للمقاس p ؟

2- أوجد جذر أساسي بالنسبة للمقاس 49 ثمّ استنتج جذر أساسي بالنسبة للمقاس 98 ؟

3- أوجد الجذور الأساسية بالنسبة للمقاس p ؟

4- ما هو عدد الجذور الأساسية بالنسبة للمقاس 98 ؟

5- عيّن الأعداد الصحيحة الموجبة تماماً والأقل من 98 والتي تحقّق الشرط $O_{98}(a) = 6$ ؟

6- أوجد $O(2^6)$ ؟

7- أثبت أنّ $\{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\}^{49}$ نظام بواقي مختزل بالنسبة للمقاس 14 ؟

TEL:0931497960 - Facebook Group: A to Z مكتبة

الحل: ① $p=7$ عدد أولي فردي حسب اختبار لوكاس:

$a \in \mathbb{Z}_7^* = \{1,2,3,4,5,6\}$ حيث a جذر أساسي بالنسبة للمقاس $p=7$ إذا كان:

$a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$ لكل قاسم أولي q لـ $(p-1)$

$\Rightarrow a^{\frac{6}{q}}$; $q \in \{2, 3\}$

- $a=1$ نلاحظ أنّ

$1^{\frac{6}{q}} \equiv 1 \pmod 7$ من أجل $q=2$ أو $q=3$

بالتالي $a=1$ ليس جذر أساسي بالنسبة للمقاس 7

- $a=2$ نلاحظ أنّ

$$2^{\frac{6}{q}} = \begin{cases} 2^{\frac{6}{2}} = 2^3 \equiv 1 \pmod 7 \\ 2^{\frac{6}{3}} = 2^2 \not\equiv 1 \pmod 7 \end{cases}$$

بالتالي $a=2$ ليس جذر أساسي بالنسبة للمقاس 7

- $a=3$ نلاحظ أنّ

$$3^{\frac{6}{q}} = \begin{cases} 3^{\frac{6}{2}} = 3^3 \not\equiv 1 \pmod 7 \\ 3^{\frac{6}{3}} = 3^2 \not\equiv 1 \pmod 7 \end{cases}$$

نستنتج أنّ العدد 3 جذر أساسي بالنسبة للمقاس 7

② نلاحظ أنّ $p^2 = 49$ حيث $p=7$ ولدينا من الطلب السابق $g=3$ جذر أساسي بالنسبة للمقاس 7

$g^{p-1} = 3^6 \not\equiv 1 \pmod{49}$

بالتالي $g=3$ جذر أساسي بالنسبة للمقاس $p^2=49$

و $g=3$ عدد فردي عندئذٍ $g=3$ جذر أساسي بالنسبة للمقاس 98.

③ لدينا $g=3$ جذر أساسي بالنسبة للمقاس 7، نشكل

TEL:0931497960 - Facebook Group: A to Z مكتبة

المجموعة التالية:

$\{3^k ;\ 1 \le k \le \phi(7) \ \& \ \gcd(k, \phi(7)) = 1\}$

$= \{3^1, 3^5\}$; $3^1 \equiv 3 \pmod 7$

$3^5 \equiv 5 \pmod 7$

الجذور هي: $\{3, 5\}$.

④ عدد الجذور الأساسية بالنسبة للمقاس 98 هو:

$$\phi(\phi(98)) = \phi(\phi(2 \times 7^2)) = \phi(\phi(2) \times \phi(7^2)) =$$

$$\phi(1 \times 42) = \phi(42) = \phi(6) \times \phi(7) = 12$$

أي لدينا 12 جذر أساسي بالنسبة للمقاس 98.

⑤ $O_{98}(a) = 6$

لدينا $g = 3$ جذر أساسي بالنسبة للمقاس 98

أياً كان $a \in \mathbb{Z}$ و $\gcd(a, 98) = 1$ عندئذٍ:

$a \equiv 3^k \pmod{98}$

$$O_{98}(a) = O_{98}(3^k)$$

$$6 = \frac{O_{98}(3)}{\gcd(k, O_{98}(3))} = \frac{\phi(98)}{\gcd(k, \phi(98))} \Rightarrow$$

$$6 = \frac{42}{\gcd(k, 42)} \Rightarrow \gcd(k, 42) = 7 \ \& \ 1 \le k \le \phi(98)$$

$k = \{7, 35\} \Leftarrow 1 \le k \le 42$

$3^7 \equiv 31 \pmod{98}$

$3^{35} \equiv 19 \pmod{98}$

بالتالي الأعداد المطلوبة هي $\{19, 31\}$

⑥ إيجاد

$$O_{49}(2^6) = \frac{O_{49}(2)}{\gcd(6, O_{49}(2))}$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

• لنوجد رتبة العدد 2 بالنسبة للمقاس 49 $O_{49}(2) = K$

$\phi(49) = 42$; $K \mid 42$; $K \in \{1, 2, 3, 6, 7, 14, 21, 42\}$

$2^1 \not\equiv 1 \pmod{49}$ $2^2 \not\equiv 1 \pmod{49}$

$2^3 \not\equiv 1 \pmod{49}$ $2^7 \not\equiv 1 \pmod{49}$

$2^6 \not\equiv 1 \pmod{49}$ $2^{14} \not\equiv 1 \pmod{49}$

$2^{21} \equiv 1 \pmod{49} \Rightarrow O_{49}(2) = 21$

$\Rightarrow O_{49}(2^6) = \frac{21}{\gcd(6,21)} = \frac{21}{3} \Rightarrow O_{49}(2^6) = 7$

(7) $14 = 2 \times 7$

$g = 3$ جذر أساسي بالنسبة للمقاس 7

و $g = 3$ عدد فردي $\Leftarrow$ $g = 3$ جذر أساسي بالنسبة للمقاس 14

عندئذٍ المجموعة التالية:

$\{g^1, g^2, \ldots, g^{\phi(14)}\} = \{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\}$

نظام بواقي مختزل مقياس 14

انتهت المحاضرة

TEL:0931497960 - Facebook Group: A to Z مكتبة

مكتبة A to Z