كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : العاشرة/نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

- الآن سوف نقدم نظرية ويلسون لدراسة التطابق التربيعي:

$$x^2 \equiv -1 \pmod{p}$$

حيث p عدد أولي فردي.

- مبرهنة: p عدد أولي فردي عندئذٍ التطابق

$$x^2 \equiv -1 \pmod{p}$$

يقبل حلاً إذا وفقط إذا كان:

$$p \equiv 1 \pmod{4}$$

الإثبات:

$\Leftarrow$ لدينا فرضاً التطابق $x^2 \equiv -1 \pmod{p}$ قابل للحل ولكن x_0 حلاً له.

$$x_0^2 \equiv -1 \pmod{p} \Leftarrow$$

نلاحظ:

$$\gcd(x_0, p) = 1$$

لأنه إذا كان $\gcd(x_0, p) \neq 1$

$$\gcd(x_0, p) = p \Leftarrow$$

$p \mid x_0 \Rightarrow p \mid x_0^2$ ⟸

و

$p \mid (x_0^2 + 1)$ $\Rightarrow p \mid (x_0^2 + 1 - x_0^2)$

$\Rightarrow p \mid 1$

وهذا مرفوض.

* $gcd(x_0, p) = 1 \xrightarrow{\text{فيرما}} x_0^{p-1} \equiv 1 \pmod p$

$\Rightarrow (x_0^2)^{\frac{p-1}{2}} \equiv 1 \pmod p$

$\Rightarrow (-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$

$(-1)^{\frac{p-1}{2}} =$ { -1 فردي $\frac{p-1}{2}$ ، 1 زوجي $\frac{p-1}{2}$

إذا كان $(-1)^{\frac{p-1}{2}} = -1$

$-1 \equiv 1 \pmod p$ ⟸

$p \mid 2$ ⟸

وهذا مرفوض.

بالتالي:

$(-1)^{\frac{p-1}{2}} = 1$

$\frac{p-1}{2}$ زوجي

$\Rightarrow \frac{p-1}{2} = 2k \; ; \; k \in Z$

$\Rightarrow p-1 = 4k$

$\Rightarrow p \equiv 1 \pmod 4$

$\Rightarrow$ لدينا p عدد أولي فردي بحيث

$p \equiv 1 \pmod 4$

$(p = 4k+1)$

عندئذٍ ـ حسب ويلسون ـ :

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

$$(p-1)! = 1 \times 2 \times 3 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(\frac{p+1}{2}\right) \times \cdots \times (p-2) \times (p-1)$$

بالضرب:

$$\begin{cases} (p-1) \equiv -1 \pmod p \\ (p-2) \equiv -2 \pmod p \\ \frac{p+1}{2} \equiv -\left(\frac{p-1}{2}\right) \pmod p \end{cases}$$

$$\Rightarrow (p-1)! \equiv \left(1 \times 2 \times \cdots \times \frac{p-1}{2}\right)(-1)^{\frac{p-1}{2}} \left(1 \times 2 \times \cdots \times \frac{p-1}{2}\right) \pmod p$$

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

p عدد أولي فردي مضاد لشكل $4k+1$

أي $\frac{p-1}{2}$ زوجي عندئذ:

$$(p-1)! \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p$$

$$-1 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p$$

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

$\Leftarrow$ $x_0 = \left(\frac{p-1}{2}\right)!$ هو حل للمطابقة

$$x^2 \equiv -1 \pmod p$$

بالتالي المطابقة قابلة للحل.

ملاحظة: المطابقة $x^2 \equiv -1 \pmod p$ قابلة للحل

عندما: p عدد أولي فردي

$\Leftrightarrow$

$$p \equiv 1 \pmod 4$$

وله حلّان مختلفان بالنسبة للمعامل p هما:

$$x_0 = \left(\frac{p-1}{2}\right)!$$

$\Leftrightarrow$

$$x_1 = p - x_0$$

مثال: $x^2 \equiv -1 \pmod{17}$

$p = 17 \equiv 1 \pmod 4$ عدد أولي فردي ،

⇐ التطابق $x^2 \equiv -1 \pmod p$

قابل للحل وله حلان مختلفان هما.

$$x_0 = \left(\frac{p-1}{2}\right)! = 8! \equiv 13 \pmod{17}$$

$\Rightarrow x_0 = 13$

$x_1 = p - 13 = 4 \Rightarrow x_1 = 4$

ملاحظة: التطابق $x^2 \equiv -1 \pmod p$ غير قابل للحل

عندما يكون p عدد أولي فردي يحقق:

$p \equiv 3 \pmod 4$

$(p = 4k + 3)$

مثال: $x^2 \equiv -1 \pmod 7$

غير قابل للحل لأن:

$p \not\equiv 1 \pmod 4$

$p = 7 \equiv 3 \pmod 4$

* رتبة عدد صحيح بالنسبة لمقاس m:

مبيناً سابقاً أنه إذا كان

$\gcd(a, m) = 1$ عندئذ حسب أولر:

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

بالتالي المجموعة:

$$A = \{ k \; ; \; k \in \mathbb{Z}^+ \wedge a^k \equiv 1 \pmod m \} \neq \phi$$

بالتالي حسب مبدأ الترتيب الجيد (كل مجموعة جزئية من مجموعة الأعداد الصحيحة الموجبة تملك عنصر أصغر)

بالتالي A تملك عنصر أصغر

تعريف: ليكن a, m عددين صحيحين

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

عندئذٍ نسمي أصغر عدد صحيح موجب تماماً k يحقق المطابقة:

$$a^x \equiv 1 \pmod m$$

نرمز لرتبة العدد a بالنسبة للمقياس m

ونرمز بالرمز:

$$ord_m(a) \quad \text{أو} \quad \delta_m(a) = k$$

مثال: أوجد $\delta_5(2)$ ؟

نريد 2^n :

$$\begin{cases} 2^1 \not\equiv 1 \pmod 5 \\ 2^2 \not\equiv 1 \pmod 5 \\ 2^3 \not\equiv 1 \pmod 5 \\ 2^4 \equiv 1 \pmod 5 \end{cases}$$

$$\Rightarrow \quad \underset{5}{O}(2) = 4$$

مثال: أوجد $\underset{8}{O}(3)$ ؛ نوجد 3^n

$$3^1 \not\equiv 1 \pmod 8$$
$$3^2 \equiv 1 \pmod 8$$
$$\Rightarrow \quad \underset{8}{O}(3) = 2$$

ملاحظات:

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

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

$$\Rightarrow \quad O_m(a) = O_m(b)$$

3- إذا كان $\begin{cases} \gcd(a,m)=1 \\ o_m(a)=k \end{cases}$ عندئذٍ:

$$o_m(a^t)=\frac{o_m(a)}{\gcd(t,o_m(a))}=\frac{k}{\gcd(t,k)}$$

حيث $t\in\mathbb{Z}^+$

مبرهنة: لتكن a,m عددين صحيحين

$\gcd(a,m)=1$

$k=o_m(a)$

$a^n\equiv 1 \pmod m$ عندئذٍ:

حيث n عدد صحيح موجب:

$(o_m(a)\mid n) \iff k\mid n$

البرهان: $\Leftarrow$ لدينا فرضاً $a^n\equiv 1 \pmod m$

$n=q\times k+r$; $0\le r<k$

$n=q\times o_m(a)+r$; $0\le r<k=o_m(a)$

$\Rightarrow a^n=(a^{o(a)})^q \times a^r$

$1\equiv (1)^q\times a^r \pmod m$

$\Rightarrow a^r\equiv 1 \pmod m$

* إذا كان $0 < r < k$ عندئذٍ:

k ليس رتبة العدد a بالنسبة للمقاس m

وهذا مرفوض

بالتالي $\Leftarrow r = 0$

$$n = q \times o_m(a)$$

$$\Rightarrow o_m(a) \mid n \qquad (k \mid n)$$

$\Rightarrow$ لدينا فرضاً $k \mid n \Leftarrow o_m(a) \mid n$

$$n = q \times o_m(a) \Leftarrow$$

و $q \in \mathbb{Z}^+$

$$a^n = (a^{o(a)})^q$$

$$a^n \equiv (1)^q \pmod m$$

$$a \equiv 1 \pmod m$$

- نتيجة: إذا كان $\gcd(a,m) = 1$ عندئذٍ:

$$o_m(a) \mid \phi(m)$$

البرهان: $\gcd(a,m) = 1 \xrightarrow{\text{أولر}}$

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

عندئذٍ حسب الخاصة السابقة نجد:

$$o_m(a) \mid \phi(m)$$

ملاحظة: النتيجة السابقة تعفينا من اختبار خطوات حساب رتبة عدد بالنسبة لطما m حيث يكفي أن نبحث عن رتبة العدد a بالنسبة لطما m بين القواسم الطبيعية لـ $\phi(m)$

أمثلة: $O_{40}(3)$ ثم $O_{40}(27)$ ثم $O_{40}(43)$ ثم $O_{40}(3^{10})$

نتائج: ①

$$\phi(40) = \phi(8)\,\phi(5)$$
$$= \phi(2^3)\,\phi(5)$$
$$= 2^{3-1}(2-1) \times 4$$
$$= 16$$

ملاحظة:

$k = O_{40}(3)$ ف $k \mid \phi(40)$

$k \mid 16$ ⟸

$k \in \{1, 2, 4, 8, 16\}$

$n \in \{1, 2, 4, 8, 16\}$ حيث 3^n حسب

$3^1 \not\equiv 1 \pmod{40}$

$3^2 \not\equiv 1 \pmod{40}$

$3^4 \equiv 1 \pmod{40}$

$\Rightarrow O_{40}(3) = 4$

$43 \equiv 3 \pmod{40}$ ②

$\Rightarrow O_{40}(3) = O_{40}(43) = 4$

$O_{40}(27) = O_{40}(3^3)$ ③

$= \frac{O_{40}(3)}{\gcd(3, O_{40}(3))} = \frac{4}{\gcd(3,4)}$

$= \frac{4}{1} = 4$

$O_{40}(3^{10}) = \frac{O_{40}(3)}{\gcd(10, O_{40}(3))} = \frac{4}{2} = 2$ ④

مثال: أوجد $O_{13}(2)$

الحل:

$\phi(13) = 12$

نلاحظ أنه $k = O_{13}(2)$ & $k \mid \phi(13)$

$k \mid 12$ ⟸

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

$n \in \{1, 2, 3, 4, 6, 12\}$ حيث 2^n حيث

نجد:

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

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

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

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

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

$2^{12} \equiv 1 \pmod{13}$

$\Rightarrow O_{13}(2) = 12$

ملاحظة: إذا كان $O_m(b) = h$ و $O_m(a) = k$

وكان

$$\gcd(h, k) = 1$$

حينئذ:

$$O_m(a \times b) = O_m(a) \times O_m(b)$$

مثال: أوجد $O_7(12)$

الحل:

$$12 = 2 \times 6$$

$O_7(2) = 3$

$O_7(6) = 2$

$\Rightarrow O_7(12) =$

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

$= 3 \times 2$

$= 6$

حيث $\gcd(3, 2) = 1$

انتهت المحاضرة