

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 .

(2)

- If $a|b \wedge b|a$, then $(a=b) \vee (a=-b)$
- An integer p is prime whenever $d|p$ 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.

$\{p_1, p_2, p_3, \dots, p_k\}$ and +ve

integers $\{e_1, e_2, e_3, \dots, e_k\}$ s.t

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

(3)

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

OR.

$$n = \prod_{i=1}^k p_i^{e_i} \quad \text{is called}$$

prime decomposition of n .

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

④
• If $d|a \wedge d|b$, then $d|\gcd(a,b)$

Proof: Let $a = x \cdot d \wedge b = y \cdot d$

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

- $\gcd(a,b) = \gcd(b,a)$
- $\gcd(a,0) = a$
- $\gcd(a,b) \times \text{LCM}(a,b) = a \times b$

Proof: 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 $\frac{a \times b}{c}$

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

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

(5)

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

⑥
Let a and b be two positive integers. For any integer r we have the following result :

$$\text{GCD}(a, b) = \text{GCD}(b, a - rb)$$

The above result implies :

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

which is equivalent to :

$$\text{GCD}(a, b) = \text{GCD}(b, a \bmod b)$$

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

$GCD(b, a \bmod b)$

Example :

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

Note : 1st argument reduces by at least 50 per cent after every two recursive calls.

Complexity : $O(\log a)$

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.

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

$$a \bmod d = a - \left\lfloor \frac{a}{d} \right\rfloor d$$

$$= a - hd \quad \text{where } h = \left\lfloor \frac{a}{d} \right\rfloor$$

$$= a - h(i \cdot a + j \cdot b)$$

$$= a(1 - hi) + b(-hj)$$

$$\Rightarrow a \bmod d = 0 \quad \text{--- (2)}$$

(9)

Similarly we can prove that

$$b \bmod d = 0 \quad \text{--- (3)}$$

From (2) and (3) we have :

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

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

$$\Rightarrow d \leq gcd(a, b) \quad \text{--- (4)}$$

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

Thm : Given $Z_n = \{0, 1, 2, \dots, n-1\}$,

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

$$\text{iff } gcd(x, n) = 1$$

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

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

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

$\Rightarrow i \pmod{n}$ is the MI of x

Let's prove other way

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

$$\therefore xy = kn + 1 \text{ for some } k$$

$$1 = xy - kn$$

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

(11)

Thm: Given $Z_n = \{0, 1, 2, \dots, n-1\}$

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

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

Proof: $x \cdot i \equiv_n x \cdot j$ implies $i \equiv_n j$

or $i \not\equiv_n j$ implies $x \cdot i \not\equiv_n x \cdot j$

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

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

(12)

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

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

$$\text{Let } S = \{1, 2, 3, \dots, p-1\}$$

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

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

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

From the previous thm we know that
 $S = S'$

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

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

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

Euler's Thm :

(13)

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 $x \in \mathbb{Z}_n^*$

If $\mathbb{Z}_n^* = \{u_1, u_2, u_3, \dots, u_{\phi(n)}\}$, then

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

(14)

$$u_1 \cdot u_2 \cdot u_3 \cdots u_{\phi(n)} = x^{\phi(n)} \cdot u_1 \cdot u_2 \cdots u_{\phi(n)}$$

$$u_1 \cdot u_2 \cdots u_{\phi(n)} \equiv_n x^{\phi(n)} \cdot u_1 \cdot u_2 \cdots u_{\phi(n)}$$

Each u_i is coprime to n

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