كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : الخامسة/نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

2025

يمكنكم طلب المحاضرات برسالة نصية (SMS) أو عبر (What's app-Telegram) على الرقم 0931497960

مبرهنة:

العلاقة $\equiv_m$ بالنسبة لقاسم m المعرفة على مجموعة الأعداد الصحيحة $\mathbb{Z}$ بالشكل:

$$\forall a,b \in \mathbb{Z} : a \equiv_m b \Leftrightarrow m \mid (a-b)$$

$$(a \equiv b \pmod m)$$

هي علاقة تكافؤ

ملاحظة:

ليكن $a \in \mathbb{Z}$

$$\bar{a} = \{ b \in \mathbb{Z} : b \equiv_m a \}$$
$$\bar{a} = \{ b ; b \in \mathbb{Z} ; b \equiv a \pmod m \}$$
$$\bar{a} = \{ b ; b \in \mathbb{Z} ; b = a + qm ; q \in \mathbb{Z} \}$$
$$\bar{a} = \{ a + qm ; q \in \mathbb{Z} \}$$

مثلاً:

$$\bar{0} = \{ qm ; q \in \mathbb{Z} \}$$
$$\bar{1} = \{ 1 + qm ; q \in \mathbb{Z} \}$$

ملاحظة:

$a \equiv b \pmod m \iff \bar{a} = \bar{b}$

$(a \underset{m}{\equiv} b)$

مبرهنة:

مجموعة صفوف تكافؤ العلاقة $\underset{m}{\equiv}$ هي:

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$$

مبرهنة:

إذا كانت a, b, c, m أعداد صحيحة، $m > 0$

و لكن

$a \equiv b \pmod m$

عندئذٍ:

1- $a \pm c \equiv b \pm c \pmod m$

2- $ac \equiv bc \pmod m$

الإثبات:

1- تترك بوصفها

2- لدينا $a \equiv b \pmod m$

$a = b + qm \quad ; q \in \mathbb{Z}$

نضرب الطرفين بالعدد c نجد:

$ac = bc + qcm$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$\Rightarrow ac - bc = qcm$

$\Rightarrow m \mid (ac - bc)$

$\Rightarrow ac \equiv bc \pmod{m}$

برهنة: إذا كان $a \equiv b \pmod{m}$

و $c \equiv d \pmod{m}$

حيث m عدد صحيح موجب

عندئذ:

1- $a \mp c \equiv b \mp d \pmod{m}$

2- $ac \equiv bd \pmod{m}$

3- $a^k \equiv b^k \pmod{m}$

حيث k عدد صحيح موجب.

مثال: أثبت أن $13 \mid (3^{n+2} + 4^{2n+1})$

حيث n عدد صحيح موجب

الحل:

يجب أن نثبت أن:

$3^{n+2} + 4^{2n+1} \equiv 0 \pmod{13}$

$3^{n+2} = 3^2 \times 3^n = 9 \times 3^n$

★ $3^{n+2} \equiv -4 \times 3^n \pmod{13}$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$$4^{2n+1} = 4 \times 16^n$$

$$4^{2n+1} \equiv 4 \times 3^n \pmod{13} \quad (**)$$

بجمع * و ** نجد:

$$3^{n+2} + 4^{2n+1} \equiv 0 \pmod{13}$$

$$\Rightarrow 13 \mid (3^{n+2} + 4^{2n+1})$$

مثال: من أجل $n \in \mathbb{Z}^+$ فإن:

$$15 \mid (2^{4n} - 1)$$

الحل:

$$2^{4n} - 1 \equiv 0 \pmod{15}$$
$$2^{4n} \equiv 16^n \pmod{15}$$
$$2^{4n} \equiv 1^n \pmod{15}$$
$$2^{4n} \equiv 1 \pmod{15}$$
$$\Rightarrow 2^{4n} - 1 \equiv 0 \pmod{15}$$
$$\Rightarrow 15 \mid (2^{4n} - 1)$$

ملاحظة

مربع أي عدد فردي يطابق العدد 1 بالمقاس 8.

TEL:0931497960 - Facebook Group: A to Z مكتبة

الإثبات:

ليكن a عدد فردي ولبرهن أنّ:

$a^2 \overset{?}{\equiv} 1 \pmod 8$

a عدد فردي $\Leftarrow$

$a = 2K+1 \quad ; K \in \mathbb{Z}$

$a^2 = 4K^2 + 1 + 4K$

$a^2 = \underbrace{4K(K+1)}_{} + 1$

$K \; , \; K+1$ عددين صحيحين متتاليين $\Leftarrow$

أحدهما فردي والآخر زوجي

$\Rightarrow$

$a^2 = 8q + 1 \quad ; q \in \mathbb{Z}$

$a^2 \equiv 1 \pmod 8$

مثال:

أوجد باقي قسمة $x = \sum_{K=1}^{1000} K!$ على العدد 24

الحل:

$x \overset{?}{\equiv}$ باقي قسمة x على العدد 24 $\pmod{24}$

$x = \sum_{k=1}^{1000} k! = 1! + 2! + 3! + 4! + \cdots + 1000!$

نلاحظ $4! = 24 \Leftarrow 4! \equiv 0 \pmod{24}$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$n \geq 4$ حيث $n! \equiv 0 \pmod{24}$

$\Rightarrow x \equiv 1+2+6 \pmod{24}$

$x \equiv 9 \pmod{24}$

بالتالي باقي قسمة العدد x على العدد 24 هو 9

مثال:

$$x = \left(\sum_{k=0}^{99} (K+1)!\right)^2$$

أوجد باقي قسمة x على العدد 10 ؟

الحل:

نفرض $y = \sum_{k=0}^{99} (K+1)!$

$y = 1! + 2! + 3! + 4! + 5! + \ldots + 50!$

نلاحظ أنّ:

$n! \equiv 0 \pmod{10}$

حيث $n \geq 5$

$\Rightarrow y \equiv 1+2+6+24 \pmod{10}$

$y \equiv 33 \pmod{10}$

$\Rightarrow y \equiv 3 \pmod{10}$

$\Rightarrow y^2 \equiv 9 \pmod{10}$

$\Rightarrow x \equiv 9 \pmod{10}$

بالتالي باقي قسمة العدد x على 10 هو العدد 9

نظرية:

أثبتنا أنّه إذا كان $a \equiv b \pmod{m}$

$\Leftarrow ac \equiv bc \pmod{m}$

وذلك أيّاً كان $c \in \mathbb{Z}$

من الطبيعي أن نتساءل ماذا يحدث عندما نقسم طرفي التطابق على عدد صحيح.

مبرهنة:

إذا كان $ca \equiv cb \pmod{m}$

و $d = gcd(c, m)$

عندئذٍ:

$$a \equiv b \pmod{\left(\frac{m}{d}\right)}$$

الإثبات:

- لدينا: $d = gcd(c, m)$

$\Rightarrow \exists\, c_0, m_0 \in \mathbb{Z} : gcd(c_0, m_0) = 1$

ف $c = c_0 d$

$m = m_0 d$

- لدينا: $ca \equiv cb \pmod{m}$

$\Rightarrow m \mid (ca - cb)$

$\Rightarrow m \mid c(a-b)$

$\Rightarrow m_0 d \mid c_0 d (a-b)$

$\Rightarrow m_0 \mid c_0 (a-b)$

$\Rightarrow gcd(c_0, m_0) = 1$ بما أنّ

$\Rightarrow m_0 \mid (a-b)$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$$\Rightarrow a \equiv b \pmod{m_0}$$

$$\Rightarrow a \equiv b \pmod{\left(\frac{m}{d}\right)}$$

ملاحظة: إذا كان $ca \equiv cb \pmod{m}$ و $\gcd(c,m)=1$

عندئذٍ:

$$a \equiv b \pmod{m}$$

مثال:

$$16 \equiv -12 \pmod{14}$$

$$4 \times 4 \equiv -3 \times 4 \pmod{14}$$

$$d = \gcd(4,14) = 2$$

$$\Rightarrow 4 \equiv -3 \pmod{7}$$

مبرهنة:

ليكن a,b عددين صحيحين، وليكن $n_1, n_2, \ldots, n_r$ أعداد صحيحة موجبة.

عندئذٍ:

$$a \equiv b \pmod{m} \iff a \equiv b \pmod{n_i} \quad \forall\, 1 \le i \le r$$

حيث

$$m = \text{Lcm}(n_1, n_2, \ldots, n_r)$$

الإثبات:

$\Leftarrow$ لنبدأ فرضاً

$$a \equiv b \pmod{n_i} \quad \forall\, 1 \le i \le r$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$n_i \mid (a-b)$

$\Leftarrow$ $(a-b)$ مضاعف مشترك للأعداد $n_1, n_2, \dots, n_r$

ولدينا m مضاعف مشترك أصغر للأعداد $n_1, n_2, \dots, n_r$

$\Rightarrow m \mid (a-b)$

$\Rightarrow a \equiv b \pmod{m}$

$\Leftarrow$ لدينا فرضاً:

$a \equiv b \pmod{m}$

حيث $m = \text{Lcm}(n_1, n_2, \dots, n_r)$

$\Rightarrow m \mid (a-b)$

و $n_i \mid m$

بالتالي:

$\forall\, 1 \le i \le r \quad n_i \mid (a-b)$

$\Rightarrow a \equiv b \pmod{n_i}$

- نتيجة:

ليكن a, b عددين صحيحين

$n_1, n_2, \dots, n_r$ أعداد صحيحة موجبة أولية فيما بينها

مثنى مثنى، عندئذٍ:

$a \equiv b \pmod{(n_1 \times n_2 \times \dots \times n_r)} \iff a \equiv b \pmod{n_i}$

$\forall\, 1 \le i \le r$

الإثبات:

بالاعتماد على المرحلة السابقة:

$a \equiv b \pmod{n_i}$

$\Leftrightarrow \quad a \equiv b \pmod{m}$

حيث: $m = Lcm(n_1, \dots, n_r)$

$\Leftrightarrow \quad a \equiv b \mod \left(\frac{n_1 n_2 \dots n_r}{\gcd(n_1, \dots, n_r)} \right)$

$\Leftrightarrow \quad a \equiv b \mod (n_1, n_2, \dots, n_r)$

مثال:

ليكن $F_n = 2^{2^n} + 1$ عدد فيرما

حيث $n \geq 1$

أثبت أن $F_n \equiv 5 \pmod{12}$

الحل:

لنثبت أن:

$F_n \equiv 5 \pmod 4$

و

$F_n \equiv 5 \pmod 3$

$F_n = 2^{2^n} + 1 \equiv 1 \pmod 4$

$\Rightarrow F_n \equiv 5 \pmod 4 \quad \dots (1)$

$F_n = 2^{2^n} + 1 \equiv (-1)^{2^n} + 1 \pmod 3$

$\equiv 2 \pmod 3$

$\Rightarrow F_n \equiv 5 \pmod 3 \quad \dots (2)$

TEL:0931497960 - Facebook Group: A to Z مكتبة

من (1) و (2) وكون

$gcd(3,4) = 1$

عندئذ

$F_n \equiv 5 \pmod{(3 \times 4)}$

$\Rightarrow F_n \equiv 5 \pmod{12}$

انتهت

TEL:0931497960 - Facebook Group: A to Z مكتبة