كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : التاسعة /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

تمرين (1): إذا كان $gcd(n,m)=1$ أثبت أنّ

$$n^{\phi(m)} + m^{\phi(n)} \equiv 1 \pmod{nm}$$

الإثبات:

$$gcd(n,m)=1 \xrightarrow{\text{أويلر}} n^{\phi(m)} \equiv 1 \pmod{m} \quad \text{...①}$$

$$\Rightarrow m^{\phi(n)} \equiv 1 \pmod{n} \quad \text{...②}$$

ونعلم أنّ $n^{\phi(m)} \equiv 0 \pmod{n}$ ...③

$m^{\phi(n)} \equiv 0 \pmod{m}$ ...④

بجمع ① مع ④ نجد: $n^{\phi(m)} + m^{\phi(n)} \equiv 0+1 \pmod{m}$

$$\Rightarrow n^{\phi(m)} + m^{\phi(n)} \equiv 1 \pmod{m}$$

بجمع ② مع ③ نجد: $n^{\phi(m)} + m^{\phi(n)} \equiv 0+1 \pmod{n}$

$$\Rightarrow n^{\phi(m)} + m^{\phi(n)} \equiv 1 \pmod{n}$$

ولأنّ $gcd(n,m)=1$

$$n^{\phi(m)} + m^{\phi(n)} \equiv 1 \pmod{nm}$$

تمرين (2): إذا كان $p$ عدداً أولياً فردياً فأثبت أنّ:

$$(p-1)! \equiv (p-1) \bmod \left[\frac{p(p-1)}{2}\right]$$

الإثبات:

$p$ عدد أولي فردي $\Leftarrow$ حسب ويلسون:

$$(p-1)! \equiv -1 \pmod{p}$$

$$\Rightarrow \boxed{(p-1)! \equiv p-1 \pmod{p}} \quad \text{...①}$$

وبما أنّ $p-1 = 2 \times \frac{p-1}{2}$ بالتّالي:

$$p-1 \equiv 0 \pmod{\frac{p-1}{2}}$$

$$\Rightarrow (p-1)! \equiv 0 \mod \left(\frac{p-1}{2}\right)$$

$$\boxed{(p-1)! \equiv (p-1) \mod \left(\frac{p-1}{2}\right)} \quad (2)$$

من (1) و (2)

وكون $\gcd\left(p, \frac{p-1}{2}\right) = 1$ نجد:

$$(p-1)! \equiv (p-1) \mod \left(p \times \frac{p-1}{2}\right)$$

## • رتبة عدد صحيح بالنّسبة لمقاس m:

ليكن $a, m$ عددين صحيحين حيث $m > 0$ و $\gcd(a,m) = 1$

نسمي أصغر عدد صحيح موجب تماماً $k$ يحقق التطابق:

$a^k \equiv 1 \mod m$ أي $a^x \equiv 1 \pmod m$

برتبة $a$ بالنّسبة للمقاس $m$ ونرمز بـ $O_m(a)$.

مثال: أوجد $O_5(2)$ ؟

الحل:

$a = 2 \quad , \quad m = 5$

نحسب $2^n$ بالنّسبة للمقاس $m = 5$.

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

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

$$2^3 \not\equiv 1 \pmod 5$$

$$2^4 \equiv 1 \pmod 5 \Rightarrow O_5(2) = 4$$

أي $2^4$ يطابق 1 بالمقاس 5.

مثال: أوجد رتبة 3 بالنسبة للمقاس 8 ؟ أي أوجد $O_8(3)$ ؟

الحل:

$a = 3 \quad m = 8$

نحسب $3^n$ بالنّسبة للمقاس $m = 8$:



TEL:0931497960 - Facebook Group: A to Z مكتبة

$3^1 \not\equiv 1 \pmod 8$

$3^2 \equiv 1 \pmod 8 \Rightarrow O_8(3) = 2$

مثال: أوجد $O_7(4)$ ؟ تُترك للطالب

سيكون الناتج $O_7(4) = 3$

• بعض الملاحظات:

1 - إذا كان $\gcd(a,m) \neq 1$ عندئذٍ $O_m(a)$ غير موجود (غير معرّف)

2 - إذا كان $\gcd(a,m) = \gcd(b,m) = 1$ و $a \equiv b \pmod m$ عندئذٍ: $O_m(a) = O_m(b)$

مثال: إنّ $2 \equiv 7 \pmod 5$ بالتالي $O_3(2) = O_5(7) = 4$

مثال: أوجد $O_2(99)$ ؟

الحل: $99 \equiv 1 \pmod 2$

$O_2(99) = O_2(1) = 1 \Leftarrow$

مبرهنة: ليكن $a, m$ عددين صحيحين و $m > 1$ و $K = O_m(a)$ عندئذٍ: $a^n \equiv 1 \pmod m \iff O_m(a) \mid n$ حيث $n \in \mathbb{Z}^+$

الإثبات:

$\Leftarrow$ لدينا فرضاً $a^n \equiv 1 \pmod m$ حيث $n \in \mathbb{Z}^+$ حسب القسمة الإقليدية:

$n = q \times O_m(a) + r \quad ; \quad 0 \leq r < O_m(a)$

$a^n = \left((a^m)^{O_m(a)}\right)^q + a^r$

$a^n \equiv 1^q \times a^r \pmod m \Rightarrow 1 \equiv a^r \pmod m \Rightarrow$



TEL:0931497960 - Facebook Group: A to Z مكتبة

$a^r \equiv 1 \pmod m$

إنّ $r=o$ لأنّه لو كان $o < r < O_m(a)$ ولدينا:

$a^r \equiv 1 \pmod m$ بالتالي $r$ ليست رتبة $a$ بالنسبة للمقاس $m$ وهذا مرفوض بالتالي $r=o$ عندئذٍ:

$n = 2 \times O_m(a) \Rightarrow O_m(a) \backslash n$

لدينا فرضاً $\Rightarrow$ $O_m(a) \backslash n \Leftarrow n = q \times O_m(a)$

$a^n = (a^{O_m(a)})^q \equiv (1)^q \pmod m$

$\equiv 1 \pmod m$

**نتيجة:** ليكن $gcd(a,m)=1$ عندئذٍ: $O_m(a) \backslash \phi(m)$

الاثبات:

لدينا $gcd(a,m)=1$ عندئذٍ حسب أويلر

$a^{\phi(m)} \equiv 1 \pmod m$

عندئذٍ من المبرهنة السابقة نجد $O_m(a) \backslash \phi(m)$.

**ملاحظة:** النتيجة السّابقة تفيدنا في اختصار خطوات حساب رتبة عدد بالنسبة لمقاس $m$ حيث يكفي أن نبحث عن رتبة العدد $a$ بالمقاس $m$ بين القواسم الموجبة لـ $\phi(m)$.

**مثال:** أوجد رتبة 5 بالنسبة للمقاس 42 (أوجد $O_{42}(5)$ ؟)

**الحل:**

نضع $K = O_{42}(5)$

عندئذٍ $K$ أحد القواسم الموجبة للعدد $\phi(42)$:

$O_{42}(5) \backslash \phi(42)$

حيث $\phi(42) = \phi(6).\phi(7) = \phi(2).\phi(3).\phi(7)$



TEL:0931497960 - Facebook Group: A to Z مكتبة

$= 1 \times 2 \times 6 = 12 \Rightarrow k \in \{$ قواسم الـ 12 $\}$

$\Rightarrow k = \{1, 2, 3, 4, 6, 12\}$

نحسب $5^k$ فنجد:

$5^1 \not\equiv 1 \pmod{42}$

$5^2 \not\equiv 1 \pmod{42}$

$5^3 \not\equiv 1 \pmod{42}$

$5^4 \not\equiv 1 \pmod{42}$

$5^6 \equiv 1 \pmod{42} \Rightarrow O_{42}(5) = 6$

ملاحظة (1): إذا كانت $k = O_m(a)$ وليكن $i, j$ عددين صحيحين موجبين فإنّ:

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

ملاحظة (2): إذا كانت $k = O_m(a)$ عندئذٍ العناصر $a^1, a^2, a^3, \ldots, a^{O_m(a)}$ غير متطابقة مثنى مثنى بالنسبة للمقياس $m$

ملاحظة (3): إذا كانت $gcd(a, m) = 1$ حيث $m \in \mathbb{Z}^+$ و $t \in \mathbb{Z}^+$ عندئذٍ:

$$O_m(a^t) = \frac{k}{gcd(k, t)} \quad ; \; t \in \mathbb{Z}^+$$

مثال: نعلم أنّ $O_7(3) = 6$ عندئذٍ

$$O_7(3^4) = \frac{O_7(3)}{gcd(4, O_7(3))} = \frac{6}{2} = 3$$

ملاحظة (4): ليكن $a, b \in \mathbb{Z}$ و $m \in \mathbb{Z}^+$ حيث $gcd(a, m) = gcd(b, m) = 1$ , $O_m(a) = h$ ,



TEL:0931497960 - Facebook Group: A to Z مكتبة

عندئذٍ: $\gcd(h,k)=1$ و $O_m(b)=k$

$$O_m(a,b)=O_m(a)\times O_m(b)=h.k$$

مثال: أوجد رتبة 2 بالنسبة للمقاس 7

$O_7(2)$ ، $O_7(6)$ ، $O_7(12)$ ، $O_7(5)$ ، $O_7(125)$ ؟

الحل:

• إيجاد $O_7(2)$: إنّ $\phi(7)=6$ و k هو أحد القواسم الموجبة للعدد 6

$k\in\{1,2,3,6\}$

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

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

$2^3 \equiv 1 \pmod 7 \Rightarrow O_7(2)=3$

• إيجاد $O_7(6)$: يترك للطالب.

• إيجاد $O_7(12)$:

$$O_7(12)=O_7(2\times 6)=O_7(2)\times O_7(6)=6$$

حيث $\gcd(O_7(2),O_7(6))=1$

• إيجاد $O_7(5)$: لدينا $5\equiv 12 \pmod 7$

$$O_7(5)=O_7(12)=6$$

• إيجاد $O_7(125)$:

$$O_7(125)=O_7(5^3)=\frac{O_7(5)}{\gcd(3,O_7(5))}=\frac{6}{\gcd(3,6)}=2$$

مثال: أوجد $O_{13}(2)$ ، $O_{13}(3)$ ، $O_{13}(4)$ ، $O_{13}(12)$

الحل: • إيجاد $O_{13}(2)$:

إنّ $O_{13}(2)=k$ حيث $k\mid\phi(13)$ علماً أنّ $\phi(13)=12$

$k\in\{1,2,3,4,5,6,12\}$



TEL:0931497960 - Facebook Group: A to Z مكتبة

$2^1 \not\equiv 1 \pmod{13}$

$2^2 \not\equiv 1 \pmod{13}$

$2^3 \not\equiv 1 \pmod{13}$

$2^4 \not\equiv 1 \pmod{13}$

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

$O_{13}(2) = 12$

بسهولة نجد $O_{13}(4) = 6$ و $O_{13}(3) = 3$.

• ايجاد $O_{13}(12)$:

لدينا $O_{13}(12) = k \Leftarrow k \mid 12$

حيث $K = \{1, 2, 3, 4, 6, 12\}$

$12^1 \not\equiv 1 \pmod{13}$

$12^2 \equiv 1 \pmod{13} \Rightarrow O(12) = 2$

■ مفهوم الجذور الأساسيّة (الأوليّة) بالنّسبة لمقاس m:

**تعريف**: ليكن $g, m$ عددين صحيحين موجبين حيث

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

يُقال بأنّ $g$ جذر أساسي بالنّسبة للمقاس $m$ إذا تحقّق الشّرط:

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

مثال (1): $O_5(2) = 4 = \phi(5)$ نلاحظ بأنّ $g=2$ جذر أساسي بالنّسبة للمقاس $m=5$

مثال (2): $O_7(5) = 6 = \phi(7)$ إذن $g=5$ جذر أساسي بالنّسبة للمقاس $m=7$

مثال (3): $O_7(2) = 3 \neq \phi(7)$ إذن $g=2$ ليس جذر أساسي بالنّسبة للمقاس $m=7$.



TEL:0931497960 - Facebook Group: A to Z مكتبة

ملاحظة: الجذر g بالنسبة للمقاس m ينتمي دائماً إلى $Z_m^*$ نظام البواقي المختزل الطبيعي قياس m.

مثال: m = 8 لايملك جذور أساسية:

للبحث عن الجذور الأساسية لـ m = 8 نبحث ضمن المجموعة

$$Z_m^* = Z_8^* = \{1, 3, 5, 7\}$$

$O_8(1) = 1 \neq \phi(8) = 4 \Leftarrow$ 1 ليس جذر أساسي بالنسبة للمقاس 8

$O_8(3) = 2 \neq \phi(8) = 4 \Leftarrow$ 3 ليس " " " " "

$O_8(5) = 2 \neq \phi(8) = 4 \Leftarrow$ 5 " " " " "

$O_8(7) = 2 \neq \phi(8) \Leftarrow$ 7 " " " " "

بالتالي العدد 8 لايملك جذور أساسية بالنسبة للمقاس 8

$\Leftarrow$ العدد 8 لايملك جذور أساسية

مبرهنة: إذا كان m عدداً صحيحاً موجباً وكان g جذراً أساسياً بالنسبة للمقاس m عندئذٍ:

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

نظام بواقي مختزل قياس m

الإثبات:

لدينا g جذر أساسي بالنسبة للمقاس m عندئذٍ

$$O_m(g) = \phi(m) \qquad gcd(g, m) = 1$$

• بما أنّ $gcd(g, m) = 1$

$\forall x \in A \; ; \; gcd(x, m) = 1$ وهو الشرط الأول من شرط البواقي المختزل.

• سنثبت أنّ $g^i \not\equiv g^j \pmod m$ حيث $1 \leq i, j \leq \phi(m)$ ; $i \neq j$

نفرض جدلاً أنّ $g^i \equiv g^j \pmod m$ حيث:



TEL:0931497960 - Facebook Group: A to Z مكتبة

$1 \le i, j \le \phi(m)$ . نستنتج من ملاحظة سابقة أنّ

$i \equiv j \pmod{K}$ ; $K = O_m(g) = \phi(m)$

$\Rightarrow i \equiv j \pmod{\phi(m)} \Rightarrow \phi(m) \mid (i-j)$

وهذا مرفوض لكون $0 < i-j < \phi(m)$ .

بالتالي الفرض الجدلي خاطئ بالتالي عناصر المجموعة A غير متطابقة مثنى مثنى بالنسبة للمقاس m

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

نستنتج ممّا سبق أنّ A نظام بواقي مختزل طبيعي .

**مبرهنة** (دون برهان) :

إذا كان g جذر أساسي بالنّسبة للمقاس m و $n \in \mathbb{Z}^+$

عندئذٍ : $g^n$ جذر أساسي للمقاس m $\Leftrightarrow \gcd(n, \phi(m)) = 1$

**ملاحظة :**

إذا كان يوجد جذر أساسي g بالنّسبة للمقاس m فإنّهُ يوجد بالضّبط $\phi(\phi(m))$ جذر أساسي بالنّسبة للمقاس m

انتهت المحاضرة



TEL:0931497960 - Facebook Group: A to Z مكتبة