Primes

Positive Integers
- Number 1 [Exactly one divisor]
- Primes [two]
- Composites [more than two]

Coprimes :- $\gcd(a,b) = 1$

Cardinality of Primes :-

→ Infinite No. of Primes

set $\{2,3,5,7,11,13,17\}$ $P = 510510$

$P+1 = 510511 = 19 \times 97 \times 277$ {3 Primes greater than 17}

→ No. of Primes

$\pi(10) = 4$ $\{2,3,5,7\}$

$$\boxed{\left[\frac{n}{\log_e n}\right] < \pi(n) < \left[\frac{n}{(\ln n - 1.08366)}\right]}$$

Checking for Primeness :-

Sieve of Eratosthenes -

Euler's Phi Function :- (Euler's totient fn) :-

finds the no. of integers that are both smaller than n and relatively prime to n.

function

① $\phi(1) = 0$

② $\phi(P) = P-1$ if P is a prime

③ $\phi(m \times n) = \phi(m) \times \phi(n)$ $\gcd(m,n) = 1$

④ $\phi(P^e) = P^e - P^{e-1}$ if P is a prime.

Ex. $Z_{14}^* = \phi(14) = \phi(2) \times \phi(7) = 1 \times 6 = 6$

$\{1,3,5,9,11,13\}$

Note. if $n > 2$, $\phi(n)$ is even

Fermat's Little Theorem :-

First version :- $a^{p-1} \equiv 1 \bmod p$ $\boxed{a^{p-1} \bmod p = 1}$ { p is prime, $\gcd(a,p) = 1$ }

Second version :- $a^{p} \equiv a \bmod p \Rightarrow \boxed{a^{p} \bmod p = a}$

Ex. (i) $6^{10} \bmod 11$
$= 1$

(ii) $3^{12} \bmod 11$
$= 3^{10} \bmod 11 \times 3^{2} \bmod 11$
$= 1 \times 9 = 9$

Multiplicative Inverses :-

$$\boxed{a^{-1} \bmod p = a^{p-2} \bmod p}$$

from first version of fermat's little theorem.

{ p is prime, $\gcd(a,p) = 1$ }

Euler's Theorem

generalization of fermat's little theorem -

First version $a^{\phi(n)} \equiv 1 \pmod n$ { → a, n is any integer → $\gcd(a,n) = 1$ }

$$\boxed{a^{\phi(n)} \bmod n = 1}$$

Second version $a^{k \times \phi(n)+1} \equiv a \pmod n$ { $\gcd(a,n)$ may or may not equal to 1 (means no condition) }

$$\boxed{a^{k \cdot \phi(n)+1} \bmod n = a}$$

Generating Primes :-

Mersenne Primes - $\boxed{M_p = 2^{p} - 1}$ { → p is prime → it fails on $p = 11$ }

Fermat Primes - $\boxed{F_n = 2^{2^n} + 1}$ { it fails on $n = 5$ }

Primality Testing :- n is prime or not

Algo that deal with this issue can be divided into two broad categories :

① deterministic algo ② probabilistic algo

Deterministic Algo

Factorization

Fermat's Factorization Method

is based on observation that any odd integer N can be expressed as

$$N = x^2 - y^2$$

$$\Rightarrow \quad N = (x-y)(x+y)$$

$y^2 = x^2 - N$

$y = \sqrt{\infty}$

Steps for fermat's

Step ① select x as the smallest int greter than $\sqrt{N}$

② Compute $x^2 - N$. If x^2-N is a perfect sqare say y^2 then $N = (x-y)(x+y)$

③ If $x^2 - N$ is not a perfect squre increment x and repeat.

~~Pollard~~'s ~~p-1 method~~ :-

```
Feramat_Factorization(n)
{
    x ← √n                 // smallest int greater than √n
    while (x < n)
    {
        w ← x²-n
        if (w is perfect square)
            Y ← √w; a ← x+y; b ← x-y; return a and b
        x ← x+1
    }
}
```

T.C. :- $O(\sqrt{n})$ $(\sqrt{n}\log n)$

Fermat's Algo

Idea.
- → To factor n
- → $n = x \cdot y$
- → works well when x and y are close.

formula:
$$n = x^2 - y^2$$
$$x^2 = n + y^2$$
$$x = \sqrt{n + y^2}$$

Ex. factor $n = 187$.

Solⁿ.
$$x = \sqrt{n + y^2}$$
$$x = \sqrt{187 + y^2}$$

$= \sqrt{187 + 1^2} = \sqrt{199} \neq$ Integer

$= \sqrt{187 + 2^2} = \sqrt{191} \neq$ Int

$= \sqrt{187 + 3^2} = \sqrt{196} = 14$

$x = 14$ and $y = 3$

Recall

$n = x^2 - y^2$

$= (14+3)(14-3) = 17 \times 11 = 187$ ✓

Factorization

Fundamental Theorem of Arithmetic

$$n = P_1^{e_1} \times P_2^{e_2} \times \cdots \times P_K^{e_K}$$

GCD :-

$$a = P_1^{a_1} \times P_2^{a_2} \times \cdots \times P_K^{a_K}$$
$$b = P_1^{b_1} \times P_2^{b_2} \times \cdots \times P_K^{b_K}$$

$$\gcd(a,b) = P_1^{\min(a_1,b_1)} \times P_2^{\min(a_2,b_2)} \times \cdots \times P_K^{\min(a_K,b_K)}$$

CM :-

$$a = P_1^{a_1} \times P_2^{a_2} \times \cdots \times P_K^{a_K}$$
$$b = P_1^{b_1} \times P_2^{b_2} \times \cdots \times P_K^{b_K}$$

$$\mathrm{lcm}(a,b) = P_1^{\max(a_1,b_1)} \times P_2^{\max(a_2,b_2)} \times \cdots \times P_K^{\max(a_K,b_K)}$$

$$\boxed{\mathrm{lcm}(a,b) \times \gcd(a,b) = a \times b}$$

Trial Division Method

[Sieve of Eratosthenes]

Trial_Division_Factorization(n) // n is the number to be factored

```
{   a ← 2
    while (a ≤ √n)
    {
        while (n mod a = 0)
        {
            output a
            n = n/a
        }
        a ← a+1
    }
    if (n > 1) output n   // n has no more factors
}
```

$\log_a n$ $\{ n = a^k$, $k = \log_a n$

$\sqrt{n}$

Ex. → $1233 = 3^2 \times 137$

→ $72 = 2 \times 2 \times 2 \times 3 \times 3 \times 3$

→ $24 = 2^3 \times 3$

least efficient algo.

Time Comp. $(\sqrt{n} \log_a n)$

36
2x18
3x12
4x9
6x6
9x4

$[2, \sqrt{n}]$

Pollard p-1 Method

a method that finds a prime factor p of a no. based on the condition that p-1 has no factor larger than a predefined value B, called the Bound.

Pollard-rho-Fact (n, B)

```
{
    x ← 2
    y ← 2
    p ← 1
    while (p = 1)
    {
        x ← f(x) mod n
        y ← f(f(y) mod n) mod n
        p ← gcd(x-y, n)
    }
    return p      // if p = n the program has failed
}
```

$\boxed{\text{Time Com} \rightarrow O(n^{1/4})}$

Ex.

$n = 21 \quad B = 10$

$f(n) = n^2 + 1$

$x \leftarrow 2$

$y \leftarrow 2$

$p \leftarrow 1$

first it :-

$x = f(2) \bmod 21 = 2^2 + 1 \bmod 21 = 5$

$y = f(f(2)) \bmod 21 = f(5) \bmod 21 = 26 \bmod 21 = 5$

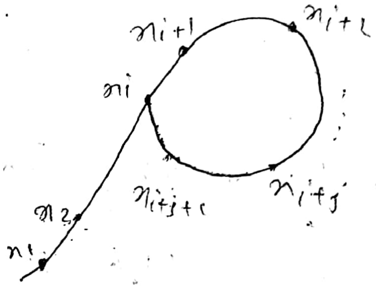
$p = gcd(5-2, 21) = 3$

pollard rho method

kisi no. n ka prime factor dhoondhne ke liye use hota hai, khas kar jab no. ke prime factor chhote hai.

Basic Idea :- hum ek sequence of no. generate krte hai aur unme se do numbers dhoondhte hain jinka difference, no. ke kisi prime factor p se devide ho ske.

pollard rho ke sequence ek time ke bad repeat hota hai aur woh sequence Greek letter rho (ρ) jaisa dikhta hai isiliye isko pollard rho method khte hain.



Ex. $n = 91$ (7×13)

$x = y = 2$

$f(x) = x^2 + 1 \bmod 91$

$\gcd(x-y, n) = p$

$(7, 91) = 7$

$$\boxed{\begin{array}{c} T.C. \\ O(n^{1/4}) \end{array}}$$

$O\left(2^{nb/4}\right)$

Other methods (more Efficient Methods)

→ **Quadratic Sieve :-** (find value of $x^2 \bmod n$) is used to factor integer ≥ 100 digits

T.C. $O(e^C)$: $C \simeq (\ln n \ln\ln n)^{1/2}$.

→ **Number Field Sieve :-** (find value $x^2 \equiv y^2 \bmod n$)

≥ 120 digits $O(e^C)$: $C \simeq 2(\ln n)^{1/3}(\ln\ln n)^{2/3}$

Pollard p-1 method - a method that finds a prime factor p of a number based on the condition that p-1 has no factor larger than a predefined value B, called the Bound.

→ ek aise prime factor p ko dundhta hai ~~iss~~ jis se ki p-1 kaafi choti values ka factor ho.

```
pollard_(p-1)_Factorization (n, B)
{
        a ← 2
        e ← 2
        while (e ≤ B)
        {
            a ← a^e mod n
            e ← e+1
        }
        p ← gcd(a-1, n)
        if 1<p<n return p
        return failure
}
```

T.C. $O(B \log n)$

The CRT :-

The CRT is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime as shown below.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv a_k \pmod{m_k}$$

$\gcd(m_1, m_2)$
$= \gcd(m_2, k)$
$= \gcd(m_k, m_1) = 1$

Sol^n follow these steps:

1. Find $M = m_1 \times m_2 \times \cdots \times m_k$ This is common modulus
2. Find $M_i = \frac{M}{m_i}$ / $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, ...
3. Find multiplicative inverse of $M_1, M_2, \ldots M_k$ using the corresponding moduli $(m_1, m_2, \ldots m_k)$ call the inverses $M_1^{-1}, M_2^{-1}, \ldots M_k^{-1}$
4. Solution $x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \ldots + a_k \times M_k \times M_1^{-1}) \bmod M$

Chinese Remainder Theorem

4

$x \equiv r_1 \pmod{m_1}$

$x \equiv r_2 \pmod{m_2}$

$x \equiv r_3 \pmod{m_3}$

* GCD $(m_1 m_2) \mid (m_2, m_3) \mid (m_1, m_3)$

$= 1$

Sol

Let $M = m_1 m_2 m_3$

$M_1 = \frac{M}{m_1}$

$M_2 = \frac{M}{m_2}$, $M_3 = \frac{M}{m_3}$

$M_1 x \equiv 1 \pmod{m_1} \rightarrow S_1$

$M_2 x \equiv 1 \pmod{m_2} \rightarrow S_2$

$M_3 x \equiv 1 \pmod{m_3} \rightarrow S_3$

$X = (M_1 S_1 r_1 + M_2 S_2 r_2 + M_3 S_3 r_3) \bmod M$

Ques

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

$M = 3 \times 5 \times 7 = 105$

$M_1 = \frac{105}{3} = 35$

$M_2 = \frac{105}{5} = 21$

$M_3 = \frac{105}{7} = 15$

$\Rightarrow 35x \equiv 1 \pmod 3$

$21x \equiv 1 \pmod 5$

$15x \equiv 1 \pmod 7$

$2x \equiv 1 \pmod 3$

$x \equiv 1 \pmod 5$

$x \equiv 1 \pmod 7$

$S_1 = 2, \; S_2 = 1, \; S_3 = 1$

$X = (35 \times 2 \times 2 + 21 \times 1 \times 3 + 15 \times 1 \times 2) \bmod 105$

$\boxed{X = 233} \bmod 105$

Now $x = 233 \equiv ? \pmod{105}$

$x = 233 \equiv \underline{23} \pmod{105}$ Ans

Chinese Remainder theorem states that there always exists an 'x' that satisfies the given congruence.

$$x \equiv rem[0] \pmod{num[0]}$$
$$x \equiv rem[1] \pmod{num[1]}$$

and $\gcd(num[0], num[1]) = 1$

eg. ①

$x \equiv 2 \bmod 3$
$x \equiv 3 \bmod 4$
$x \equiv 1 \bmod 5$

$\gcd(3,4) = \gcd(4,5) = \gcd(3,5) = 1$

Then only x exists.

here $x = 11$

eg. ②

$x \equiv 1 \bmod 5$
$x \equiv 3 \bmod 7$

→ 5 and 7 are coprime

here $x = 31$

Ques.

N chocolates

5 students → rem → 1

7 students → rem → 3

$x \equiv 1 \bmod 5$
$x \equiv 3 \bmod 7$

$\gcd(5,7) = 1$

$M = 5 \times 7 = 35$

$M_1 = 7, \quad M_2 = 5$

$7 M_1^{-1} \equiv 1 \pmod{5}$ $2 M_1^{-1} \equiv 1 \bmod 5$ $\boxed{M_1^{-1} = 3}$

$5 M_2^{-1} \equiv 1 \pmod{7}$ $\boxed{M_2^{-1} = 3}$

$X = (7 \times 3 \times 1 + 5 \times 3 \times 3) \bmod 35$
$= 21 + 45$
$= 66 \bmod 35 = 31$

$x \equiv 3 \pmod{5}$
$x \equiv 1 \pmod{7}$
$\gcd(5,7) = 1$
$M = m_1 \times m_2 = 5 \times 7 = 35$
$M_1 = \frac{M}{m_1} = \frac{35}{5} = 7$
$M_2 = 5$
$M_1 \cdot M^{-1} \pmod{M} \equiv 1 \pmod{M}$
$7 M^{-1} \equiv 1 \pmod{35}$

Ques. Can be → If we have N books and if we divide it in 5 students remainder = 3 and if we devide it in 4 students books left = 2.
So find no. of books? (N = 58)

Explain CRT

if $x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$x \equiv a_3 \pmod{m_3}$

(i) $\gcd(m_1, m_2) = \gcd(m_2, m_3) = \gcd(m_3, m_1) = 1$
ie all coprime

(ii) $x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3 \cdots + M_n x_n a_n) \bmod M$

$M = m_1 * m_2 * m_3 * \cdots * m_n$

$M_i = \frac{M}{m_i}$

Soln
$x \equiv 3 \pmod{5}$
$x \equiv 2 \pmod{4}$
$\gcd(5,4) = 1$

$M = m_1 \times m_2 = 5 \times 4$

$M = 20$

$M_1 = \frac{M}{m_1} = \frac{20}{5} = 4$

$M_2 = \frac{M}{m_2} = \frac{20}{4} = 5$

Now $M_1 x \equiv 1 \pmod{m_1}$
$M_2 x \equiv 1 \pmod{m_2}$
$\Rightarrow$ $4x \equiv 1 \pmod{5}$
$5x \equiv 1 \pmod{4}$

$\Rightarrow$ $4x \equiv 1 \pmod{5}$ → $S1 = 4$
$x \equiv 1 \pmod{4}$ $S2 = 1$

$X = m_1 S_1 r_1 + m_2 S_2 r_2$

$= 4 \times 4 \times 3 + 5 \times 1 \times 2 = 48 + 10$

$\boxed{X = 58}$

<u>Ques.</u>

$x \equiv 1 \pmod{5}$

$x \equiv 1 \pmod{7}$

$x \equiv 3 \pmod{11}$

<u>Sol^n.</u>

$\gcd(5,7) = \gcd(7,11) = \gcd(5,11) = 1$

$M = m_1 m_2 m_3 = 5 \times 7 \times 11$

$M = 385$

$M_1 = \frac{M}{m_1} = \frac{385}{5} = 77$

$M_2 = \frac{M}{m_2} = \frac{385}{7} = 55$

$M_3 = \frac{M}{m_3} = \frac{385}{11} = 35$

Now

$77x \equiv 1 \pmod{5} \Rightarrow 2x \equiv 1 \pmod{5}$

$55x \equiv 1 \pmod{7} \Rightarrow 6x \equiv 1 \pmod{7}$

$35x \equiv 1 \pmod{11} \Rightarrow 2x \equiv 1 \pmod{11}$

$S_1 = 3, \quad S_2 = 6 \quad S_3 = 6$

$X = (M_1 S_1 r_1 + M_2 S_2 r_2 + M_3 S_3 r_3) \bmod M$

$X = (77 \times 3 \times 1 + 55 \times 6 \times 1 + 35 \times 6 \times 3) \bmod 385$

$X = 231 + 330 + 630 = 1191$

$X = 1191 \bmod 385$

$\boxed{X = 36}$

11 21 31 41 51 61 71 81

8 13 18 23 28 33 38 43

48 53 58 63 68

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

$x \equiv a \pmod{m_1}$
$x \equiv b \pmod{m_2}$
$x \equiv c \pmod{m_3}$

Solⁿ.

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

$$M = m_1 \times m_2 \times m_3 = 5 \times 7 \times 11 = 385$$

$$M_1 = \frac{M}{m_1} = \frac{385}{5} = 77$$

$$M_2 = \frac{M}{m_2} = \frac{385}{7} = 55$$

$$M_3 = \frac{M}{m_3} = \frac{385}{11} = 35$$

Multiplicative inverse

$\rightarrow$ $M_1 \cdot M_1^{-1} \equiv 1 \pmod{m_1}$
$77\, M_1^{-1} \equiv 1 \pmod 5$
$2\, M_1^{-1} \equiv 1 \pmod 5$ $\qquad \boxed{M_1^{-1} = 3}$

$\rightarrow$ $M_2 \cdot M_2^{-1} \equiv 1 \pmod{m_2}$
$55 \cdot M_2^{-1} \equiv 1 \pmod 7$
$6 M_2^{-1} \equiv 1 \pmod 7$ $\qquad \boxed{M_2^{-1} = 6}$

$\rightarrow$ $M_3 \cdot M_3^{-1} \equiv 1 \pmod{m_3}$
$35 \cdot M_3^{-1} \equiv 1 \pmod{11}$
$2\, M_3^{-1} \equiv 1 \pmod{11}$ $\qquad \boxed{M_3^{-1} = 6}$

$$X = (M_1 M_1^{-1} a + M_2 M_2^{-1} b + M_3 M_3^{-1} c) \bmod M$$
$$= (77 \times 3 \times 1 + 55 \times 6 \times 1 + 35 \times 6 \times 3) \bmod 385$$
$$= (231 + 330 + 630) \bmod 385$$
$$= 1191 \bmod 385$$
$$= 36$$

Scanned with OKEN Scanner