المحاضرة التاسعـة

مبرهنة (19):

التطابق قياس n علاقة تكافؤ على $\mathbb{Z}$. أي أن :

(أ) $a \equiv a \pmod{n}$ لكل $a \in \mathbb{Z}$.

(ب) إذا كان $a,b \in \mathbb{Z}$ ، وكان $a \equiv b \pmod{n}$ ، فإن $b \equiv a \pmod{n}$.

(ج) إذا كان $a,b,c \in \mathbb{Z}$ ، وكان $b \equiv c \pmod{n}$ ، $a \equiv b \pmod{n}$ ، فإن $a \equiv c \mod n$.

البرهان:

(أ) بما أن $a - a = 0$ لكـل $a \in \mathbb{Z}$ ، وبمـا أن $n \setminus 0$ لكـل $n \neq 0$. إذاً $a \equiv a$ لكل $a \in \mathbb{Z}$.

(ب) بما أن $a \equiv b \pmod{n}$. إذاً $n \setminus a - b$ ، وعليه يوجد $r \in \mathbb{Z}$ بحيث أن $a - b = nr$ ، وعليه فإن $b - a = n(-r)$ ، $-r \in \mathbb{Z}$ ، وبالتالي فـإن $b \equiv a \pmod{n}$.

(ج) بما أن $a \equiv b \pmod{n}$ و $b \equiv c \pmod{n}$. إذاً يوجد $r,s \in \mathbb{Z}$ بحيث أن $a - b = nr$ ، $b - c = ns$ ، ومنهـا نجـد أن $a - c = n(r+s)$. لكن $r,s \in \mathbb{Z}$. إذاً $a \equiv c \pmod{n}$.

مبرهنة (20):

إذا كـان $a,b,c,d \in \mathbb{Z}$ وكـان $n \in \mathbb{N}^*$ ، $a \equiv b \pmod{n}$ ، $c \equiv d \mod n$ ، فإن :

(أ) $a \mp c \equiv b \mp d \pmod{n}$ ، (ب) $ac \equiv bd \pmod{n}$

(ج) $a+e\equiv b+e(\text{mod}\, n)$ لكل $e\in Z$ ، (د) $ae\equiv be(\text{mod}\, n)$ لكل $e\in Z$

(هـ) $ar+cs\equiv br+ds$ لكل $r,s\in Z$.

البرهان:

(أ) ، (ب) بما أن

$$a\equiv b(\text{mod}\, n)\Rightarrow \exists x\in Z:\ a=b+nx \quad \ldots(1)$$

$$c\equiv d(\text{mod}\, n)\Rightarrow \exists y\in Z:\ c=d+ny \quad \ldots(2)$$

إذا بجمع المعادلتين (1) ، (2) ينتج أن $a+c=b+d+n(x+y)$ لكن $x+y\in Z$. إذاً $a+c\equiv b+d(\text{mod}\, n)$.

وبطرح المعادلة (2) من (1) ينتج أن $a-c=b-d+n(x-y)$ ، $x-y\in Z$. إذاً $a-b\equiv c-d(\text{mod}\, n)$.

وبضرب المعادلتين (1) ، (2) ينتج أن $ac=bd+n(by+xd+nxy)$ لكن $by+xd+nxy\in Z$. إذاً $ac\equiv bd(\text{mod}\, n)$.

(ج) ، (د) بما أن $a\equiv b \bmod n$ ، $e\equiv e\,(\text{mod}\, n)$ لكل $e\in Z$. إذاً $a+e\equiv b+e(\text{mod}\, n)$ و $ae\equiv be(\text{mod}\, n)$ حسب (أ ، ب) .

(هـ) بما أن $a\equiv b(\text{mod}\, n)$ ، $c\equiv d(\text{mod}\, n)$ بالفرض. إذاً $ar\equiv dr(\text{mod}\, n)$ و $cs\equiv ds(\text{mod}\, n)$ لكل $r,s\in Z$ حسب (د) ، وعليه فإن $ar+cs\equiv br+ds(\text{mod}\, n)$ حسب (أ) .

ملاحظة:

إذا كان $ac \equiv bc(\text{mod } n)$ ، فإن $a \not\equiv b(\text{mod } n)$ ، كمـا يوضـح ذلـك المثال الآتي : $7 \times 4 \equiv 6 \times 4(\text{mod } 2)$ بينما $7 \not\equiv 6(\text{mod } 2)$. لكن يمكن أن نبرهن ما يلي :

نتيجة (6):

إذا كان $a,b,c \in Z$ وكان $n \in N^*$ ، $d=(c,n)$ ، فإن $ac \equiv bc(\text{mod } n)$ إذاً وإذا فقط كان $a \equiv b \text{ mod}(\frac{n}{d})$.

نتيجة (7):

إذا كان $a,b,c \in Z$ ، $n \in N^*$ وكان $ac \equiv bc(\text{mod } n)$ ، $(c,n)=1$ ، فإن $a \equiv b(\text{mod } n)$.

مبرهنة (21):

إذا كان $a_i \equiv b_i(\text{mod } n)$ لكل $i=1,\cdots,m$ ، فإن :

$$\sum_{i=1}^{m} a_i \equiv \sum_{i=1}^{m} b_i(\text{mod } n) \quad (\text{أ}) \qquad ، \qquad \prod_{i=1}^{m} a_i \equiv \prod_{i=1}^{m} b_i \quad (\text{ب})$$

مبرهنة (22)

إذا كان $a \equiv b(\text{mod } n)$ وكان $m \in \mathbb{N}^*$ ، فإن $a^m \equiv b^m \,(\text{mod } n)$.

البرهان:

افرض ان $a_i = a$ و $b = b_i$ لكل $i = 1, \cdots, m$ وطبق مبرهنة (14)، تجد ان

$a^m \equiv b^m \,(\text{mod } n)$.

ملاحظة:

اذا كان $a \equiv b \,(\text{mod } n)$ ، فان $ac \equiv bc \,(\text{mod } n)$ حيث ان c اي عدد صحيح، ومن البديهي ان نتساءل هنا فيما اذا كان العكس صحيحاً.

وللإجابة هي **نفي**، وسوف نوضح ذلك من خلال المثال التالي:

لاحظ ان $7 \times 2 \equiv 4 \times 2 = 2 \,(\boldsymbol{mod}\ 6)$ **، ولكن** $7 \not\equiv 4 (\boldsymbol{mod}\ 6)$.

Dr. Ghada M. Al-Naemi