كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : الرابعة /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

ملاحظات:

1- $\forall a,b \in \mathbb{Z}$; $a \equiv b \pmod 1$

2- أي عدد صحيح a يطابق باقي قسمته على العدد m بالقياس العدد m حيث $m > 0$ ورمزاً: $0 \le r < m$; $a = q.m + r$

$a \equiv r \pmod m$

3- $m \mid a \iff a \equiv 0 \pmod m$

4- إذا كان $m \mid n$ و $a \equiv b \pmod n \Rightarrow a \equiv b \pmod m$

لدينا: $a \equiv b \pmod n \Leftarrow n \mid (a-b)$ و $m \mid n$

$\Leftarrow m \mid (a-b) \Leftrightarrow a \equiv b \pmod m$.

مبرهنة: إذا كان $a,b \in \mathbb{Z}$ وكان $a \equiv b \pmod m$ حيث $m > 0$ عدد صحيح موجب $\Leftrightarrow$ باقي قسمة a على العدد m يساوي باقي قسمة b على العدد m

مبرهنة: علاقة التطابق $\equiv_m$ بالنسبة للمقياس m المعرّفة على مجموعة الأعداد الصحيحة $\mathbb{Z}$ بالشكل:

$\forall a,b \in \mathbb{Z}$; $a \equiv b \pmod m \Leftrightarrow m \mid (a-b)$

هي علاقة تكافؤ، صفوف تكافؤها هن الشكل:

$\bar{a} = \{n \in \mathbb{Z} \text{ و } n \equiv a \pmod m\} = \{n \in \mathbb{Z},\ n = a + q.m ;\ q \in \mathbb{Z}\}$

فمثلاً $\bar{0} = \{q.m \text{ و } q \in \mathbb{Z}\}$ & $\bar{1} = \{1 + q.m ;\ q \in \mathbb{Z}\}$

$\overline{(m-1)} = \{(m-1) + q.m \text{ و } q \in \mathbb{Z}\}$

ملاحظة: إذا كانت $a \equiv b \pmod m \iff \bar{a} = \bar{b}$

مبرهنة: مجموعة صفوف تكافؤ العلاقة $\equiv_m$ هي:

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

مبرهنة: إذا كانت m و c و b و a أعداد صحيحة حيث $m > 0$ و:

$a \equiv b \pmod m$ عندئذٍ:

1. $a + c \equiv b + c \pmod m$
2. $a - c \equiv b - c \pmod m$
3. $a \cdot c \equiv b \cdot c \pmod m$

إثبات [1]: لدينا فرضاً $a \equiv b \pmod m$

$\Rightarrow a = b + q \cdot m \quad ; q \in \mathbb{Z}$

$\Rightarrow a + c = b + c + q \cdot m \quad ; q \in \mathbb{Z}$

$\Rightarrow (a+c) - (b+c) = q \cdot m \quad ; q \in \mathbb{Z}$

$\Rightarrow m \mid [(a+c) - (b+c)] \Rightarrow a + c \equiv b + c \pmod m$

• إثبات ② و ③ تُترك للطالب

مثال: $7 \equiv -2 \pmod 9$

$\Rightarrow 7 + 11 = -2 + 11 \pmod 9$

$\Rightarrow 18 = 9 \pmod 9$

مبرهنة: إذا كانت m و d و c و b و a أعداد صحيحة حيث $m > 0$

و كانت $a \equiv b \pmod m$ & $c \equiv d \pmod m$

عندئذٍ

1) $a + c = b + d \pmod m$
2) $a - c = b - d \pmod m$
3) $a \cdot c = b \cdot d \pmod m$

إثبات [1]: لدينا فرضاً $a \equiv b \pmod m$;

TEL:0931497960 - Facebook Group: A to Z مكتبة

$a = b + q_1 m$ و $q_1 \in \mathbb{Z}$ ... (*)

ولدينا $c \equiv d \pmod m \Leftarrow c = d + q_2 m$ (**) حيث $q_2 \in \mathbb{Z}$

نجمع (*) و (**) طرفاً إلى طرف:

$$a + c = b + d + (q_1 + q_2) m$$

$$\Rightarrow a + c \equiv b + d \pmod m$$

مبرهنة: إذا كان $a, b, m \in \mathbb{Z}$ حيث $m > 0$ إذا كان $a \equiv b \pmod m$ عندئذٍ:

$\forall n \in \mathbb{N}^*$; $a^n \equiv b^n \pmod m$

الإثبات: نثبت بالاستقراء الرياضي:

- نثبت صحة العلاقة من أجل $n = 1$:

$a \equiv b \pmod m$ محققة

- نفرض صحة العلاقة من أجل $n = k$: $\Rightarrow a^k \equiv b^k \pmod m$

- نثبت صحة العلاقة من أجل $n = k+1$: أي يجب أن نثبت أن:

$$a^{k+1} \stackrel{?}{\equiv} b^{k+1} \pmod m$$

لدينا $a \equiv b \pmod m$ & $a^k \equiv b^k \pmod m$

بضرب العلاقتين $\Rightarrow a \cdot a^k = b \cdot b^k \pmod m$

$$\Rightarrow a^{k+1} = b^{k+1} \pmod m$$

$\Rightarrow$ العلاقة صحيحة من أجل $k+1$ بالتالي مما سبق نجد أن العلاقة صحيحة $\forall n \in \mathbb{N}^*$

مثال: أثبت أن $13 \mid (3^{n+2} + 4^{2n+1})$ وذلك $\forall n \in \mathbb{N}$ ؟

الحل: يجب أن نثبت أن:

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

لدينا $3^{n+2} = 9 \times 3^n \Rightarrow 3^{n+2} \equiv -4 \times 3^n \pmod{13}$ (1)

TEL:0931497960 - Facebook Group: A to Z مكتبة

$4^{2n+1} = (16)^n \cdot 4 \Rightarrow \boxed{4^{2n+1} = (3)^n \times 4 \pmod{13}}$ ②

من ① و ② نجد أنّ

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

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

مثال: أثبت أنّ $15 \mid (2^{4n} - 1)$ وذلك $\forall n \in \mathbb{N}$ ؟

الحل: يجب أن نثبت أنّ:

$2^{4n} - 1 \overset{?}{\equiv} 0 \pmod{15}$

$2^{4n} = (2^4)^n \equiv (16)^n$ & $16 \equiv 1 \pmod{15}$

$\Rightarrow (16)^n \equiv 1^n \pmod{15}$

$\Rightarrow 2^{4n} \equiv 1 \pmod{15} \Rightarrow 2^{4n} - 1 \equiv 0 \pmod{15}$

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

ملاحظة: مربع أي عدد فردي يطابق العدد 1 بالقاس 8 أي:

[a عدد فردي $\Leftarrow a^2 \equiv 1 \pmod{8}$]

الإثبات: a عدد فردي أي: $a = 2k+1$; $k \in \mathbb{Z}$

$\Rightarrow a^2 = 4k^2 + 1 + 4k = 4k(k+1) + 1$

نلاحظ بأنّ k و $(k+1)$ عددين صحيحين متتاليين بالتالي أحدهما زوجي والآخر فردي $\Leftarrow k(k+1)$ عدد زوجي

$\Rightarrow k(k+1) = 2q$; $q \in \mathbb{Z}$

$\Rightarrow a^2 = 8q + 1 \Rightarrow a^2 - 1 = 8q$

$\Rightarrow 8 \mid (a^2 - 1) \Rightarrow a^2 \equiv 1 \pmod{8}$

مثال: أثبت أنّ: $22 \mid (3^{5n+2} + 5^{5n+3} - 2)$ $\forall n \in \mathbb{N}$

الحل:

يجب أن نثبت أنّ $3^{5n+2} + 5^{5n+3} - 2 \overset{?}{\equiv} 0 \pmod{22}$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$3^{5n+2} = (3^5)^n \times 9 = 1^n \times 5 \pmod{22}$

$\Rightarrow \boxed{3^{5n+2} \equiv 5 \pmod{22}}$ ①

$5^{5n+3} = (5^5)^n \times 125 = 1^n \times 15 \pmod{22}$

$\Rightarrow \boxed{5^{5n+3} \equiv 15 \pmod{22}}$ ②

بجمع ① و ② :

$3^{5n+2} + 5^{5n+3} \equiv 5 + 15 \pmod{22}$

$\Rightarrow 3^{5n+2} + 5^{5n+3} \equiv 20 \pmod{22}$

$\Rightarrow 3^{5n+2} + 5^{5n+3} - 2 \equiv 22 \pmod{22} \equiv$

$0 \pmod{22}$

$\Rightarrow 22 \mid (3^{5n+2} + 5^{5n+3} - 2)$

مبرهنة: إذا كانَ $ca \equiv cb \pmod{m}$ وَ $d = \gcd(c, m)$

عندئذٍ $a \equiv b \pmod{\frac{m}{d}}$

الاثبات:

لدينا $d = \gcd(c, m)$ عندئذٍ يوجد $c_0, m_0 \in \mathbb{Z}$ بحيث

$\gcd(c_0, m_0) = 1$ و $m = m_0 d$ و $c = c_0 d$

لدينا $ca \equiv cb \pmod{m}$

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

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

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

لكن $\gcd(m_0, c_0) = 1 \Rightarrow m_0 \mid (a-b)$

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

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

ملاحظة: اذا كانَ $ca \equiv cb \pmod{m}$ وَ $d = \gcd(c, m) = 1$

TEL:0931497960 - Facebook Group: A to Z مكتبة

عندئذٍ $a \equiv b \pmod{m}$

مثال: $16 \equiv -12 \pmod{14}$

$4 \equiv -3 \pmod{7} \Leftarrow 4 \times 4 \equiv 4 \times (-3) \pmod{14}$

برهنة: ليكن $a, b \in \mathbb{Z}$ ولتكن $n_1, n_2, \ldots, n_r$ أعداد صحيحة موجبة عندئذٍ

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

وذلك $\forall\, r \geq i \geq 1$ حيث $m = \text{Lcm}(n_1, \ldots, n_r)$

الإثبات:

$\Rightarrow$ لدينا فرضاً $a \equiv b \pmod{n_i}$ وذلك $\forall\, r \geq i \geq 1$

$\Rightarrow n_i \mid (a-b) \Rightarrow$ مضاعف مشترك لـ n_i $(a-b)$

$(\forall\, r \geq i \geq 1)$ ولدينا m المضاعف المشترك الأصغر لـ $n_1, n_2, \ldots, n_r$

بالتالي: $m \mid (a-b) \Rightarrow a \equiv b \pmod{m}$

$\Rightarrow$ لدينا فرضاً $a \equiv b \pmod{m}$ حيث $m = \text{Lcm}(n_1, \ldots, n_r)$

بالتالي $m \mid (a-b)$ و $n_i \mid m$

$\Rightarrow n_i \mid (a-b) \Rightarrow a \equiv b \pmod{n_i}$ $\forall\, r \geq i \geq 1$

نتيجة: ليكن $a, b \in \mathbb{Z}$ حيث:

$n_1, n_2, \ldots, n_r$ أعداد صحيحة موجبة أولية فيما بينها مثنى مثنى عندئذٍ

$a \equiv b \bmod (n_1 \ldots n_r) \iff a \equiv b \pmod{n_i}$ $\forall\, r \geq i \geq 1$

الإثبات:

بالاعتماد على برهنة سابقة:

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

حيث: $m = \text{Lcm}(n_1, n_2, \ldots, n_r)$ وبما أنّ:

$$\text{Lcm}(n_1, n_2, \ldots, n_r) = \frac{n_1 \cdot n_2 \cdots n_r}{\gcd(n_1, n_2, \ldots, n_r)} = n_1 \cdot n_2 \cdots n_r$$

بالتّالي:

TEL:0931497960 - Facebook Group: A to Z مكتبة

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

$a \equiv b \pmod{(n_1, n_2, \ldots, n_r)}$

مثال: $\begin{cases} 17 \equiv 2 \pmod 3 \\ 17 \equiv 2 \pmod 5 \end{cases}$ وبما أنّ $\gcd(3,5) = 1$

$\Rightarrow 17 \equiv 2 \pmod{3 \times 5}$

$17 \equiv 2 \pmod{15}$

تمارين: تمرين (1): أوجد باقي قسمة العدد $\sum_{k=1}^{1000} k!$ على العدد 24.

الحل:

لنضع $x = \sum_{k=1}^{1000} k! \Leftarrow$

$x = 1! + 2! + 3! + \ldots + 1000!$

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

$x = \sum_{k=1}^{1000} k! \equiv 1 + 2 + 6 + 0 + \pmod{24}$

$\Rightarrow \sum_{k=1}^{1000} k! = 9 \pmod{24}$

كل عدد يطابق باقي قسمته ميث 9 باقي قسمة x على 24.

تمرين (2): أوجد باقي قسمة العدد $x = \left(\sum_{k=0}^{99} (k+1)!\right)^2$ على العدد 10؟

الحل: لنضع $y = \left(\sum_{k=0}^{99} (k+1)!\right)$ عندئذٍ $x = y^2$

$y = \sum_{k=0}^{99} (k+1)! = 1! + 2! + 3! + 4! + 5! + \ldots + 100!$

$\forall n \geq 5 \quad ; \quad n! \equiv 0 \pmod{10}$

$y = 1 + 2 + 6 + 24 + \pmod{10} \Rightarrow y = 33 \pmod{10}$

$y \equiv 3 \pmod{10} \Rightarrow y^2 \equiv 9 \pmod{10}$

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

نلاحظ أنّ باقي قسمة العدد x على العدد 10 هو 9.

تمرين (3): أوجد باقي قسمة العدد $\sum_{k=0}^{1000} k!$ على العدد 20؟

TEL:0931497960 - Facebook Group: A to Z مكتبة

الحل: $\sum_{k=0}^{1000} k! = 0! + 1! + 2! + 3! + 4! + 5! + \dots + 1000!$

$\forall n \geq 5 \quad n! \equiv 0 \pmod{20}$

$\Rightarrow \sum_{k=0}^{1000} k! \equiv 1 + 1 + 2 + 6 + 24 \pmod{20}$

$= 34 \pmod{20} \equiv 14 \pmod{20}$.

وبالتالي باقي قسمة العدد $\sum_{k=0}^{1000} k!$ على العدد 20 هو 14.

ملاحظة: $1 + 3 + 5 + 7 + \dots + (2n-1) = n^2$ وذلك $\forall n \in \mathbb{N}^*$

تمرين (4): أوجد باقي قسمة $x = \sum_{k=1}^{100} x^5$ على العدد 4؟

الحل:

إذا كان a زوجي: $a = 2r \Rightarrow a^5 = 2^5 \times r^5$

$\Rightarrow a^5 \equiv 0 \pmod 4$

إذا كان a فردي عندئذٍ $a^2 \equiv 1 \pmod 4$

$\Rightarrow a^5 = a^2 \times a^2 \times a \equiv 1 \times 1 \times a \pmod 4$

$\Rightarrow a^5 \equiv a \pmod 4$

$x = 1^5 + 2^5 + 3^5 + 4^5 + \dots + 99^5 + 100^5$

$\equiv 1 + 0 + 3 + 0 + 5 + \dots + 99 \pmod 4$

$x \equiv 1 + 3 + 5 + \dots + 99 \pmod 4$

$2n - 1 = 99 \Rightarrow 2n = 100 \Rightarrow n = 50$

$x \equiv (50)^2 \pmod 4 \equiv 0 \pmod 4$

باقي قسمة x على 4 هو صفر

تمرين (5): بيّن بمثال أنّه إذا كان $a^2 \equiv b^2 \pmod n$ فليس من الضروري أن يكون $a \equiv b \pmod n$؟

الحل:

إذا أخذنا $n = 16$ و $b = 3$ و $a = 5$ نلاحظ بأنّ:

TEL:0931497960 - Facebook Group: A to Z مكتبة

$a^2 \equiv b^2 \pmod n$

ولكن $a \not\equiv b \pmod n$

ولذا أخذنا $n=5$ و $b=2$ و $a=3$

نلاحظ بأنّ $a^2 \equiv b^2 \pmod n$

ولكن $a \equiv b \pmod n$

انتهت المحاضرة

TEL:0931497960 - Facebook Group: A to Z مكتبة