06/12/2021

$\mathbb{Z}_p$ è un campo

$\mathbb{Z}_p^*$ gruppo ciclico rispetto a $\cdot$

in $\mathbb{Z}_p$ $(x+y)^p = x^p + y^p$

**SOGNO della MATRICOLA**
è possibile solo in $\mathbb{Z}_p$

$\mathbb{Z}_7$ $(\bar{1}+\bar{2})^7 = 1^7 + 2^7$

$(x+y)^2 = x^2 + 2xy + y^2$ in $\mathbb{Z}_2$ $= 2 = 0$

**TH: (PICCOLO TH di FERMAT)** caso particolare di EULERO

sia $\mathbb{Z}_p$ campo con $p$ primo allora

$\forall a \in \mathbb{Z}_p$ $\quad \bar{a}^p = \bar{a}$

$(a^p \equiv a \bmod p)$

a divide la differenza

se $a \neq 0$ in $\mathbb{Z}_p$ (ovvero se $p \nmid a$)

allora $\bar{a}^{p-1} = \bar{1}$ $\quad (a^{p-1} \equiv 1 \bmod p)$

IMPORTANTE nelle prove
- PRIMO $p$
- INTERO $a$

**TH di EULERO**

Sia $a \in \mathbb{Z}$ COPRIMO con $n$ allora

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

$MCD(a,p) = 1$
$MCD(x,7) = 1$

$\varphi(p) = p-1$

se $n = p$ primo

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

$x^{\text{un grande esponente}}$ modulo $n = ?$ OBBIETTIVO

$MCD(a, n) = 1$ coprimo

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

$a^{k \cdot \varphi(n)} \equiv ? = (a^{\varphi(n)})^k \equiv 1^k \bmod n \equiv 1 \bmod n$ sempre

---

$a^{\boxed{m}} \bmod (n)$ $\varphi(n) =$

$a^m \equiv a^{k \cdot \varphi(n) + r} \equiv a^{k\varphi(n)} \cdot a^r \equiv a^r \bmod n$

$0 \leq r \leq \varphi(n) - 1$

ES

$3^{51} \bmod 10$

SONO COPRIMI? $MCD(3,10) = 1$ SI!

1) calcolo $\varphi(10) = \varphi(2) \cdot \varphi(5) = 4$

$3^{51} \equiv 3^{12 \cdot \varphi(10) + 3} \equiv 3^3 \bmod 10 \equiv 27 \bmod 10$

$\equiv 7 \bmod 10$

modulo $10 = 9$

$7^{2543120489} \bmod 11$ → $MCD(7,11) = 1$

$\varphi(11) = 10$

$7^{\text{alla} \cdots} \equiv 7^9 \bmod 11$

$7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7$

$49 \equiv 5 \bmod 11$

$7$

$35 \bmod 11 = 2$

$7$

$14 \bmod 11$

OPPURE

$7^4 = 7 \cdot 7 \cdot 7 \cdot 7 \Rightarrow (7^2) \cdot (7^2)$

3 PRODOTTI — 2 OPERAZIONI

$7^6 = 7 \cdot 7^2 \cdot 7^4 \Rightarrow$ 3 OPERAZIONI

SQUARE and MULTIPLY

ESPONENTE BASE 2

$11 = 1 + 2 + 2^3$

$a^{11} = a \cdot a^2 \cdot a^8$

$a$

$a^2$

$(a^2)^2 = a^4$

$(a^4)^2 = a^8$

se lavoro con mod n

RIDURRE

---

$7^{25} \bmod 31$

$25 = 16 + 8 + 1 =$

$7^{25} \equiv 7^{16} \cdot 7^8 \cdot 7^1 = 7 \cdot 10 \cdot 7 =$

$= (49 \bmod 31) \cdot 10$

$= 18 \cdot 10 = 180$

$= 180 \bmod 31$

$= 25 \bmod 31$

$7$

$7^2 = 49 \bmod 31 = 18$

$7^4 = (18)^2 = 324 \bmod 31 = 14$

$7^8 = (14)^2 = 196 \bmod 31 = 10$

$7^{16} = 100 \bmod 31 = 7$

# CRITERI di DIVISIBILITÀ

$X = a_n a_{n-1} \dots a_0$ (cifre DECIMALI)

$2 \mid X \iff 2 \mid a_0$ $\qquad X \equiv_2 a_0$

$X \equiv_3 (a_n + a_{n-1} + \dots + a_0)$

$7541 \equiv_3 17 \equiv_3 2$

$7541$ (+ + + = 17)

$X \equiv_5 a_0$ basta guardare ultima cifra

ovvero $X \equiv_{2^i} a_{i-1} \dots a_1 a_0$

$7541 \bmod 4 \equiv 41 \bmod 4$ ($4 = 2^2$)

$7541 \bmod 8 \equiv 541 \bmod 8$

$X \equiv_{5^i}$ solo le ultime $i$ cifre

$7541 \bmod 25 \equiv 41 \bmod 25 = 16$

$X \equiv_9 (a_n + a_{n-1} + \dots + a_0)$

$7541 \equiv_9 17 \equiv_9 8$

## DIVISIONE per 11

SOMMA CIFRE POSTO PARI
SOMMA CIFRE POSTO DISPARI
} si ottiene il MODULO

D P D P D P D P D P
$a_6$ $a_4$ $a_2$ $a_0$
1 7 4 5 6 7 2 1 0 9

mod 2 → D 1

mod 3 → D 0 perché 42 è divisibile per 3 (6 ✗)

mod 5 → 4

mod 4 → 1 + 8 (4·2)

mod 25 → 9

mod 9 → 6

mod 11 → 29 − 13 = (16) ≡ 5

---

P P P P
TROVARE · 1 2 3 4 5 6 7 mod

// 4 → 67 ≡₄ (3)
8 → 567 ≡₈ (7)
11 → 16 − 12 = (4)
9 → (1)

DETERMINARE INVERSO di (se esiste)

3 in $\mathbb{Z}_{100}$

$100 = 9 \cdot 11 + 1$ ✗

$9 = 1 \cdot 9 + 0$ ✗

INVERSO

$1 = 1 \cdot 100 - 9 \cdot (11)$

$\alpha$ $a$ $b$ $\beta$

$\mathbb{Z}_n$ $\quad ax \equiv b \bmod n$

$0x = 0$ INDET.
$0x = 3$ IMP.

TH: $\boxed{ax \equiv b \bmod n}$ eq. MODULARE

ammette soluzione se e solo se

$MCD(a, n) \mid b$

(ES)

$3x \equiv 1 \bmod 6$ non ha SOLUZIONI

$MCD(3,6) \nmid 1$

$3x \equiv 1 \bmod 5$

$MCD(3,5) \mid 1$

---

$\boxed{ax + ny = b}$ DIOFANTEA

HA soluzioni $(x,y) \in \mathbb{Z}^2$

$ax = b - ny \iff ax \equiv b \bmod n$

(ES)

$7x \equiv 3 \bmod 8$

$MCD(7,8) \mid 3$ compatibile ☑

$x \equiv 3 \cdot 7^{-1} \bmod 8$ come TROVO $7^{-1} \equiv_8 -1 \bmod 8$

$x \equiv -3 \bmod 8 = 5 \bmod 8$

$4x \equiv 2 \mod 6$

$MCD(4,6) \mid 2$ è compatibile

l'inverso è fattibile se 4 è coprimo con 6

ALLORA SEMPLIFICO

$2x \equiv 1 \mod 3$

$MCD(2,3) \mid 1$

$x \equiv 1 \cdot (2) \mod 3$

inverso di 2

$x \equiv 2 \mod 3$

# SISTEMI eq MODULARI

$$(*) \begin{cases} a_1 x \equiv b_1 \mod n_1 \\ a_2 x \equiv b_2 \mod n_2 \\ \vdots \\ a_r x \equiv b_r \mod n_r \end{cases}$$

TH cinese dei resti

supponiamo di avere un SISTEMA (*) di eq MODULARI COMPATIBILI T.C. il $MCD(n_i; n_j) = 1 \ \forall \ i \neq j$ allora il SISTEMA (*) ammette un unico SOL. MODULO $n_1 \cdot n_2 \cdot \ldots \cdot n_r$

anche se non rispetta la condizione il sistema si può fare comunque ma non con questo metodo

particolare SOLUZIONE $\overline{x}$

GENERALE // $\overline{x} + k\, n_1 \cdot n_2 \cdot \ldots \cdot n_r$

ES

$$\begin{cases} 2x \equiv 1 \bmod 5 \\ 3x \equiv 4 \bmod 7 \end{cases}$$

sono coprimi quindi cineri

$$\overline{x} + k \cdot 35$$

$$\begin{cases} x_1 = b_1 \bmod n_1 \\ \vdots \\ x_r \equiv b_r \bmod n_r \end{cases}$$

$N = n_1 \cdot n_2 \cdot \ldots \cdot n_r$

$N_i = \dfrac{N}{n_i}$ $\quad \overline{x}_i \rightsquigarrow N_i \overline{x}_i \equiv b_i \bmod n_i$

$MCD(N_i, n_i) = 1$

$$\overline{x} = N_1 \overline{x}_1 + N_2 \overline{x}_2 + \ldots + N_r \overline{x}_r \in \mathbb{Z}$$

ES

$$\begin{cases} 2x \equiv 1 \bmod 5 \\ 3x \equiv 4 \bmod 7 \end{cases}$$

- controllo compatibilità
- // SEMPLIFICAZIONE

$$\begin{cases} x \equiv 3 \cdot 1 \bmod 5 \\ x \equiv \underbrace{5 \cdot 4}_{20} \bmod 7 \end{cases} \quad \begin{cases} x \equiv 3 \bmod 5 \\ x \equiv 6 \bmod 7 \end{cases}$$

$N = 5 \cdot 7 = 35$

$N_1 = 7 \quad N_2 = 5$

$N_1 \quad \bar{x}_1 \equiv b_1 \mod 5$

$7 \quad \bar{x}_1 \equiv 3 \mod 5$

$11$

$2 \quad \bar{x}_1 \equiv 3 \mod 5$

$\bar{x}_1 \equiv 3 \cdot 3 \mod 5$

$\bar{x}_1 \equiv \boxed{4} \mod 5$

$N_2 \quad \bar{x}_2 \equiv b_2 \mod a_2$

$5 \quad \bar{x}_2 \equiv 6 \mod 7$

$\bar{x}_2 \equiv 3 \cdot 6 \mod 7$

$\bar{x}_2 \equiv \boxed{4} \mod 7$

$$\bar{X} = N_1 \bar{x}_1 + N_2 \bar{x}_2 =$$

$$= 7 \cdot 4 + 5 \cdot 4 = 48 \mod 35$$

$$= 13 \mod 35$$

$$\bar{X} = 13 + 35k$$