كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

المادة : نظرية الاعداد

المحاضرة : التاسعة/نظري/

{{ A to Z مكتبة }}

Facebook Group : A to Z مكتبة

• ملاحظة:

يمكن الاستفادة من مبرهنة فيرما في إثبات أولية عدد إذا استطعنا إيجاد عدد صحيح a

بحيث:

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

&

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

عندئذٍ: m ليس عدداً أولياً

• مثال: $m = 117$ ليس عدداً أولياً لأنه يوجد $2 \in \mathbb{Z}$

& $\gcd(2, m) = 1$

& $2^{117-1} \equiv 22 \pmod{117}$

$$2^{117-1} \not\equiv 1 \pmod{117}$$

* مبرهنة ويلسون:

إذا كان m عدداً صحيحاً موجباً أولياً عندئذٍ:

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

الإثبات:

• الحالة الأولى: $m=2$

$(2-1)! = 1! \equiv -1 \pmod{2}$

• الحالة الثانية: m عدد أولي فردي:

★ نأخذ $A = Z_m^* = \{0, 1, 2, \dots, m-1\}$

$|A| = \phi(m) = m-1$

★ التطابق $ax \equiv \pmod{m}$

$\forall a \in A$

قابل للحل ويملك حل وحيد لأن:

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

&

$d \backslash 1$

وهذا الحل نرمزله $\bar{a}$ حيث $\bar{a} \in A$

$(a\bar{a} \equiv \pmod{m})$

★ $a = \bar{a} \Rightarrow a^2 \equiv 1 \pmod{m}$

$m \backslash (a^2-1)$

$m \backslash (a-1)(a+1)$

ولكون m عدد أولي فردي

إما: $m \mid (a-1) \Rightarrow a-1 \equiv 0 \pmod{m}$

$$a \equiv 1 \pmod{m} \Rightarrow \boxed{a=1}$$

أو: $m \mid (a+1) \Rightarrow a+1 \equiv 0 \pmod{m}$

$$a \equiv -1 \pmod{m}$$

$$a \equiv m-1 \pmod{m}$$

$$\Rightarrow \boxed{a = m-1}$$

نستنتج أن:

$a \in \{1, m-1\}$ عندما $a = \bar{a}$

$a \in A \setminus \{1, m-1\}$ عندما $a \neq \bar{a}$

$$= \{2, 3, \dots, m-2\}$$

$$2 \times 3 \times \dots \times (m-2) \equiv 1 \pmod{m}$$

$$1 \times 2 \times 3 \times \dots \times (m-2) \equiv 1 \pmod{m}$$

$$1 \times 2 \times 3 \times \dots \times (m-2)(m-1) \equiv (m-1) \pmod{m}$$

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

نستنتج من الحالة الأولى والثانية نكون قد حصلنا على المطلوب.

* عكس نظرية ويلسون:

إذا كان m عدداً صحيحاً موجباً بحيث

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

فإن m عدد أولي

الإثبات:

نفرض جدلاً بأن m ليس بعدد أولي بالتالي m يملك عامل أولي p

حيث $p \mid m$

$$1 < p \leq m-1$$

$$(m-1)! = 1 \times 2 \times \dots \times (m-1)$$

نلاحظ:

$$p \mid (m-1)!$$

لدينا فرضاً

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

ولدينا $m \mid ((m-1)! + 1)$

$$p \mid m$$

$$\left.\begin{array}{l} \Rightarrow p \mid ((m-1)+1) \\ \quad\& \\ p \mid (m-1)! \end{array}\right\} \Rightarrow p \mid 1$$

وهذا مرفوض

بالتالي الفرض الجدلي خاطئ $\Leftarrow$ m عدد أولي

نتيجة من مبرهنة ويلسون:

- إذا كان m عدداً صحيحاً موجباً أولياً

عندئذٍ:

$$(m-2)! \equiv 1 \pmod{m}$$

الإثبات:

m عدد أولي $\Leftarrow$ حسب ويلسون

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

$$(m-1)(m-2)! \equiv -1 \pmod{m}$$

$$-(m-2)! \equiv -1 \pmod{m}$$

$$\boxed{(m-2)! \equiv 1 \pmod{m}}$$

مثال

أثبت أن $23 \mid (18! + 1)$

الحل:

يجب أن نثبت أن:

$$18! + 1 \equiv 0 \pmod{23}$$

23 عدد أولي $\Leftarrow$ حسب ويلسون

$$(23-1)! \equiv -1 \pmod{23}$$

$$22! \equiv -1 \pmod{23}$$

$22 \times 21 \times 20 \times 19 \times 18! \equiv -1 \pmod{23}$

$(-1)(-2)(-3)(-4)\,18! \equiv -1 \pmod{23}$

$24 \times 18! \equiv -1 \pmod{23}$

$18! \equiv -1 \pmod{23}$

$18!+1 \equiv 0 \pmod{23}$

$\Rightarrow 23 \mid (18!+1)$

مثال أوجد باقي قسمة $96!$ على العدد الأولي $p=97$

$96! \equiv \boxed{} \pmod{97}$

97 عدد أولي $\xleftarrow{\text{ويلسون}}$

$(97-1)! \equiv -1 \pmod{97}$

$96! \equiv -1 \pmod{97}$

$\equiv 96 \pmod{97}$

الباقي هو 96

مثال أثبت أن $67 \mid ((43!)(65!)+41!)$

الحل:

67 عدد أولي $\Leftarrow$ حسب نتيجة ويلسون

$(67-2)! \equiv 1 \pmod{67}$

$65! \equiv 1 \pmod{67}$

نضرب ب 43 $\Longrightarrow$ $43 \times 65! \equiv 43 \pmod{67}$

نضيف $41!$ $\Longrightarrow$ $43 \times 65! + 41! \equiv 43 + 41! \pmod{67}$

$$43 \times 65! + 41! \equiv 67 \pmod{67}$$

$$43 \times 65! + 41! \equiv 0 \pmod{67}$$

$$\Longrightarrow 67 \mid \left((43) \times (65!) + 41!\right)$$

مثال

ليكن p عدداً أولياً فردياً والمطلوب:

أثبت العلاقة التالية:

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

الحل: يجب أن نثبت أن:

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

$$\&$$

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

★ p عدد أولي فردي $\Longrightarrow$ ويلسون

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

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

★

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

ولدينا:

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

$$(p-1) \equiv 0 \left(\bmod \frac{p-1}{2}\right)$$

عندئذٍ:

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

من 1 و 2 وكون:

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

نجد:

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

انتهت المحاضرة