int a, b

DIVISIONE INTERA

$\exists$ 1 sola coppia intera q e r con $0 \le r < |b|$

tale che

$$a = q \cdot b + r$$

(divisione intera)

$a \backslash b$

$a \% b$ modulo

"a modulo b"

$a = -3 \qquad b = 7$

<u>Es.</u>

$$-3 = \underset{q}{\underset{\uparrow}{-1}} \cdot 7 + \underset{r}{\underset{\uparrow}{4}}$$

$$a \% b = 4 = r$$

$$a \backslash b = -1 = q$$

$\boxed{m}$

$r_1 = a \% m$

$r_2 = b \% m$

$(a \cdot b) \% m = (r_1 \cdot r_2) \% m =$

$= ((a \% m) \cdot (b \% m)) \% m$

$$\begin{cases} a = q_1 \cdot m + r_1 \\ b = q_2 \cdot m + r_2 \end{cases}$$

$$a \cdot b = q_1 \cdot q_2 \cdot m^2 + q_1 \cdot r_2 \cdot m + r_1 \cdot q_2 \cdot m + r_1 \cdot r_2$$

$$a \pm b = (q_1 \pm q_2)\, m + (r_1 \pm r_2)$$

$$(a \pm b) \% m = ((a \% m) \pm (b \% m)) \% m$$

$$\cancel{(a/b)\%n = (a\%n / b\%n)\%n}$$

Non Vale

$$a^b \% n = (\underbrace{a \cdot a \cdots\cdots a}_{b\text{-Volte}}) \% n = \Big((a\%n) \cdot \underbrace{(a \cdots a)}_{\substack{b-1 \\ \text{Volte}}} \% n\Big) \% n =$$

$$= (a\%n)^b \% n$$

$$\boxed{a^b \% n = (a\%n)^b \% n}$$

INVERSO MODULO

incognita

$$a \cdot x = 1 \pmod{m} \longrightarrow a \cdot x = q \cdot m + 1$$

$$(a \cdot x) \% m = 1$$

$$a x - q m = 1$$

Se $MCD(a, m) = 1$ allora $x \ \exists$

$$\underline{\underline{a}}\, x + \underline{\underline{n}}\, y = MCD(\underline{\underline{a}}, \underline{\underline{n}})$$

x e y $\exists$ mediante Euclide esteso

$$a x - q n = 1$$

$\uparrow$ $\uparrow$

1) $p \quad q$ 2) $\underline{\underline{n}} = p \cdot q$ 3) $z = (p-1)(q-1)$

4) $2 \leq e < z$: $MCD(e, n) = 1$ 5) d : $d \cdot e \equiv 1 \pmod{n}$

$d \cdot e = x \cdot n + 1$ d è l'inverso modulo di e

$a \cdot x = 1 \pmod{n}$ si può anche $x = a^{-1}$

$Ci = m^{e} \% n$ $de = Ci^{d} \% n$

POTENZA MODULO

$a^b \% M$ in $(\log_2 b)$ passi

$$5^3 = 5 \cdot 5 \cdot 5 = 5^{(11)_2} = 5^{2^1+2^0} = 5^2 \cdot 5^1$$

$$5^9 = 5^{2^3+1} = 5^{2^3+0\cdot 2^2+0\cdot 2^1+1} = 5^{2^3} \cdot 5^{0\cdot 2^2} \cdot 5^{0\cdot 2^1} \cdot 5^1 =$$

$$= 5^{2^3} \cdot 5$$

9	1	1
4	0	2^1
2	0	2^2
1	1	2^3
0		

5^9

$$5^{2^3} \cdot \frac{5^{0\cdot 2^2}}{1} \frac{5^{0\cdot 2^1}}{1} \cdot 5^1 =$$

$$= 5^{1} \cdot 5^{0\cdot 2} \cdot 5^{0\cdot 2^2} \cdot 5^{2^3}$$

$b = 10^{10}$

$\log_2 b = 10 \cdot \log_2 10 = 40$

1) $\frac{b}{2}$

2) $\frac{b}{2^2}$

3) $\frac{b}{2^3}$

$\vdots$

k) $\frac{b}{2^k} = 1 \rightarrow b = 2^k$

$$\boxed{k = \log_2 b}$$

$$5^9 = 5^1 \cdot 5^{0\cdot 2} \cdot 5^{0\cdot 2^2} \cdot 5^{2^3}$$

$$(a\cdot b)\%m = \left[(a\%m)\cdot(b\%m)\right]\%m$$

$$1 \qquad 1\cdot 2 \qquad \times 2 \qquad \times 2$$

$$5^9\%m = \left[(5^1\%m)^{\%m}\cdot(5^{0\cdot 2}\%m)\cdot(5^{0\cdot 2^2}\%m)\cdot(5^{2^3}\%m)\right]\%m$$

$$(a\%m)\%m = a\%m$$

```
modPole(a, b, m)
{
    p = a;  pole = 1;
    if (b == 0) return 1;
    if (b == 1) return a % m;
    d = b / 2;  r = b % 2;
    while (d != 0) {
        if (r != 0) pole = (pole * p) % m;
        p = (p * p) % m;  r = d % 2;  d = d / 2;
}
    return pole;
```

5^1

$5^9 = 5^1 \cdot \cancel{5^2} \cdot \cancel{5^4} \quad 5^8$

$5^2 \quad 5^4 \quad 5^8$