المحاضرة الثامنـة

التطابقات Congruencies

التطابق هو تعبير اخر لمفهوم القسمة، قدم من قبل الالماني جاوس (1777م -1855م)، عام 1801م بطريقة جعلته اداة فعالة لتسهيل البراهين ووسيلة اخرى لدراسة نظرية الاعداد.

تعريف:

إذا كـــان $n \in N^*$ ، $a,b \in Z$ ، فيقـــال عـــن a أنـــه يطـــابق أو يوافـــق (Congruent) b قياس (modulo) n ، ونكتـــب $a \equiv b(\bmod n)$ أو $a \equiv_n b$ إذا كان $a-b$ يقبل القسمة على n .

إذا كان a لا يطابق b قياس n ، فيعبر عن ذلك بالشكل $a \not\equiv b(\bmod n)$.

امثلـة:

(ا)$\mathbf{31 \equiv 1(\boldsymbol{mod}\ 2)}$ ، لان **30=31-1** يقبل القسمة على 2.

(ب) $\mathbf{31 \not\equiv 1(\boldsymbol{mod}\ 4)}$، لان **30=31-1** لايقبل القسمة على 4.

(جـ) $\mathbf{22 \equiv 4(mod\ 9)}$، لان **18=(22-4)** يقبل القسمة على 9.

(د) $\mathbf{3 \equiv -6(\boldsymbol{mod}\ 9)}$، لان **9=(3-(-6))** يقبل القسمة على 9.

(هـ) $\mathbf{13 \not\equiv 5(\boldsymbol{mod}\ 9)}$، لان $\mathbf{13-5=8 \neq 9}$ لايقبل القسمة على 9.

تعريف:

يقـــال أن a قيـــاس n يـــساوي r ، ونكتـــب $a \pmod n = r$ ، إذا كـــان $a = ns + r$ ، $0 \le r < n$.

امثلـة:

(أ) $5 \pmod 3 = 2$ ، لأن $5 = 1 \times 3 + 2$ ، $2 \bmod 3 = 2$ ، لأن $2 = 0 \times 3 + 2$ ، $3 \bmod 3 = 0$ ، لأن $3 = 1 \times 3 + 0$.

(ب) $31 \equiv 1 \pmod 3$ و $31 \pmod 3 = 1$ ، لأن $31 = 10 \times 3 + 1$
$4 \pmod 3 = 1$ ، لأن $4 = 1 \times 3 + 1$ ، وعليه فإن
$31 \pmod 3 = 4 \pmod 3$.

(جـ)

لاحـــــــظ أن $32 \equiv 5 \pmod 9$ وأن $3 \equiv -15 \pmod 9$ ولكـــــن
$22 \not\equiv 5 \pmod 9$. □

مبرهنة (18):

إذا كان $n \in N^*$ ، $a, b \in Z$ ، فإن $a \equiv b \pmod n$ ، إذا وإذا فقط كان $a \pmod n = b \pmod n$. أي أن

$a \equiv b \pmod n \iff$ (باقي قسمة a على n) = (باقي قسمة b على n)

البرهان:

نفرض أن $a \equiv b (\mathrm{mod}\ n)$ ، إذاً $n \backslash a-b$ ، وعليه يوجد $r \in Z$ بحيث أن $a=b+nr$. لكن $b, n \in Z$ إذاً بإستخدام القسمة الخوارزمية يمكننا أن نوجد $m, s \in Z$ بحيث أن $b=mn+s$ ، $0 \le s < n$ ، وعليه فإن $a=(m+r)n+s$ ، $(m+r) \in Z$. إذاً باقي قسمة a على n يساوي باقي قسمة b على n ، وعليه فإن $a\ (\mathrm{mod}\ n)=b (\mathrm{mod}\ n)$.

ولإثبات العكس نفرض أن $a\ (\mathrm{mod}\ n)=b (\mathrm{mod}\ n)$. إذاً $a=nr+t$ ، $b=ns+t$ ، وبالتالي فإن $a-b=(r-s)n$ ، $r-s \in Z$ وهذا يعني أن $n \backslash a-b$ ، وعليه فإن $a \equiv b (\mathrm{mod}\ n)$.

مثال: $19 \equiv -2(mod\ 7)$ و $19=-2+3(7)$.

تعريف:

يقال عن علاقة R على مجموعة A أنها علاقة تكافؤ (Equivalence Relation) على A، إذا كان:

i. R علاقة منعكسة (reflexive) على A، أي أن $\forall a \in A, aRa$.

ii. R علاقة متناظرة (symmetric) ، أي ان اذا كان $a, b \in A$، وكان aRb،فأن bRa.

iii. R علاقة متعدية (transitive)، أي ان اذا كان $a, b, c \in A$، وكان aRb،و bRc، فان aRc.

مثال:

اذا كان لدينا المجموعة $B=\{a, b, c, d\}$، هل العلاقة R تمثل علاقة تكافئ؟

$R=\{(a, a),(b, b),(c, c),(d, d),(b, c),(c, d),(c, b),(d, b)\}.$

الحل:

$a \in B \;\&\; (a,a) \in R$ $b \in B \;\&\; (b,b) \in R$ $c \in B \;\&\; (c,c) \in R$ $d \in B \;\&\; (d,d) \in R$ **اذاً هي انعكاسية**	$(a,a),(b,b),(c,c),(d,d) \in R$ $(b,c) \;\&\; (c,b) \in R$ $(c,d) \in R \;\&\; (d,c) \notin R$ **اذاً هي ليست متناظرة** **اذاً لا تمثل R علاقة تكافئ**	لا نحتاج لإكمال الاختبار حول المتعدية

مثال:

(أ) إذا كانت $A = \{1,2,3\}$ ، فإن كـلاً مـن $R_1 = \{(1,1),(2,2),(3,3)\}$ ،
$R_2 = \{(1,1),(2,2),(3,3),(1,2),(2,1)\}$ ،
$R_3 = \{(1,1),(2,2),(3,3),(1,3),(3,1)\}$ ،
$R_4 = \{(1,1),(2,2),(3,3),(2,3),(3,2)\}$ ،
$R_5 = \{(1,1),(2,2),(3,3),(1,2),(2,1),(1,3),(3,1),(2,3),(3,2)\}$
علاقة تكافؤ على A .

فمثلا لو اننا سوف نقوم باختبار R_5، فنلاحظ ان:

$1 \in A \;\&\; (1,1) \in R_5$ $2 \in A \;\&\; (2,2) \in R_5$ $3 \in A \;\&\; (3,3) \in R_5$ **اذاً هي انعكاسية**	$(1,2) \;\&\; (2,1) \in R_5$ $\Longrightarrow (1,1) \in R_5$ $(2,1) \;\&(1,3) \in R_5$ $\Longrightarrow (2,3) \in R_5$

$(1,1),(2,2),(3,3) \in R_5$ $(1,2)$ & $(2,1) \in R_5$ $(1,3)$ & $(3,1) \in R_5$ $(2,3)$ & $(3,2) \in R_5$ **اذاً هي متناظرة**	$(1,3)$ & $(3,1) \in R_5$ $\Longrightarrow (1,1) \in R_5$ $(2,3)$ & $(3,2) \in R_5$ $\Longrightarrow (2,2) \in R_5$ **اذاً هي متعدية** **اذاً العلاقة $\boldsymbol{R_5}$ تمثل علاقة تكافئ**

على الطالب اختبار بقية العلاقات $(\boldsymbol{R_1, R_2, R_3}$ &$\boldsymbol{R_4})$ المذكورة أعلاه كلاً على حدى.
