Page
Date

Info sec

① Primes → Definition { smallest prime 2
1 not

② co prime → which gcd(a,b) = 1
or relatively prime

① If p prime 1 to p-1 all Integers are co-prime

② z^*_n

③ cardinality of primes → no. of prime in fixed ?

Ex 2, 3, 5

⇒ 2×3×5+1 = 31 is a prime

④ No. of primes less than n
but range can be done

Ex $\frac{n}{\ln n} < \pi(n) < \left(\frac{n}{\ln n} - 1.08366\right)$

⇒

Ex 72,383 < 1000000 < 78543

78,498

⑤ Checking for primeness

Ex 97 is a prime

$\sqrt{97} = 9$ se less prime

2, 3, 5, 7 if any of these no. divide
9 not prime

if not, 97 is prime

Spiral

Page
Date

इरेटोस्थेनेस

✱ Sieve of Eratosthenes

⇒ which prime less than or = n

Ex 16 $\sqrt{16} = 4 \rightarrow 2, 3$

2 3 4 5 6 7 8 9 10

11 12 13 14 15 16

5, 7, 11

✱ Euler's phi function → tells no. of Integer (starting from 1) which is co-prime to n

(1) $\phi(1) = 0$

(2) $\phi(p) = p-1$ if p is prime

(3) $\phi(m \times n) = \phi(m) \times \phi(n)$ [m & n is prime, gcd(m,n) = 1]

(4) $\phi(p^e) = p^e - p^{e-1}$. p prime

Ex $\phi(240)$

$\phi(60) = \phi(2^2) \times \phi(3) \times \phi(5)$

$= 2^2 - 2^1 \times 2 \times 4 = 16$

Ex Z_{14}^* [n>2 n is even]

$\phi(14) = \phi(7) \times \phi(2)$

$= 6 \times 1 = 6$

1, 3, 5, 9, 11, 13

✱ Fermat little Thm (where p is prime)

60

2 3

2 2

1

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

{where p is prime & gcd(a, p) = 1

Spiral

Page
Date

Second

$a^p_{\text{mod } p} = a \bmod p$ — p is prime; gcd (a, p) is any

Ex

$6^{10} \bmod 11$

$3^5 \bmod p_5 = 3 \bmod 5$
$= 3$

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

*** Multiplicative Inverse**

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

Ex $8^{-1} \bmod 3 \Rightarrow 8x \bmod 3$ — p = prime, gcd (8, 3) = 1
$x = 2$
ans (2)

gcd (16, 3) = 1

$6^{-1} \bmod 5 \Rightarrow 6x \bmod 5 = 1 \bmod 5$

$8^{-1} \bmod 3 = 8^{3-2} \bmod 3 = 2$

*** Euler's theorem**

First Theorem version $\rightarrow a^{\phi(n)}_{\text{mod } n} = 1 \bmod n$ — gcd(a, n) = 1

gcd (6, 35) == 1 — $\phi(n) \rightarrow$ no. of prime less than n

Ex $6^{24} \bmod 35$

$\phi(35) = \phi(7) \times \phi(5) \Rightarrow 6 \times 4 = 24$ so ans is 1

Second version — if $n = p \times q$ — p & q gcd = 1, p, q & r = prime

gcd (p, q) = 1.

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

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

Ex $20^{62} \bmod 77 \Rightarrow \phi(77) = \phi(11) \times \phi(7)$
$10 \times 6 = 60$

$(20)^{60} \bmod 77 \times (20)^2 \bmod 77 \Rightarrow 1 \times 15 = 15$ Ans

Spiral

mul

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

Page
Date

generate prime

Mersenne $2^{p} - 1$ (p → Prime) but it fail on some $2^{11}-1 = 2047 = 23 \times 89$

Fermat $2^{(2)^n} + 1$ but it fail on some $2^{2^5}+1$ = 4294967297
$= 641 \times 6700417$

$n = 0$

Primality testing

Deterministic algorithm

Divisi — √n [2 to √n]

AKS — start divide
if divide n prime
if not prime

probabilistic algorithm — if it is 1 so we can't sure n is prime

Fermat → $a^{n-1} \bmod n = 1$ ⇒ n prime
$a^{n-1} \bmod n \neq 1$ ⇒ n composite

Miller Rabin

Ex $n = 561$ prime or not

① $n-1 = m \times 2^k$ [form]
$560 = 35 \times 2^4$

② [let a = 2]
$T = a^m \bmod n = 2^{35} \bmod 561$
$= 263 \bmod 561$
if ±1 pri
if not non

③ for (i = 1 to k-1)

$k = 1$ $T^2 = (263)^2 \bmod 561 = 166$ = +1 not pri
$-1 = n-1$ pri

$T = (166)^2 \bmod 561 = 67$

$k = k-1$ $T = (67)^2 \bmod 561 = +1$ not prim

④ return composite if loop fail

Spiral

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.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv a_K \pmod{m_K}$$

$\gcd(m_1, m_2) = \gcd(m_2, K) = \gcd(m_K, m_1) = 1$

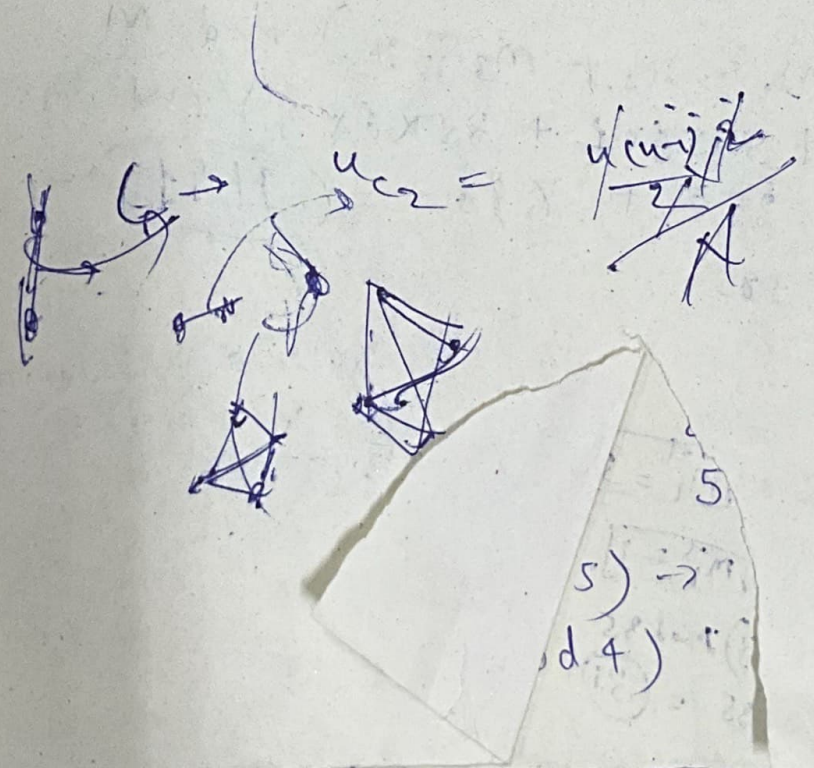
Soln follow these steps:

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 $x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \ldots + a_K \times m_K \times M_1^{-1}) \bmod M$



$X = m_1 s_1 r_1 + m_2 s_2 r_2$

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

$\boxed{X = 58}$

Ques. $x \equiv 1 \pmod 5$

$x \equiv 1 \pmod 7$

$x \equiv 3 \pmod{11}$

Sol^n $\gcd(5,7) = \gcd(7,11) = \gcd(5,11) = 1$

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

$M = 385$

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

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

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

Now

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

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

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

$S1 = 3, \quad S2 = 6 \quad S3 = 6$

$X = (m_1 s_1 r_1 + m_2 s_2 r_2 + m_3 s_3 r_3) \bmod M$

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

$X = 231 + 330 + 630 = 1191$

$X = 1191 \bmod 385$

$\boxed{X = 36}$

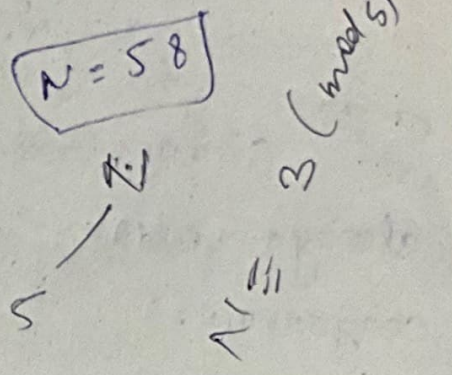
11 21 31 41 51 61 71 81

8 13 18 23 28 33 38 43

48 53 58 63 68 .

Ques. Can be → If we have N books and if we devide it in 5 students remainder = 3 and if we devide it in 4 students book left = 2.

So find no. of books?



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

$4x \equiv 1 \pmod 5 \rightarrow S1 = 4$

$\Rightarrow x \equiv 1 \pmod 4 \quad S2 = 1$

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

$x = 233 \equiv 23 \pmod{105}$ 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 $gcd(num[0], num[i]) = 1$

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, 3

$x \equiv 1 \bmod 5$, $x \equiv 3 \bmod 7$ $\quad gcd(5,7) = 1$

$M = 5 \times 7 = 35$, $M_1 = 7$, $M_2 = 5$

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

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

$X = (7 \times 3 \times 1 + 5 \times 3 \times 3) \bmod 35$

$\equiv 21 + 45 \bmod 35 = 66 \bmod 35 = 31$

$x \equiv 3 \pmod 5$

$x \equiv 1 \pmod 7$

$gcd(5,7) = 1$

$M = m_1 \times m_2 = 5 \times 7 = 35$

$M_1 = \frac{M}{m_1} = \frac{35}{5} = 7$

$M_2 = 5$

$M_1 \cdot M^{-1} \pmod M \equiv 1 \pmod M$

$M^{-1} \equiv 1 \pmod{35}$

Chinese Remainder Theorem

$x \equiv r_1 \pmod{m_1}$

$x \equiv r_2 \pmod{m_2}$

$x \equiv r_3 \pmod{m_3}$

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

$= 1$

Soln

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

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

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

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

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

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

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

$21x \equiv 1 \pmod 5$

$15x \equiv 1 \pmod 7$

$2x \equiv 1 \pmod 3$

$x \equiv 1 \pmod 5$

$x \equiv 1 \pmod 7$

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

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

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

Ques $x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

$\gcd(3,5) = \gcd(5,7) = \gcd(3,7) = 1$

① $M = 3 \times 5 \times 7 = 105$

② $M_1 = \frac{105}{3} = 35 \quad M_2 = \frac{105}{5} = 21$

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

③ $35\, M_1^{-1} \equiv 1 \pmod 3$

$2\, M_1^{-1} \equiv 1 \pmod 3$

$\boxed{M_1^{-1} = 2}$

$21\, M_2^{-1} = 1 \pmod 5$

$M_2^{-1} = 1 \pmod 5$

$\boxed{M_2^{-1} = 1}$

$15\, M_3^{-1} \equiv 1 \pmod 7 \qquad \boxed{M_3^{-1} = 1}$

$M_3^{-1} \equiv 1 \pmod 7$

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

$= (140 + 63 + 30)$

$= 233 \bmod 105 = \boxed{23}$

The CRT is used to solve a set of congruent Eq^n with one variable but different moduli which are relatively prime

$x \equiv a \pmod{m_1}$

$x \equiv b \pmod{m_2}$

$\vdots$

$x \equiv c \pmod{m_k}$

- $\gcd(m_1, m_2) = \gcd(m_2, m_3) = \gcd(m_{k-1}, m_k) = 1$

① $M = m_1 \times m_2 \times m_3 \times \cdots m_k$

② $M_i = \frac{M}{m_i} \quad / \quad M_1 = \frac{M}{m_1}$

③ m.i. of $(M_1, M_2, \cdots M_k)$ using the corresponding moduli $(m_1, m_2 \cdots m_k)$ $\quad M_i^{-1}$

④ $x = (M_1 M_1^{-1} a + M_2 M_2^{-1} b \cdots + M_k M_k^{-1} c) \bmod M$

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

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

Sol^n. $\gcd(m_1, m_2) = \gcd(m_2, m_3) = \gcd(m_1, m_3) = 1$

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

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

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

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

Multiplicative inverse

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

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

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

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

Factorization

Fermat's Factorization Method

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

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

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

$y^2 = x^2 - N$
$= \omega$
$y = \sqrt{\omega}$

Steps for fermat's

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

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

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

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

```
Feramat_factorization(n)
{
    x ← √n          // smallest int greater than √n
    while (x < n)
    {
        ω ← x^2 - n
        if (ω is perfect square)
            y ← √ω ; 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

Ideq. → 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

Acc. to **Fundamental Theorem of Arithmetic**

$$n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_K^{e_K}$$

GCD :-

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_K^{a_K}$$

$$b = p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_K^{b_K}$$

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \cdots \times p_K^{\min(a_K,b_K)}$$

LCM :-

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_K^{a_K}$$

$$b = p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_K^{b_K}$$

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} \times p_2^{\max(a_2,b_2)} \times \cdots \times p_K^{\max(a_K,b_K)}$$

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

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
}
```

(outer loop: $\sqrt{n}$; inner loop: $\log_a n$, since $n = a^k$, $k = \log_a n$)

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.

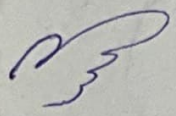
Time Comp. $(\sqrt{n} \log_a n)$

36
2×18
3×12
4×9
6×6
9×4
12×3

$[2, \sqrt{n}]$

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
}
```

Time Com → $O(n^{1/4})$

Ex. $n = 21$ $B = 10$ $f(n) = x^2 + 1$

$x \leftarrow 2$
$y \leftarrow 2$
$p \leftarrow 1$

first it :-

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

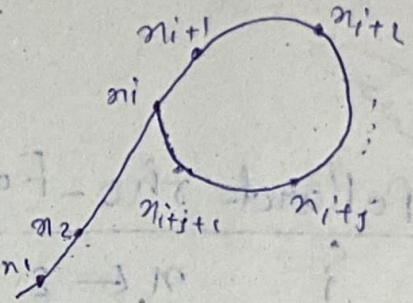
$y = f(f(2)) \bmod 21 = f(5) \bmod 21 = 26 \bmod 21 = 5$

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

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 Ideq :- 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 slee.



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

Ex. $n = 91 \quad (7 \times 13)$

$x = y = 2$

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

.....

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

$(7, 91) = 7$

T.C. $O(n^{1/4})$

$O(2^{nb/4})$

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 $\quad O(e^C) \; ; C \simeq 2(\ln n)^{1/3}(\ln\ln n)^{2/3}$

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 ~~jisse~~ 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. $O(B \log n)$

n, B 5

a → 2
e → 2

$a \leftarrow a^e \bmod n$

$a \leftarrow a^e \bmod n$

$a \leftarrow 2^{\cdots} \bmod n$

gcd(a-1, n)

55
11 5

17

16
2×2×2×2

96
2 5 3 1

97

Pollarad-(P-1) :→

Pollarad-(P-1)_Fact (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
}

Example: n = 8051 , B = 5

a = 2

- e = 2, $a = 2^2 \bmod 8051 = 4$
- e = 3, $a = 4^3 \bmod 8051 = 64$
- e = 4, $a = 64^4 \bmod 8051 = 2877$
- e = 5, $a = 2877^5 \bmod 8051 = 1441$

P = gcd(1441-1, 8051) = gcd(1440, 8051)

P = 97

P-1 = 96 isme 2 aur 3 —
fail B ko badhake retry

Factorization

⇒ $72 = 2^3 \times 3^2 = 2 \times 2 \times 2 \times 3 \times 3$.

$n = p_1^{a_1} \times p_2^{a_2} \times p_3^{a_3} \times \dots \times p_k^{a_k}$

GCD:

$72 = 2^3 \times 3^2 \times 5^0$

$45 = 2^0 \times 3^2 \times 5$

$2^{\min(3,0)} \times 3^{\min(2,2)} \times 5^{\min(0,1)}$

$= 2^0 \times 3^2 \times 5^0 = 9$ ✓

LCM

$72, 45$

$= 2^3 \times 3^2 \times 5^1$

$= 360$ ✓

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

(1) Trial_Div_Fac(n)

{

$a \to 2$

$a = 2\ 3\ 4$

$72\ 36\ 18\ 9\ 3\ 1$

}

$a \to 3$

(2) $72\ 36\ 18\ 9\ 3\ 1$

$a \to 2$

(3) $72\ 36\ 18\ 9\ 3\ 1$

(4) $\sqrt{72}$

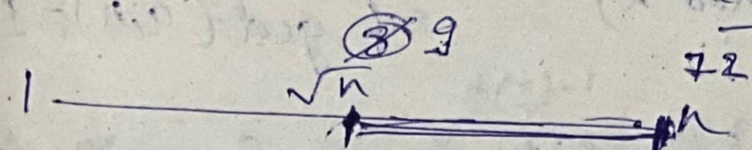
$2 \times 2 \times 2 \times 3 \times 3$

$\boxed{2 \times 2 \times 2 \times 3 \times 3 \times 1}$

(i) $n =$

$n = x^2 - y^2$

$n = (x+y) \times (x-y)$



$x \to \sqrt{n}$

$n = 9$

$y^2 = x^2 - n$

$w = x^2 - n$

$w \leftarrow x^2 - n$

$w \leftarrow 81 - 72 \Rightarrow 9$

$y^2 = 9$

$72 = 9^2 - 3^2$

$= 81 - 9$

$72 = \boxed{12} \times \boxed{6}$

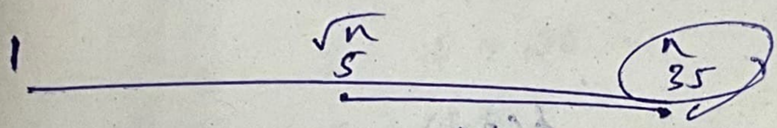
n is odd

$\boxed{n = x^2 - y^2}$

0, 1, 4, 9, 16, 25, 36

1, 3, 5, 7, 9, 11, 13, 15

Fermat. $n = 35$



$x \to 5$ 6

$w \leftarrow x^2 - n$

First $\boxed{7} \times \boxed{5}$

n odd

$n = x^2 - y^2$

$81 = 9 \times 9$

$36 = 4 \times 9$

$w \leftarrow x^2 - n$

$y^2 = \sqrt{1}$

$x = 6$

$a = 7$

$b = 5$

7

$n = x^2 - y^2$

$\sqrt{n}$ 0

Pollard $(P-1)(\ldots (n, B)$

Euler's

① $a^{\phi(n)} \equiv 1 \pmod{n}$ if $\gcd(a,n) = 1$

$\phi(n)$: no. of int which are co-prime with n

② $a^{k \times \phi(n)}$ $n = p \times q$

(i) → if a is not a factor of p/q

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

(ii) → $$a^{k \times \phi(n)} \bmod n = a \bmod n$$

Ques. $6^{24} \bmod 35 = 6^{\phi(35)} \bmod 35$

$= 1$ Ans

$35 = 5 \times 7$

$24 = k \times \phi(n) + 1 = k \times 24 + 1$

$\phi(35) = \phi(5) \times \phi(7)$

$= 4 \times 6$

$= 24$

Fermat

① $a^{p-1} \bmod p = 1$

② $a^p = a \bmod p$

2^1 2^6

Ques. $20^{62} \bmod 77$

$20^{60} \times 20^2 \bmod 77$

$20^{60} \bmod 77 \times 20^2 \bmod 77$

$1 \times (20)^2 \bmod 77$

$400 \bmod 77$

(15)

$\phi(77) = \phi(7) \times \phi(11)$

$= 6 \times 10$

$= 60$

$k \times 60 + 1 = 2$

$k \times 60 = 1$

$k = \frac{1}{60}$

Multiplicative Inverses

$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$ $\quad \gcd(a, n) = 1$.

① $8^{-1} \bmod 3 = 8^{\phi(3)-1} \bmod 3$

$= 8^{2-1} \bmod 3$

$= 8 \bmod 3 = 2$

② $71^{-1} \bmod 100 = 71^{\phi(100)-1} \bmod 100$

$= 71^{40-1} \bmod 100$

$= 71^{39} \bmod 100$

$\phi(100) = 2^2 \times 5^2$

$= (2^2 - 2^1) \times (5^2 - 5^1)$

$= 2 \times 20$

$= 40$

$\phi(100)$

$= \phi(10) \times (\cdot$

$= \phi(2) \times \phi(5) \times ($

$= 1 \times 4 \times (1 \times 4$

$= 16$

③ Generating Primes

→ $M_p = 2^p - 1$ (mersenne primes)

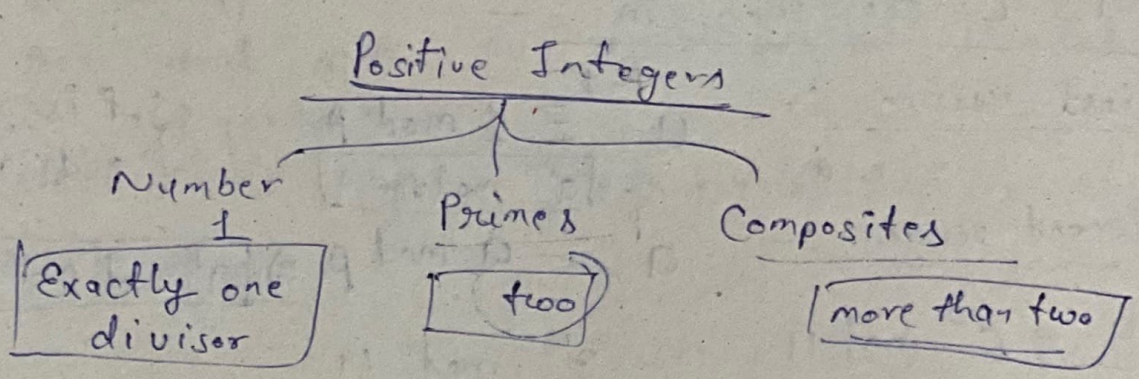
→ $F_n = 2^{2^n} + 1$ (Fermat tested)

Sieve of Eratosthenes

```
fun(N)
{
    prime [N+1]
    for ( i=2 → N )  prime[i] = 1                    ] O(n)

    for ( i=2 → √N )
    {
        if (prime[i] == 1)
        {
            for( j = ixi ; j<=N ; j+=i)              ] O(Nlog(logN))
                prime[i] = 0;
        }
    }
}
```

Primes



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

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

$$\left[n/\log_e n\right] < \pi(n) < \left[n/(\ln n - 1.08366)\right]$$

Checking for Primeness :-

Sieve of Eratosthenes -

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

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

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 :-

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

{ p is prime
gcd(a, p) = 1

(from first version of fermat's little theorem)

Euler's Theorem

generalization of fermat's little theorem -

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

{ → a, n is any integer
→ gcd(a, n) = 1

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

Second version $a^{K \times \phi(n)+1} \equiv a \pmod n$

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

{ gcd(a, n) may or may not equal to 1 (means no condition)

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 :- no. 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