كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

المادة : نظرية الاعداد

المحاضرة : الثامنة /عملي/

{{ A to Z مكتبة }}

Facebook Group : A to Zمكتبة

8

المحاضرة الثامنة
(عملي)

السؤال الأول: ليكن $m = 5$

1. هل العدد 2 جذر أساسي بالنسبة للمقاس 5 أم لا ولماذا؟
2. ما هو عدد الجذور الأساسية بالنسبة للمقاس 5.
3. ماهي الجذور الأساسية بالنسبة للمقاس 5.
4. هل المجموعة $\{3^1, 3^2, 3^3, 3^4\}$ نظام بواقي مختزل بالقياس للعدد m أم لا ولماذا؟
5. أوجد $O_5(2^6)$

الحلّ:

1. لنحسب $O_5(2)$

لنضع $O_5(2) = k$ عندئذ $k \mid \phi(5)$

بالتالي k أحد القواسم الموجبة للعدد $\phi(5) = 4$.

$$(2)^1 \not\equiv 1(mod\ 5)$$

$$(2)^2 \not\equiv 1(mod\ 5)$$

$$(2)^4 \equiv 1(mod\ 5)$$

نلاحظ بأنّ $O_5(2) = 4 = \phi(5)$

بالتالي العدد 2 جذر أساسي بالنسبة للمقاس 5.

2. عدد الجذور الأساسية بالنسبة للمقاس 5 هو $\phi\big(\phi(5)\big)$ أي

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

3. نشكّل المجموعة التالية علماً أنّ 2 جذر أساسي بالنسبة للمقاس 5:

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

$$\{(2)^k; 1 \le k \le 4\ \&\ \gcd(k, 4) = 1)\} = \{(2)^1, (2)^3\}$$

نوجد بواقي قسمة عناصر المجموعة $\{(2)^1, (2)^3\}$ على العدد 5 فنجد:

$$(2)^1 \equiv 2(mod\ 5)$$

$$(2)^3 \equiv 3(mod\ 5)$$

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

4. المجموعة $\{3^1, 3^2, 3^3, 3^4\}$ نظام بواقي مختزل بالقياس للعدد 5 لأنه:

لدينا 3 جذر أساسي بالنسبة للمقاس 5 عندئذ المجموعة

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

نظام بواقي مختزل بالقياس للعدد 5

.5 $O_5(2^6) = \frac{O_5(2)}{\gcd(6,O_5(2))} = \frac{\phi(5)}{\gcd(6,\phi(5))} = \frac{4}{\gcd(6,\phi(5))} = 2$

السؤال الثاني: أوجد جذر أساسي بالنسبة للمقاس $p = 23$ حسب اختبار لوكاس، ثم أوجد جميع الجذور الأساسية الآخرى بالنسبة للمقاس 23.

الحلّ: إيجاد جذر أساسي بالنسبة للمقاس $p = 23$ (اختبار لوكاس)

$a \in \mathbb{Z}_{23}^* = \{1,2,3,4,5,6,7,\dots,22\}$ جذر أساسي بالنسبة للمقاس $p = 23$ إذا تحقق الشرط التالي:

$$a^{\frac{p-1}{q}} \not\equiv 1(mod\ p)$$

وذلك من أجل كل قاسم أولي q للعدد $p - 1 = 22$.

نلاحظ بأنّ $q = 2$ أو 11

- الشرط لا يتحقق من أجل $a = 1$، بالتالي $a = 1$ ليس جذر أساسي بالنسبة للمقاس 23.
- من أجل $a = 2$ نلاحظ بأنّ

$$2^{\frac{22}{q}}: \begin{cases} 2^{\frac{22}{2}} = 2^{11} \equiv 1(mod\ 23) \\ 2^{\frac{22}{11}} = 2^2 \not\equiv 1(mod\ 23) \end{cases}$$

بالتالي $a = 2$ ليس جذر أساسي بالنسبة للمقاس 23.

- من أجل $a = 3$ نلاحظ بأنّ

$$3^{\frac{22}{q}}: \begin{cases} 3^{\frac{22}{2}} = 3^{11} \equiv 1(mod\ 23) \\ 3^{\frac{22}{11}} = 3^2 \not\equiv 1(mod\ 23) \end{cases}$$

بالتالي $a = 3$ ليس جذر أساسي بالنسبة للمقاس 23.

- من أجل $a = 4$ نلاحظ بأنّ:

$$4^{\frac{22}{q}}: \begin{cases} 4^{\frac{22}{2}} = 4^{11} \equiv 1(mod\ 23) \\ 4^{\frac{22}{11}} = 4^2 \not\equiv 1(mod\ 23) \end{cases}$$

بالتالي $a = 4$ ليس جذر أساسي بالنسبة للمقاس 23.

- من أجل $a = 5$ نلاحظ بأنّ

$$5^{\frac{22}{q}}: \begin{cases} 5^{\frac{22}{2}} = 5^{11} \not\equiv 1(mod\ 23) \\ 5^{\frac{22}{11}} = 5^2 \not\equiv 1(mod\ 23) \end{cases}$$

بالتالي $a = 5$ جذر أساسي بالنسبة للمقاس 23 .

إيجاد الجذور الأساسية بالنسبة للمقاس 23

لدينا $a = 5$ جذر أساسي بالنسبة للمقاس 23 .

نشكّل المجموعة التالية علماً أنّ 5 جذر أساسي بالنسبة للمقاس 23:

$$\{(5)^k; 1 \le k \le \phi(23)\ \&\ \gcd\big(k,\phi(23)\big) = 1\}$$

$$\{(5)^k; 1 \leq k \leq 22 \,\&\, \gcd(k,22)=1\}$$
$$= \{(5)^1,(5)^3,(5)^5,(5)^7,(5)^9,(5)^{13},(5)^{15},(5)^{17},(5)^{19},(5)^{21}\}$$

نوجد بواقي قسمة عناصر المجموعة السابقة على العدد 23 فنجد:

$$(5)^1 \equiv 5(mod\ 23)$$
$$(5)^3 \equiv 10(mod\ 23)$$
$$(5)^5 \equiv 20(mod\ 23)$$
$$(5)^7 \equiv 17(mod\ 23)$$
$$(5)^9 \equiv 11(mod\ 23)$$
$$(5)^{13} \equiv 21(mod\ 23)$$
$$(5)^{15} \equiv 19(mod\ 23)$$
$$(5)^{17} \equiv 15(mod\ 23)$$
$$(5)^{19} \equiv 7(mod\ 23)$$
$$(5)^{21} \equiv 14(mod\ 23)$$

بالتالي الجذور الأساسية بالنسبة للمقاس 23 هي $\{5,7,10,11,14,15,17,19,20,21\}$

السؤال الثالث: ليكن $m = 19$

1. أوجد جذر أساسي بالنسبة للمقاس 19.
2. ما هو عدد الجذور الأساسية بالنسبة للمقاس 19.
3. ماهي الجذور الأساسية بالنسبة للمقاس 19.
4. هل المجموعة $\{15^1, 15^2, 15^3, \dots, 15^{18}\}$ نظام بواقي مختزل بالقياس للعدد m أم لا، ولماذا
5. أوجد جميع الأعداد الصحيحة الموجبة a الأقل من 19 والتي تحقق الشرط التالي: $O_{19}(a) = 6$

الحلّ:

1. إيجاد جذر أساسي بالنسبة للمقاس $p = 19$ (اختبار لوكاس)

$a \in \mathbb{Z}_{19}^* = \{1,2,3,4,5,6,7,\dots,18\}$ جذر أساسي بالنسبة للمقاس $p = 19$ إذا تحقق الشرط التالي:

$$a^{\frac{p-1}{q}} \not\equiv 1(mod\ p)$$

وذلك من أجل كل قاسم أولي q للعدد $p - 1 = 18$.

نلاحظ بأنّ $q = 2$ أو 3

- الشرط لا يتحقق من أجل $a = 1$. بالتالي $a = 1$ ليس جذر أساسي بالنسبة للمقاس 19.
- من أجل $a = 2$ نلاحظ بأنّ

$$2^{\frac{18}{q}}:\quad \begin{cases} 2^{\frac{18}{2}} = 2^9 \not\equiv 1(mod\ 19) \\ 2^{\frac{18}{3}} = 2^6 \not\equiv 1(mod\ 19) \end{cases}$$

بالتالي $a = 2$ جذر أساسي بالنسبة للمقاس 19.

2. عدد الجذور الأساسية بالنسبة للمقاس 19 هو $\phi\big(\phi(19)\big)$ أي:

$$\phi\big(\phi(19)\big) = \phi(18) = 6$$

3. لدينا $a = 2$ جذر أساسي بالنسبة للمقاس 19 .

نشكّل المجموعة التالية علماً أنّ 2 جذر أساسي بالنسبة للمقاس 19:

$$\{(2)^k; 1 \le k \le \phi(19)\ \&\ \gcd\big(k, \phi(19)\big) = 1\}$$

$$\{(2)^k; 1 \le k \le 18\ \&\ \gcd(k, 18) = 1)\} = \{(2)^1, (2)^5, (2)^7, (2)^{11}, (2)^{13}, (2)^{17}\}$$

نوجد بواقي قسمة عناصر المجموعة السابقة على العدد 19 فنجد:

$$(2)^1 \equiv 2(mod\ 19)$$
$$(2)^5 \equiv 13(mod\ 19)$$
$$(2)^7 \equiv 14(mod\ 19)$$
$$(2)^{11} \equiv 15(mod\ 19)$$
$$(2)^{13} \equiv 3(mod\ 19)$$
$$(2)^{17} \equiv 10(mod\ 19)$$

بالتالي الجذور الأساسية بالنسبة للمقاس 19 هي $\{2, 3,10,13,14,15\}$

4. المجموعة $\{15^1, 15^2, 15^3, \dots, 15^{18}\}$ نظام بواقي مختزل بالقياس للعدد 19 لأنه:

لدينا 15 جذر أساسي بالنسبة للمقاس19 عندئذ المجموعة

$$\{15^1, 15^2, 15^3, \dots, 15^{\phi(19)}\} = \{15^1, 15^2, 15^3, \dots, 15^{18}\}$$

نظام بواقي مختزل بالقياس للعدد 19.

5. لدينا 2 جذر أساسي بالنسبة للمقاس 19 عندئذ أياً كان $a \in \mathbb{Z}$ بحيث $\gcd(a, 19) = 1$ فإنّ $a \equiv 2^k(mod\ 19)$ حيث $1 \le k \le \phi(19)$ بالتالي

$$O_{19}(a) = O_{19}(2^k)$$

$$6 = \frac{O_{19}(2)}{\gcd\big(k, O_{19}(2)\big)} = \frac{\phi(19)}{\gcd\big(k, \phi(19)\big)} = \frac{18}{\gcd(k, 18)}$$

بالتالي $\gcd(k, 18) = 3$ عندئذٍ $k \in \{3,15\}$

بالتالي:$2^k \in \{(2)^3, (2)^{15}\}$

وبما أنّ $(2)^3 \equiv 8(mod\ 19)$ و $(2)^{15} \equiv 12(mod\ 19)$

عندئذٍ الأعداد الصحيحة الموجبة a الأقل من 19 التي تحقق العلاقة $O_{19}(a) = 6$ هي:$\{8, 12\}$.
