

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 $\rightarrow$
$$\begin{array}{l} \text{for } (i=2; i \leq n; i++) \\ \quad \text{if } (n \% i == 0) \\ \quad \quad \text{return COMPOSITE!} \\ \text{return PRIME} \end{array} \quad \left. \vphantom{\begin{array}{l} \text{for } (i=2; i \leq n; i++) \\ \quad \text{if } (n \% i == 0) \\ \quad \quad \text{return COMPOSITE!} \\ \text{return PRIME} \end{array}} \right\} O(n)$$

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

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

$$\begin{array}{l} n = a \times b \\ > \sqrt{n} \times \sqrt{n} \\ = n \end{array}$$

}
}

$n > n$
Contradiction!

FIX

$$\begin{array}{r} 96 \\ 13 \\ \hline 288 \\ 96 \times 3 \end{array}$$

Prime Sieve

All int 1 to n prime:

~~2~~ ~~3~~ ~~5~~ *

~~7~~ ~~11~~ ~~13~~ ~~17~~ ~~19~~ ~~23~~ ~~29~~ ~~31~~

~~37~~ ~~41~~ ~~43~~ ~~47~~ ~~53~~ ~~59~~ ~~61~~ ~~67~~

~~71~~ ~~73~~ ~~79~~ ~~83~~ ~~89~~ ~~97~~

~~101~~ ~~103~~ ~~107~~ ~~109~~ ~~113~~ ~~127~~

→ boolean array!

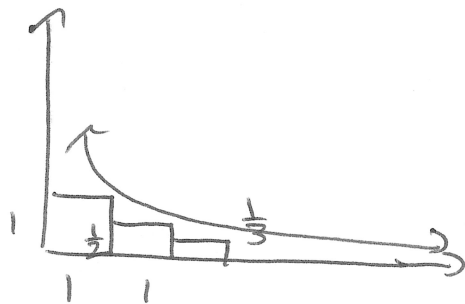
for (i = 2; i ≤ n; i++)

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

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

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

$$= n \ln n$$

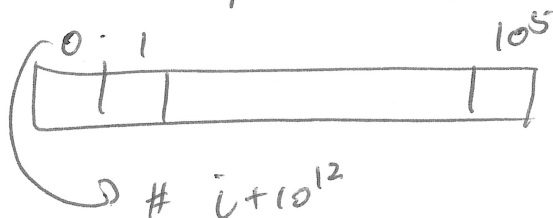


$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} < 1 + \ln n$$

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

generate all primes from 10^{12} to $10^{12} + 10^5$

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



for (all x = primes)

y = minval in range
divisible by x

while (y < length) {

 y = 10¹²
 isprime[y - 10¹²] = false
 y += x

Prime Factorization

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

$$n = 1248 \quad d = 2$$

$$1248 \rightarrow 624 \rightarrow 312 \rightarrow 156 \rightarrow 78 \rightarrow 39$$

exp +1 +1 +1 +1 +1 (while)

$$39 \rightarrow 13$$

↓ from

$(2, 5), (3, 1), (13, 1)$

GCD

Greatest common divisor

$$gcd(42, 96)$$

		96	
42	42	12	

$$42 \div 6 = 7 \quad \checkmark$$

$$96\%6 = 0 \quad \checkmark$$

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

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

least common multiple

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

Mod Inverse

Answer mod 10^9+7

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

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

How on earth do you divide in mod?

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

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

$$\text{if } b \times (?) \equiv 1 \bmod n$$

then

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

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

b^{-1} equals that value such that

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

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

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

$$7x \equiv 11 \pmod{15}$$

What is x ?

$$\underline{13 \times 7}x \equiv 13 \times 11 \pmod{15}$$

$$x \equiv 143 \equiv 8 \pmod{15}$$

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

Compute $\frac{a^n - 1}{a - 1} \pmod{10^9 + 7}$

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

$$x = (\text{modpow}(a, n) - 1 + \text{mod}) \% \text{mod}$$

$$y = \text{modinv}(a - 1, \text{mod})$$

$$\text{return } (x * y) \% \text{mod}$$

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

Number of Divisors of an int

$$n = p_1^{a_1} p_2^{a_2} \dots = 2^5 \times 3^2 \times 5^3 \\ = 2^a \times 3^b \times 5^c$$

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

$$\begin{array}{l} 0 \leq a \leq 5 \quad 6 \times \\ 0 \leq b \leq 2 \quad 3 \times \\ 0 \leq c \leq 3 \quad 4 \end{array}$$

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

↓

$$(1 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5) (1 + 3^1 + 3^2) (1 + 5^1 + 5^2 + 5^3) \\ \frac{2^6 - 1}{2 - 1} \quad \frac{3^3 - 1}{3 - 1} \quad \frac{5^4 - 1}{5 - 1}$$

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

Euler ϕ function

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

$\phi(6) = 2$ because $\gcd(6, 1) = 1$ and $\gcd(6, 5) = 1$
but $\gcd(6, 2), \gcd(6, 3), \gcd(6, 4), \gcd(6, 6) > 1$.

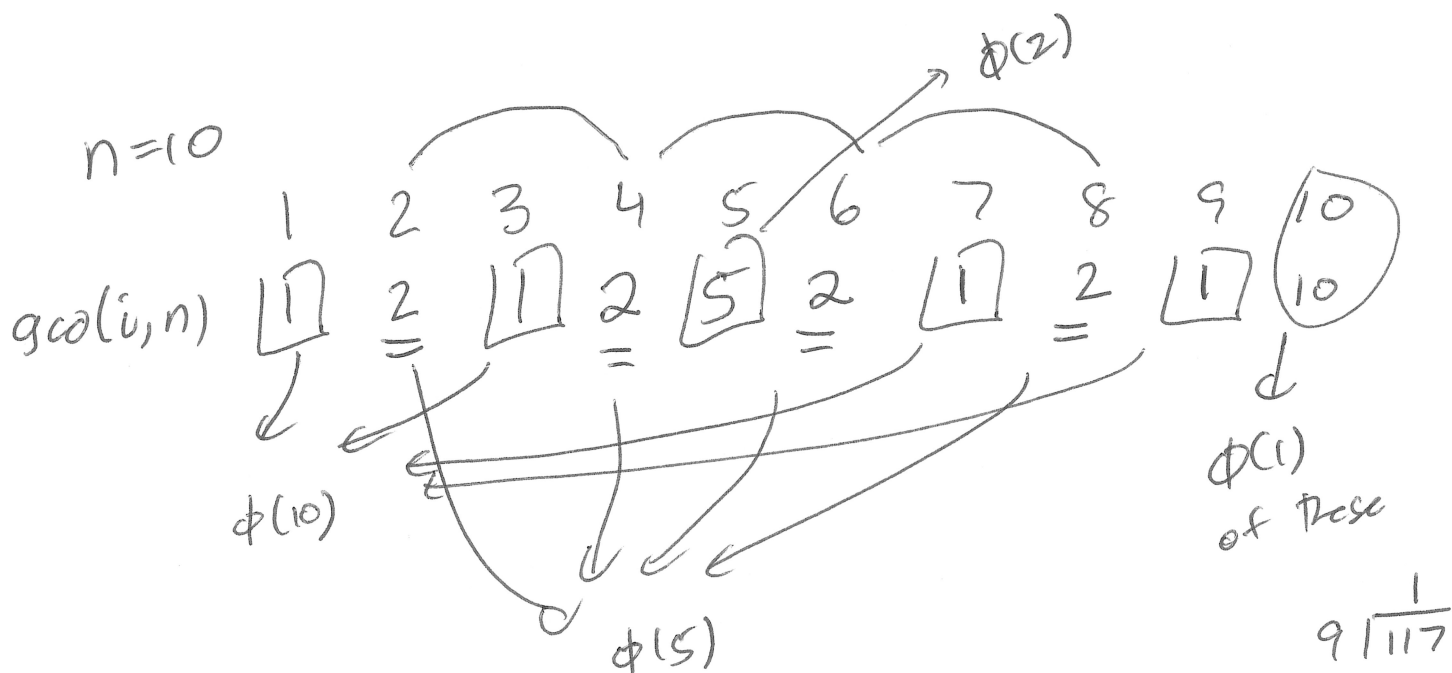
$\phi(p) = p-1$, rel prime to all of $1, 2, 3, \dots, p-1$

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

if $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m) \times \phi(n)$,
 ϕ is a multiplicative function!

$$\begin{aligned} n = p^a q^b r^c &\rightarrow \phi(n) = (p^a - p^{a-1})(q^b - q^{b-1})(r^c - r^{c-1}) \\ &= p^a \left(1 - \frac{1}{p}\right) q^b \left(1 - \frac{1}{q}\right) r^c \left(1 - \frac{1}{r}\right) \\ &= p^a \left(\frac{p-1}{p}\right) q^b \left(\frac{q-1}{q}\right) r^c \left(\frac{r-1}{r}\right) \\ &= n \left(\frac{p-1}{p}\right) \left(\frac{q-1}{q}\right) \left(\frac{r-1}{r}\right) \end{aligned}$$

res = n
if $n \bmod p = 0$
res = res / p * (p-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 sieve but instead of setting value to false, if it's (-1) uninitialized reset to i (value you're dividing by)

$$117 \rightarrow (3^2) \rightarrow (13)$$

$$117$$

$$(3)$$

Euler's Theorem

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

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

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

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

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

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

$n=15$ $p=2$

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

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 $\frac{n - \phi(n)}{n} = g(n)$

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

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

$p=2, q=3, r=5, s=7, \text{ etc.}$

critical #s are 2

6

30

210

etc.

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

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

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

$$\phi(210) = 1 \times 2 \times 4 \times 6 \times 10 \times 14 \times 20 \times 28 \times 35 \times 42 \times 56 \times 70 \times 84 \times 105 \times 126 \times 140 \times 168 \times 182 \times 210 \times 252 \times 280 \times 315 \times 350 \times 378 \times 420 \times 462 \times 490 \times 504 \times 546 \times 560 \times 630 \times 660 \times 672 \times 714 \times 728 \times 735 \times 756 \times 784 \times 798 \times 840 \times 882 \times 910 \times 924 \times 945 \times 980 \times 1008 \times 1050 \times 1064 \times 1120 \times 1140 \times 1155 \times 1176 \times 1260 \times 1280 \times 1287 \times 1344 \times 1365 \times 1400 \times 1414 \times 1440 \times 1470 \times 1482 \times 1512 \times 1540 \times 1560 \times 1575 \times 1616 \times 1638 \times 1680 \times 1701 \times 1722 \times 1764 \times 1792 \times 1820 \times 1848 \times 1875 \times 1904 \times 1925 \times 1932 \times 1960 \times 1980 \times 1995 \times 2016 \times 2030 \times 2058 \times 2072 \times 2100 \times 2121 \times 2142 \times 2160 \times 2184 \times 2205 \times 2212 \times 2240 \times 2268 \times 2280 \times 2310 \times 2324 \times 2352 \times 2378 \times 2400 \times 2421 \times 2436 \times 2464 \times 2478 \times 2520 \times 2541 \times 2562 \times 2592 \times 2610 \times 2632 \times 2646 \times 2688 \times 2700 \times 2716 \times 2730 \times 2744 \times 2772 \times 2784 \times 2800 \times 2814 \times 2828 \times 2835 \times 2856 \times 2870 \times 2882 \times 2912 \times 2925 \times 2940 \times 2968 \times 2982 \times 3024 \times 3025 \times 3040 \times 3052 \times 3080 \times 3096 \times 3120 \times 3136 \times 3150 \times 3168 \times 3192 \times 3200 \times 3213 \times 3222 \times 3240 \times 3256 \times 3276 \times 3292 \times 3300 \times 3312 \times 3325 \times 3344 \times 3360 \times 3372 \times 3396 \times 3408 \times 3420 \times 3432 \times 3450 \times 3464 \times 3478 \times 3500 \times 3512 \times 3528 \times 3540 \times 3552 \times 3564 \times 3584 \times 3596 \times 3600 \times 3612 \times 3624 \times 3640 \times 3654 \times 3672 \times 3684 \times 3696 \times 3700 \times 3712 \times 3724 \times 3736 \times 3750 \times 3768 \times 3780 \times 3792 \times 3808 \times 3822 \times 3840 \times 3852 \times 3864 \times 3876 \times 3888 \times 3900 \times 3912 \times 3924 \times 3936 \times 3948 \times 3960 \times 3972 \times 3984 \times 3996 \times 4000 \times 4012 \times 4024 \times 4036 \times 4048 \times 4060 \times 4072 \times 4084 \times 4096 \times 4100 \times 4112 \times 4124 \times 4136 \times 4148 \times 4160 \times 4172 \times 4184 \times 4196 \times 4200 \times 4212 \times 4224 \times 4236 \times 4248 \times 4260 \times 4272 \times 4284 \times 4296 \times 4300 \times 4312 \times 4324 \times 4336 \times 4348 \times 4360 \times 4372 \times 4384 \times 4396 \times 4400 \times 4412 \times 4424 \times 4436 \times 4448 \times 4460 \times 4472 \times 4484 \times 4496 \times 4500 \times 4512 \times 4524 \times 4536 \times 4548 \times 4560 \times 4572 \times 4584 \times 4596 \times 4600 \times 4612 \times 4624 \times 4636 \times 4648 \times 4660 \times 4672 \times 4684 \times 4696 \times 4700 \times 4712 \times 4724 \times 4736 \times 4748 \times 4760 \times 4772 \times 4784 \times 4796 \times 4800 \times 4812 \times 4824 \times 4836 \times 4848 \times 4860 \times 4872 \times 4884 \times 4896 \times 4900 \times 4912 \times 4924 \times 4936 \times 4948 \times 4960 \times 4972 \times 4984 \times 4996 \times 5000$$

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

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

2, 6, 30, 210

↑

list

then

find

largest value

↳ query