التطابقات

تعريف: ليكن $a,b \in \mathbb{Z}$ و $m \in \mathbb{Z}^+$ نقول إن العدد a يطابق b بالمقاس m ونكتب $a \equiv b \pmod{m}$ إذا كان $m \mid a-b$ وإذا كان $m \nmid a-b$ فإننا نقول إن a لا يطابق b بالمقاس m ونكتب $a \not\equiv b \pmod{m}$

مثال: $37 \equiv 2 \pmod{7}$

صفوف البواقي: $m \in \mathbb{Z}^+$ و $n \in \mathbb{Z}$ فإنه يوجد عددان وحيدان q, r بحيث يكون: $n = mq + r$ ، $0 \le r < m$ القيم التي يأخذها r هي: $r_i = 0, 1, 2, \dots, m-1$ عدد ها m لنضع جميع الأعداد الصحيحة التي باقي قسمتها على m يساوي أحد الأعداد r_i في صف واحد نسميه صف الباقي r_i فنحصل بالتالي على m من هذه الصفوف ونلاحظ أنه إذا كان الفرق بين عددين صحيحين مضاعفاً لـ m فإنهما يقعان في صف واحد وأن الفرق بين أي عددين من صف واحد هو مضاعف لـ m نسمي هذه الصفوف صفوف البواقي للعدد m

مثال: $m = 6 \Rightarrow$ صفوف البواقي هي $0, 1, 2, 3, 4, 5$

صف الباقي $r=0$ هو $\{\dots, -12, -6, 0, 6, 12, \dots\}$

صف الباقي $r=1$ هو $\{\dots, -11, -5, 1, 7, 13, \dots\}$

صف الباقي $r=2$ هو $\{\dots, -10, -4, 2, 8, 14, \dots\}$

صف الباقي $r=3$ هو $\{\dots, -9, -3, 3, 9, 15, \dots\}$

صف الباقي $r=4$ هو $\{\dots, -8, -2, 4, 10, 16, \dots\}$

صف الباقي $r=5$ هو $\{\dots, -7, -1, 5, 11, 17, \dots\}$

مجموعة البواقي التامة:

نسمي مجموعة الأعداد الصحيحة A التي عددها m وكل عنصر فيها ينتمي إلى صف باقي واحد بالمقاس m، مجموعة البواقي بالمقاس m هي:

$A = \{0, 1, 2, \dots, m-1\}$

مثال: $m = 5 \Rightarrow A = \{0, 1, 2, 3, 4\}$

هل A_1 مجموعة بواقي تامة؟ $A_1 = \{0, 11, 22, 33, 59\}$

الجواب: نعم، A_1 مجموعة بواقي تامة.

★ المجموعة $A = \{0, 1, 2, \dots, m-1\}$ نسميها مجموعة البواقي التامة الصغرى

مثال جانبي: $-500 \equiv 4 \pmod 6$ ⟸ -500 ينتمي إلى صف الباقي 4 للمقاس 6.

$500 \equiv 2 \pmod 6$ ⟸ 500 ينتمي إلى صف الباقي 2 بالمقاس 6.

كنتيجة: إذا كان $a \equiv b \pmod n$ فإن a, b ينتميان إلى صف باقي واحد

إذا كان $n = mq + r$ ، $0 \le r < n$ ⟸ $n \equiv r \pmod m$

$n - r = mq \Rightarrow m \backslash n - r$.

خواص التطابقات:

أ- التطابق ($\equiv$) علاقة تكافؤ أي:

1) $a \equiv a \pmod m$ ؛ $a \in \mathbb{Z}$ "انعكاسية"

2) $a \equiv b \pmod m \Longrightarrow b \equiv a \pmod m$ "تناظرية"

3) $a \equiv b \pmod m \wedge b \equiv c \pmod m \Longrightarrow a \equiv c \pmod m$ "متعدية"

ب- إذا كان $a \equiv b \pmod m$ ، $k \in \mathbb{Z}$

فإن: $k.a \equiv k.b \pmod m$

جـ- إذا كان $a \equiv b \pmod m \wedge c \equiv d \pmod m$

فإن: $a \pm c \equiv b \pm d \pmod m$

د- إذا: 1) $a \equiv b \pmod m$ ، 2) $c \equiv d \pmod m$ ⟸ $a.c \equiv b.d \pmod m$.

لأنه من 1) و ب $\times c$ ⟸ $c.a \equiv c.b \pmod m$ وحسب خاصية المتعدية يكون

من 2) $\xleftarrow{(\times b)}$ $c.b \equiv b.d \pmod m$ ⟸ $a.c \equiv b.d \pmod m$

هـ- إذا كان $a \equiv b \pmod m$ فإن $a^n \equiv b^n \pmod m$ ؛ $n \geq 1$

ز- إذا كان $a \equiv b \pmod m$ و الدالة $f(x) = \sum_{i=1}^{n} a_i x^i$ "متسلسلة منتهية"

فإن: $f(a) \equiv f(b) \pmod m$

حسب هـ- $a \equiv b \pmod m$ فإن $a^i \equiv b^i \pmod m$

و لنضرب الطرفين بقيمة عددية a_i:

$a_i a^i \equiv a_i b^i \pmod m$ ، $(i = 1, \dots, n)$

$$\sum_{i=1}^{n} a_i a^i \equiv \sum_{i=1}^{n} a_i b^i \pmod m$$

⟸ $f(a) \equiv f(b) \pmod m$

الموضوع: ....

/ /

ع) إذا كان $K.a \equiv K.b \pmod{m}$ (*) , $(k,m)=d$

فإن :
$$a \equiv b \left(\bmod \frac{m}{d}\right)$$

لأنّ : بما أن $d=(k,m)$ فيمكن أن نكتب :

$K=K_0 d \quad , m=m_0 d$

و $(K_0,m_0)=1$ ، وبما أن $K.a=K.b \pmod{m}$:

فإن : $K(a-b)=Mm \Leftarrow K_0 . d(a-b)=Mm_0 . d$

أي أن $K_0(a-b)=Mm_0$ $m_0 \backslash K_0(a-b)$

ولما كان $(K_0,m_0)=1$ ينتج أن : $m_0 \backslash a-b$

أي $a \equiv b \pmod{m_0}$ حيث $m_0=\frac{m}{d}$

أما إذا كان $(k,m)=1 \Leftarrow a \equiv b \pmod{m}$

مثال : $10 \equiv 6 \pmod{4} \Leftarrow 5 \not\equiv 3 \pmod{4}$

$(10,4)=2=d \Leftarrow 5 \equiv 3 \pmod{2}$

ص) إذا كان $a \equiv b \pmod{m}$ ∧ $n \backslash m$ فإن : $a \equiv b \pmod{n}$ ؟2 سؤال مو لازم نكتب

ك) المضاعف :

إذا كان $a \equiv b \pmod{m_i}$ ، $i=1,\dots,k$: $a,b \in \mathbb{Z}, m_i \in \mathbb{Z}^+$

فإن : $a \equiv b \pmod{m}$ ؛ $m=L.C.M(m_1,\dots,m_k)$

وإذا كان m_i أولية مثنى مثنى أي هي أولية فيما بينها فإنّ :

$m=m_1 . m_2 \dots m_k$

نتيجة : إذا كان : $m=P_1^{\alpha_1} . P_2^{\alpha_2} \dots P_r^{\alpha_r}$

فإن : $a \equiv b \pmod{P_i^{\alpha_i}} \Leftarrow a \equiv b \pmod{m}$ حيث $i=1,\dots,k$

ق) إذا كان $a \equiv b \pmod{P^r}$: $r \geq 1$ وأولي P

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

الإثبات : بطريقة الاستقراء الرياضي

الخطوة الأساسية : من أجل $S=0 \Leftarrow a=b \pmod{P^r}$ محققة

خطوة الاستقراء : لنفرض العلاقة صحيحة من أجل $S=k$

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

ولنثبت صحتها من أجل $S=k+1$

24

لدينا: $a^{p^k} - b^{p^k} = M.p^{r+k}$

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

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

نفكها بطريقة ثنائي الحد نيوتن:

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

$+ \cdots + M^p(p^{r+k})^p$

نلاحظ أن قوى p ابتداءً من الحد الثاني هي:

$r+k+1$ و $2r+2k+1$ و ...

حتى $2r+2k$ وجميعها أكبر من $r+k+1$

إذاً: جميع الحدود ابتداءً من الحد الثاني يترك صفراً بالمقاس p^{r+k+1}

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

وبالتالي محققة

أي العلاقة صحيحة من أجل $s \geq 0$

ملاحظة إضافية: يقبل العدد القسمة على 9 إذا كان مجموع أرقامه من مضاعفات الرقم 9

يقبل العدد $N = a + 10b$ القسمة على 7 إذا قبل العدد $b - 2a$ القسمة على 7

مثال: العدد $N = 3741$ فإن $N = 1 + 10(374)$ ومنه

$b - 2a = 374 - 2 = 372$ نطبق مرة أخرى

$372 = 2 + 10(37)$

وبما أن $b - 2a = 37 - 4 = 33$ فإن $7 \nmid 33$ $7 \nmid N$ (لا يقبل N القسمة على 7)

مثال آخر: العدد 1470 فإن $N = 0 + (147)10$

ومنه $b - 2a = 147 - 0 = 147$ نطبق مرة أخرى:

$147 = 7 + 10(14)$

ومنه $b - 2a = 14 - 14 = 0$ ومنه فإن $7 \mid N$

(N يقبل القسمة على 7)

تمرين (1) :

اثبت أن الفرق بين أي عدد صحيح N بالنظام العشري ومجموع أرقامه يقبل القسمة على 9

$$N = \sum_{i=0}^{n} a_i 10^i = a_0 + a_1 \times 10 + \cdots + a_n \times 10^n$$

$$10 \equiv 1 \pmod 9$$

$$10^i \equiv 1 \pmod 9$$

$$a_i 10^i \equiv a_i \pmod 9 \qquad : i = 0, 1, \ldots, n$$

$$N \equiv \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i \pmod 9$$

$$N - \sum_{i=0}^{n} a_i \equiv \pmod 9$$

مثال :
$$N = 3741 = 1 + 4\times 10 + 7\times 10^2 + 3\times 10^3$$

$$N = 3741 \equiv 1+4+7+3 \pmod 9 \longrightarrow N = 3741 \equiv 15 \pmod 9$$

$$3741 - 15 = 3726 \equiv 0 \pmod 9$$

★ لمعرفة ميزان عدد: نحذف من مجموع أرقامه 9 أو مضاعفها مثلاً ميزان

3741 هو $15 - 9 = 6$

مثال : أوجد أصغر عدد صحيح موجب k يحقق العلاقة :

$$31 \backslash 33(26)^2 - k \qquad \text{أي } "33(26)^2 \equiv k \pmod{31}"$$

$$33 \equiv 2 \pmod{31}$$

$$26 \equiv -5 \pmod{31} \Longrightarrow 26^2 \equiv 25 \pmod{31}$$

$$(33)(26)^2 \equiv 50 \pmod{31}$$

$$(33)(26) \equiv 19 \pmod{31} \longrightarrow k = 19$$

مثال : أوجد باقي قسمة $\sum_{i=1}^{1000} k!$ على 24

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

$$4! = 24 \ , 5! = 24.5$$

$$\sum_{i=1}^{1000} k! \equiv 1 + 2 + 6 + 0 \pmod{24} \equiv 9 \pmod{24}$$

حل تمارين الكتاب ص 46

5) هل العبارات التالية صحيحة أم خاطئة وإذا كانت صحيحة فأثبت صحتها وإن كانت خاطئة فأعط مثال يبين ذلك.

① إذا كان $a\mid b$, $a\mid c \Rightarrow a^2\mid bc$

الحل: بما أن $a\mid b \Rightarrow b=k_1.a \;;\; k_1\in\mathbb{Z}$

و بما أن $a\mid c \Rightarrow c=k_2.a \;;\; k_2\in\mathbb{Z}$

صحيحة ^^ $\Rightarrow b.c=k_1.k_2.a^2 \Rightarrow a^2\mid b.c$

② إذا كان $a\mid b \Leftrightarrow ac\mid b.c$ حيث $c\neq 0$ صحيحة وضوحاً

③ إذا كان $a\mid b+c$ فإن إما $a\mid b$ أو $a\mid c$ خاطئة

مثال: $3\mid 5+4$ ولكن $3\nmid 5$, $3\nmid 4$

④ إذا كان $a\mid b^2+1$ فإن $a\mid b^4+1$ خاطئة

مثال: $5\mid 3^2+1$ ولكن $5\nmid 3^4+1=82$

⑤ إذا كان $a^2\mid b^3$ فإن $a\mid b$ خاطئة

$8^2\mid 4^3$ ولكن $8\nmid 4$

⑥ إذا كان $a^2\mid n \wedge b^2\mid n \wedge a^2\le b^2 \Rightarrow a\mid b$ خاطئة

$2^2\mid 36 \wedge 3^2\mid 36 \wedge 2^2\le 3^2$ ولكن $\not\Rightarrow 2\mid 3$

إذ أن $2\nmid 3$

⑨ $gcd(198,288,512)=198x+288y+512z$

الحل:

$512=288\times 1+224$

$288=224\times 1+64$

$224=64\times 3+32$

$64=32\times 2+0 \longrightarrow gcd(512,288)=32$

$198=6\cdot 32+6$

$32=6\times 5+2$

$6=3\times 2+0$

$\Rightarrow gcd(198,288,512)=2$

$2=1\times 32-5\cdot 6$

$2 = 1\times 32 - 5(198 - 6\times 32)$
$= -5\cdot 198 + 31\times 32$
$= -5\times 198 + 31(224 - 3\times 64)$
$= -5\times 198 + 31\times 224 - 93\times 64$
$= -5\times 198 + 31\times 224 - 93(288 - 1\times 224)$
$= -5\times 198 + 124\times 224 - 93\times 288$
$= -5\times 198 + 124(512 - 1\times 288) - 93\times 288$

$$= \underbrace{-5}_{x}\times 198 \underbrace{- 217}_{y}\times 288 + \underbrace{124}_{z}\times 512$$

$x = -5$, $y = -217$, $z = 124$

أوجد الحلول الموجبة للمعادلات:

$221x + 91y = 117$

$$\left.\begin{aligned} 221 &= 2\times 91 + 39 \\ 91 &= 2\times 39 + 13 \\ 39 &= 3\times 13 + 0 \end{aligned}\right\} \rightarrow d = (221, 91) = 13$$

إذن المعادلة حل $13 \mid 117 = 13\times 9$

$13 = 91 - 2\times 39$
$= 91 - 2(221 - 2\times 91)$
$13 = -2\times 221 + 5\times 91$

نضرب الطرفين بـ 9: $117 = (-18)(221) + (45)(91)$

إذن إن: $(-18, 45)$ حل المعادلة: $x_0 = -18$, $y_0 = 45$

وجميع الحلول تعطى بالعلاقات:

$x = x_0 + \frac{b}{d}t = -18 + 7t$

$y = y_0 - \frac{a}{d}t = 45 - 17t$

$$\left.\begin{aligned} -18 + 7t > 0 &\longrightarrow t > \frac{18}{7} = 2\frac{4}{7} \\ 45 - 17t > 0 &\longrightarrow t < \frac{45}{17} = 2\frac{11}{17} \end{aligned}\right\} \longrightarrow 2\frac{4}{7} < t < 2\frac{11}{17}$$

إذن لا توجد حلول موجبة للمعادلة

28

4) أوجد جميع ثلاثيات فيثاغورث من أجل $y=28$

$y=28=2(r.s) \longrightarrow r.s=14$

لدينا الشكل:

① $r=14$ ، $s=1$ $\longleftarrow$ $(r^2-s^2, 2rs, r^2+s^2)$

$(195,28,197)$

② $r=7$ ، $s=2$ $\longleftarrow$ $(45,28,53)$

إذا كان: $Z=125 \longleftarrow Z=r^2+s^2=10^2+5^2$

$\Longrightarrow r=10, s=5$ مرفوضة r,s أوليان فيما بينهما

مقبولة $Z=(11)^2+(2)^2$; $r=11, s=2$

$x=r^2-s^2=121-4=117$

$y=2.r.s=2(11)(2)=44$

$(117,44,125)$

إذا كان: $x=21$

$x=r^2-s^2=21$

$r^2-s^2=(r+s)(r-s)=21$

① $r+s=7$, $r-s=3$

$2r=10 \longrightarrow r=5$

$2s=4 \longrightarrow s=2$

مقبولة إذاً،

الثلاثية $(21, 20, 29)$

② $r+s=21$, $r-s=1$

$2r=22 \longrightarrow r=11$

$2s=20 \longrightarrow s=10$

r,s أوليان فيما بينهما مقبولة ^^

الثلاثية $(21,220,221)$

التطابقات الخطية $ax\equiv b \pmod m$ والمطلوب إيجاد قيمة x

نفرض أن التطابقة حل x_0: $ax_0\equiv b \pmod m$

وهي معادلة ديوفانتس: $ax_0-b=my_0 \Longrightarrow ax_0-my_0=b$

يؤول حل التطابق الخطي $ax\equiv b \pmod m$ إلى حل معادلة ديوفانتس $ax-my=b$

شرط $d=(a,m)$ تقسم b

انتهت المحاضرة