كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

المادة : نظرية الاعداد

المحاضرة : **الحادية 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

مبرهنة: إذا كانت $O_m(a)=k$ عندئذٍ إذا كان i, j عددين صحيحين موجبين فإنّ:

$$i \equiv j \pmod{k} \iff a^i \equiv a^j \pmod{m}$$

ملاحظة: إذا كانت $O_m(a)=k$ عندئذٍ العناصر التالية

$$a^1, a^2, a^3, \dots, a^k$$

غير متطابقة مثنى مثنى بالنسبة للمقاس m

* مفهوم الجذور الأساسية بالنسبة لمقاس m:

- تعريف: ليكن g, m عددين صحيحين موجبين حيث

$$gcd(g,m)=1$$

يُقال بأنّ g جذر أساسي بالنسبة لـ m إذا كان

$$O_m(g)=\phi(m)$$

مثال: أوجد $O_5(2)$ وهل 2 جذر أساسي بالنسبة للمقاس 5.

الحل:

$$k \mid \phi(5) \quad \& \quad O_5(2)=k$$

$$k \in \{1,2,4\}$$

$2^1 \not\equiv 1 \pmod 5$

$2^2 \not\equiv 1 \pmod 5$

$2^4 \equiv 1 \pmod 5$

$\Rightarrow \mathcal{O}_5(2) = 4 = \phi(5)$

$\Leftarrow$ 2 جذر أساسي بالنسبة للمقاس $m=5$

مثال: $\mathcal{O}_7(2) = 3 \neq \phi(7)$

$\Leftarrow$ 2 ليس جذر أساسي بالنسبة للمقاس $m=7$

ملاحظة: أي جذر أساسي (g) بالنسبة للمقاس m

- حقق أن: $g \in \mathbb{Z}_m^*$

ملاحظة: إذا كان g جذر أساسي بالنسبة للمقاس m

عندئذٍ:

$A = \{g^1, g^2, \dots, g^{\phi(m)}\}$

نظام بواقي مختزل متبع m.

البرهان: * g جذر أساسي بالنسبة للمقاس m

عندئذٍ: $\mathcal{O}_m(g) = \phi(m)$

$gcd(g, m) = 1$

$\forall x \in A : gcd(x, m) = 1$

TEL:0931497960 - Facebook Group: A to Z مكتبة

* سنبرهن الآن:

$$g^i \not\equiv g^j \pmod m$$

حيث $1 \le i, j \le \phi(m)$ و $i \ne j$

- نفرض: $g^i \equiv g^j \pmod m$

عندئذٍ: $i \equiv j \pmod k$

حيث $k = o_m(g) = \phi(m)$

$\Rightarrow \phi(m) \mid (i-j)$

وهذا مرفوض، لأنّ: $0 < i-j < \phi(m)$ ☺

* $|A| = \phi(m)$

فنتيجة ما سبق بأنّ A نظام بواقيا مختزل مقاييس m

مبرهنة: إذا كان g جذر أساسي بالنسبة للمقياس m

عندئذٍ g^n جذر أساسي بالنسبة للمقاس m

إذا وفقط إذا كان

$$\gcd(n, \phi(m)) = 1$$

حيث n عدد صحيح موجب.

TEL:0931497960 - Facebook Group: A to Z مكتبة

ملاحظة: إذا كان هناك جذور أساسي بالنسبة للمقاس m
فإنه يوجد بالضبط $\phi(\phi(m))$
جذر أساسي بالنسبة للمقاس m.

* قسم عاوص مبرهنة بيّن من خلالها الأعداد الصحيحة الموجبة m التي تملك جذور أساسية.

مبرهنة عاوص (1801):
إذا كان m عدداً صحيحاً موجباً فإنّ m تملك جذور أساسية إذا وفقط إذا كان:

$$m \in \{2, 4, p^k, 2p^k\}$$

حيث p عدد أولي فردي و $k \geq 1$

مثال: * العدد $m=8$ لا يملك جذور أساسية وذلك حسب مبرهنة عاوص.

* $m=35=5\times7$ لا يملك جذور أساسية وذلك حسب مبرهنة عاوص.

* $m=50$ يملك جذور أساسية.

TEL:0931497960 - Facebook Group: A to Z مكتبة

سؤال: إذا كان g جذر أساسي بالنسبة للمقاس m عندئذٍ لمعرفة جميع الجذور الأساسية الأخرى بالنسبة للمقاس m نقوم بما يلي:

1- نشكّل المجموعة: $\{ g^k ; 1 \le k \le \phi(m) \text{ و } \gcd(k, \phi(m)) = 1 \}$

2- نعيد بوامي صفة عناصر المجموعة السابقة على العدد m فنحصل على جميع الجذور الأساسية بالنسبة للمقاس m

مثال: ليكن $m = 7$

1) هل $g = 3$ جذر أساسي بالنسبة للمقاس 7 أم لا؟ وفي حال كان $g = 3$ جذر أساسي بالنسبة للمقاس m فأوجد جميع الجذور الأخرى.

2) ما المجموعة $\{ 5^1, 5^2, 5^3, 5^4, 5^5, 5^6 \}$ تطابق بوامي مختلفة أم لا بالنسبة للمقاس m.

الحل: 1- حتى يكون العدد $g = 3$ جذر أساسي بالنسبة للمقاس $m = 7$ يجب أن يكون $o_7(3) = \phi(7)$

نوجد $o_7(3)$.

نلاحظ: $o_7(3) \in \{1, 2, 3, 6\}$

TEL:0931497960 - Facebook Group: A to Z مكتبة

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

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

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

$3^6 \equiv 1 \pmod 7$

نلاحظ $\phi_7(3) = 6 = \phi(7)$

نستنتج بأنّ $g=3$ جذر أساسي

بالنسبة للمقاس $m=7$

* عدد الجذور الأساسية بالنسبة للمقاس $m=7$ هو:

$\phi(\phi(m)) = \phi(\phi(7))$

$\phi(6) = 2$

* لنوجد جميع الجذور الأساسية بالنسبة للمقاس $m=7$:

نشكل المجموعة:

$\{ 3^k \quad ; \quad 1 \le k \le \phi(m) \quad \&$

$\gcd(k, \phi(m)) = 1 \}$

$= \{ 3^k \quad ; \quad 1 \le k \le 6 \quad \&$

$\gcd(k, 6) = 1 \}$

$= \{ 3^1, 3^5 \}$

لنوجد بواقي قسمة عناصر المجموعة السابقة على العدد m

$3^1 \equiv 3 \pmod 7$

$3^5 \equiv 5 \pmod 7$

TEL:0931497960 - Facebook Group: A to Z مكتبة

بالتالي الجذور الأساسية بالنسبة للمقاس $m=7$ هي

$\{3, 7\}$

2- نلاحظ بأنّ $g=5$ جذر أساسي بالنسبة للمقاس $m=7$ بالتالي المجموعة

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

$= \{5, 5^2, 5^3, 5^4, 5^5, 5^6\}$

نظام بواقي مختزل مقاس $m=7$

* اختبار ليوكاس: في حال كان $m=p$ حيث p عدد أولي فردي عندئذٍ:

$a \in Z_m^*$ جذر أساسي بالنسبة للمقاس m إذا كان:

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

من أجل كل قاسم أولي q للعدد $m-1$.

مثال: ليكن $m=13$

① عيّن جذر أساسي بالنسبة للمقاس m.

② أوجد عدد الجذور الأساسية بالنسبة للمقاس m.

③ أوجد جميع الجذور الأساسية بالنسبة للمقاس m.

④ هل المجموعة $\{6^1, 6^2, 6^3, \dots, 6^{12}\}$ نظام بواقي مختزل بالنسبة للمقاس m أم لا؟ ولماذا؟

TEL:0931497960 - Facebook Group: A to Z مكتبة

⑤ عيّن جميع الأعداد الصحيحة الموجبة a الأقل من m والتي تحقق الشرط:

$$o_{13}(a) = 3$$

الحل: $m = 13$ عدد أولي فردي نطبق اختبار لوكاس

$$a \in Z_{13}^{*} = \{1, 2, \dots, 12\}$$

جذر أساسي بالنسبة للمقاس $m = 13$ إذا كان:

$$a^{\frac{p-1}{q}} \not\equiv 1 \pmod{13}$$

من أجل كلّ قاسم أولي q للعدد $p - 1 = 12$

$\Leftarrow$ نلاحظ أنّ:

$$q = 2 \quad \text{or} \quad 3$$

* عندما $a = 1$ نلاحظ أنّ

$$1^{\frac{12}{q}} \equiv 1 \pmod{13}$$

حيث $q = 2$ or 3

ومنه $a = 1$ ليس جذر أساسي بالنسبة للمقاس 13

* عندما $a = 2$ نلاحظ أنّ

$$2^{\frac{12}{q}} \quad ; \quad q = 2 \text{ or } 3$$

$$2^{\frac{12}{2}} = 2^{6} \not\equiv 1 \pmod{13}$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$2^{\frac{12}{3}} = 2^4 \not\equiv 1 \pmod{13}$

وهذا يعني أن $g=2$ ليس جذر أساسي بالنسبة للمقاس 13.

2- عدد الجذور الأساسية بالنسبة للمقاس 13 هو:

$$\phi(\phi(13)) = \phi(12)$$
$$= \phi(3\times 4) = \phi(3)\times\phi(4)$$
$$= 2\times 2 = 4$$

3- لدينا $g=2$ جذر أساسي بالنسبة للمقاس 13 بالتالي نشكل المجموعة:

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

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

$$2^1 \equiv 2 \pmod{13}$$
$$2^5 \equiv 6 \pmod{13}$$
$$2^7 \equiv 11 \pmod{13}$$
$$2^{11} \equiv 7 \pmod{13}$$

بالتالي الجذور الأساسية بالنسبة للمقاس 13 هي:

$$\{ 2, 6, 7, 11 \}$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

4- نلاحظ بأن العدد 6 جذر آحادي بالنسبة للمعامل 13
بالتالي:
$\{6^1, \dots, 6^{12}\}$
نظام بواقي مختزل بالنسبة للمعامل 13.

5- $\phi_{13}(a) = 3$
* لدينا $\forall a \in \mathbb{Z}$ $\gcd(a, m) = 1$
$a \equiv r \pmod m \; ; \; r \in \mathbb{Z}_m^*$

بالتالي:
$\gcd(r, m) = 1$

* لدينا $\{2^1, 2^2, \dots, 2^{12}\}$
نظام بواقي مختزل مقياس $m = 13$
بالتالي:
$r \equiv 2^k \pmod m$
$a \equiv 2^k \pmod m \Leftarrow$
$\phi_{13}(a) = \phi_{13}(2^k)$

$$3 = \frac{\phi_{13}(2)}{\gcd(k, \phi_{13}(2))}$$

$$3 = \frac{\phi(13)}{\gcd(k, \phi(13))}$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$\Rightarrow 3 = \frac{12}{\gcd(k,12)}$

$\Rightarrow \gcd(k,12) = 4$

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

$2^4 \equiv 3 \pmod{13}$

$2^8 \equiv 9 \pmod{13}$

الأعداد الصحيحة الموجبة الأقل من 13 والتي تحقق الشرط $O_{13}(9) = 3$ هي $\{3, 9\}$

انتهت المحاضرة.

TEL:0931497960 - Facebook Group: A to Z مكتبة