1. Modulus of a number:

$29 \bmod 6 = 5$

$$\begin{array}{r} 4 \\ 6\overline{)\,29} \\ -24 \\ \hline 5 \end{array}$$

$\therefore\ 29 = 6 \times 4 + 5$

i.e. Dividend = Divisor x Quotient + Remainder

2. Modulus of Negative number:

$-29 \bmod 6 = ?$

$-29 = 6 \times (-4) + (-5)$

Here, we got negative remainder,
but we want positive remainder,

$\therefore\ -29 = 6 \times (-5) + \boxed{1}$ ← positive remainder

Note:- To get positive remainder,

(i) Add negative remainder to divisor
i.e. $6 + (-5) = 6 - 5 = 1$

(ii) Subtract 1 from negative quotient
i.e. $-4 - 1 = -5$

Hence, we get,
$-29 = 6 \times (-5) + 1$ $\quad \therefore\ -29 \bmod 6 = 1$

few more examples:

$9 \bmod 10 = 9$ $\quad$ i.e. $9 = 10 \times 0 + 9$

&

$-9 \bmod 10 = 1$ $\quad$ i.e. $-9 = 10 \times (-1) + 1$

3. Congruent modulo n :

Two integers a & b are said to be congruent modulo n , if

$a \bmod n = b \bmod n$

i.e. we get same remainder when
a is divided by n &
b is divided by n .

The notation is,

$$\boxed{a \equiv b \pmod{n}}$$

e.g. ① $73 \bmod 23 = 4 \bmod 23$

we get same remainder i.e. 4

Hence,

$$73 \equiv 4 \pmod{23}$$

② $21 \bmod 10 = -9 \bmod 10$

$\therefore \quad 21 \equiv -9 \pmod{10}$

4. Modular Arithmetic :

properties :

(i) $[a \bmod n + b \bmod n] \bmod n$

$= (a+b) \bmod n$

(ii) $[a \bmod n - b \bmod n] \bmod n = (a-b) \bmod n$

(iii) $[a \bmod n * b \bmod n] \bmod n = (a * b) \bmod n$

e.g. $n = 8$, $a = 27$ & $b = 34$

for Addition,

$[27 \bmod 8 + 34 \bmod 8] \bmod 8$

$= [3 + 2] \bmod 8$

$= 5$

& $(27 + 34) \bmod 8 = 61 \bmod 8 = 5$

Thus, property for addition satisfied.

Similarly, Subtraction & Multiplication can be satisfied.

5. Finding Modulus of Large Numbers:

(i) $24^5 \bmod 11 = ?$

⇒ first take $24^2 \bmod 11 = 576 \bmod 11 = 4$

i.e. $24^2 = 576 \equiv 4 \bmod 11$ // congruent Modulo

Then take 24^4

$\therefore (24^2)^2 = (576)^2 \equiv (4)^2 \bmod 11 \equiv 16 \bmod 11$

$\therefore (24^2)^2 = 24^4 \equiv 5 \bmod 11$

$24^5 = 24^4 \times 24^1$

$\therefore 24^5 \bmod 11 = [24^4 \bmod 11 \times 24 \bmod 11] \bmod 11$

$24^5 \bmod 11 = [5 \times 2] \bmod 11 = 10 \bmod 11$

$\therefore \boxed{24^5 \bmod 11 = 10}$

(ii) $19^9 \bmod 13 = ?$

$\Rightarrow$ $19^2 \bmod 13 = 361 \bmod 13 = 10 \bmod 13 = 10$

$\therefore$ $19^4 \bmod 13 = (10)^2 \bmod 13 = 100 \bmod 13 = 9$

$19^9 \equiv 19 \times 19^4 \times 19^4 \bmod 13 \equiv 19 \times 9 \times 9 \bmod 13$

$\therefore 19^9 \equiv 1539 \bmod 13 = 5 \bmod 13$

$\therefore 19^9 \bmod 13 = 5$

6. Relative prime Numbers :- (co prime)

Two integers are relatively prime if, their GCD (Greatest Common Divisor) is 1

i.e. if $\gcd(a, b) = 1$,

Then, a & b are relatively prime numbers.

7. Euclidean Algorithm / Euclid's Algorithm :

$\Rightarrow$ Used to find gcd of two numbers.

$\Rightarrow$ $\gcd(a, b) = \gcd(b, a \bmod b)$ — (1)

$\Rightarrow$ Repeat equ^n (1) until b becomes zero.

8. Example of Euclid's Algorithm

$$
\begin{aligned}
gcd(161, 112) &= gcd(112, 161 \bmod 112) \\
&= gcd(112, 49) \\
&= gcd(49, 112 \bmod 49) \\
&= gcd(49, 14) \\
&= gcd(14, 49 \bmod 14) \\
&= gcd(14, 7) \\
&= gcd(7, 14 \bmod 7) \\
&= gcd(7, 0)
\end{aligned}
$$

$\therefore \; gcd(161, 112) = 7.$

Note :- $gcd(a, 0) = a$

In steps, we can write,

$161 = 112 \times 1 + 49$

$112 = 49 \times 2 + 14$

$49 = 14 \times 3 + \boxed{7}$

$14 = 7 \times 2 + 0$

when you get remainder as zero,
The gcd is obtained in its above step
ie. $gcd(161, 112) = 7$.

9. Fermat's Theorem

- If p is prime & a is +ve integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

- Used to find mod of very large numbers

(i) eg. $a = 7$ & $p = 19$ // p is prime and a is not divisible by p.

Let, we have to find $7^{22} \bmod 19$,
Then,
Using fermat's theorem,

$$7^{19-1} \equiv 1 \bmod 19$$

i.e. $7^{18} \bmod 19 = 1$
we need 7^{22}, Hence,
$7^{22} = 7^{18} \times 7^{4}$

$\therefore$ $7^{22} \bmod 19 = (7^{18} \bmod 19 \times 7^{4} \bmod 19) \bmod 19$
$= (1 \times 2401 \bmod 19) \bmod 19$
$7^{22} \bmod 19 = (1 \times 7) \bmod 19 = 7.$

10. Extended Euclidean Algorithm :

$$\gcd(a, b) = ax + by$$

i.e. gcd of a & b is written as linear combination of two integers x & y.

Let's say, $\gcd(888, 54) = 888x + 54y$
we have to find out values of x & y

step 1 : Use Euclidean Algorithm to find out gcd

step 2 : find x & y using Extended Euclidean Algorithm.

Step 1 :-

$$888 = 54 \times (16) + 24 \quad — \text{(I)}$$
$$54 = 24 \times (2) + \boxed{6} \quad — \text{(II)}$$
$$24 = 6 \times 4 + 0$$
$$\therefore \gcd(888, 54) = 6$$

step 2 :- Use Back Substitution Method.
As, per Extended Euclidean Algorithm,

$$6 = 888x + 54y.$$

from equ^n (II),

$$6 = 54 - 24 \times (2) = 54 + 24 \times (-2)$$

put value of 24 from equ^n (I),
we get,

$6 = 54 + 24 \times (-2)$

$6 = 54 + [888 - 54 \times (16)] \times (-2)$

Solve this, we get,

$6 = 54 + 888 \times (-2) + 54 \times (16 \times 2)$

$= 54 + 888 \times (-2) + 54 \times (32)$

$6 = 54 \times (33) + 888 \times (-2)$

i.e. $6 = 888 \times (-2) + 54 \times (33)$ — (A)

$\therefore \quad x = -2$ & $y = 33$

Note :- Solve Until you get original numbers in the equation (see equ^n (A), gcd is '6' & 6 is written as in terms of original numbers 888 & 54.

11. Multiplicative Inverse

a is multiplicative Inverse of b, if

$$\boxed{a \times b \equiv 1 \bmod n}$$

eg. if $b = 3$ & $n = 5$, $a = ?$

If a is taken as 7,

then $7 \times 3 = 21$ & $21 \bmod 5 = 1$

Hence,

7 is Multiplicative Inverse of 3 when we take mod 5

12. Euler's Totient function $\phi(n)$:

It is the number of positive integers less than n & relatively prime to n.

for prime number p, $\phi(p) = p-1$

e.g. $\phi(5) = 5-1 = 4$

$\phi(7) = 7-1 = 6$.

for Non-prime number,

eg. $\phi(4) = ?$

Step 1: Take all nos. less than 4, here, 1, 2, & 3

Step 2: Out of 1, 2 & 3,

$gcd(1,4) = 1$ ⇒ 1 & 4 are co-prime/relative prime

$gcd(2,4) = 2$ ⇒ Not relative prime

& $gcd(3,4) = 1$ ⇒ Relative prime.

Hence, $\phi(4) = 2$ [Because only 1 & 3 are relative prime to 4]

$\phi(6) = 2$ [Because only 1 & 5 are relative prime to 6]

$\phi(10) = 4$ [Because only 1, 3, 7 & 9 are relative prime to 10].

$\phi(30) = \phi(5) \times \phi(6) = 4 \times 2 = 8$

$\phi(77) = \phi(7) \times \phi(11) = 6 \times 10 = 60$

13. Euler's Theorem :-

for Every a & n, that are relatively prime,

$$a^{\phi(n)} \equiv 1 \pmod n$$

⇒ Again, it is also used for finding mod of very large numbers.

eg. $97^{121} \bmod 143 = ?$

Here,

$a = 97, \; n = 143$

$\therefore \; \phi(n) = \phi(143) = ?$

143 is not prime

$\phi(143) = \phi(11) \times \phi(13)$

$\phi(143) = 10 \times 12 = 120$

$\therefore \; 97^{\phi(143)} \equiv 1 \bmod 143$

$\therefore \; 97^{120} \equiv 1 \bmod 143$

$\therefore \; 97^{120} \times 97^{1} \equiv (1 \times 97) \bmod 143$

$\therefore \; 97^{121} \equiv 97 \bmod 143$

$\therefore \; 97^{121} \bmod 143 = 97.$

14. Multiplicative Inverse Using Extended Euclidean Algorithm :-

If, $\gcd(m, b) = 1$, then b has a multiplicative inverse modulo m.
i.e. for +ve integer $b < m$, there exist a 'b^{-1}' such that $b \cdot b^{-1} \equiv 1 \bmod m$.

* Condition is that gcd must be 1.

let, $m = 43$ & $b = 17$,
$\gcd(43, 17) = 1$.

Here,
$17 \times (?) \equiv 1 \bmod 43$
$\uparrow$ b $\uparrow$ $\times (b^{-1})$ $\uparrow$ m

Now,
$43 = 17 \times 2 + 9$ — (I)
$17 = 9 \times 1 + 8$ — (II)
$9 = 8 \times 1 + 1$
$8 = 1 \times 8 + 0$

Now Use Extended Euclidean, to find x & y
Such that $\gcd(43, 17) = 1 = 43x + 17y$.

Steps :-

$1 = 9 - 8 \times 1 = 9 + [8 \times (-1)]$
put value of 8 from equ^n (II)

$\therefore 1 = 9 + [17 - 9 \times 1] \times (-1)$
$\therefore 1 = 9 + 17(-1) + 9$
$1 = 9 \times (2) + 17(-1)$
put value of 9 from equ^n (I)
$\therefore 1 = [43 - 17 \times (2)] \times 2 + 17 \times (-1)$
$\therefore 1 = 43 \times 2 - 17 \times 4 + 17 \times (-1)$
$\therefore 1 = 43 \times 2 - 17 \times 5 = 43 \times 2 + 17 \times (-5)$

P.T.O.

$\therefore \quad 1 = 43 \times (2) + 17(-5)$ — III

we got gcd in terms of original numbers 43 & 17.

$\therefore \quad x = 2$ & $y = -5$

Still, we have to find b^{-1} such that

$$b \cdot b^{-1} \equiv 1 \bmod m$$

Note:- $17^{-1} \neq \frac{1}{17}$

i.e.

$$17 \cdot 17^{-1} \equiv 1 \bmod 43$$

Now, we can use equ^n III to find 17^{-1}

Rewrite equ^n III,

$$1 = 43 \times (2) + 17 \times (-5)$$

Multiply both sides by 17^{-1} & take mod 43

$$\therefore \quad 17^{-1} \bmod 43 = [43 \times (2) \times 17^{-1}] \bmod 43 + (-5) \times 17 \times 17^{-1} \bmod 43$$

$$\therefore \quad \boxed{17^{-1} \bmod 43 = 0 + (-5) \bmod 43}$$

17 & 17^{-1} gets cancelled

This term came out to be zero because we are taking mod 43 of $43 \times 2 \times 17^{-1}$, which is a multiple of 43 & will always be divided by 43, hence mod will be zero.

$$\therefore \quad 17^{-1} \bmod 43 = -5 \bmod 43 = 38$$

$\therefore \quad 17^{-1} = 38$

Now,

$$17 \times 38 \equiv 1 \bmod 43$$

Hence, 38 is multiplicative inverse of 17 when mod 43 is taken.

$$17 \times (?) \equiv 1 \bmod 43$$

Our Answer is 38

Because 38 is such a number when we multiply it by 17 & divide by 43, we get 1 as remainder.

Multiplicative Inverse plays a very Vital & Important Role in

Chinese Remainder Theorem

15. Chinese Remainder theorem : (CRT)

If we have few congruences like

$x \equiv a_1 \bmod n_1$
$x \equiv a_2 \bmod n_2$
$x \equiv a_3 \bmod n_3$
$x \equiv a_k \bmod n_k$,

where,
$n_1, n_2, n_3 \cdots n_k$ are +ve integers that are pairwise co-prime & $a_1, a_2 \cdots a_k$ are any integers, then CRT is used to find value of x

As per CRT,

$$x \equiv (a_1 m_1 y_1 + a_2 m_2 y_2 + \cdots + a_k m_k y_k) \bmod M$$

where, $M = n_1 \times n_2 \times n_3 \times \cdots \times n_k$

& $m_i = \dfrac{M}{n_i}$ &

$$m_i y_i \equiv 1 \bmod n_i$$

$\downarrow$

This y_i is calculated using Multiplicative Inverse

16. Solve using chinese Remainder Theorem:
$x = 1 \bmod 5$, $x = 6 \bmod 7$ & $x = 8 \bmod 11$

$\Rightarrow$ Here, 5, 7 & 11 are pairwise co-prime
i.e. (5, 7), (7, 11) & (11, 5) are coprimes
Here, $n_1 = 5$, $n_2 = 7$ & $n_3 = 11$

$M = 5 \times 7 \times 11 = 385$

$m_1 = \frac{M}{n_1} = \frac{385}{5} = 77$

$m_2 = \frac{M}{n_2} = \frac{385}{7} = 55$

& $m_3 = \frac{M}{n_3} = \frac{385}{11} = 35$

$a_1 = 1$
$a_2 = 6$
$a_3 = 8$

As per CRT,

$x \equiv (a_1 m_1 y_1 + a_2 m_2 y_2 + a_3 m_3 y_3) \bmod M$

$\therefore x \equiv (1 \times 77 \times y_1 + 6 \times 55 \times y_2 + 8 \times 35 \times y_3) \bmod 385$ —— (A)

Now, we have to find y_1, y_2 & y_3 from equ^ns

$77\, y_1 \equiv 1 \bmod 5$
$55\, y_2 \equiv 1 \bmod 7$
& $35\, y_3 \equiv 1 \bmod 11$

(i) To find y_1 use Multiplicative Inverse.

$5 = 77 \times 0 + 5$ —(I)
$77 = 5 \times 15 + 2$ —(II)
$5 = 2 \times 2 + \boxed{1}$
$2 = 1 \times 2 + 0$

P.T.O.

$1 = 5 - 2\times2 \quad = 5 + 2\times(-2)$

put value of 2 from (II)

$\therefore 1 = 5 + [77 - 5\times15]\times(-2)$

$\therefore 1 = 5 + 77(-2) + 5\times30$

$\therefore 1 = 77(-2) + 5(31) \quad$ — (III)

Now, $y_1 = 77^{-1} \Rightarrow$ is to be found.

$\therefore$ Multiply both sides of equ^n (III) by 77^{-1} & take mod 5

$77^{-1} \bmod 5 = 77^{-1}\times77\times(-2) \bmod 5 + \underbrace{(5\times31\times77^{-1}) \bmod 5}_{\text{divisible by 5 completely}}$

$= -2 \bmod 5 \quad + 0$

$\therefore \quad 77^{-1} = 3$

Hence $\boxed{y_1 = 3}$

i.e. $77\times3 = 1 \bmod 5$

(ii) $y_2 = ?$

we have $55\,y_2 \equiv 1 \bmod 7$.

$7 = 55\times0 + 7 \quad$ — (IV)

$55 = 7\times7 + 6 \quad$ — (V)

$7 = 6\times1 + \boxed{1}$

$6 = 1\times6 + 0$

$1 = 7 - 6\times1 \quad = 7 + 6\times(-1)$

put value of 6 from equ^n (V)

$1 = 7 + [55 - 7\times 7](-1)$

$\therefore 1 = 7 + 55(-1) + 7\times 7$

$\therefore 1 = 55(-1) + 7(8)$ — VI

Now, To find 55^{-1} i.e. y_2,
Multiply both sides of equ^n VI by 55^{-1} & take mod 7.

$55^{-1} \bmod 7 = 55\cdot(-1)\cdot 55^{-1} \bmod 7 + (7\times 8\times 55^{-1} \bmod 7)$

$\therefore 55^{-1} \bmod 7 = -1 \bmod 7 + 0$

$\therefore 55^{-1} = 6$

$\therefore \boxed{y_2 = 6}$

(iii) Similarly solve for y_3.

$35y_3 \equiv 1 \bmod 11.$

$11 = 35\times 0 + 11$

$35 = 11\times 3 + 2$ — VII

$11 = 2\times 5 + \boxed{1}$

$2 = 1\times 2 + 0$

$1 = 11 - 2\times 5 = 11 + 2\times(-5)$

put value of 2 from equ^n VII

$1 = 11 + (35 - 11\times 3)\times(-5)$

$\therefore 1 = 11 + 35(-5) + 11\times 15$

$\therefore 1 = 35(-5) + 11(16)$ — VIII

To find 35^{-1}, i.e. y_3, multiply both sides of equ^n (VIII) by 35^{-1} & take mod 11.

$\therefore \quad 35^{-1} \bmod 11 = 35 \times 35^{-1} \times (-5) \bmod 11 + 11 \times 16 \times 35^{-1} \bmod 11$

$\therefore \quad 35^{-1} \bmod 11 = -5 \bmod 11 + 0$

$\therefore \quad 35^{-1} \bmod 11 = 6$

$\therefore \quad \boxed{y_3 = 6}$

from equ^n (A),

$x \equiv (1 \times 77 \times y_1 + 6 \times 55 \times y_2 + 8 \times 35 \times y_3) \bmod 385$

put values of y_1, y_2 & y_3

$x \equiv (77 \times 3 + 6 \times 55 \times 6 + 8 \times 35 \times 6) \bmod 385$

$x \equiv (231 + 1980 + 1680) \bmod 385$

$x \equiv 3891 \bmod 385$

$\therefore \quad \boxed{x = 41}$

Thus, $41 \equiv 1 \bmod 5$

$41 \equiv 6 \bmod 7$

$41 \equiv 8 \bmod 11$

Hence, $x = 41$ solves all the equations