COP 4516 3/10/26

1) △ Syllabus - +codeforces round, - writing assn → 3/26 evening

2) Number Theory

1) primality check

if n is composite and
$n = a \times b$, $a > 1$, $b > 1$, then
either $a \le \sqrt{n}$ or $b \le \sqrt{n}$

```
for (int i = 2; i*i <= n; i++)
    if (n % i == 0)
        return false;
return true;
```

$O(\sqrt{n})$ or upto $n = 10^{12}$ or 10^{13}

prime sieve list all primes from 2 to n

```
boolean[] isPrime = new boolean[n+1];
// Make all true
for (int i = 2; i*i <= n; i++)
    for (int j = 2*i; j <= n; j += i)
        isPrime[j] = false
```

↙ letter i

Prime Fact

```
i=2
while (i*i <= n) {
    int exp = 0;
    while (n%i == 0) {
        exp++;
        n /= i;
    }
    if (exp > 0) fct.add(i, exp)
    i++;
}
if (n > 1) fct.add(n, 1);
```

$n = 2^5 \times 3^3 \times 5^2 \qquad d = 2^a 3^b 5^c$

divisors = $(5+1)(3+1)(2+1)$

$0 \le a \le 5$ 6
$0 \le b \le 3$ 4
$0 \le c \le 2$ 3

Sum divisors =

$$\left(\frac{2^6-1}{2-1}\right) \times \left(\frac{3^4-1}{3-1}\right) \times \left(\frac{5^3-1}{5-1}\right)$$

Mult under mod val = (val + x) %MOD every time!

Calculations under mod

$$val = (val - x \bmod MOD + MOD) \bmod MOD$$

$$val = (val + x) \bmod MOD \quad // \text{assume } x \geq 0$$

Dividing under mod

If I "want" $val = (val / x) \bmod MOD$

Do this instead:

$$val = (val * modInverse(x, MOD)) \bmod MOD$$

CO23100

code → in typed notes

* Fermat's theorem gives us another way IF MOD VAL is prime

Number of times prime p divides evenly into $n!$

$n! = 1 \times 2 \times 3 \ldots \times p \times \ldots \times (2p) \ldots (p^2) \ldots (p+1)p \ldots$ (ignore)

$\lfloor \frac{n}{p} \rfloor$ # cancels: 1, 2, 3, ..., p, $p+1 = \lfloor \frac{n}{p} \rfloor !$

What about how many times 24 divides into $125! = 2^{119} \times 3^{59} \times \ldots$

$24 = 2^3 \cdot 3$ solve(2) solve(3)

$2 \mid 125$
$2 \mid 62$
$2 \mid 31$
$2 \mid 15$
$2 \mid 7$
$2 \mid 3$
1

$62 + 31 + 15 + 7 + 3 + 1 = 119$

$3 \mid 119$ → 59

$3 \mid 125$
$3 \mid 41$
$3 \mid 13$
$3 \mid 4$
1

$54 + 5 = 59$

$$\min\left(\frac{\#\text{num times } p \text{ divides into } n!}{\text{exp of } p}\right)$$

$$\frac{2^{119} \times 3^{59} \times \cdots}{24^k} = \frac{2^{119} \times 3^{59}}{2^{3k} \cdot 3^k}$$

$$2^{119-3k} - 3^{59-k}$$

Fermat's Thm

If $\gcd(a, p) = 1$ and $p \in$ Prime then

$$a^{p-1} \equiv 1 \mod p$$

$$a^{p-2} \times a \equiv 1 \mod p \qquad a^{-1} \equiv a^{p-2} \mod p$$

$$a \times a^{-1} \equiv 1 \mod p$$

More General Version
Euler's Thm

If $\gcd(a,n)=1$ then

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

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

($\gcd(a,n)=1$)

$\phi(15) = 8$ $\quad$ 1, 2, ~~3~~, 4, ~~5~~, ~~6~~, 7, 8, ~~9~~, ~~10~~, 11, ~~12~~, 13, 14, ~~15~~

$\phi(n)$ • via prime factorization of n

$n = p_1^{q_1} \cdot p_2^{q_2} \cdot p_3^{q_3} \ldots$ $\quad \phi(n) = (p_1^{q_1} - p_1^{q_1-1})(p_2^{q_2} - p_2^{q_2-1})$

$\phi(96) = \phi(2^5 \times 3)$

$= (2^5 - 2^4) \times (3-1)$

$= p_1^{q_1}\left(1 - \frac{1}{p_1}\right)$

$= p_2^{q_2}\left(1 - \frac{1}{p_2}\right)$

$= n\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right)\ldots$

175 →

$\phi(300000)$ $\quad$ ~~300000~~ ....

$175 = 7 \times 25$

$\phi(175) = \phi(7) \times \phi(25)$

$= 6 \times 20 = 120$