CLASS-38

Number Theory

Seive of Eratthonesis

@ 1 - n $n \log(\log(n))$

```
For (i=0; i<n; i++)
{
    [ For (j=0; j<n; j++)
      {
      }
      n ]
}
```

T.C = n^2 ?

n

i.e. $\underbrace{n + n + n + \cdots}_{n} \Rightarrow n * n = n^2$

Highest Prime and lowest Prime

Prime factorization → i = 3 -- n

```
while(n%i)
{
}
```

O(n)

n

$n \log(n)$

Using Seive

O(log(n))

highest - Prime factor

lowest - Prime factor

hp, lp

0 →

36 ⇒ 2 * 2 * 3 * 3

lp = 2

hp = 3

Vector <int> Prime_factors;

num

num = $p_1^{\square} * \square * \square$

num=1

lp

p1

p2

hp[num] = i ⇒ p3

Prime factor

while (num > 1)

11, 2

log(n)

int prime_factor = hp[num];

while (num % p_factor == 0)

num =

8 % 2 == 0

num = p_factor;

Prime factors.push_back(prime_factor)

11, 2

n → ---- 1

log(n)

88 → 2 * 2 * 2 * 11

88

86

11

lp[88] = 2

8

hp[88] = 11

hp[8] = 2

Prime factors.

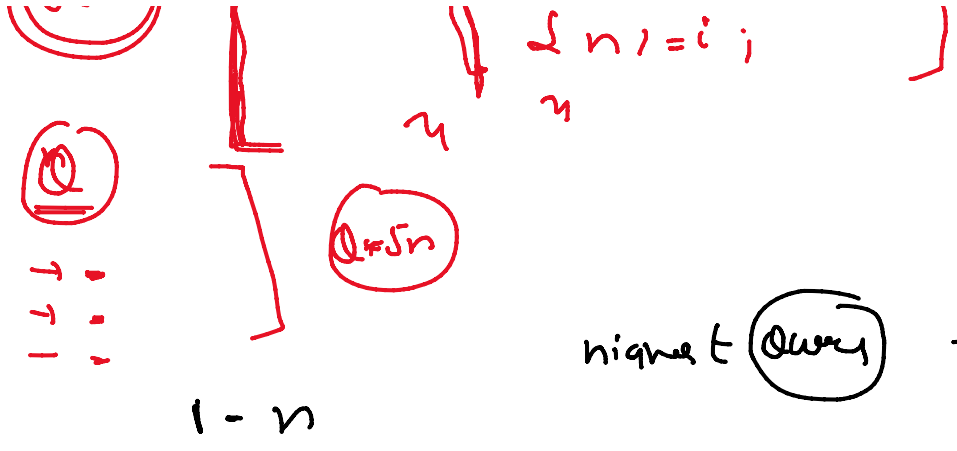
11 | 2 | 2 | 2

88

5 7 9 11

O(√n)

```
for (i=3; i*i <= n; i+=2)
{
    while (n%i==0)
    {
        n = i;
```



highest Query → 10^5 → 10^7 One time operation

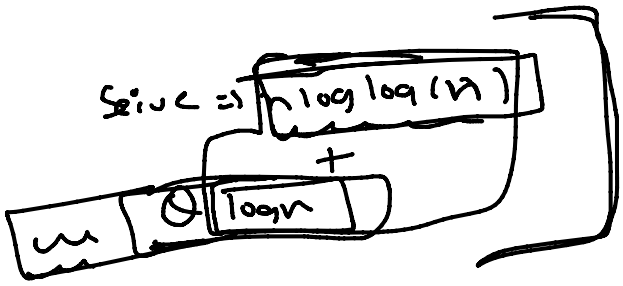
6 = 2, 3

hp[6] = 3 hp[2] = 0

while (6 % 3 == 0) (2 % 0 =)

n = 2

6 = 2 * 3



Seive → 1 - n Prime Nos] → nloglogn / → nloglogn

- Higheet Prime % lP
- Prime factorization
- Divisors ?

1 - N

36 → 1, 2, 3, 4, 6, 9, 12, 36, 18

1 → Divisor

For element

```
for (i=1; i*i <= N; i++)
    if (n%i == 0)
        print i
```

```
for (i=1; i<=n; i++)
{
}
```

$n\sqrt{n}$

Seive

2 3 4 5 6 7 8 9 10 11 12 ...

2, 4, 6, 8, 10, 12 ...

```
vector<int> divisors[N];
for (i=1; i<=n; i++)
{
  for (j=i; j<=N; j+=i)
  {
    divisors[j].push_back(i);
  }
}
```

i = 3 → 6, 9, 12 ...

T.C = ?

i^{th} element divisor of j^{th} element

$N \log N$

6, 12, 18

3 → 3
6 → 3, 6
9 → 3
12 → 3, 6

3, 6, 9, 12, 15, 18 ...

$$N + \frac{N}{2} + \frac{N}{3} + \frac{N}{4} + \frac{N}{5} + \dots$$

$$N\left[1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots\right]$$

log n

$N \log n$

→ Facts about Numbers

Goldbach's Conjecture

Goldbach's Conjecture

Every even number greater than 4 can be written as sum of 2 odd Prime

1 → Prime

6 → 3+3 | 12 → 7+5 | 18 → 13+5

8 → 5+3 | 14 → 7+7 | 20 → 17+3

10 → 7+3 | 16 → 11+5

Twin Prime Conjecture

There are many twin primes

→ Prime Nos with diff of 2

(5,3) (7,5) (11,13) (17,19) (29,31) - - -

- - - -

Legendre's Conjecture

$n^2 < p < (n+1)^2$

Btw any 2 consecutive perfect squared we always have atleast Prime No

4, 9 | 4 < 3,5 < 9

73 89

4 9 16 25 36 49 64 81 100

2 3 5 7 11 13 19 23 29 31 37 ... 53 61

Modular / Binary Exponentiation → log(p)

(n^p) % m

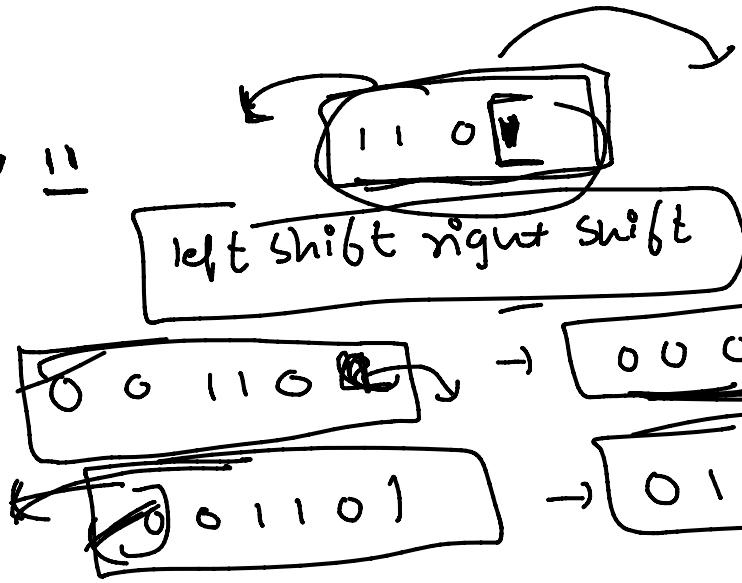
pow(n,p) % m

```
int ans = 1;
for ( i = 1; i <= p; i++ )
{
    ans = (ans * n) % mod;
}
```

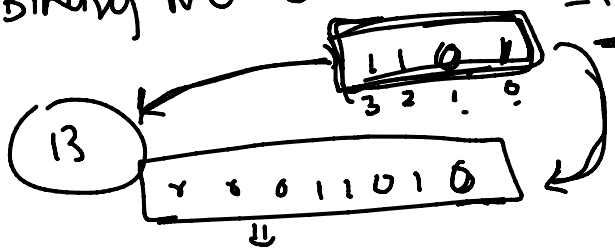
O(n) O(p)

Bits

3 → 11



Binary NO decimal No →



→ $2^0 * 1 + 2^1 * 0 + 2^2 * 1 + 2^3 * 1$

→ 1 + 0 + 4 + 8 = 13

$2^1 * 0 + 2^1 * 1 + 2^2 * 0 + 2^3 * 1 + 2^4 * 1$

$= 0 + 2 + 0 + 8 + 16 = 26$

0 0 0 -- 1 1 0 → $2^0 * 0 + 2^1 * 1 + 2^2 * 1$

0 0 0 -- 1 1 0 → $2^0 * 0 + 2 * 1 + 2^2 * 1$

$= 2 + 4 = 6$

Binary No → left shift (no * 2)

Right shift (no / 2)

$\frac{13}{2} = 6$

(n) n >> = 1

n = n >> 1

n = n / 2

n << = 1

n = n << 1

n = n * 2

```
int Power (int n, int y, int m)
{
    int res = 1;
    while (y > 0)
    {
        if (y & 1 == 1)
        {
            res = (res * n) % M
        }
        y = y >> 1
        n = (n * n) % M
    }
}
```

y & 1 ≥ 1

T.C = O(log n)

n → (log(n))

Modular exponentiation

O(n) → O(log n)

13 → 1101

$2^0 * 1 + 2^1 * 0 + 2^2 * 1 + 2^3 * 1$

$= 1 + 0 + 4 + 8$

Decimal Representation

res = 1

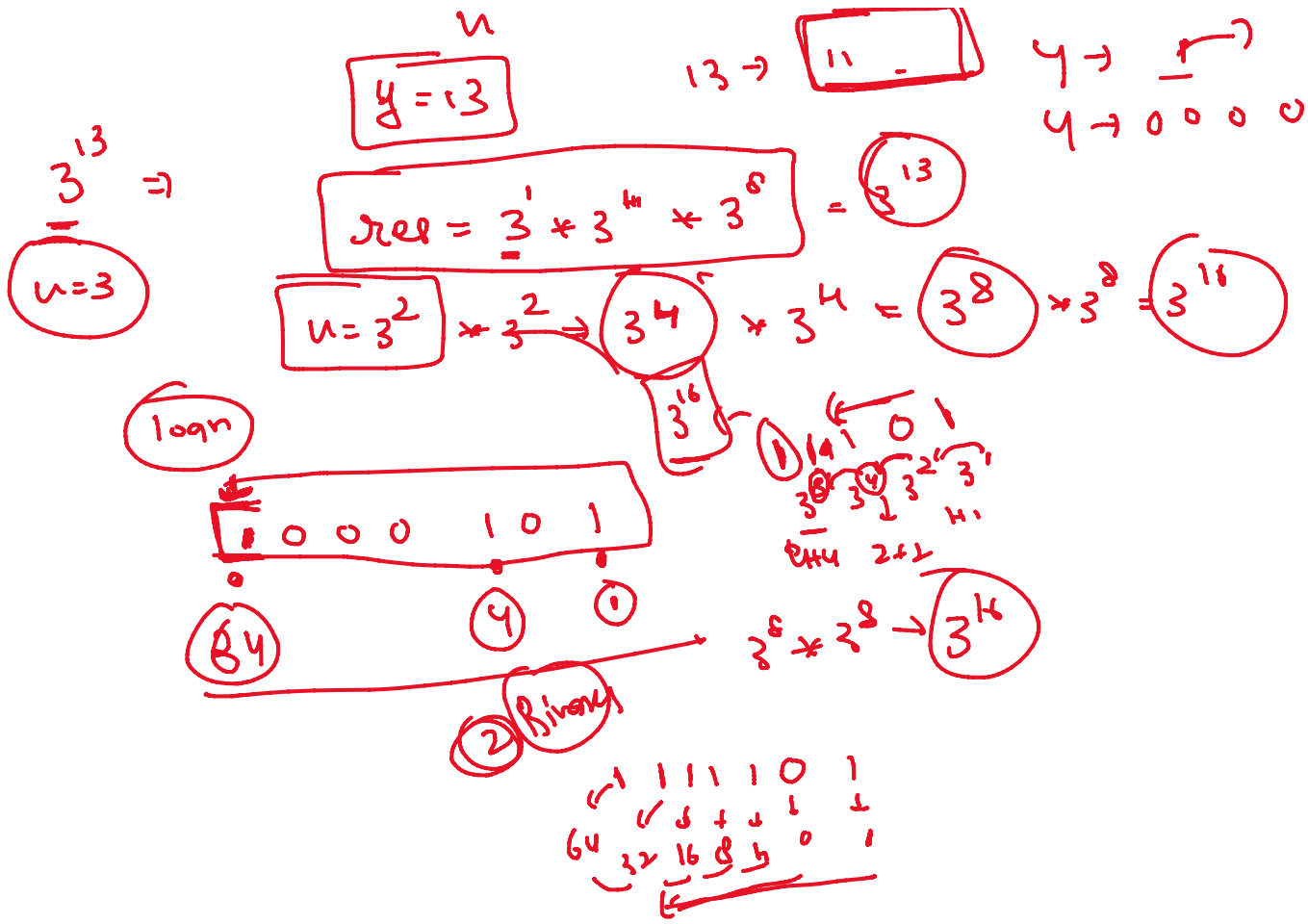
y → —

n

n - - 2

13 → 11 _

y → _


n
y = 13
13 → 11 .
y → _
y → 0 0 0 0
3^13 ⇒
n = 3
rel = 3^1 * 3^4 * 3^8 = 3^13
n = 3^2
* 3^2 → 3^4
* 3^4 = 3^8 * 3^8 = 3^16
3^16
log n
1 0 0 0 1 0 1
64
4
1
2 Binary
3^8 * 3^8 → 3^16
1 1 1 1 1 0 1
64 32 16 8 4 0 1