ELEMENTARY NUMBER THEORY

- Given +ve integers a, b, we write $a|b$ to indicate that a divides b.

- If $a|b$, then we know that there is an integer k s.t
$$b = a \cdot k$$

- If $a|b \wedge b|c$, then $a|c$
- If $a|b \wedge a|c$, then $a|(bi + cj)$ for all integers i and j.

- If $a \mid b \wedge b \mid a$, then $(a=b) \vee (a=-b)$

- An integer p is prime whenever $d \mid p$ implies $(d=1) \vee (d=p)$

- A number which is not prime is called a composite number.

FUNDAMENTAL THM. OF ARITHMETIC

Let $n > 1$ be an integer. Then there is a unique set of prime nos. $\{p_1, p_2, p_3, \ldots, p_K\}$ and +ve integers $\{e_1, e_2, e_3, \ldots, e_K\}$ s.t

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_K^{e_K}$$

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_k^{e_k}$$

OR.

$$n = \prod_{i=1}^{k} p_i^{e_i}$$ is called prime decomposition of n.

- $GCD(a, b)$ is the largest integer that divides both a and b.
- If $GCD(a, b) = 1$, then a and b are said to be co-prime or relatively prime.

- If $d|a \wedge d|b$, then $d|\gcd(a,b)$

  <u>Proof</u>: Let $a = x \cdot d \wedge b = y \cdot d$

  Now $\gcd(a,b) = d \cdot \gcd(x,y)$

- $GCD(a,b) = GCD(b,a)$
- $GCD(a,0) = a$
- $GCD(a,b) \times LCM(a,b) = a \times b$

  <u>Proof</u>: c is a divisor of a and b iff $\frac{a \times b}{c}$ is a multiple of a and b

  So larger the c, smaller is $\frac{a \times b}{c}$

<u>Modulo</u> <u>operator</u>: $a \bmod n$ is the remainder of a when divided by n.

- $a \bmod n$ is between $[0, n-1]$

- $a \bmod n = a - \lfloor \frac{a}{n} \rfloor n$

- If $a \bmod n = b \bmod n$ then we say that a is congruent to b modulo n.

- $a \equiv b \pmod{n}$ means that a is congruent to b modulo n.

- $\equiv_n$ is an equivalence relation. That is, reflexive, symmetric & transitive.

Let a and b be two positive integers. For any integer r we have the following result:

$$GCD(a,b) = GCD(b,\ a - rb)$$

The above result imples :

$$GCD(a,b) = GCD\left(b,\ a - \left\lfloor \frac{a}{b} \right\rfloor b\right)$$

which is equivalent to :

$$GCD(a,b) = GCD(b,\ a \bmod b)$$

We now have an algorithm to find GCD of two numbers.

EUCLID'S ALGO :

GCD(a, b) [Suppose $a > b$]

If $b = 0$, then return(a)

Else

GCD(b, a mod b)

Example :

a	412	260	152	108	44	20	4
b	260	152	108	44	20	4	0

<u>Note</u> : Ist argument reduces by at least 50 per cent after every two recursive calls.

<u>Complexity</u> : $O(\log a)$

Alternative Characterization of GCD

Thm: For any +ve integers a and b, gcd(a, b) is the smallest +ve integer d s.t $d = ai + bj$ for some integers i and j.

Proof: Suppose d is the smallest +ve integer s.t $d = i \cdot a + j \cdot b$

Any common divisor of a and b is a divisor of d also.

$$\therefore \gcd(a, b) \leq d \qquad \text{——— (1)}$$

$$\begin{aligned}
a \bmod d &= a - \left\lfloor \frac{a}{d} \right\rfloor d \\
&= a - hd \quad \text{where } h = \left\lfloor \frac{a}{d} \right\rfloor \\
&= a - h(i \cdot a + j \cdot b) \\
&= a(1 - hi) + b(-hj)
\end{aligned}$$

$\Rightarrow$ a mod d = 0 —— 2

Similarly we can prove that

b mod d = 0 —— 3

From 2 and 3 we have :

$d | a \;\wedge\; d | b$

$\Rightarrow d \,|\, \gcd(a, b)$

$\Rightarrow d \leq \gcd(a, b)$ —— 4

From 1 & 4 we get $d = \gcd(a, b)$.

<u>Thm</u> : Given $Z_n = \{0, 1, 2, \ldots, n-1\}$,

an element $x \in Z_n$ has a multipicative inverse (MI) in Z_n

iff $\gcd(x, n) = 1$

Suppose $\gcd(x, n) = 1$

$\therefore \exists i, j \in \mathbb{Z}$ s.t $1 = xi + nj$

$$1 \equiv xi \pmod{n}$$

$\Rightarrow$ $i \bmod n$ is the MI of x

Let's prove other way

$\exists y \in \mathbb{Z}_n$ s.t $x \cdot y \bmod n = 1$

$\therefore$ $xy = kn + 1$ for some k

$1 = xy - kn$

$\therefore \gcd(x, n) = 1$

<u>Thm</u>: Given $Z_n = \{0, 1, 2, \ldots, n-1\}$

Let $x > 0$ be an element of Z_n s.t $\gcd(x, n) = 1$. Now the following holds:

$$\{ i \mid i \in Z_n \} = \{ x \cdot i \bmod n \mid i \in Z_n \}$$

<u>Proof</u>: $x \cdot i \equiv_n x \cdot j$ implies $i \equiv_n j$

or $i \not\equiv_n j$ implies $xi \not\equiv_n xj$

<u>Fermat's</u> <u>Little</u> <u>Theorem</u>: Let p be a prime and x be an integer s.t $x \bmod p \neq 0$. We then have:

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

Proof: It is sufficient to prove the result for $0 < x < p$, as.

$$x^{p-1} \bmod p \equiv (x \bmod p)^{p-1} \bmod p$$

Let $S = \{1, 2, 3, \ldots, p-1\}$ $\wedge$

$$S' = \{x \bmod p, \quad 2x \bmod p,$$

$$3x \bmod p, \ldots, x^2 \bmod p, \ldots,$$

$$(p-1)\cdot x \bmod p\}$$

From the previous thm we know that

$$S = S'$$

$$\underline{|p-1} = x^{p-1} \cdot \underline{|p-1}$$

$$\underline{|p-1} \equiv x^{p-1} \cdot \underline{|p-1} \pmod p$$

$\underline{|p-1}$ and p are co-prime, $\therefore$ $1 \equiv x^{p-1} \pmod p$

Euler's Thm :

Let n be a +ve integer and let x be an integer s.t $\gcd(x, n) = 1$. Then we have :

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

Proof : Since $x^{\phi(n)} \equiv_n (x \bmod n)^{\phi(n)}$, it is sufficient to assume that $0 < x < n$

we know $x \in Z_n^*$

If $Z_n^* = \{u_1, u_2, u_3, \ldots, u_{\phi(n)}\}$, then

$$\{(x \cdot u_i) \bmod n \mid 1 \leq i \leq \phi(n)\} = Z_n^*$$

$$U_1 \cdot U_2 \cdot U_3 \cdots U_{\phi(n)} = x^{\phi(n)} \cdot U_1 \cdot U_2 \cdots U_{\phi(n)}$$

$$U_1 \cdot U_2 \cdots U_{\phi(n)} \equiv_n x^{\phi(n)} \cdot U_1 \cdot U_2 \cdots U_{\phi(n)}$$

Each U_i is coprime to n

$$\therefore \quad 1 \equiv x^{\phi(n)} \pmod{n}$$