

# CLASSI DI RESTO • 3 [CASO D'USO]

CONGRUENZE LINEARI ➤ RISOLVIBILE  $\wedge \text{MCD}(a,b)=1$   
 Date le congruenze  $qx = 12 \pmod{51}$ , risolvere l'equazione

- Determino se c'è è invertibile:

$$51/q \rightarrow 51 = 5 \cdot q + 6 \quad \text{MCD}(q, 51) \text{ non è invertibile}$$

$$q/6 \rightarrow q = 1 \cdot 6 + 3 \quad \text{Procedo...}$$

$$6/3 \rightarrow 6 = 2 \cdot 3 + 0$$

- Determino  $x \equiv d/b$ :  $12/3 \in \mathbb{Z}$  è divisore.

Divido tutti i termini per  $d$ :

$$qx \equiv 12 \pmod{51} \Rightarrow qx + g \cdot 51 = 12$$

$$\frac{3x}{3} + g \cdot \frac{51}{3} = \frac{12}{3} \Rightarrow 3x + g \cdot 17 = 4$$

$$3x \equiv 4 \pmod{17} \quad \text{MCD}(3, 17) = 1$$

$$- 17(3) : 17 = 5 \cdot 3 + 2 \quad 1 = 17 - 5 \cdot 3$$

$$3 = 1 \cdot 2 + 1 \quad \text{Bezout } 2 = 6 \cdot 3 - 17 \cdot 1$$

$$2 = 2 \cdot 1 + 0 \quad 2 = 3 - 1 \cdot 2$$

$$* \exists \overline{1} = \overline{6 \cdot 3} - \overline{17}$$

$$* 2 = 17 - 5 \cdot 3 \Rightarrow 1 = 3 - 1 \cdot (17 - 5 \cdot 3)$$

$$\text{L'inverso di } \alpha = \overline{6}$$

$$1 = 3 - 17 + 5 \cdot 3$$

$$\overline{6} \cdot \overline{3}x = \overline{4} \cdot \overline{6}$$

$$x = \overline{24} \Rightarrow \overline{x} \in \mathbb{Z}_{17} \quad \text{Elenco le sarebbero}$$

$$\dots -27, -10, 7, 24, 41, 58 \dots$$

$$\left[ \begin{array}{c} \overline{7} \\ \overline{24} \\ \overline{41} \end{array} \right]_{51}$$

gli altri fanno opp. sempre a uno dei 3

## EULERO/FERMAT ➤ Ultime n cifre

"Determinare le ultime 2 cifre del numero  $17^{894283}$  cioè equivalente a dire quanto vale  $17^{\text{ultime 2 cifre}}$  modulo 100"

- Si calcola  $\varphi(N)$  con  $N = 100$

100 non è primo per cui lo si scomponga

$$\varphi(100) = \varphi(5^2) \cdot \varphi(2) \Rightarrow 5 \cdot 4 \cdot 2 - 1 = 40$$

- Si scomponga la potenza facendo in modo che sia multiplo di  $\varphi(N)$   
 $894283/40 \rightarrow 22357 \cdot 40 + 3$  per cui  $17^{894283} \equiv 17^3 \pmod{100}$

- Si riscriva la potenza, ossia che riporti nel T. Eulero  $a^{\varphi(N)} \equiv 1 \pmod{100}$   
 $17^{22357 \cdot 40 + 3} \equiv (17^{40})^{22357} \cdot 17^3$  per eulero  $17^{40} \equiv 1 \pmod{100}$   
 per cui  $\equiv 1 \cdot 17^3 \pmod{100} \Rightarrow 1513$  che dà per cento  
 da dove ultime 2 cifre 13

quindi  $17^{894283} \equiv 13 \pmod{100}$

## EULERO/FERMAT ➤ Ultime n cifre

"Determinare la cifra finale di  $3^{405041} + 7^{448065}$ "

- Si calcola  $\varphi(10)$

10 non è primo:  $\varphi(10) = \varphi(2) \cdot \varphi(5) \Rightarrow \varphi_{10} = 4$

- Si scompongono le potenze di entrambi i numeri:

$$405041/4: 226260 \cdot 4 + 1 \quad 448065/4: 112016 \cdot 4 + 1$$

- Si riscrivono le potenze:

$$3^{405041} = 3^{226260 \cdot 4 + 1} = (3^4)^{226260} \cdot 3 = 3 \pmod{10}$$

$$7^{448065} = 7^{112016 \cdot 4 + 1} = (7^4)^{112016} \cdot 7 = 7 \pmod{10}$$

$$\text{RCD}(4, 10) = 1$$

quindi  $3^{405041} + 7^{448065} = 3 + 7 \pmod{10} = 0 \pmod{10} = 0$  cifra finale

## CLASSI DI RESTO •

## [CASO DIVISO]

RESTO DI DIVISIONE &gt; SOMMA NUM

Calcola il resto della divisione per 27 del numero  $3^{12007} + 5^{36184}$ - Si calcola  $\varphi(27)$ : 27 non è primo:  $\varphi(27) = \varphi(3^3) \Rightarrow 3^2 \cdot 2 = 18$ 

- Si fa un check sui componenti affinché siano co-primi con N

• MCD(3, 27)  $27 = 3 \cdot 3 + 0 \neq 3$  non si può usare Eulero

Si può comunque risolvere tramite le potenze di 3

$$3^2 = 9 \text{ mod } 27 \quad 3^3 = 27 \text{ mod } 27 \text{ allora } 3^{12007} = 3^{12004+3} \Rightarrow$$

$$N \cdot \overline{27} \text{ cu } \overline{27} = \overline{0}$$

$$3^{12004} \cdot 3^3 = 0 \text{ mod } 27$$

• MCD(5, 27)  $27 = 5 \cdot 5 + 2 = 2 \text{ cu c'è zero}$ 

$$5/2 = 2 \cdot 2 + 1$$

$$2/1 = 2 \cdot 1 + 0$$

- Risoluzione  $S \stackrel{36184}{:} 27 \quad 36184 / 18 = 2009 \cdot 18 + 4 \quad 5 \stackrel{36184}{=} S \Rightarrow$   
 $(S^4)^5 \cdot S^4 \Rightarrow S^4 \text{ mod } 27$ 

$$\text{quindi } 0 + S^4 \text{ mod } 27 : \frac{025}{4} \text{ mod } 27$$

$$\text{quindi } 3^{12007} + 5^{36184} \equiv 4 \text{ mod } 27$$

RESTO DI DIVISIONE  $\rightarrow$  NON INVERTIBILE

<sup>7SS</sup> Calcolare il resto della divisione per 62 del numero 6  $\stackrel{7SS}{\dots}$

$$\text{- } \varphi(6) = 62 \text{ non è primo} = \varphi(62) = \varphi(2) \cdot \varphi(3) = 1 \cdot 30 = 30$$

$$\text{- MCD deck: } \text{MCD}(62, 6) : 62/6 = 10 \cdot 6 + 2$$

$$6/2 = 3 \cdot 2 + 0$$

non è possibile usare Eulero e  $\alpha \not\equiv 0$

In questo caso conviene scomporre il membro in elementi più piccoli in cui si sia compatibile con MCD

$$\text{- } 6 \stackrel{7SS}{=} (3 \cdot 2) \stackrel{7SS}{=} 3 \stackrel{7SS}{\dots} \cdot 2 \stackrel{7SS}{\dots}$$

- Risoluzione per  $3 \stackrel{7SS}{\dots}$   $\text{MCD}(62, 3) : 62/3 = 20 \cdot 3 + 2$  sono coprimi

$$7SS(30) = 20 \cdot 30 + 5 \quad 3/2 = 1 \cdot 2 + 1 \text{ parede con Eulero}$$

$$3 \stackrel{7SS}{=} 3 \stackrel{20S}{\dots} \cdot 3 \stackrel{5}{\dots} \quad 2/1 = 2 \cdot 1 + 0$$

$$3 \stackrel{7SS}{=} 3 \stackrel{5}{\dots} \text{ mod } 62 \stackrel{7SS}{=} 57 \text{ mod } 62$$

- Risoluzione per  $2 \stackrel{7SS}{\dots}$

$$\text{MCD}(62, 2)$$

$$62/2 = 21 \cdot 2 + 0$$

Non si può usare Eulero, allo stesso tempo 62 non è rappresentabile come  $2^n$

Costruendo il "giò" di  $[a]_{62}$  con 2:

$$2^0 \equiv 1 \text{ mod } 62, 2^1 \equiv 2 \text{ mod } 62, 2^2 \equiv 4 \text{ mod } 62$$

$$2^3 \equiv 8 \text{ mod } 62, 2^4 \equiv 16 \text{ mod } 62, 2^5 \equiv 32 \text{ mod } 62$$

$$2^6 \equiv 2 \text{ mod } 62$$

Per cui è possibile semplificare la potenza Nuelle

$$2^{7SS} = (2^{12S}) \cdot 2^5 \Rightarrow 2^{12S} \cdot 2^5 \rightarrow (2^6)^{20} \cdot 2^5 \times$$

$$2^6 \equiv 2 \text{ mod } 62 \quad * \quad 2^{20} \cdot 2^5 \cdot 2^5 \text{ mod } 62 \Rightarrow 2^{20} \text{ mod } 62$$

$$2^{30} \equiv 2^6 \cdot 2^5 \cdot 2^5 \text{ mod } 62$$

$$32 \text{ mod } 62$$

$$3 \stackrel{7SS}{\dots} \cdot 2 \stackrel{7SS}{\dots} \text{ mod } 62 = 57 \cdot 32 \text{ mod } 62 \\ = 26 \text{ mod } 62$$

SOLUZIONI INTERE DI EQUAZIONI ➤ È RIUSCITO AVERE

3. Calcolare MCD dei Termini BEZOUT

2.? SE MCD 1000 divide il termine noto:

2.T allora NON è risolvibile [FWI]

2.F Continuare.

3. Altrimenti moltiplicare i coefficienti dell'identità di bezout ottenuti precedentemente per l'altro membro della scomposizione.

ES: "Dato Bezout  $3 = 3522 \cdot (-36) + 321 \circ 395$   
Dai le 2 equazioni  $10 = 3522 \cdot x + 321 y$   
 $12 = 3522 \cdot z + 321 y$   
hanno soluzioni intere"

Per  $10 = 3522x + 321y$   $\text{MCD}(321, 3522) = 3 \in 3 \nmid 10$   
per cui NON ha soluzioni intere

Per  $12 = 3522z + 321y$  ha soluzioni  $\Rightarrow 12 = 34$  quindi basta moltiplicare per 4:

$$\begin{aligned} 4 \circ 3 &= 3522 \cdot (-36) + 321 \cdot 895 \\ 12 &= 3522 \cdot -144 + 321 \cdot 1580 \\ x &= -144, y = 1580 \end{aligned}$$

## OPERAZIONI BINARIE

Per operazioni binarie si intende una funzione  $f$  applicata su un insieme  $A$  definita come

$$f: A \times A \rightarrow A \quad (a, a') \mapsto a * a' .$$

\*

**PROPRIETÀ DELLE OPERAZIONI** (varia a seconda delle operazioni)

Alcune delle proprietà delle operazioni  $\forall$

- p. associativa:  $\forall a, b, c \in A \quad (a * b) * c = a * (b * c)$
- p. commutativa:  $\forall a, b \in A \quad a * b = b * a$
- p. esistenza elemento neutro:  $\exists e \in A \quad \forall a \in A \quad a * e = a$
- p. esistenza degli inversi:  $\forall x \in A, \exists y \in A \quad x * y = y * x = e$

### ALCUNI ESEMPI

$$1. \text{ ADDIZIONE } A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R} \quad * = + \quad a + b$$

$$2. \text{ MOLTIPLICAZ. } A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R} \quad * = * \quad a * b$$

$$3. \text{ SOTTRAZIONE } A = \mathbb{Z}, \mathbb{Q}, \mathbb{R} \quad * = - \quad a - b \quad \begin{cases} \text{size } \mathbb{Q} \\ \text{size } \mathbb{R} \end{cases}$$

$$4. \text{ DIVISIONE } A = \mathbb{R} \setminus \{0\} \quad * = \div \quad \begin{cases} a \neq 0 \\ a \in \mathbb{R} \end{cases}$$

$$5. \text{ UNIONE LINEARE } \times \neq \emptyset \quad A = \mathbb{R}^n \quad * = \cup \quad a_1, a_2 \in \mathbb{R}^n$$

$$6. \text{ COMPOSIZIONE } X \neq \emptyset \quad A = \{f: X \rightarrow X\} \quad * = \circ \quad g, f \in A \quad g \circ f$$

In base alle quantità di proprietà soddisfatte i gruppi possono essere classificati in:

- SEMIGRUPPO: Gruppi in cui vale p. 1 - associativa
- MONOIDE: Gruppi in cui valgono p2, p3 associativa, elem. neutro
- GRUPPO: // in cui valgono p1, p2, p3 ass, elem. neutro, inversi

Inoltre, esso (semigruppo, monoide, gruppo) è commutativo se p2 commutativo

### ESEMPI

- $(\mathbb{N}, +)$ :  $P_1, P_2, P_3, P_4$  è un monoide commutativo
- $(\mathbb{R}, \cdot)$ :  $P_1, P_2, P_3, P_4$   $0 \cdot y = 0 \neq 1$

### ESEMPIO (FOND. INF.)

Per alfabeto si intende un insieme finito formato da lettere  $\Lambda = \{a, b, c, \dots\}$ , mentre per parola si intende una successione di lettere finita  $\in P$  e insieme parole.

Ese hanno un'operazione di concatenazione  $ba + ac = bac$

- $P_1$ :  $a, b \in P$  ( $a * b + c \equiv a + (b * c) \equiv abc$ ) ✓
- $P_2$ :  $a, b \in P$   $a * b \equiv ab \quad ab \neq ba$  ✗
- $P_3$ :  $a \in P \quad \exists e \in P$  ( $a + e = a \equiv a = e$ ) ✗ ✓ solo se  $e = \epsilon$  stringa vuota
- $P_4$ :  $x \in P \quad \exists y \in P$  ( $x + y = \epsilon$ ) ✗ nessuna concat può dare  $\epsilon$   $x \in P$

La parola è un monoide non commutativo ( $a \in P$ )