# NUMBER THEORY

1. GCD → Greatest Common Divisor

(The largest integer which can divide both a & b)

Eg. a) gcd (3, 5) = 1

As 3 & 5 are relatively prime to each other

b) gcd (12, 60) =

$12 = \underline{2 \times 2 \times 3}$

$60 = \underline{2 \times 2 \times 3} \times 5$

c) gcd (40, 20)

Factors of 40 ⇒ $\underline{2 \times 2} \times 2 \times \underline{5}$

Factors of 20 ⇒ $\underline{2 \times 2} \times \underline{5}$

c) $\underline{\gcd(40, 20)}$

Factors of 40 $\Rightarrow$ $\underline{2 \times 2} \times 2 \times \underline{5}$

Factors of 20 $\Rightarrow$ $\underline{2 \times 2} \times \underline{5}$

d) $\underline{\gcd(15, 12)}$

Factors of 15 $\Rightarrow$ $\underline{3} \times 5$

Factors of 12 $\Rightarrow$ $\underline{3} \times 4$

## 2. Modular Arithmetic

Modular arithmetic is a simple concept of using Remainder which is left after an integer division.

a) Let $a, b \in Z$ & $n \in N$,

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

if $[(a-b)/n]$

where

$Z \Rightarrow$ set of integers.

$N \Rightarrow$ set of Natural Numbers.

**Example :**

$$23 \equiv 1 \pmod{11}$$

Congruence calculus is often called a Modular arithmetic. It considers that 23 & 11 mod (12) is equivalent as both the operations leave same remainder 11.

b) If $a, b \in \mathbb{Z}$ be any integers, then $\exists q, r$ such that $b = aq + r$ where $0 \leq r < a$

where $q \Rightarrow$ quotient, $r \Rightarrow$ remainder.

c) Modular Arithmetic exhibits the following properties:

1) $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

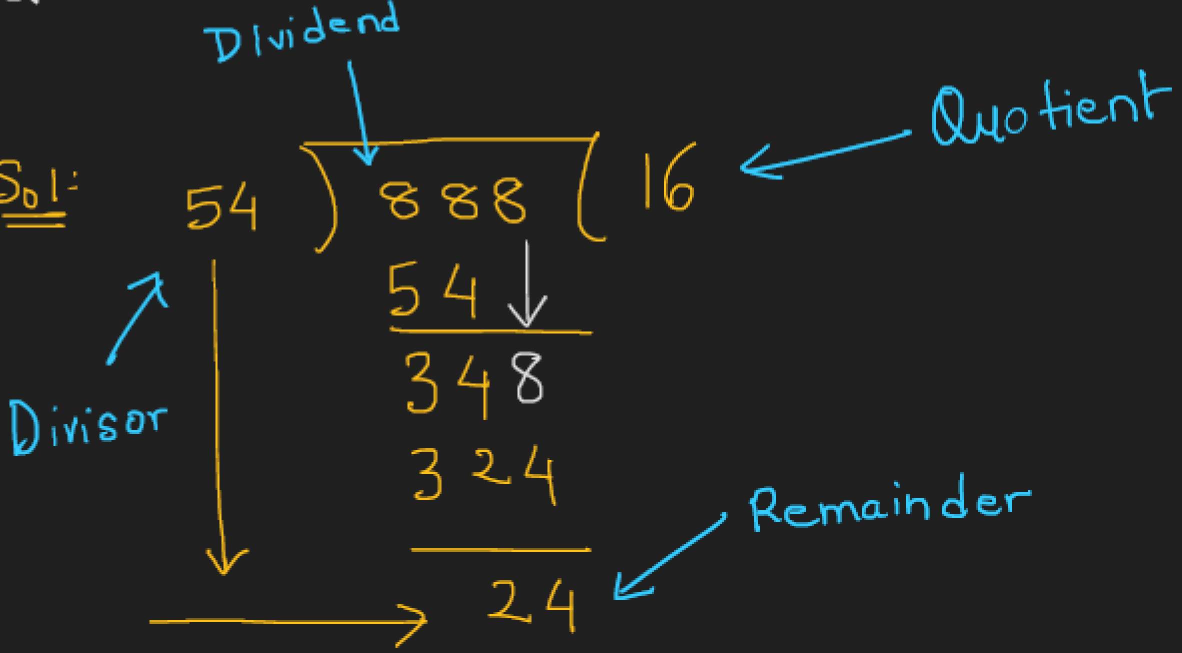
2) $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$

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

# 3. Euclidean Algorithm

Q. Calculate GCD of 54 & 888

**Sol:**




If the remainder is less than the divisor, continue the process with the remainder as the new divisor & the old divisor as the dividend

$24 \overline{)54} (2$

$48$

$6 \overline{)24} (4$

$24$

$0$

At some point of time, if we keep on continuing the division, we will eventually get 0 as the remainder.

The divisor for that operation will be the required GCD, ie. 6

Hence, we can show the complete operation as follows:-

$$888 \Rightarrow 54(16) + 24$$

$$54 \Rightarrow 24(2) + 6$$

$$24 \Rightarrow 6(4) + \underline{\underline{0}}$$

This also obeys

$$b = aq + r$$

# Euclidean Algorithm

It is a basic technique or method for calculation of GCD of two positive integers.

Suppose we have 2 integers $a, b$ such that $d = \gcd(a, b)$

Assume $a > b > 0$

Now dividing $a$ by $b$, we can state that:

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$$

Where $q_1 \Rightarrow$ quotient, $r_1 =$ remainder

Suppose that $r_1 \neq 0$ because $b > r_1$, we can divide $b$ by $r_1$ & apply division to obtain:

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

if $r_2 = 0$, then $d = r_1$ & if $r_2 \neq 0$, then $d = \gcd(r_1, r_2)$.

The division process continues till the remainder is 0.

Euclid $(x, y)$

1. $x \rightarrow x$ , $y \rightarrow y$

2. If $y = 0$ , return $x = \gcd(x, y)$

3. $R = x \bmod y$

4. $x \leftarrow y$

5. $y \leftarrow R$

6. Go to Step 2.

Q. 1: GCD of $(40, 20)$

Sol: We know that :-

$$\gcd(x, y) = \gcd(y, x \bmod y)$$

$\therefore$ $\gcd(40, 20) = \gcd(20, 40 \bmod 20)$

$= \gcd(20, 0)$

$\therefore$ New $y = 0$,

if $y = 0$, return

$x = \gcd(20, 0) = 20$

$\therefore$ $GCD(40, 20) = 20$

## Q.2, GCD of (36, 10)

$\gcd(36, 10) \Rightarrow \gcd(10, 36 \bmod 10)$

$\Rightarrow \gcd(10, 6)$

$\therefore \gcd(10, 6) \Rightarrow \gcd(6, 10 \bmod 6)$

$\Rightarrow \gcd(6, 4)$

$\therefore \gcd(6,4) \Rightarrow \gcd(4, 6 \bmod 4)$

$\Rightarrow \gcd(4, 2)$

$\therefore \gcd(4,2) \Rightarrow \gcd(2, 4 \bmod 2)$

$\Rightarrow \gcd(2,0)$

$\therefore y = 0,$

$\boxed{\text{Hence } GCD(36,10) = 2}$

## Q.3: GCD of (48, 30)

$$\gcd(48,30) = \gcd(30, 48 \bmod 30)$$
$$= \gcd(30, 18)$$

$$\therefore \gcd(30,18) = \gcd(18, 30 \bmod 18)$$
$$= \gcd(18, 12)$$

$$\gcd(18,12) = \gcd(12, 18 \bmod 12)$$
$$= \gcd(12, 6)$$

$$\therefore \gcd(12,6) = \gcd(6, 12 \bmod 6)$$
$$= \gcd(6, 0)$$

$\therefore$ $\boxed{\text{GCD of } 48, 30 \text{ is } 6}$

**Q.4** GCD of 105, 80

As $\gcd(105, 80) = \gcd(80, 105 \bmod 80)$

$$= \gcd(80, 25)$$

$\therefore \gcd(80, 25) = \gcd(25, 80 \bmod 25)$

$$= \gcd(25, 5)$$

$\therefore \gcd(25, 5) = \gcd(5, 25 \bmod 5)$

$$= \gcd(5, 0)$$

$$\boxed{\therefore \ GCD(105, 80) = 5}$$

# Fermat's Theorem

Fermat's Theorem plays an important role in Cryptography. To understand this theorem, one needs to have basic knowledge of GCD, Prime numbers & Prime Factorisation.

Theorem: For any prime number p, 'a' is the integer which is not divisible by p, then

$$a^{p-1} \equiv 1 \pmod p \longrightarrow (1)$$

A variant of this theorem is:-

If p is a prime no. & a is a coprime to p (i.e gcd (a,p) = 1), then

$$a^{p} \equiv a \pmod p \longrightarrow (2)$$

Basically this theorem is useful in public key cryptography such as RSA.

# Examples on Fermat's Theorem

1. Let's have $a = 3$, $p = 5$

Eq. 1 & 2, both are satisfied. So we will test both the equations with these values.

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

$\Rightarrow 3^4 \Rightarrow 81$

$\therefore$ $81 \bmod 5 = 1$

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

$\therefore \quad \underline{a^p \equiv a \pmod p}$

$\therefore \quad 3^5 \Rightarrow 243$

Also $3 \pmod 5 = 3$

Now, if we take 243 mod 5, it will give same result

$\therefore \quad 243 \equiv 3 \pmod 5$

$\therefore \quad (243) \bmod 5 \equiv (3 \bmod 5) \bmod 5$

$\Rightarrow \quad 3 = 3 \quad \therefore$ LHS = RHS

② **Solve :** $6^{10} \bmod 11$

**Sol:** Acc. to Fermat's Theorem

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

Hence $p-1 = 10$, $a = 6$

$\therefore p = 11$

Hence $6^{10} \equiv 1 \bmod 11$

Now, $6^{10} \Rightarrow (6^8 \bmod 11)\,(6^2 \bmod 11) \bmod 11$

$\Rightarrow (4 \times 3) \bmod 11$

$\Rightarrow \underline{1}$

$\therefore 6^{10} \bmod 11 = 1$ ✓

# Euler's Totient Function

$\phi(n)$ is called as Euler's Totient Function which states that how many numbers are between 1 and $n-1$ that are relatively prime to $n$.

For example, if $n = 4$, $\phi(4) = 1, 3 = 2$ because they are relatively prime to 4.

## Euler's Theorem:

It states that for every $a$ & $n$ that are relatively prime:

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

For example: Prove using Euler's Theorem,

$a = 3$, $n = 10$, $\phi(10) = ?$

Sol: $\phi(n) = \phi(10) = \{1, 3, 7, 9\} = 4$

Then according to Euler's Theorem:

$$3^4 \equiv 1 \pmod{10}$$

$\because$ $3^4 = 81$

$\therefore$ $81 \bmod 10 = 1$ As LHS = RHS

Hence Proved.

# CHINESE REMAINDER THEOREM

A famous problem was presented as : There are certain numbers repeatedly divided by 3 and remainder is 2, repeatedly divided by 5 and remainder is 3 and repeatedly divided by 7 and remainder is 2.

What will be that number??

What will be that number??

$$\left.\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ x &\equiv a_3 \bmod m_3 \end{aligned}\right\}$$ Find the value of $x$

Where $m_1$ $m_2$ & $m_3$ are relatively prime

$\therefore \gcd(m_1, m_2) = \gcd(m_1, m_3) = \gcd(m_2, m_3) = 1$

Also, $M = m_1 \times m_2 \times m_3 \cdots\cdots m_r$

$\therefore x = (M_1 X_1 a_1 + M_2 X_2 a_2 + M_3 X_3 a_3 \cdots + M_r X_r a_r) \bmod M$

where, $M_i = \dfrac{M}{m_i}$, &

$1 . a_1 \bmod m_1$

$M_i X_i \equiv 1 \pmod{m_i}$

Example

$$x \equiv 1 \pmod 5$$
$$x \equiv 1 \pmod 7$$
$$x \equiv 3 \pmod{11}$$

Find $x$

Sol: Here $a_1 = 1$, $a_2 = 1$, $a_3 = 3$

$m_1 = 5$, $m_2 = 7$, $m_3 = 11$

$\therefore x = (M_1 X_1 a_1 + M_2 X_2 a_2 + M_3 X_3 a_3)$

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

$$M_1 = \frac{385}{5} = 77$$

$$M_2 = \frac{385}{7} = 55$$

$$M_3 = \frac{385}{11} = 35$$

$\therefore$ $77 X_1 \equiv 1 \pmod 5$

$55 X_2 \equiv 1 \pmod 7$

$35 X_3 \equiv 1 \pmod{11}$

Congruence means mod on either side should give same result. We can take mod n. no. of times.

i.e $77 X_1 \equiv 1 \pmod 5$

$\Rightarrow$ $77 \bmod 5 . X_1 \equiv 1 \pmod 5 \pmod 5$

$\Rightarrow$ $2 X_1 \equiv 1 \pmod 5$ Multiply by 3

$\Rightarrow$ $6 X_1 \equiv 3 \pmod 5$

$\Rightarrow$ $1 . X_1 \equiv 3$

$\Rightarrow$ $\boxed{X_1 = 3}$

Now, $55 X_2 \equiv 1 \pmod 7$

$$55 \pmod 7 \, X_2 \equiv 1 \pmod 7 \pmod 7$$

$$\left[ 6 X_2 \equiv 1 \pmod 7 \right] \times 6$$

$$36 X_2 \equiv 6 \pmod 7$$

$$36 \pmod 7 \, X_2 \equiv 6$$

$$\boxed{X_2 = 6}$$

Similarly,

$$35 X_3 \equiv 1 \pmod{11}$$

$$\Rightarrow 35 \pmod{11} \, X_3 \equiv 1 \pmod{11} \pmod{11}$$

$$\Rightarrow \left[2 X_3 \equiv 1 \bmod 11\right] \times 6$$

$$\Rightarrow 12 X_3 \equiv 6 \bmod 11$$

$$\Rightarrow 12 (\bmod 11)\, X_3 \equiv 6$$

$$\Rightarrow 1 \cdot X_3 \equiv 6$$

$$\Rightarrow \boxed{X_3 = 6}$$

$$\therefore\ x = \left[(77 \times 3 \times 1) + (55 \times 6 \times 1) + (35 \times 6 \times 3)\right] \bmod M$$

$$= (1191) \bmod 385$$

$$= 36$$