كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : العاشرة /نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

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

ملاحظة: إذا كان g جذر أساسي بالنسبة للمقياس m فكيف نوجد الجذور الأخرى بالنسبة للمقياس الأخرى.

1- نشكل المجموعة التالية $\{g^n ; 1 \le n \le \phi(m) \ \& \ \gcd(n, \phi(m)) = 1\}$

2- نوجد بواقي قسمة عناصر المجموعة السابقة على العدد m عندئذٍ البواقي الناتجة هي الجذور الأساسية المطلوبة.

• مبرهنة غاوص (1801)

إذا كان m عدداً صحيحاً موجباً فإنّ m يملك جذور أساسية إذا وفقط إذا كان: $m \in \{2, 4, p^k, 2p^k\}$ حيث:

$1 \le k \in \mathbb{Z}^+$ و p عدد أولي فردي.

مثال: العدد $m = 8$ لا يملك جذور أساسية

$m = 21$ لا يملك جذور اساسية

$m = 125 = 5^3$ يملك جذور أساسية

مثال: ليكن $m = 7$ والمطلوب:

1- هل $g = 3$ جذر أساسي بالنسبة للمقياس 7 ؟

2- ما عدد الجذور الأساسية بالنسبة للمقياس 7 ثمّ حدّد هذه الجذور؟

3- هل المجموعة $\{5^1, 5^2, 5^3, 5^4, 5^5, 5^6\}$ نظام بواقي مختزل قياس العدد 7 ؟

الحل:

مكتبة A to Z - كلية العلوم (جامعة طرطوس) - TEL:0931497960

① نوجد $O_7(3)$: نضع $O_7(3)=k$ حيث $k \mid o(7) \Leftarrow$

$k \mid 6 \Rightarrow k = \{1, 2, 3, 6\}$

$3^1 \not\equiv 1 \pmod 7 \qquad 3^2 \not\equiv 1 \pmod 7$

$3^6 \not\equiv 1 \pmod 7 \qquad 3^3 \not\equiv 1 \pmod 7$

$\Rightarrow O_7(3) = 6 = \phi(7)$

نستنتج أن العدد 3 هو جذر أساسي بالنسبة للمقاس 7.

② عدد الجذور هو:

$\phi(\phi(m)) = \phi(\phi(7)) = \phi(6) = \phi(2).\phi(3) = 2$

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

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

$= \{3^k ; 1 \le k \le 6 \ \& \ \gcd(k, 6) = 1\} = \{3^1, 3^5\}$

نوجد باقي قسمة عناصر الجموعة $\{3, 3^5\}$ على العدد $m=7$:

$3 \equiv 3 \pmod 7$

$3^5 \equiv 5 \pmod 7$

عندئذٍ الجذور الأساسية هي $\{3, 5\}$.

③ لدينا $g=5$ جذر أساسي بالنسبة للمقاس $m=7$ عندئذٍ الجموعة:

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

نظام بواقي مختزل قياس $m=7$.

مبرهنة اختبار لوكاس:

ليكن $m=p$ عدداً أولياً فردياً عندئذٍ $a \in \mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$

جذر أساسي بالنسبة للمقاس m إذا كان:

TEL:0931497960 - Facebook Group: A to Z مكتبة

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

مثال: ليكن $m=13$.

1- أوجد جذر أساسي بالنسبة للمقاس 13 ؟

2- أوجد عدد الجذور الأساسية بالنسبة للمقاس 13 ؟

3- أوجد جميع الجذور الأساسية بالنسبة للمقاس 13 ؟

4- هل المجموعة $\{11^1, 11^2, \ldots, 11^n\}$ نظام بواقي مختزل قياس 13 ؟

5- أوجد رتبة $(11)^7$ بالنسبة للمقاس 13 ؟

6- عيّن الأعداد الصحيحة الموجبة الأقل من 13 والتي تحقق الشرط $O_{13}(a)=3$ ؟

الحل: ① - اختبار لوكاس:

$a \in \mathbb{Z}_{13}^* = \{1, 2, 3, \ldots, 12\}$ جذر أساسي بالنسبة للمقاس 13 إذا تحقق الشرط:

$a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$; $p=13$ حيث $q \in \{2,3\}$

من أجل $a=1$ نجد:

$(1)^{\frac{12}{q}} \equiv 1 \pmod{13}$; $\forall q \in \{2,3\}$

نجد أنّ $a=1$ ليس جذر أساسي بالنسبة للمقاس 13 .

من أجل $a=2$ نجد:

$$2^{\frac{p-1}{q}} = 2^{\frac{12}{q}} = \begin{cases} 2^{\frac{12}{2}} = 2^6 \not\equiv 1 \pmod{13} \\ 2^{\frac{12}{3}} = 2^4 \not\equiv 1 \pmod{13} \end{cases}$$

نستنتج أنّ العدد $a=2$ جذر أساسي بالنسبة للمقاس 13

② - عدد الجذور الأساسية بالنسبة للمقاس 13 هو:

$$\phi(\phi(13)) = \phi(12) = \phi(3 \times 4) = \phi(3) \times \phi(4)$$

$= \phi(3) \times \phi(2^2) = 4$

③ لدينا $g=2$ جذر أساسي بالنسبة للمقاس $m=13$ عندئذٍ نشكل المجموعة التالية:

$\{2^k ; \ 1 \le k \le \phi(3) \ \& \ gcd(k, \phi(13)) = 1\}$

$= \{2^k ; \ 1 \le k \le 12 \ \& \ gcd(k, 12) = 1\}$

$= \{2^1, 2^5, 2^7, 2^{11}\}$

$2^1 \equiv 2 \pmod{13}$, $2^5 \equiv 6 \pmod{13}$

$2^7 \equiv 11 \pmod{13}$, $2^{11} \equiv 7 \pmod{13}$

نستنتج أن الجذور هي: $\{2, 6, 7, 11\}$

④ لدينا $g=11$ جذر أساسي بالنسبة للمقاس 13 حسب الطلب السابق عندئذٍ:

$\{g^1, g^2, \dots, g^{\phi(13)}\} = \{11^1, 11^2, \dots, 11^{12}\}$

نظام بواقي مختزل قياس 13

⑤ $O_{13}(11^7) = \dfrac{O_{13}(11)}{gcd(7, O_{13}(11))} = \dfrac{12}{gcd(7,12)} = 12$

⑥ لدينا $\{2^1, 2^2, \dots, 2^{12}\}$ نظام بواقي مختزل قياس $m=13$

عندئذٍ أياً كان $r \in \mathbb{Z}_m^*$ بالتالي $r \equiv 2^k \pmod{m}$

$\Rightarrow a \equiv 2^k \pmod{m} \Rightarrow O_{13}(a) = O_{13}(2^k)$

$3 = \dfrac{O_{13}(2)}{gcd(k, O_{13}(2))} = \dfrac{12}{gcd(k,12)}$; $gcd(k,12) = 4$

حيث $k \in \{4, 8\}$

$\Rightarrow 2^k \in \{2^4, 2^8\}$; $2^4 \equiv 3 \pmod{13}$

بالتالي الأعداد الصحيحة المطلوبة $2^8 \equiv 9 \pmod{13}$

هي $\{3, 9\}$

انتهت المحاضرة

TEL:0931497960 - Facebook Group: A to Z مكتبة

مكتبة A to Z