3rd May

Tuesday, May 3, 2022 2:10 PM

DIVISIBILITY AND STUFF

★ we write $a|b$ iff $\exists c \in \mathbb{Z}$ st $b=ac$

$2|6 \quad \exists c \in \mathbb{Z} \quad 6 = 2\cdot 3$ ($c=3$)

$15|60 \quad 60 = 15\cdot 4$

★ we write "$a \equiv b \bmod m$" iff $m|a-b$ ✓✓

$2 \equiv 7 \bmod 5 \rightarrow 5|2-7 \Rightarrow 5|-5$ ($r=2$, $r=2$; -5)

$17 \equiv 3 \bmod 7$ ($r=3$, $r=3$) $\quad 7|17-3=14$

★ $x \equiv a \bmod m \Rightarrow x = a+mk \quad k \in \mathbb{Z}$

$x \equiv 2 \bmod 5 \Rightarrow 5|x-2 \Rightarrow x-2=5c \Rightarrow x=2+5c$

$x \equiv 3 \bmod 10 \Rightarrow x = 3+10k \quad k \in \mathbb{Z}$

$k=5 \quad x=53$

★ If $a \equiv b \bmod m$ then $a \pm c \equiv b \pm c \bmod m$

$17 \equiv 3 \bmod 7 \Rightarrow 17+5 \equiv 3+5 \bmod 7 \Rightarrow 22 \equiv 8 \bmod 7$ ($\times 3$, $\times 3$)

$\Rightarrow 7|22-8=14$

★ If $a \equiv b \bmod m$ then $ac \equiv bc \bmod m$

$\Rightarrow 51 \equiv 9 \bmod 7 \equiv 2 \bmod 7 \Rightarrow 51 \equiv 2 \bmod 7$

★ If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $ac \equiv bd \bmod m$ and $a \pm c \equiv b \pm d \bmod m$ ⟺ $a=b$, $c=d$

$a \pm c = b \pm d$

$ac = bd$

★ If $\gcd(m,c)=1$ and $ac \equiv bc \bmod m$ then $a \equiv b \bmod m$

$a\cancel{c} = b\cancel{c} \Rightarrow a=b$

$51 \equiv 9 \bmod 7 \Rightarrow 3\cdot 17 \equiv 3\cdot 3 \bmod 7$

$\Rightarrow 17 \equiv 3 \bmod 7$

$2\cdot 3 \equiv 0 \bmod 6$

$2\cdot 3 \equiv 2\cdot 0 \bmod 6$

⚠ $\Rightarrow 3 \equiv 0 \bmod 6$ ✗

★ If $a \equiv b \bmod m$ then $a^n \equiv b^n \bmod m$

Pf:- Given:- $a \equiv b \bmod m \Leftrightarrow m \mid a-b$

RTP:- $a^n \equiv b^n \bmod m \Leftrightarrow m \mid a^n - b^n$

$m \mid a-b \Rightarrow a-b = cm$

$\Rightarrow (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}) = \underbrace{c(a^{n-1} + \cdots + b^{n-1})}_{c'} m$

$\Rightarrow a^n - b^n = c'm$

$\Rightarrow m \mid a^n - b^n \Rightarrow a^n \equiv b^n \bmod m$

Q. What is the remainder when 77^{89} is divided by 5?

→ $77 \equiv 2 \bmod 5 \Rightarrow 77^{89} \equiv 2^{89} \bmod 5$

$\equiv 2^{89} \equiv (2^4)^{22}\, 2 \bmod 5$

$\equiv \boxed{2} \bmod 5$

★ Modular Inverse :- [$5x \equiv 1 \bmod 7 \Rightarrow x \equiv ? \bmod 7$]

If $\gcd(a,m) = 1$ then $\exists!\ b$, s.t. $0 \le b < m$.

and $ab \equiv 1 \bmod m$.

"b" is called modular inverse of a mod m.

$a=5 \quad m=7 \quad \gcd(a,m) = 1 \quad 5b \equiv 1 \bmod 7$

$b = 3$ ✓

b	5b	5b mod 7
0	0	0
1	5	5
2	10	3
(3)	15	1 ←
4	20	6
5	25	4
6	30	2

Pf:- $\gcd(a,m) = 1$

$\exists\, x, y \in \mathbb{Z} \quad ax + my = 1$

$\Rightarrow ax = 1 \bmod m$

$(ax + my) \bmod m \equiv 1 \bmod m$ ∎

$\Rightarrow (ax) \bmod m + \underbrace{my \bmod m}_{=0} \equiv 1 \bmod m$

$\left(\begin{array}{c|c|c} 5 & 25 & 4 \\ 6 & 30 & 2 \end{array}\right)$

$\Rightarrow (ax) \bmod m + \underbrace{my \bmod m}_{=0} \equiv 1 \bmod m$

$\Rightarrow ax \equiv 1 \bmod m.$

★ CRT (Chinese Remainder Theorem):-

$(\mathbb{Z}/pq\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$

The system of congruences $x \equiv a_1 \bmod m_1$ and $x \equiv a_2 \bmod m_2$ has a unique soln. modulo $m_1 m_2$ if $\gcd(m_1, m_2) = 1$.

→ $m_1 = 3$, $m_2 = 5$ $a_1 = 2$ $a_2 = 3$

$x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 5$ $x \equiv ? \bmod 15$

Pf:- Let $a = m_1 a_2 (m_1)^{-1}_{m_2} + m_2 a_1 (m_2)^{-1}_{m_1}$

$(m_1)^{-1}_{m_2} = x$: $m_1 x \equiv 1 \bmod m_2$

$a \equiv m_2 a_1 (m_2)^{-1}_{m_1} \bmod m_1$

$\equiv a_1 \bmod m_1$

$a \equiv m_1 a_2 (m_1)^{-1}_{m_2} \equiv a_2 \bmod m_2$

$x \equiv m_1 a_2 (m_1)^{-1}_{m_2} + m_2 a_1 (m_2)^{-1}_{m_1} \bmod m_1 m_2$

$x \equiv 2 \bmod 3$ $x \equiv 3 \bmod 5$, $m_1 = 3$ $m_2 = 5$

$a_1 = 2$ $a_2 = 3$

$(3^{-1})_5 = ? = 2$ $(5)^{-1}_3 = ? = 2$

$x \equiv 3 \times 3 \times 2 + 5 \times 2 \times 2 \bmod 15$

$\equiv 18 + 20 \bmod 15 \equiv 38 \bmod 15 \equiv \underline{8} \bmod 15$

★ Complete Residue System:- A set S is said to be a complete residue system modulo m if $\forall x \in \mathbb{Z}\ \exists y \in S$ such that $x \equiv y \bmod m$. $|S| = m$

Ex:- $m = 5$ then $S = \{0, 1, 2, 3, 4\}$ $17 \bmod 5 = 2$

$= \{6, 7, 8, 9, 10\} = \{1, 7, 8, 4, 0\}$

$\downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow$

$1\ \ 2\ \ 3\ \ 4\ \ 0$

★ If $S = \{a_1, \ldots, a_m\}$ is complete residue system mod m

★ If $S = \{a_1, \ldots, a_m\}$ is complete residue system mod m
then $S' = \{ ka_i + b : 1 \le i \le m, \gcd(k, m) = 1, b \in \mathbb{Z} \}$
is also a complete residue system mod m.

$S' = \{3, 5, 7, 9, 11\} \rightarrow$ complete residue syst mod 5
$= 2\{0, 1, 2, 3, 4\} + 3$

★ Reduced Residue System :- A set R is said to be a reduced residue system mod m if $R = \{ r_i : 1 \le i \le \phi(m) \}$ st $\gcd(r_i, m) = 1 \ \forall i$ and $r_i \not\equiv r_j \bmod m$ whenever $i \neq j$.

★ "Euler's" totient function :- $\phi : \mathbb{N} \rightarrow \mathbb{N}$

$\phi(n)$ = the number of elements between 1 and n which are coprime to n.

$\phi(6) = 2$
$\phi(5) = 4$

$\{1, 2, 3, 4, 5, 6\}$
✓ ✗ ✗ ✗ ✓ ✗

$\{1, 2, 3, 4, 5\}$
✓ ✓ ✓ ✓ ✗

Reduced Residue System mod 6 $\rightarrow \{1, 5\}$
" " " " 5 $\rightarrow \{1, 2, 3, 4\}$
$\downarrow$
$\{3, 7, 9, 12\}$ ✓✓

★ If $R = \{a_1, \ldots, a_{\phi(m)}\}$ is a reduced residue system mod m and if $k \in \mathbb{Z}$ is such that $\gcd(k, m) = 1$, then $R' = \{ ka_1, ka_2, \ldots, ka_{\phi(m)} \}$ is also a reduced residue system.

Pf :- (i) $|R'| = \phi(m) \rightarrow ka_i \not\equiv ka_j \bmod m$ if $i \neq j \bmod m$

(ii) $\gcd(ka_i, m) = 1$

(i) $\rightarrow$ Suppose $ka_i \equiv ka_j \bmod m \Rightarrow m \mid k(a_i - a_j)$, WLOG assume $a_i > a_j$

$\Rightarrow m \mid (a_i - a_j) \Rightarrow \boxed{m \le (a_i - a_j)}$

$1 \le a_i - a_j < m \rightarrow \boxed{a_i - a_j \le m}$

$\Rightarrow m \mid (a_i - a_j) \Rightarrow \boxed{m \leq (a_i - a_j)}$

and $0 \leq a_j < a_i \leq m \Rightarrow \boxed{a_i - a_j \leq m}$

$\Rightarrow a_i - a_j = m \Rightarrow a_i \equiv a_j \bmod m$ ($\Leftarrow$) ■

(ii) $\gcd(ka_i, m) = 1$

suppose $\gcd(ka_i, m) = g > 1$

$\Rightarrow g \mid ka_i$ and $g \mid m$

$\Rightarrow g \mid a_i$ and $g \mid m$

$\Rightarrow g \mid \gcd(a_i, m) = 1 \Rightarrow g = 1$ ($\Leftarrow$) □

* **Euler's theorem:-** If $\gcd(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \bmod m$$

Pf:- $R = \{a_1, \ldots, a_{\phi(m)}\}$, $R' = \{aa_1, \ldots, aa_{\phi(m)}\}$

$\prod R \equiv \prod R' \bmod m$

$\Rightarrow a_1 \cdot a_2 \cdots a_{\phi(m)} \equiv aa_1 \cdot aa_2 \cdots aa_{\phi(m)} \bmod m$

$\Rightarrow 1 \equiv a^{\phi(m)} \bmod m$ ■

* **Fermat's theorem:-** If p is a prime and $\gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \bmod p.$$

Pf:- $a^{\phi(p)} \equiv 1 \bmod p$

RTP:- $\boxed{\phi(p) = p - 1}$ $\Rightarrow a^{p-1} \equiv 1 \bmod p$

* **Multiplicative function:-** An arithmetic function ($f : \mathbb{N} \to \mathbb{C}$) is called multiplicative if $f(mn) = f(m) f(n)$ whenever $\gcd(m, n) = 1$.

* **Claim:-** ϕ is multiplicative. i.e if $\gcd(m, n)$ then

$$\phi(mn) = \phi(n)\,\phi(m)$$

$$\phi(mn) = \phi(n)\,\phi(m)$$

Pf:-

$$S = \begin{bmatrix} 1 & 2 & \cdots & j & \cdots & m \\ m+1 & m+2 & & m+j & & 2m \\ \vdots & & & & & \vdots \\ (i-1)m+1 & (i-1)m+2 & \cdots & (i-1)m+j & & im \\ \vdots & & & & & \vdots \\ (n-1)m+1 & & & (n-1)m+j & & nm \end{bmatrix}$$

If $\gcd(j, m) = 1$ then all elements of the column will be coprime to m. There are $\phi(m)$ such columns.

$S = \{ m\cdot 0 + j,\ m\cdot 1 + j,\ \ldots\ m\cdot(n-1)+j \}$

$S' = \{ 0, 1, \ldots, n-1 \} \rightarrow$ CRS mod n.

It contains $\phi(n)$ elements coprime to n.

So we have $\phi(m)\,\phi(n)$ elements in the matrix which are coprime to mn.

$$\Rightarrow \phi(mn) = \phi(m)\,\phi(n) \quad \text{if } \gcd(m,n) = 1$$ ∎

* $\phi(p^k)$ ⇒ $S = \{ 1\cdot p, 2\cdot p, \ldots, p^{k-1} p \}$ $|S| = p^{k-1}$

$$\phi(p^k) = p^k - p^{k-1}$$

* $\phi(100) = \phi(2^2 5^2) = \phi(2^2)\,\phi(5^2) = (2^2 - 2)(5^2 - 5)$

$= 2 \times 20 = 40$

$\phi(100)$

57 $\quad 57^{40} \equiv 1 \bmod 100$ ∎