Number Theory

√ 1) Primality Testing (1 #)
√ 2) Prime Sieve
√ 3) Prime Factorization
√ 4) GCD, LCM
√ 5) Mod Inverse
√ 6) # Divisors of n, Sum of Divisors
7) Euler Phi Function
8) Euler's Thm (Fermat's Thm), trick mod inverse...
9) # times a prime divides n!

Prime - int ≥ 2, with only 2 divisors 1 and itself.

SLOW →

```
for (i=2; i<n; i++)
    if (n%i == 0)
        return COMPOSITE!
return PRIME
```

$O(n)$

i*i<=n

$n = a \times b$ and $a \le b$ then $a \le \sqrt{n}$.

Assume the opposite: $a > \sqrt{n}$ and $b > \sqrt{n}$.

$$\left.\begin{aligned} n &= a \times b \\ &> \sqrt{n} \times \sqrt{n} \\ &= n \end{aligned}\right\} \quad n > n$$

Contradiction!

FIX

96
13
288
96

Prime Sieve

All int 1 to n prime:

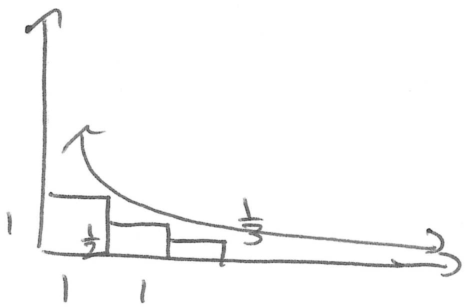
~~1~~ 2 3 ~~4~~ 5 ~~6~~
~~8~~ 7 ~~9~~ ~~9~~ ~~10~~ → booleen array!
11 ~~12~~ 13 ~~14~~ ~~15~~
~~16~~ 17 ~~18~~ 19 ~~20~~
~~21~~ ~~22~~ 23 ~~24~~ ~~25~~

```
for (i = 2; i*i <= n; i++)
    for (j = 2*i; j <= n; j += i)
        isprime[j] = false
```

$$\frac{n}{2} + \frac{n}{3} + \frac{n}{4} + \cdots \frac{n}{n} = n\left(\frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{n}\right) = O(n \lg n)$$

$$< n\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{n}\right)$$

$$= nH_n$$

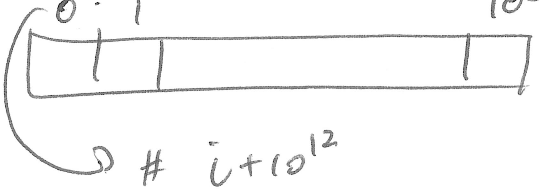


$$1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{n} < 1 + \ln n$$

$$\int_1^n \frac{1}{x}\,dx = \ln x \Big|_1^n = \ln x$$

generate all primes from 10^{12} to $10^{12} + 10^5$ $\qquad (10^6 + 10^3)^2 > 10^{12} + 10^5$

1) Gen all primes upto $10^6 + 10^3$




```
for (ll x : primes)
    y = minval in range
        divisible by x
    while (y < length) {
        y-10^12
        isprime[y-10^12] = false
        y += x;
    }
```

Prime Factorization

Like primality test, but when you find a divisor, store it!

$n = 1248 \qquad d = 2$

$1248 \xrightarrow{} 624 \xrightarrow{} 312 \xrightarrow{} 156 \xrightarrow{} 78 \xrightarrow{} 39$

exp $+1 \quad +1 \quad +1 \quad +1 \quad +1$ (while)

$39 \xrightarrow[+1]{} 13$

$\downarrow$ prime

$$\boxed{(2,5),\ (3,1),\ (13,1)}$$

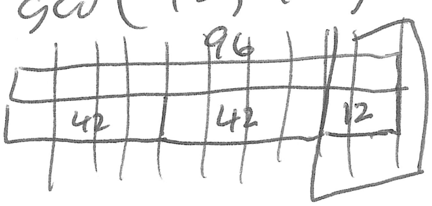
GCD

greatest common divisor

gcd(42, 96)

$42 \% 6 = 0$ ✓

$96 \% 6 = 0$ ✓



$$\underset{a\ \ \ b}{\gcd(96, 42)} = \gcd(\underset{b}{42}, \underset{a \% b}{96 \% 42})$$

return b == 0 ? a : gcd(b, a%b)

least common multiple

$$\operatorname{lcm}(a, b) = \frac{a * b}{\gcd(a,b)}$$

Mod Inverse

Answer mod 10^9+7

$\frac{a}{b}$ } super large int

$\frac{a}{b}$ mod n ?

How on earth do you divide in mod?

$\left(\frac{a}{b}\right) \times b \equiv a \mod n$ Ought to be true!

$(a \times b)(?) \equiv a \mod n$

If $b \times (?) \equiv 1 \mod n$

then $(a \times b)(?) \equiv a \mod n$

? denote as $b^{-1} \mod n$

b^{-1} equals that value such that

$b \times b^{-1} \equiv 1 \mod n$

$7 \times 13 \equiv 1 \mod 15$

means that $7^{-1} \equiv 13 \mod 15$

$$7x \equiv 11 \mod 15$$

What is x?

$$13 \times 7x \equiv 13 \times 11 \mod 15$$

$$x \equiv 143 \equiv 8 \mod 15$$

$b^{-1} \bmod n$ exists if and only if $\gcd(b, n) = 1$.

Compute $\dfrac{a^n - 1}{a-1} \mod 10^9+7$

$\rightarrow (a^n - 1) \times (a-1)^{-1} \mod 10^9+7$

```
x = (modpow(a, n, mod) - 1 + mod) % mod
y = modInv(a-1, mod)
return (x*y) % mod
```

Ans is $\frac{a}{b}$ instead compute $a \times b^{-1} \mod 10^9+7$

Number of Divisors of an int

$n = p_1^{a_1} p_2^{a_2} \cdots$ $= 2^5 \times 3^2 \times 5^3$

$= 2^a \times 3^b \times 5^c$

$d(n) = \prod_{p_i \in \text{primes}} (a_i + 1)$

$0 \le a \le 5$ $\quad 6 \times$

$0 \le b \le 2$ $\quad 3 \times$

$0 \le c \le 3$ $\quad 4$

$2^5 \times 3^2 \times 5^3$

$\downarrow$

$(1 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5)(1 + 3^1 + 3^2)(1 + 5^1 + 5^2 + 5^3)$

$\frac{2^6 - 1}{2 - 1} \qquad \frac{3^3 - 1}{3 - 1} \qquad \frac{5^4 - 1}{5 - 1}$

$$\boxed{\sigma(n) = \prod_{p_i \in \text{prime}} \frac{p_i^{a_i + 1} - 1}{p_i - 1}}$$

Euler ϕ function

$\phi(n) = \#$ integers in set $\{1,2,3,\ldots n\}$ that are relatively prime to n.

$\phi(6) = 2$ because $\gcd(6,1)=1$ and $\gcd(6,5)=1$

but $\gcd(6,2)$, $\gcd(6,3)$, $\gcd(6,4)$, $\gcd(6,6) > 1$.

$\phi(p) = p-1$, rel prime to all of $1,2,3,\ldots,p-1$

$p \in$ Prime

$\phi(p^k) = p^k - p^{k-1}$] all numbers upto p^k subtract out $\cancel{p}$ multiples of p, so $\frac{p^k}{p} = p^{k-1}$ such multiples

$= p^k\left(1-\frac{1}{p}\right)$

if $\gcd(m,n)=1$, then $\phi(mn) = \phi(m) \times \phi(n)$,

ϕ is a multiplicative function!

$n = p^a q^b r^c \rightarrow \phi(n) = (p^a - p^{a-1})(q^b - q^{b-1})(r^c - r^{c-1})$

$= p^a\left(1-\frac{1}{p}\right) \cancel{p} q^b\left(1-\frac{1}{q}\right) r^c\left(1-\frac{1}{r}\right)$

$= \underline{p^a}\left(\frac{p-1}{p}\right) \underline{q^b}\left(\frac{q-1}{q}\right) \underline{r^c}\left(\frac{r-1}{r}\right)$

$= n\left(\frac{p-1}{p}\right)\left(\frac{q-1}{q}\right)\left(\frac{r-1}{r}\right)$

res = n

if n % p == 0

res = res/p * (p-1)

$n=10$

$\phi(2)$

1 2 3 4 5 6 7 8 9 10

gcd(i,n) $\boxed{1}$ 2 $\boxed{1}$ 2 $\boxed{5}$ 2 $\boxed{1}$ 2 $\boxed{1}$ 10

$\phi(10)$ $\phi(5)$ $\phi(1)$ of these

$9 \overline{)117}$ 1

List of all values of phi

1 2 3 4 . . . 117 n

$\phi(1)$ $\phi(2)$ $\phi(3)$ . . .

$\phi(117) = \phi(3^2 \times 13)$

$= \phi(3^2) \times \phi(13)$

1 2 3 4 5 6 7 8 9 10 11 12 13 14

2 3 2 5 2 7 2 3 2 11 2 13 2

Run prime sive but instead of setting value to false, if it's (-1) uninitialized reset to i (value you're dividing by)

117

3

$117 \rightarrow 3^2 \rightarrow 13$

Euler's Theorem

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

Let's say I want to calculate $a^{-1} \mod n$.

$$\boxed{a^{-1} \equiv a^{\phi(n)-1} \mod n}$$

$$a^{\phi(n)-1} \times a^{1} = a^{\phi(n)} \equiv 1 \mod n$$

Built in Java, Python

modular exponentiation

```
ll modexp(ll base, ll exp, ll mod) {
    if (exp == 1) return base % mod;
    if (exp % 2 == 0) {
        ll tmp = modexp(base, exp/2, mod);
        return (tmp*tmp) % mod;
    }
    return (modexp(base, exp-1, mod) * base) % mod;
}
```

times a prime p divides into n! is

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

$n=15$ $p=2$

$$1 \times \overset{1}{\cancel{2}} \times 3 \times \overset{2}{\cancel{4}} \times 5 \times \overset{3}{\cancel{6}} \times 7 \times \overset{4}{\cancel{8}} \times 9 \times \overset{5}{\cancel{10}} \times 11 \times \overset{6}{\cancel{12}} \times 13 \times \cancel{14} \times 15$$

$$\rightarrow 1 \times \overset{1}{\cancel{2}} \times 3 \times \overset{2}{\cancel{4}} \times 5 \times \overset{3}{\cancel{6}} \times 7$$

```
int numTimesDivide(int n, int p) {
    int res = 0;
    while (n > 0) {
        res += n/p;
        n /= p;
    }
    return res;
}
```

Common Factors

minimizing $\phi(n)$, maximizes ratio $\frac{n-\phi(n)}{n} = g(n)$

$$\phi(n) = n \times \frac{p-1}{p} \times \frac{q-1}{q} \times \ldots$$

$$\frac{\phi(n)}{n} = \frac{p-1}{p} \times \frac{q-1}{q} \times \frac{r-1}{r} \ldots$$

$p=2, q=3, r=5, s=7$, etc.

critical #s are 2, 6, 30, 210, etc.

$\phi(2) = \frac{1}{2}$

$\phi(6) = \frac{1}{2} \times \frac{2}{3}$

$\phi(30) = 30 \cdot \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5}$ etc.

~~$30\ \phi(30) = 1 \times 2 \times 4$~~

2, 6, 30, 210

↑

list

then find largest value ≤ query

$\frac{\phi(2)}{2} = \frac{1}{2}$

$\frac{\phi(6)}{6} = \frac{1}{2} \times \frac{2}{3}, \ldots$