Teoría de números

Bernardo Hernandez Hernandez

Aritmética modular

Decimos que dos enteros *a* y *b* son congruentes módulo *n* cuando se cumple:

$n \mid a - b \quad =$

$a \equiv b \pmod{n} \quad =$

$a \,\%\, n \;=\; b \,\%\, n$

Existe una única forma de escribir

$a = n \cdot q + r$, con $0 \leq r < n$.

Aritmética modular

$a + b \equiv r \pmod{n} \Rightarrow a \,\%\, n + b \,\%\, n \equiv r \pmod{n}$

$a - b \equiv r \pmod{n} \Rightarrow a \,\%\, n - b \,\%\, n \equiv r \pmod{n}$

$a \cdot b \equiv r \pmod{n} \Rightarrow a \,\%\, n \cdot b \,\%\, n \equiv r \pmod{n}$

Pequeño Teorema de Fermat

Dado p primo y $a \% n \neq 0$, $a^{p} \equiv a \pmod{p}$

$\Rightarrow a^{p-2} \equiv a^{-1} \pmod{p}$

$a \cdot b^{p-2} \equiv a / b \pmod{p}$

Exponenciación Binaria Modular

$$a^{b+c} = a^b \cdot a^c$$
$$a^{2b} = a^b \cdot a^b$$

$$3^{13} = 3^{0b1101} = 3^8 \cdot 3^4 \cdot 3^1$$

Problema para practicar

Binomial Coefficients

https://cses.fi/problemset/task/1079

Hints:

- Precálculo de factoriales
- Precálculo de sus inversos $(n!)^{-1}$
- $C(n, k) = n! \cdot (n-k)!^{-1} \cdot k!^{-1}$

Teorema fundamental de la aritmética

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$$

Criba de Eratóstenes

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	~~16~~
2	**3**	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~
2	**3**	~~4~~	**5**	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~
2	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~
2	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~	**11**	~~12~~	13	~~14~~	~~15~~	~~16~~
2	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~	**11**	~~12~~	**13**	~~14~~	~~15~~	~~16~~

GCD
LCM

```
#include <algorithm>

using ll = long long;

ll lcm (ll a, ll b){
    return (a * b)/__gcd(a, b);
}
```

Material a revisar

https://cp-algorithms.com/

(Sieve of Eratosthenes)

(Sieve of Eratosthenes, Linear Time Complexity)

https://tc-arg.tk/index.html

(2018: Aritmética y Teoría de Números)

(2020: Combinatoria)