بسم الله الرحمن الرحيم.

* التطبيقات:

نقول أن a يطابق b بالمقاس m ونكتب $a \equiv b \pmod{m}$ إذا كان $m \mid a-b$

$m \in N$, $m \geq 1$, $a, b \in \mathbb{Z}$

وإذا كان a لا يطابق b بالمقاس m نكتب $a \not\equiv b \pmod{m} \Leftrightarrow m \nmid b-a$

مثال: $5 \equiv 2 \pmod{3}$

* صفوف البواقي:

$m \in \mathbb{Z}^+$, $m \geq 1$ إذا أخذنا عدد صحيح $n \in \mathbb{Z}$

$\exists r, q$, $n = mq + r$; $0 \leq r < m$

r باقي القسمة يأخذ القيم $0, 1, 2, 3, \ldots, m-1$

نأخذ كل الأعداد الصحيحة التي تترك باقي r في صف باقي فنجد أن الفرق بين أي عددين من هذا الصف يكون بينهما من مضاعفات m.

كل عددين الفرق بينهما يساوي مضاعفات العدد m ينتميان إلى صف واحد.

مثال: $m = 6$ فإن مجموعة البواقي r نأخذ القيم $0, 1, 2, 3, 4, 5$ إذاً للعدد 6 يوجد ستة صفوف بواقي

صف الباقي

$r = 0 \Rightarrow \{ \ldots, -12, -6, 0, 6, 12, 18, \ldots \}$

$r = 1 \Rightarrow \{ \ldots, -17, -11, -5, 1, 7, 13, \ldots \}$

$r = 5 \Rightarrow \{ \ldots, -7, -1, 5, 11, 17, \ldots \}$

كل عدد صحيح يجب أن ينتمي إلى أحد هذه الصفوف وهذه الصفوف تغطي كل الـ Z

تقاطع أي صفين يساوي $\emptyset$

* مجموعة البواقي التامة:

نسمي مجموعة من الأعداد الصحيحة والتي عددها m وكل عنصر ينتمي إلى صف باقي واحد مجموعة بواقي تامة.

$m = 6$ $\{-6, 1, 2, -9, -2, -7\}$

/ /

الموضوع : .....

كذلك $\{0,1,2,3,4,5\}$ مجموعة بواقي رئيسية.

إذا كان $a \equiv b \pmod m \Leftarrow a, b$ ينتميان إلى نفس الصف

و $a \not\equiv b \pmod m \Leftarrow a, b$ ينتميان إلى صفين مختلفين

* نتيجة:

$n = mq + r \Rightarrow n - r = mq \Leftarrow m \mid n-r \Rightarrow m \equiv r \pmod m$

كل عدد يطابق باقي قسمته على العدد m.

* خواص المطابقة:

1) علاقة المطابقة تحقق علاقة التكافؤ: $\forall a,b,c,d \in \mathbb{Z} \; ; \; n \geq 1$

$a \equiv a \pmod m$

2) إذا كان $a \equiv b \pmod m$ ؛ $b \equiv c \pmod m$

$\Rightarrow a \equiv c \pmod m$

3) $b \equiv a \pmod m \Leftarrow a \equiv b \pmod m$

4) إذا كان

$k \in \mathbb{Z} \; ; \; a \equiv b \pmod m$

$\Rightarrow k.a \equiv kb \pmod m$

5) إذا كان

$\begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases} \Rightarrow$

أ) $a + c \equiv b + d \pmod m$

ب) $a.c \equiv b.d \pmod m$

6) إذا كان $a \equiv b \pmod m$ فإن:

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

7) إذا كان $a \equiv b \pmod m$ وكان لدينا $F(x) = \sum_{i=0}^{n} a_i x^i \; ; \; a_i \in \mathbb{Z}$

فإن: $F(a) = F(b) \pmod m$

* مثال:

$z \equiv -n \pmod 6$

$f(n) = x^2 - x + 5$

$f(2) = 4 - 2 + 5 = 7$
$f(-4) = 16 + 4 + 5 = 25$
$\Rightarrow 7 \equiv 25 \pmod 6$
$f(2) \equiv 25 \pmod 6$
$\Rightarrow f(2) \equiv f(-4) \pmod m$

8) إذا كان $k.a \equiv k.b \pmod m$
وكان $d = (k,m)$ فإن $a \equiv b \pmod{\frac{m}{d}}$

البرهان:
$d(m,k) \Leftarrow m = dm_0$, $(m_0, R_0) = 1$
$k = dk_0$

$k.a \equiv k.b \pmod m \Rightarrow m \mid k(a-b)$
$m_0 d \mid k_0 d (a-b) \Rightarrow m_0 \mid R_0 (a-b)$

بما أن $(m_0, R_0) = 1$
أي $m_0 \mid (a-b)$

$\Rightarrow a \equiv b \pmod{m_0} \Rightarrow a \equiv b \pmod{\frac{m}{d}}$

* مثال:

$10 \equiv 4 \pmod 6 \Rightarrow \frac{10}{2} \equiv \frac{4}{2} \pmod{\frac{6}{2}}$
$5 \equiv 2 \pmod 3$

* $R.a \equiv k.b \pmod p$
$a \equiv b \pmod p$ فإن $p \nmid k$ و p عدد أولي
أي إذا كان $(k,m) = 1$ « أوليين » و $k.a \equiv k.b \pmod m$
فإن $a \equiv b \pmod m$

9) إذا كان $a \equiv b \pmod m$ فإن $a \equiv b \pmod n$ حيث $n \mid m$

10) إذا كان $a \equiv b \pmod{m_i}$; $m_i \in \mathbb{Z}$ فإن: $\forall i = 1, 2, \dots, k$
$a \equiv b \pmod m$; $m = l.c.m(m_1, m_2, \dots, m_k)$

إذا كان $n = p_1^{q_1} ; p_2^{q_2} \dots p_k^{q_k}$ فإن
$a \equiv b \pmod n$ فإن $a \equiv b \pmod{p_i^{r_i}}$

11) إذا كان $a \equiv b \pmod{p^r}$; $r \geq 1$ فإن $a, b \in \mathbb{Z}$ عدد أولي p .

الموضوع: .... / /

فإنّ $a^{p^s} \equiv b^{p^s} \pmod{p^{r+s}}$; $s \geq 0$

الإثبات:

نستخدم الاستقراء الرياضي

1- خطوة البداية: $s=0 \Leftarrow a \equiv b \pmod{m}$

2- خطوة الاستقراء نفرض صحتها من أجل $s=k \geq 0$ ولنفرض التطابقة صحيحة من أجل

$a^{p^k} \equiv b^{p^k} \pmod{p^{k+r}}$

ولنثبت صحة التطابقة من أجل $s=k+1$ أي أنّ

$a^{p^{k+1}} \equiv b^{p^{k+1}} \pmod{p^{r+k+1}}$

$a^{p^k} \equiv b^{p^k} \pmod{p^{r+k}} \Leftrightarrow a^{p^k} - b^{p^k} = M p^{r+k}$

$a^{p^k} = b^{p^k} + M p^{r+k}$

$(a^{p^k})^p = a^{p^{k+1}} = (b^{p^k} + M p^{r+k})^p$

$b^{p^{k+1}} + \frac{p}{1!} b^{p^k(p-1)} \cdot M p^{r+k} + \frac{p(p-1)}{2!} b^{p^k(p-2)} M^2 (p)^{(r+k)\cdot 2} + \cdots$

حوى p ابتداءً من الحد الثاني:

$r+k+1$, $2+2(r+k)$, $2r+2k+1$ وهكذا!

~~حوى p ابتداءً من الحد الثاني~~ إذا أخذنا بالمقياس p^{r+k+1} ابتداءً من الحد الثاني

كل حد يطابق بالمقياس p^{r+k+1}

$a^{p^{k+1}} \equiv b^{k+1} \pmod{p^{r+k+1}}$

أي التطابقة صحيحة من أجل $s=k+1$

وبالتالي صحيح من أجل $s \geq 0$

وانتهت المحاضرة

yehia . D