كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : الثامنة /نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

• مبرهنة ويلسون: إذا كان m عدداً صحيحاً موجباً أولياً عندئذٍ

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

الإثبات:

• الحالة الأولى $m=2$ بالتالي:

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

• الحالة الثانية: m عدد فردي، لنأخذ المجموعة:

$A = Z_m^* = \{1, 2, \dots, m-1\}$ نظام البواقي المختزل الطبيعي قياس m

$$|A| = \phi(m) = m-1 \qquad \forall a \in A,\ gcd(a,m) = 1$$

بالتالي التطابق الخطي $ax \equiv 1 \pmod m$ يملك حل وحيد لأنّ:

$$gcd(a,m) = 1 \ \&\ 1 \mid b;\ b=1$$

هذا الحل الوحيد نرمز له بـ $\bar{a}$ (المعكوس الضربي للعدد a بالنسبة للمقاس m) نلاحظ $\bar{a} \in A$.

السؤال ماهي العناصر في المجموعة A التي معكوسها يساويها

$$a = \bar{a} \Rightarrow a^2 \equiv 1 \pmod m \Rightarrow m \mid (a^2-1)$$

بالتالي $m \mid (a-1)(a+1)$ عدد أولي بالتالي:

$$m \mid (a-1) \Rightarrow a = 1 \qquad m \mid (a+1) \Rightarrow a = m-1$$

نستنتج بأنّ $a = \bar{a}$ إذا كان $a=1$ أو $a=m-1$

$a \neq \bar{a}$ إذا كان $a \in A \setminus \{1, m-1\}$ عددها زوجي

$$\Rightarrow a \in \{2, 3, \dots, m-2\}$$

$2.3.4.5.\ldots\ldots m-2 \equiv 1 \pmod m$

$1.2.3.4.5.\ldots\ldots m-2 \equiv 1 \pmod m$

$1.2.3.4.5.\ldots\ldots (m-2)(m-1) \equiv (m-1) \pmod m$

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

عكس ويلسون:

إذا كان m عدداً صحيحاً موجباً بحيث $(m-1)! \equiv -1 \pmod m$

فإنّ m عدد أولي

الإثبات: نفرض جدلاً بأنّ m عدد ليس أولي عندئذٍ يوجد عدد أولي p

بحيث $p \mid m$ & $1 < p \leq m-1$

بالتالي $p \mid (m-1)!$ بحيث $(m-1)! = (m-1)(m-2)\ldots 2 \times 1$

بالتالي $m \mid ((m-1)! + 1)$ وبما أنّ $p \mid m$ عندئذٍ

$p \mid ((m-1)! + 1)$ وبما أنّ $p \mid (m-1)!$ عندئذٍ $p \mid 1$ وهذا

مرفوض وبالتالي الفرض الجدلي خاطئ بالتالي نتبع أنّ m عدد أولي

نتيجة: m عدد صحيح موجب أولي $\Leftrightarrow$ $(m-1)! \equiv -1 \pmod m$

نتيجة: إذا كان m عدداً صحيحاً موجباً أولياً عندئذٍ:

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

الإثبات:

لدينا m أولي $\xrightarrow{\text{حسب ويلسون}}$ $(m-1)! \equiv -1 \pmod m$

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

$-1\,(m-2)! \equiv -1 \pmod m$

$\Rightarrow (m-2)! \equiv 1 \pmod m$ نضرب الطرفين بـ (-1)

مثال: أثبت أنّ $23 \mid (18! + 1)$

الحل: يجب أن نثبت أنّ $18! + 1 \equiv 0 \pmod{23}$

لدينا 23 عدد أولي ⟸ حسب ويلسون

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

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

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

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

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

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

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

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

مثال: أثبت أن $67 \mid (43 \times 65! + 4!)$

الحل: لدينا 67 عدد أولي ⟸ حسب ويلسون

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

$66! \equiv -1 \pmod{67}$

$66 \times 65! \equiv -1 \pmod{67}$

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

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

$43 \times 65! + 4! \equiv 43 + 4! \pmod{67}$

$43 \times 65! + 4! \equiv 67 \pmod{67}$

$\Rightarrow 67 \mid (43 \times 65! + 4!)$

مثال: أوجد باقي قسمة $2 \times (96!)$ على العدد 97 ؟

الحل:

97 عدد أولي ⟸ حسب ويلسون

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

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

$2 \times 96! \equiv -2 \pmod{97}$

$2 \times 96! \equiv 95 \pmod{97}$

فنتج أنّ الباقي هو 95

مثال وظيفة: ليكن p عدداً أولياً فردياً والمطلوب أثبت أنّ

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

• الآن سوف نستخدم نظرية ويلسون لدراسة التطابق التربيعي

$x^2 \equiv -1 \pmod{p}$ حيث p عدد أولي فردي.

مبرهنة: ليكن p عدد أولي فردي عندئذٍ التطابق $x^2 \equiv -1 \pmod{p}$

قابل للحل إذا وفقط إذا كان $p \equiv 1 \pmod{4}$

الإثبات:

⇐ لدينا فرضاً التطابق $x^2 \equiv -1 \pmod{p}$ قابل للحل وليكن x_0

حلاً له أي: $x_0^2 \equiv -1 \pmod{p}$

نلاحظ بأنّ $\gcd(x_0, p) = 1$ التعليل: لأنّه لو كان $\gcd(x_0, p) \neq 1$

عندئذٍ $\gcd(x_0, p) = p$ بالتالي:

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

ولدينا $p \mid (x_0^2 + 1)$ وبالتالي $p \mid 1$ وهذا مرفوض

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

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

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

لدينا p عدد أولي فردي بالتالي:

$(-1)^{\frac{p-1}{2}} = \begin{cases} -1 & ; \frac{p-1}{2} \text{ فردي} \\ 1 & ; \frac{p-1}{2} \text{ زوجي} \end{cases}$

إذا كان $\frac{p-1}{2}$ فردي $\Leftarrow$ $-1 \equiv 1 \pmod p$

$\Leftarrow$ $p \nmid (-2)$ وهذا مرفوض بالتالي:

$\frac{p-1}{2}$ زوجي $\Leftarrow$ $\frac{p-1}{2} = 2K$ حيث $K \in \mathbb{Z}$

$\Rightarrow p-1 = 4K \Rightarrow p = 1+4K$

$\Rightarrow p \equiv 1 \pmod 4$

$\Rightarrow$ لدينا فرضاً $p \equiv 1 \pmod 4$ ولنثبت أنّ $x^2 \equiv -1 \pmod p$ قابل للحل

لدينا p عدد أولي فردي $\Rightarrow$ ويلسون $(p-1)! \equiv -1 \pmod p$

$(p-1)! = 1 \; 2 \; 3 \; \dots \; \frac{p-3}{2} \cdot \frac{p-1}{2} \cdot \left(\frac{p+1}{2}\right)\left(\frac{p+3}{2}\right) \dots (p-2)(p-1)$

$\frac{p-1}{2}$ عددهم $\qquad$ $\frac{p-1}{2}$ عددهم

نعلم أنّ

$p-1 \equiv -1 \pmod p$

$p-2 \equiv -2 \pmod p$

$\vdots$

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

بالتالي:

$(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left[1 \times 2 \times 3 \times \dots \times \left(\frac{p-3}{2}\right)\left(\frac{p-1}{2}\right)\right]^2 \pmod p$

لدينا $p \equiv 1 \pmod 4$

$\Rightarrow p-1 \equiv 0 \pmod 4$

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

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

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

$\Rightarrow x_0^2 \equiv -1 \pmod p$

بالتالي التطابق $x^2 \equiv -1 \pmod p$ قابل للحل

ملاحظة: إذا كان التطابق $x^2 \equiv -1 \pmod p$ (p حيث عدد أولي فردي) قابلاً للحل فهو يملك حلّان مختلفان بالنسبة للمقاس p هما: $x_0 = \left(\frac{p-1}{2}\right)!$, $x_1 = p - \left(\frac{p-1}{2}\right)!$

مثال: إنّ التطابق $x^2 \equiv -1 \pmod{17}$ قابل للحل لأنّ $17 \equiv 1 \pmod 4$ حيث $p = 17$ عدد أولي فردي

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

بالتالي الحل الأول هو 13

$x_1 = p - \left(\frac{p-1}{2}\right)! = 17 - 8! \equiv 4 \pmod{17}$

الحل الثاني هو 4

ملاحظة: إذا كان p عدد أولي فردي من الشكل $4K+3$ أي $p \equiv 3 \pmod 4$ بالتالي التطابق $x^2 \equiv -1 \pmod p$ غير قابل للحل

مثال: التطابق $x^2 \equiv -1 \pmod 7$ غير قابل للحل لأنّ $p = 7 \not\equiv 1 \pmod 4$

ونلاحظ بأنّ $p \equiv 3 \pmod 4$

انتهت المحاضرة