m a $\rightarrow$ $a = m \cdot q + r$ con $0 \leq r < m$

$a \equiv r \pmod m$ $\iff$ $a - r$ è divisibile per m

$a \equiv r \pmod m$ $\quad b \equiv r' \pmod m$

$a + b \equiv r + r' \pmod m$ $\quad a - b \equiv r - r' \pmod m$

$a \cdot b \equiv r \cdot r' \pmod m$ $\rightarrow$ / ?? DOPO

$MOD = 1000000007$;

$a \,\%\, MOD$ $\Leftarrow$ resto della divisione per MOD

$MOD \,\%\, MOD = 0$

$-1 \,\%\, MOD = -1$

$((a \,\%\, MOD) + MOD) \,\%\, MOD$

$[-MOD+1, MOD-1]$

$[1, 2\,MOD - 1]$

$\%\, MOD \rightarrow 0 \leq x < MOD$

$a \cdot b$ NON sta necessariamente in int $\rightarrow$ long long!

$a = p_1^{e_1} \cdots p_k^{e_k}$ $\qquad 12 = 2^2 \cdot 3$

$128 = 2^7$

- a è un primo
- oppure $(\min p_i)^2 \le a$

```
for (int i = 2; i*i <= a; i++) {
    if (a % i == 0) {
        // i è un fattore primo di a
        a /= i;
        i--;
    }
}
// a è primo o 1
```

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~
11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19

$$\frac{n}{2} + \frac{n}{3} + \frac{n}{5} + \frac{n}{7} \cdots \rightarrow \sum_{p_i \le \sqrt{n}} \frac{n}{p_i} \le n \sum_{i \le \sqrt{n}} \frac{1}{\sqrt{n}}$$

$$= O(n \log n)$$

MCD - GCD

MCM - LCM

$GCD(a, b) = d$ t.c. $a \% d = 0$ $b \% d = 0$ d è il massimo num. con questa proprietà.

$(6, 8) = 2$ $(11, 7) = 1$ $(2, 4) = 2$

$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$

$(a, b) = p_i^{\min(a_1, b_1)} \dots$

$a = 2^7 5^3 11^2$ $b = 2^6 3^4 7^{12}$

$d = 2^6 \cdot 3^0 \cdot 5^0 \cdot 7^0 \cdot 11^0 = 2^6 = 64$

$(a, b) = (a, b + k \cdot a) \quad \forall k \in \mathbb{Z}$

$a = n \cdot d$ $b + ka = (n + km) \cdot d$

$b = m \cdot d$

$(a, b) = (a, b + ka - ka)$

$(a, 0) = a$

```
int gcd (int a, int b) {
    if (a < b) return gcd (b, a);
    if (b == 0) return a;
    return gcd (b, a % b);
}
```

$r : a = kb + r \rightarrow r = a - kb$

$O(\log a)$

$(a, b) = 1$ coprimi

Dato x, esiste a : $ax \equiv 1 \mod m$?

$b / x \mod m$ def: $(b/x) \cdot x \equiv b \pmod m$

$b \cdot a$ $\qquad b \cdot a \cdot x \equiv b \cdot (a \cdot x) \equiv b \pmod m$

$\Leftrightarrow (m, x) = 1$ Se m è primo $p \Leftrightarrow x \not\equiv 0 \pmod p$

Teorema di Fermat

$$x^{p-1} = 1 \mod p \quad \text{se} \quad x \not\equiv 0 \mod p$$

$$x^{p-2} \cdot x = x^{p-1} = 1 \mod p$$

$$a = x^{p-2} \Rightarrow ax = 1$$

$O(\log p)$

$\phi(m) = \#$ di numeri $\le m$ coprimi con m

$\phi(p) = p - 1 \qquad \phi(p^k) = p^{k-1}(p-1)$

$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ se $(a, b) = 1$

Teorema di Eulero

$$x^{\phi(m)} = 1 \mod m \quad \text{se} \quad (x, m) = 1$$

$x^{\phi(m)-1} \rightarrow$ inverso di $x \mod m$

$\binom{n}{k}$ = # di sottoinsiemi di dimensione k in un insieme con n elem.

$$\frac{n!}{k!\,(n-k)!}$$

Contiamo # di sottoinsiemi ordinati di k elementi in n

- $k \cdot (k-1) \cdot (k-2) \cdots 1 \cdot \binom{n}{k} = k! \binom{n}{k}$
- $n \cdot (n-1) \cdots (n-k+1) = \dfrac{n \cdot (n-1) \cdots (n-k+1) \cdot (n-k) \cdots 1}{(n-k) \cdots 1} = \dfrac{n!}{(n-k)!}$

$$k! \binom{n}{k} = \frac{n!}{(n-k)!} \Rightarrow \binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}{k!}$$

- calcolare $\binom{n}{0} \binom{n}{1} \cdots \binom{n}{n}$

$$\binom{n}{k+1} = \frac{n!}{(k+1)!\,(n-k-1)!} = \frac{n!}{k!\,(n-k)!} \cdot \frac{n-k}{k+1} = \frac{n-k}{k+1} \binom{n}{k}$$

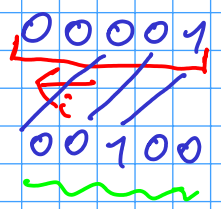
- calcolare $\binom{k}{k}, \binom{k+1}{k} \cdots \binom{n}{k}$

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{n}{n-k} \cdot \frac{(n-1)!}{k!\,(n-k-1)!} = \frac{n}{n-k} \binom{n-1}{k}$$

- $\binom{n}{0} + \cdots + \binom{n}{n} = 2^n$

$\{a, b, c, d, e\}$
$0\ 1\ 0\ 0\ 1 \iff \{b, e\}$

(a) controllare appartenenza: $i \in A \iff ((1ULL << i) \,\&\, A) \neq 0$



$$\begin{array}{r} 00101 \\ \& \\ 01011 \\ = \\ 00001 \end{array}$$

- se l'i-esimo bit di A è 1,
- altrimenti, 0

(b) intersezione A, B : $C = A \cap B \iff C = A \,\&\, B$

(c) unione A, B : $C = A \cup B \iff C = A \mid B$

$$\begin{array}{r} 01001 \\ | \\ 11010 \\ = \\ 11011 \end{array}$$

(d) $A \leftarrow A \cup \{i\}$ $\quad A \mid (1ULL << i)$

(e) A^c $\quad \sim A$ $\quad \sim 01001 = 10110$

(f) $A \setminus B$ $\quad A \,\&\, (\sim B)$

(g) togliere un elemento $A \,\&\, \sim(1ULL << i)$

(h) differenza simmetrica $A \Delta B$ $\quad A \wedge B$

$$\begin{array}{r} 01001 \\ \wedge \\ 10011 \\ = \\ 11010 \end{array}$$

(i) cambiare (toggle) un elemento $\quad A \wedge (1ULL << i)$

$0x1F00 \Rightarrow 0001111100000000$

$0b\ 01011100$

$A\&(\sim((\sim 0ULL) << 5))$

$111\ldots100000$

$0000\ldots011111$

$|A| = \_\_BUILTIN\_POPCOUNTLL(A);$

$n \,\&\, -n \qquad -n = (\sim n) + 1$ ESERCIZIO

COMMESSO VIAGGIATORE

G, n nodi, completo, archi pesati

trovare il ciclo con n nodi di costo minimo

Esiste algo. $O(n^2 2^n) << O(n!)$

Q: per ogni sottoinsieme S di nodi, quale è il cammino di costo minimo che li visita tutti, partendo da $a \in S$ e ritorna in a?

$a, S = \{a, b, c, \ldots\}$

$b, S \setminus \{a\}$ $\quad c, S \setminus \{a\}$ $\quad - - -$

$a, \{a\} \Rightarrow W(a, a)$

$$\sum_{A \subseteq \{1\ldots n\}} |A|^2 = n^2 2^n$$

- for (ull long long sub = 0; sub < (1ULL << n); sub++) ...

1ULL & (A == 0)

{1, .. n} 1 2 3 4 → 4 2 1 3

STD:: NEXT_PERMUTATION

```
VECTOR<INT> PERM(n);
IOTA(PERM.BEGIN(); PERM.END(); 0);
do{
...
} while (next_permutation(PERM.begin(), PERM.end()));
```

PERM. INVERSA:

- INV_PERM[PERM[i]] == i;

PERM[INV_PERM[i]] == i;

DECOMP. CICLI

1 2 3 4 → 4 2 1 3

3

1 → 4

2 → 2

1 → 4 → 3

2

PERM[ ] = {4, 2, 1, 3};

1 → 4