

## DISCRETA: GRUPPI • GRUPPI G PT. 2

omomorfismo

- $F: G \rightarrow H$ ,  $H' \subset H \models F(H') \subset G$ , Ovvero, dato un omomorfismo  $F$ , applicando la contro-immagine di elementi di un sotto-gruppo del codominio, essi restituiscono elementi di un sottogruppo del dominio.

### DIMOSTRAZIONE

- $e_H \in F^{-1}(H')$  perché per definizione  $e_H \in H'$  e per la P1 l'elemento  $e_G \in F^{-1}(e_H) \subseteq F(H)$  neutro di  $G$  appartiene alla contro-immagine di  $e_H$  la quale a sua volta è contenuta nella contro-immagine di  $H'$
- Se  $g \in F^{-1}(H')$  se un elemento di  $G$  appartiene alla contro-immagine di  $H'$ , allora il suo inverso appartiene ad  $H'$  per poter generare l'elemento neutro.  

$$\overbrace{F(g) \cdot F(g^{-1})}^{e_H} = F(g \cdot g^{-1})$$

$\xrightarrow{\text{su } F}$
- Se  $g, g' \in H'$  Se due elementi di  $G$  appartengono ad  $H'$ , anche le loro operazioni sono appartenente ad  $H'$ .  

$$\begin{aligned} F(g), F(g') &\in H' \\ &\equiv F(g * g') \subseteq H' \\ &\equiv g * g' \in F^{-1}(H') \end{aligned}$$

di conseguenza gli stessi elementi saranno accessibili usando la contro-immagine di  $H'$ .

**NUCLEO DI UN ELEMENTO** >  $\text{Kernel}(F) \stackrel{\text{def}}{=} \{g \in G \mid F(g) = e_H\}$   $\text{Kernel}(F) = F^{-1}(e_H)$

Per Kernel o nucleo di un omomorfismo si intendono tutti gli elementi del gruppo che quale applicazione della funzione ritorna l'elemento neutro del codominio.

**ESEMPIO**: Dato  $F: \mathbb{R}^* \rightarrow \mathbb{R}^*$   $r \mapsto r^2$  allora  $\text{Kernel}(F) = \{r \in \mathbb{R}^* \mid F(r) = 1\}$   
 in cui  $\mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \times)$   $= \{1, -1\}$  K ⊂ ℝ ∵ lo zero non è nell'immagine

**ESEMPIO**: Dato  $F: \mathbb{Z} \rightarrow \mathbb{Z}$   $x \mapsto x \cdot k$  allora  $\text{Kernel}(F) = \{x \in \mathbb{Z} \mid F(x) = 0\}$   
 in cui  $k \in \mathbb{Z} \wedge k \neq 0$   $= \{0\}$

**INIETTIVITÀ DEGLI OMOMORFISMI** >  $F$  omomorfismo iniettivo  $\iff \text{Kernel}(F) = \{e_G\}$

Dato un omomorfismo  $F$ , esso è iniettivo se e solo se il suo nucleo è composto solo da  $e_G$ , ovvero, l'elemento neutro del dominio.

### DIMOSTRAZIONE

- Ipotesi:  $F$  è omomorfismo iniettivo.

Per definizione  $\text{Kernel}(F)$  contiene  $e_G$ , se esistesse un altro elemento dentro  $\text{Kernel}(F)$  per sua definizione  $\text{Kernel}(g) = e_G$  e se fosse che  $g \neq e_G$  NON SAREBBE INIETTIVO.

- Ipotesi:  $\text{Kernel}(F) = \{e_G\}$

Si definiscono 2 elementi  $x, y \in G$  tali che  $F(x) = F(y)$ , con la tesi che  $x = y$

Si sa che  $F(x) = F(y)$

$$F(x) \cdot F(y)^{-1} = F(y) \cdot F(y)^{-1} \quad \text{moltiplico entrambi per } F(y)^{-1}$$

$$F(x) \cdot F(y)^{-1} = e_H$$

per proprietà omomorfismi  $F(x \cdot y^{-1}) = e_H$  di conseguenza,  $x \cdot y^{-1}$  deve far parte del nucleo

$$x \cdot y^{-1} \in \text{Kernel}(F)$$

$$x \cdot y^{-1} = e_H$$

$$y \cdot x \cdot y^{-1} = e_H \cdot y$$

$$x = y$$

## DISCRETA: ARITMETICA • ARITMETICA 2

COMONI

EQUIVALENZA DI DUE  $\forall a, b, r \in \mathbb{Z} \wedge a = q \cdot b + r \wedge 0 \leq r < |b| \models \text{mcd}(a, b) = \text{mcd}_{\substack{\text{b|r} \\ \text{quoziente} \\ \text{resto}}} a, b$

Dati due numeri  $a, b \in \mathbb{Z}$ , in cui il primo è rappresentabile come  $a = q \cdot b + r$  e  $0 \leq r < |b|$  allora il massimo comun divisore tra  $a, b$  è equivalente al divisore tra  $b, r$

DIMOSTRAZIONE >

Definendo un nuovo num.  $c \in \mathbb{Z}$  che divide sia  $a$  che  $b$  ( $c|a \wedge c|b$ ), allora  $a$  e  $b$  sono nella forma  $a = k \cdot c$ ,  $b = h \cdot c$ . Aprovvittando che  $a$  è definibile come  $a = q \cdot b + r$  si ha  $a = q \cdot (h \cdot c) + r$  e si giunge alla formula inversa  $r = \frac{(k - qh) \cdot c}{\text{num } \in \mathbb{Z}}$  ed essendo un num. c allora  $c$  divide anche  $r$ . Si conclude che

$$\boxed{c \in \mathbb{Z} \wedge c|a \wedge c|b \models c|r}$$

Si definisce un nuovo num.  $c' \in \mathbb{Z}$  che divide sia  $b$  che  $r$  ( $c'|b \wedge c'|r$ ), allora essi sono definiti come  $b = i \cdot c'$ ,  $r = j \cdot c'$  per  $i, j \in \mathbb{Z}$ . di conseguenza si utilizza sempre il fatto che  $a = q \cdot b + r$  si ha  $a = q \cdot i \cdot c' + j \cdot c' \Rightarrow \frac{(qi+j) \cdot c'}{\text{num } \in \mathbb{Z}} = a$  e siccome ora  $a$  è nella forma  $a = z \cdot c'$ , allora  $c'$  divide  $a$ .

$$\boxed{c' \in \mathbb{Z} \wedge c'|b \wedge c'|r \models c'|a}$$

Si dimostra quindi per composizione che i divisori di  $a \wedge b$  dividono anche  $b$  ed  $r$  ossia  $\text{mcd}(a, b) = \text{mcd}(b, r)$

ALGORITMO DI EUCLIDE >

Esso dice che, dati 2 numeri  $a, b \in \mathbb{Z}$  in cui  $b|a$  ( $b$  è un divisore di  $a$ ) e quindi  $a$  è rappresentabile come  $a = q \cdot b + r$ , è possibile definire una successione delle definizioni. In particolare, per la successione successiva.

- Si sposta il divisore al posto del dividendo.
- Si sposta il resto al posto del divisore.

Di conseguenza, partendo da  $a = q \cdot b + r$

Ad un certo punto, essendo che la successione è **decrecente**, si arriverà al punto che il resto sarà 0 ( $r_{n-1} = q_{n+1} \cdot r_n$ ).

$$\begin{aligned} b &= q^1 \cdot r + r_1 \\ r &= q^2 \cdot r^1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n \cdot r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} \cdot r_n \end{aligned}$$

L'ultimo divisore o ultimo resto non nullo sarà il massimo comun divisore tra  $a$  e  $b$ .

DIMOSTRAZIONE >

Per il Teorema precedente,  $\text{mcd}(a, b) \equiv \text{mcd}(b, r_1) \equiv \text{mcd}(r_1, r_2) \dots \equiv \text{mcd}(r_{n-1}, r_n) \equiv \text{mcd}(r_n, 0)$  ovvero nell'ultimo passaggio non c'è resto, ma da Teoremi precedenti  $\forall z \in \mathbb{Z} (\text{mcd}(z, 0) = z)$  per cui  $\text{mcd}(a, b) \equiv \text{mcd}(r_n, 0) \equiv r_n$

## DISCREZIA: ARITMETICA • ARITMETICA 2

**IDENTITÀ DI BEZOUT** >  $a, b, d \in \mathbb{Z} \wedge d = \text{MCD}(a, b) \models \exists x, y \in \mathbb{Z} (d = x \cdot a + y \cdot b)$   
 Dati due numeri  $a, b \in \mathbb{Z}$  ed il loro massimo comune divisore  $d = \text{MCD}(a, b)$   
 allora esistono altri numeri  $x, y \in \mathbb{Z}$  utilizzabili per descrivere il divisore  
 come s  $d = x \cdot a + y \cdot b$

DIMOSTRAZIONE >

Dall'algoritmo di Euclide è possibile descrivere  $d$  come  $d = r_n$  in cui  
 $r_{n-1} = q_{n+1} \cdot r_n$ ,  $r_{n-2} = q_n \cdot r_{n-1} + r_n$ .

È possibile utilizzare la sequenza del contrario per andare a ritroso  
 fino al primo passaggio:

$$d = r_n \quad r_n = r_{n-2} - q_n \cdot r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} \cdot r_{n-2}) \\ = \underbrace{(1 + q_n \cdot q_{n-1})}_{\in \mathbb{Z}} \cdot r_{n-2} + \underbrace{(-q_n)}_{\in \mathbb{Z}} \cdot r_{n-3}$$

da cui continuando è possibile  $\in \mathbb{Z}$

ri-ottener  $x, y$ .

$a \quad b$

**ESEMPIO:** Trovate il MCD tra 3522 e 321 ed esprimilo con l'identità di Bezout.

**GUIDATO**

- Si utilizza la divisione euclidea per rappresentare 3522:  $\begin{array}{r|rr} 3522 & 321 \\ 321 & 10 \cdot 321 + 312 \\ 312 & 1 \cdot 312 + 0 \end{array}$  per cui  $3522 = 10 \cdot 321 + 321$
- Analogamente si applica l'algoritmo di Euclide:  $\begin{array}{r|rr} 321 & 312 \\ 312 & 1 \cdot 312 + 0 \end{array}$  per cui:  $321 = 1 \cdot 312 + 0$
- $\begin{array}{r|rr} 312 & 312 \\ 312 & 1 \cdot 312 + 0 \end{array}$  per cui:  $312 = 1 \cdot 312 + 0$
- $\begin{array}{r|rr} 312 & 312 \\ 312 & 1 \cdot 312 + 0 \end{array}$  per cui:  $312 = 1 \cdot 312 + 0$  non ha resto. Ciò rende  $r''=3$   $\text{MCD}(3522, 321)$ . Si procede e usce l'id. di Bezout.

Si ri-esprime 3 scendo lo 'step' in cui era resto:

- $q = 1 \cdot 6 + 3 \Rightarrow 3 = q - 1 \cdot 6$  A questo punto ri-scrivo il quoziente  $r''$  usando la formula in cui era resto
- $312 = 34 \cdot a + 6 \Rightarrow 6 = 312 - 34 \cdot a \Rightarrow 3 = a - 1 \cdot (312 - 34 \cdot a)$  si semplifica ciò che è rettangolare
- $3 = 9 - 312 + 34 \cdot a \Rightarrow 3 = -312 + a + 34 \cdot a \Rightarrow 3 = -312 + 35 \cdot a$
- $a = 321 - 312 \Rightarrow 3 = -312 + 35 \cdot (321 - 312)$  Semplificando:
- $3 = -312 + 35 \cdot 321 + 35 \cdot -312 \Rightarrow 3 = -312 + 35 \cdot -312 + 35 \cdot 321$
- $3 = 36 \cdot -312 + 35 \cdot 321 \Rightarrow 3 = -36 \cdot 312 + 35 \cdot 321$
- $312 = 3522 - 10 \cdot 321$  quindi  $3 = 35 \cdot 321 - 36 \cdot (3522 - 10 \cdot 321)$  semplificando:
- $3 = 35 \cdot 321 - (36 \cdot 3522 - 360 \cdot 321) \Rightarrow 3 = \underline{35 \cdot 321 + 360 \cdot 321} - 36 \cdot 3522$
- $3 = 35 \cdot 321 - 36 \cdot 3522$  che è nella forma  $\text{MCD} = x \cdot a + y \cdot b$  ovvero l'identità di Bezout.

=

## DISCRETA: ARITMETICA • ARITMETICA 2

LEGGE DI EQUIVALENZA TRA NUM. IRREDUCIBILI / PRIMI >

La relazione tra numeri primi e numeri irriducibili spesso coincide ma non sempre è così:

DET: CONCIDE SE SI PARLA IN  $\mathbb{Z}$  >  $\forall z \in \mathbb{Z} (z \text{ è primo} \leftrightarrow z \text{ è irriducibile})$

Per dimostrare il Teorema, si dimostrano ambe le parti della bi-implicazione:

- Ipotesi:  $z$  è irriducibile. Tesi:  $z$  è primo.

Si ipotizza che  $z$  possa dividere  $a \cdot b \in \mathbb{Z}$ :  $z | ab$ . Ciò vuol dire che  $z$  divide oppure divide  $b$  se è irriducibile. Si dimostra quindi che  $z | b$  e quindi  $z$  fa:

$$z | ab \models ab = k \cdot z, \quad k \in \mathbb{Z}$$

Siccome è irriducibile, i suoi divisori sono  $1$  &  $z$  stesso, per cui  $\text{MCD}(z, a) = 1$  e per l'identità di Bezout è rappresentabile nella forma  $1 = x \cdot a + y \cdot z$

Facendo i calcoli:  $b = b \cdot 1 \Rightarrow b \cdot (x \cdot a + y \cdot z) = ab + by \cdot z = z(ax + by)$   
ovvero  $z | b$ .

- Ipotesi:  $z$  è primo. Tesi:  $z$  è irriducibile

Si ipotizza che  $z$  sia nella forma  $z = a \cdot b \neq \pm 1 \vee b = \pm 1$ . Ipotizzando che  $z$  ~~la~~ allora  $a$  sarà nella forma  $a = k \cdot z, \quad k \in \mathbb{Z}$ . Usando la defn. precedente:

$$z = a \cdot b \Rightarrow z = k \cdot z \cdot b \Rightarrow z = k \cdot b \text{ di conseguenza } b = \pm 1 \vee b = -1$$

TEOREMA FONDAMENTALE DELL'ARITMETICA >  $\forall n \in \mathbb{Z} (n \neq \pm 1 \wedge n \neq -1 \models \exists p_i \in \mathbb{Z} (n = \pm p_1 \cdot p_2 \cdots \cdot p_s))$

Il Teorema fondamentale dell'informatica dice che, dato un numero  $n$  diverso da  $\pm 1$ , esso può essere rappresentato nella forma  $n = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdots p_s$  in cui i singoli fattori sono numeri primi positivi.

## DISCRETA: ARITMETICA • ARITMETICA 3

ARITMETICA MODULARE >

L'aritmetica modulare consente di raggruppare i numeri in  $\mathbb{Z}$  tramite le relazioni di equivalenza

In particolare:

- si fissa un  $N \in \mathbb{Z}$  in cui  $N \geq 2$

- si definisce la notazione di Modulo, ovvero

$$\alpha = q \cdot N + r \equiv \alpha \text{ mod } N = r \text{ per semplificare le espressioni successive.}$$

- Si definisce una singola classe di resto come:

$[x]_N = \{z \in \mathbb{Z} \mid z \text{ mod } N = x\}$  che, se eseguita come successione per ogni elemento minore di  $N$  allora si definisce la classe di resto modulo  $N$

- Pertanto, l'insieme delle classi di resto modulo  $N$  è  $\mathbb{Z}_N = \{[0]_N, [1]_N, [2]_N, \dots, [N-1]_N\}$

ESEMPIO > Con  $N=5$   $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$$[0]_5 = \{z \in \mathbb{Z} \mid z \text{ mod } 5 = 0\} \text{ ovvero i multipli} \equiv \{ \dots -15, -10, -5, 0, 5, 10, 15, \dots \}$$

$$[1]_5 = \{z \in \mathbb{Z} \mid z \text{ mod } 5 = 1\} \text{ ovvero i numeri che se divisi per 5 danno resto 1} \\ = \{ \dots -14, -9, -4, -1, 6, 11, 16, \dots \}$$

$$[2]_5 = \{z \in \mathbb{Z} \mid z \text{ mod } 5 = 2\} \leftarrow \text{resto 2} \\ = \{ \dots -13, -8, -3, 2, 7, 12, 17, \dots \}$$

$$[3]_5 = \{ \dots -12, -7, -2, 3, 8, 13, 18, \dots \}$$

$$[4]_5 = \{ \dots -11, -6, 1, 6, 11, 16, 21, \dots \}$$

È importante notare che le classi di equivalenza sono una partizione di  $\mathbb{Z}$ , ovvero:

$$\mathbb{Z} = \mathbb{Z}_N \cup \mathbb{Z}_{N+1} \cup \dots$$

## DISCRETA: ARITMETICA - ARITHMETICA 3

Inoltre si nota che una classe di equivalenza ha infiniti rappresentanti ovvero è possibile combinare il suo indice con  $N$ :  $\overline{[r]}_N \equiv \overline{[r+kN]}_N \equiv \overline{[Nr]}_N \equiv \overline{[kNr]}_N \equiv \overline{[3Nr]}_N \dots$

$$\text{ESEMPIO: } \overline{[-15]}_q = \overline{-6} \stackrel{3+(-6)}{\equiv} \overline{3} \stackrel{3+0}{\equiv} \overline{12} \stackrel{3+12}{\equiv} \overline{21} \stackrel{3+21}{\equiv}$$

APPARTENENZA A CLASSE DI RESTO >  $a, b \in \mathbb{Z} \models a \overline{[r]}_N \wedge b \overline{[r]}_N \Leftrightarrow N \mid a-b$

Dati 2 numeri interi  $a, b \in \mathbb{Z}$  essi appartengono alla stessa classe di resto  $\overline{[r]}_N$  se e solo se  $N$  è divisore della loro differenza.

DISTRIBUZIONE >

Se  $N$  è divisore di  $a-b$ , allora si può esprimere come  $a-b = k \cdot N \quad k \in \mathbb{Z} \Rightarrow a = b + kN$

Inoltre se  $a, b \in \overline{[r]}_N$ , allora  $a = q_1 \cdot N + r, b = q_2 \cdot N + r$  per cui facendo  $a-b$ :

$$a-b = q_1 \cdot N + r - (q_2 \cdot N + r) \Rightarrow q_1 \cdot N - q_2 \cdot N = r \Rightarrow N \mid (q_1 - q_2), \text{ ovvero} \quad a-b = N \cdot k$$

Di conseguenza, se  $a, b \in \overline{[r]}_N$ , allora sono rappresentabili come  $\overline{[a]}_N \equiv \overline{[b]}_N \equiv \overline{[r]}_N$   
oppure come  $a \equiv b \pmod{N}$  "a congruo b modulo  $N$ "

$$\forall \overline{[a]}_N, \overline{[b]}_N \in \mathbb{Z} \quad (\overline{[a]}_N \cdot \overline{[b]}_N = \overline{[ab]}_N)$$

OPERAZIONI SULLE CLASSI DI RESTO >  $\forall \overline{[a]}_N, \overline{[b]}_N \in \mathbb{Z}_N \quad (\overline{[a]}_N + \overline{[b]}_N = \overline{[a+b]}_N)$

È possibile definire delle operazioni sulle classi di resto quali somma e moltiplicazione.

In particolare, per entrambe le operazioni, si eseguirà l'operazione in  $\mathbb{Z}$  solo sugli indici

Inoltre entrambe le operazioni sono ben definite, ovvero valgono per ogni rappresentante delle classi di equivalenza:  $a' = a + u \cdot N \quad k \in \mathbb{Z}, b' = b + v \cdot N \models \overline{[a']}_N \equiv \overline{[a]}_N \wedge \overline{[b']}_N \equiv \overline{[b]}_N$

ESEMPI >

1.  $\mathbb{Z}_{12}$ . Essa è definibile come  $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$   $\overline{[a']}_N \equiv \overline{[a]}_N \wedge$

si nota come la classe  $\overline{0}$  possa essere  $\overline{[a]}_N \equiv \overline{[a+k \cdot 12]}_N$  con  $k=1$

scrivere come  $\overline{12}$  in quanto  $\overline{0} \equiv \overline{0+k \cdot 12}$  con  $k=1$   
inoltre:

$$-\overline{5+11} = \overline{16} = \overline{4+12} \equiv \overline{4} - \overline{3} + \overline{12} = \overline{3}, \quad -\overline{5-7} = \overline{-3} = \overline{-8} = \overline{-3+12}$$

$$\overline{21-42} = \overline{7-6} \quad \overline{6} \cdot \overline{2} = \overline{12} = \overline{0}, \quad \overline{5} \cdot \overline{5} = \overline{25} = \overline{1}$$

↓ DIV. PER 12 ↗

LE CLASSI DI RESTO SONO GRUPPI >

Data la struttura formata dall'insieme delle classi di resto modulo N  $\mathbb{Z}_N$ , essa è un gruppo abelliano ciclico nella struttura  $(\mathbb{Z}_N, +)$ . Questo perché:

DIMOSTRAZIONE >

- La somma in  $\mathbb{Z}_N$  è associativa:

$$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_N \quad ((\bar{a} + \bar{b}) + \bar{c} = \bar{a} + \bar{b} + \bar{c} = \bar{a} + \bar{b} + \bar{c} = \bar{a} + (\bar{b} + \bar{c}))$$

- La somma in  $\mathbb{Z}_N$  è commutativa:

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

- Esiste un elemento neutro identificato come  $k \cdot N$  per  $k \in \mathbb{Z}$

$$\forall \bar{a} \in \mathbb{Z}_N \quad (\bar{a} + \underbrace{\frac{k \cdot N}{\cancel{N}}} = \bar{a})$$

- Ogni elemento è invertibile rispetto all'operazione di somma, ovvero ogni elemento ha il suo opposto

$$\forall \bar{a} \in \mathbb{Z}_N \quad (\bar{a} + \bar{-a} = \bar{a} - \bar{a} = \bar{0} \text{ è l. neutro}). \text{ Inoltre } \bar{-a} \text{ è rappresentabile con } \bar{N-a}$$

ESEMPIO >

Dato la classe di resto modulo 10  $\mathbb{Z}_{10}$  e il gruppo  $(\mathbb{Z}_{10}, +)$ :

- L'opposto di  $\bar{z}$  è  $\bar{-z}$  perché  $\bar{z} + \bar{-z} = \bar{0}$ . Dice siccome l'opposto è rappresentabile come  $\bar{N-z}$  anche  $\bar{z} + \bar{N-z} = \bar{z}$  è opposto di  $\bar{z}$ . Infatti  $\bar{z} + \bar{8} = \bar{z} = \bar{0}$

$(\mathbb{Z}_N, +)$  è un gruppo ciclico >  $(\mathbb{Z}_N, +) = \langle \bar{1} \rangle \equiv \forall \bar{a} \in (\mathbb{Z}_N, +) \quad (\bar{a} = \bar{1} + \bar{1} + \dots)$

Essendo l'operazione  $(\mathbb{Z}_N, +)$  un gruppo ciclico, ciò vuol dire che ogni suo elemento è generabile dal generatore  $\langle \bar{1} \rangle$ .

ISOMORFISMO TRA GRUPPI CICLICI  $\in (\mathbb{Z}, +)$  >

Dato un gruppo ciclico generico  $(G, *)$  con generatore  $g \in G$   $G = \langle g \rangle$  finito  $|G| = n$ , allora esso è isomorfo rispetto a  $(\mathbb{Z}_n, +)$ . (qui per esomorfismo si intende omomorfismo biettivo)

DIMOSTRAZIONE >

Definendo la funzione  $f: (\mathbb{Z}_n, +) \rightarrow (G, *)$  come  $\bar{z} \mapsto g^z$  si procede prima di verificare che essa sia ben definita, in quanto  $\bar{z}$  per def. è rappresentabile in  $n$  modi:

- BEN DEFINITA: Dati  $\bar{r}, \bar{s} \in \mathbb{Z}_n$  t.c.  $\bar{r} = \bar{s}$

allora  $\bar{s} = \bar{r} + k \cdot N$  per  $k \in \mathbb{Z}$  di conseguenza applicando la funzione:

$$f(\bar{s}) = g^s \equiv g^{\bar{r}+kN} \text{ da per prop. potenze} \equiv g^{\bar{r}} \cdot g^{kN} \stackrel{\substack{\text{da elem neutro compiibile} \\ \text{e } g^0 = 1}}{=} g^{\bar{r}} \text{ ovvero } f(\bar{s}) = f(\bar{r})$$

- BIETTIVITÀ:  $f(\bar{a} + \bar{b}) = f(\bar{a}) * f(\bar{b})$

$$\forall \bar{a}, \bar{b} \in \mathbb{Z}_n \quad (f(\bar{a} + \bar{b}) = f(\bar{a} + \bar{b}) = g^{\bar{a} + \bar{b}} = g^{\bar{a}} * g^{\bar{b}} = f(\bar{a}) * f(\bar{b})) \text{ verificata}$$

- INIEZIONE: In questo caso per verificare che sia un isomorfismo basta verificare che sia iniettiva in quanto  $|\mathbb{Z}_n| = |G|$ . Per fare ciò ci si accetta che il Kernel  $f$  contenga solo l'elemento neutro di  $\mathbb{Z}_n$

$$\text{Ker } f = \{ \bar{e} \in \mathbb{Z}_n \mid f(\bar{e}) = e \} = \{ \bar{0} \} \text{ perché } g^{\bar{e}} = e \text{ con } \bar{e} = k \cdot N \text{ per } k \in \mathbb{Z}$$

DEFINIRE ALTRI GENERATORI DI  $(\mathbb{Z}_N, +)$  >  $\text{MCD}(N, k) = 1 \Leftrightarrow \bar{k} \in \mathbb{Z}_N$

$$f(\bar{k}) = e \text{ con } \bar{k} = \bar{0}$$

È possibile definire altri generatori di  $(\mathbb{Z}_N, +)$  usando il MCD. In particolare, dato un  $\bar{a} \in \mathbb{Z}_N$  allora se  $\text{MCD}(\bar{a}, N) = 1$  allora  $\langle \bar{a} \rangle \equiv \mathbb{Z}_N$ . Questo perché se  $\text{MCD}(\bar{a}, N) = 1$ , allora il num. più piccolo per cui  $k \cdot \bar{a} = \bar{0}$  sarà  $N$  di conseguenza il suo gruppo ciclico generato sarà per forza  $\mathbb{Z}_N$ .

ESEMPIO > Considerando  $\mathbb{Z}_{10}$ :

$$\langle \bar{1} \rangle \equiv \mathbb{Z}_{10} \text{ per def. di } \mathbb{Z}_N = \{ \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{0} \}$$

$$\langle \bar{2} \rangle \equiv \{ \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{0} \}$$

$$\langle \bar{3} \rangle \equiv \{ \bar{3}, \bar{6}, \bar{9}, \bar{1}, \bar{2}, \bar{5}, \bar{8}, \bar{7}, \bar{4}, \bar{0} \}$$

$$\text{MCD}(3, 10) = 1 \text{ generatore}$$

## DISCRETA: ARITMETICA • ARITMETICA 4

OMOMORFISMO SURRETTIVO SU  $\mathbb{Z}_N > \forall n, m \in \mathbb{Z} \wedge n|m \models \exists \phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m [\bar{a}]_n \mapsto [\bar{a}]_m$  om. surrettivo  
Data due interi  $n, m \in \mathbb{Z}$  in cui uno divide l'altro ( $n|m$ ) allora è possibile definire una funzione come omomorfismo surrettivo che mappa l'insieme delle c. resto mod dividendo nel corrispettivo del divisore

**ESEMPIO** Dati come  $n=5, m=10, \phi : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_5 [\bar{a}]_{10} \mapsto [\bar{a}]_5$  per cui  
 $- \phi([\bar{1}]_{10}) = [\bar{1}]_5, - \phi([\bar{4}]_{10}) = [\bar{4}]_5 - \phi([\bar{8}]_{10}) = [\bar{8}]_5 = [\bar{3}]_5$   
 $- \phi([\bar{5}]_{10}) = [\bar{5}]_5 = [\bar{0}]_5 - \phi([\bar{2}]_{10}) = [\bar{2}]_5 = [\bar{2}]_5 - \phi([\bar{18}]_{10}) = [\bar{18}]_5 = [\bar{3}]_5$   
Se  $n \nmid m$  allora subite le ben def.!

ISOMORFISMI CON COPPIE ORDINATE  $> a, b \in \mathbb{Z}, N=a \cdot b, \text{MCD}(a, b)=1 \models \mathbb{Z}_N \cong \mathbb{Z}_a \times \mathbb{Z}_b$

Dato un  $\mathbb{Z}_N$  con  $N=a \cdot b \in \mathbb{Z}$  se gli elementi della moltiplicazione  $a, b$  sono  $\text{c.p.}$ ,  $\text{MCD}(a, b)=1$ , allora  $\mathbb{Z}_N$  è isomorfo rispetto al prodotto cartesiano dei suoi elementi

## DISCRETA: ARITMETICA • ARITMETICA 5

### STRUTTURA MOLTIPLICATIVA CLASSI RESTO

La struttura moltiplicativa delle classi di resto  $(\mathbb{Z}_n, \cdot)$  presenta le seguenti proprietà:

- $(\mathbb{Z}_n, \cdot)$  è associativa:  $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z} (\bar{a} \cdot \bar{b}) \cdot \bar{c} \equiv \bar{a} \cdot (\bar{b} \cdot \bar{c})$
- $(\mathbb{Z}_n, \cdot)$  è commutativa:  $\forall \bar{a}, \bar{b} \in \mathbb{Z} (\bar{a} \cdot \bar{b} \equiv \bar{b} \cdot \bar{a})$
- $(\mathbb{Z}_n, \cdot)$  contiene un elemento neutro:  $\forall \bar{a} \in \mathbb{Z} (\bar{a} \cdot \bar{1} = \bar{a})$
- $(\mathbb{Z}_n, \cdot)$  possiede la proprietà distributiva:  $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z} (\bar{a} \cdot (\bar{b} + \bar{c}) \equiv \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c})$

Essa però non presenta inversi, almeno non sempre

divisori dello 0  $> \forall \bar{a} \in \mathbb{Z}_N (\exists b \in \mathbb{Z} (\bar{a} \cdot \bar{b} = \bar{0})) \vee \forall \bar{a} \neq 0 (\text{MCD}(a, N) \neq 1 \models \bar{a} \text{ è div. dello } 0)$

Per divisori dello 0 si intendono le classi di resto che, se moltiplicate con un'altra classe di resto ha come risultato 0.

Può anche essere espresso come le classi di resto NON coprime rispetto a  $N$  ( $\text{GCD}(a, N) \neq 1$ )

In particolare, dato  $\mathbb{Z}_N$  e  $\bar{a} \neq 0$  il MCD(a, N) sarà la classe di resto la quale se moltiplicata per  $\bar{a}$  darà 0 come risultato.

**ESEMPIO**: In  $\mathbb{Z}_{10}$  dato  $\bar{5}$  l' $\text{mcd}(10, 5) = 2$  per cui  $\bar{5} \cdot \bar{5} = \bar{0} \equiv \bar{0}$   $\bar{5}$  div. dello 0  
 // dato  $\bar{2}$  l' $\text{mcd}(10, 2) = \bar{2}$  per cui  $\bar{2} \cdot \bar{2} = \bar{0} \equiv \bar{0}$

N.B.: gli elementi invertibili NON possono essere div. dello 0 e vice-versa.

TROVARE ELEMENTI INVERTIBILI  $> \forall \bar{a} \in \mathbb{Z}_N (\text{MCD}(a, N) = 1 \models a \text{ è invertibile})$

Data una classe di resto  $\bar{a} \in \mathbb{Z}_N$ , essa è invertibile se è co-prima con il modulo.

Il suo inverso è ottenibile tramite l'Identità di Bezout

**DIMOSTRAZIONE** Dato  $\bar{a} \in \mathbb{Z}_N$

Se  $\text{MCD}(a, N) = 1$  allora per l'Id. Bezout può essere rappresentata come  $1 = h \cdot a + k \cdot N$  e di conseguenza  $\bar{1} = \bar{h} \cdot \bar{a} + \bar{k} \cdot \bar{N}$  ma siccome per def. degli insiemi delle cl. resto  $k \cdot N = N = \bar{0}$  allora  $\bar{1} = \bar{h} \cdot \bar{a}$  ovvero  $\bar{h}$  è l'inverso di  $\bar{a}$

**ESEMPIO** "Trovare l'inverso di  $\bar{6}$  in  $\mathbb{Z}_7$ "

1. Tramite alg. Euclide determina  $\text{MCD}(7, 6)$

$$\begin{array}{l} 7(6) \Rightarrow 17 = 2 \cdot 6 + 5 \quad 1 = 6 - 1 \cdot (17 - 2 \cdot 6) \Rightarrow 1 = 6 - 17 + 2 \cdot 6 \Rightarrow 1 = \overbrace{6 + 2 \cdot 6}^{3 \cdot 6} - 17 \Rightarrow \bar{1} = \overbrace{\bar{6} + \bar{2} \cdot 6}^{\bar{3} \cdot 6} - \bar{17} \Rightarrow \bar{1} = \bar{3} \cdot \bar{6} \\ \downarrow \text{GCD} \quad 6 = 1 \cdot 5 + 1 \quad 2 = 6 - 1 \cdot 5 \quad \uparrow \quad 5 = 17 - 2 \cdot 6 \text{ per step precedente} \\ 5/1 \quad 5 = 5 \cdot 1 + 0 \end{array}$$

2. Uso Id. Bezout per ripercorrere tutto col contrario

3.  $\bar{1} = \bar{3} \cdot \bar{6}$  ma  $\bar{3} \cdot \bar{6} = \bar{0}$  in  $\mathbb{Z}_7$  per cui  $\bar{1} = \bar{3} \cdot \bar{6}$   $h = \bar{3}$  ed è inverso di  $\bar{6}$

# DISCRETA: ARITMETICA • ARITMETICA 5

## GRUPPO MOLTIPLICATIVO DI $\mathbb{Z}_N$

Per definizione,  $(\mathbb{Z}_N, \cdot)$  non è un gruppo. È però possibile definire un gruppo a partire da  $\mathbb{Z}_N$  come l'insieme delle classi di resto invertibili rispetto a  $N$  (Indicate come  $\mathbb{Z}_N^* \subset \mathbb{Z}_N^*$ ).

### La cardinalità

Per descrivere  $\mathbb{V}$  del gruppo moltiplicativo è possibile utilizzare la funzione di Eulero:

$$\varphi: N \setminus \{0\} \rightarrow N \quad n \mapsto \{a \in N \mid \text{occa } a \text{ in } n \wedge \text{MCD}(a, n) = 1\} \quad \Rightarrow |\mathbb{Z}_N^*| \equiv \varphi(N)$$

essa ha le seguenti proprietà:

- Se  $p \in N$  è primo, allora  $\varphi(p) = p-1$ . ESEMPIO:  $p=7$  primo - I numeri coprimi con  $7$  sono  $\{1, 2, 3, 4, 5, 6\}$
- Se  $p \in N$  è primo ed  $r \leq p-1$ , allora  $\varphi(p^r) = p^{r-1} \cdot (p-1)$
- Se  $a, b \in \mathbb{Z}$  sono positivi coprimi  $\text{MCD}(a, b) = 1$  allora  $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

### ESEMPI >

- $|\mathbb{Z}_{35}^*| = \varphi(35)$  ma se non è primo  $\Rightarrow \varphi(35) \equiv \varphi(5 \cdot 7) \Rightarrow \varphi(5) \cdot \varphi(7) \Rightarrow 4 \cdot 4 = 16$
- $|\mathbb{Z}_{36}^*| = \varphi(36)$  non primo  $\Rightarrow \varphi(36) = \varphi(4 \cdot 9) \equiv \varphi(4^2 \cdot 3^2) \Rightarrow \varphi(4^2) \cdot \varphi(3^2) \Rightarrow 4 \cdot (4-1) \cdot 2 \cdot (3-1) = 48$
- $|\mathbb{Z}_{1485}^*| = \varphi(1485) = \varphi(3^3 \cdot 5 \cdot 11) \Rightarrow \varphi(3^3) \cdot \varphi(5) \cdot \varphi(11) \Rightarrow 3^2 \cdot (3-1) \cdot 4 \cdot 10 = 720$

# DISCRETA: ARITMETICA • ARITMETICA 6

## NOTAZIONE DI CONGRUENZA >

Dati 2 numeri interi  $a, b \in \mathbb{Z}$  ed un intero che usare come modulo  $N \in \mathbb{Z} \setminus \{0\}$ , allora  $a \equiv b \pmod{N}$  ovvero 'a' è congruo a 'b' modulos se e solo se  $N \mid a-b$

$$N \mid a-b \equiv a = b + k \cdot N, \quad k \in \mathbb{Z} \equiv [a]_N = [b]_N \subset \mathbb{Z}_N$$

$N$  div.  $a-b$        $a$  è rappresentabile       $[a]_N = [b]_N \subset \mathbb{Z}_N$   
 come  $b+k \cdot N$       è le classi di resto di  $a$  e  $b$   
 sono uguali.

La notazione ha le seguenti proprietà:  $\forall a, b, c, d \in \mathbb{Z}$

- $a \equiv b \pmod{N} \Leftrightarrow b \equiv a \pmod{N}$  commutazione
- $a \equiv b \pmod{N} \wedge b \equiv c \pmod{N} \Rightarrow a \equiv c \pmod{N}$  composizione
- $a \equiv b \pmod{N} \wedge c \equiv d \pmod{N} \Rightarrow a+c \equiv b+d \pmod{N} \wedge a-c \equiv b-d \pmod{N}$
- $M \mid N \wedge N \mid L \Rightarrow a \equiv b \pmod{N} \wedge a \equiv b \pmod{M}$  congruo su div. di  $L$
- $\forall a, b \in \mathbb{Z} \quad a \cdot b \equiv 1 \pmod{N} \Leftrightarrow \text{MCD}(a, N) = 1$  Esistono inversi se e solo se è coprimo

## CONGRUENZE LINEARI >

È possibile definire delle equazioni del tipo  $a \cdot x \equiv b \pmod{N}$  dati  $a, b \in \mathbb{Z}$ .

Ciò vuol dire che "a · x e b hanno lo stesso resto quando divisi per N"

RISOLUZIONE: con 'a' invertibile  $\Rightarrow \text{MCD}(a, N) = 1 \Rightarrow a \cdot x \equiv b \pmod{N} \Leftrightarrow a^{-1} \cdot a \cdot x \equiv a^{-1} \cdot b \pmod{N}$

Se il moltiplicatore dell'incognita è invertibile rispetto al modulo, allora l'equazione è risolvibile tramite il suo inverso.

ESEMPPIO > Risolvere  $5x \equiv 8 \pmod{26}$

- Si verifica se 'a' è invertibile:  $\text{MCD}(5, 26) = 1$

$$26 \mid 5 \Rightarrow 26 = 5 \cdot 5 + 1 \quad \text{per } a^{-1} = 1 \cdot 5 \text{ to}$$

- Si utilizza l'Id. di Bezout per ricavare l'inverso

$$26 = 5 \cdot 5 + 1 \Rightarrow 1 = 26 - 5 \cdot 5 \quad \text{ovvero } 1 = \overline{26} - \overline{5} \cdot 5 \quad \text{quindi } a^{-1} = -5$$

- Si calcola l'equazione con l'inverso:

$$-\overline{5} \cdot \overline{5} x = \overline{8} \cdot -\overline{5} \pmod{26} \Rightarrow x = -40 \pmod{26} \Rightarrow x = 12 \pmod{26}$$

# DISCRETA: ARITMETICA • ARITMETICA 6

RISOLUZIONE: con " $a$ " non invertibile  $\Rightarrow a, b \in \mathbb{Z}$ ,  $a$  non è invertibile

In caso l'equazione di congruenza lineare non abbia il moltiplicatore invertibile nel modolo, è comunque possibile risolvere l'equazione. Per fare ciò, partendo dall'eq. di partita  $a \cdot x \equiv b \pmod{N}$ . Per def. delle eq.  $a \cdot x$  ha lo stesso resto di  $b$  quando diviso da  $N$

$$a \cdot x = b + k \cdot N$$

Quindi il resto di  $a \cdot x$  sarà lo stesso di  $b$ , ma con l'aggiunta di  $k \cdot N$

$$a \cdot x \equiv b \pmod{N}$$

Per cui per ottenere  $b$  basta spostare il termine  $a \cdot x$

$$a \cdot x + g \cdot N = b$$

In fine per convenienza si sostituisce  $k$  con il suo opposto

equazione normale in  $\mathbb{Z}$

A questo punto, se  $a$  non è invertibile, allora  $N$  è coprimo con  $a$ :  $\text{MCD}(a, N) = d$ ,  $d \neq 1$ . se  $d$  non divide  $b$ , allora  $N$  si può risolvere l'equazione.

Altimenti, se  $d \mid b$ , allora esso divide anche  $a \in \mathbb{N}$   $d \mid a \wedge d \mid N$ . Questo perché ne è il Massimo Comun Divisore, per cui è possibile dividere i termini per  $d$ :

$$a \cdot x + g \cdot N = b \Rightarrow \frac{a}{d} + g \cdot \frac{N}{d} = \frac{b}{d} \quad \leftarrow \begin{array}{l} \text{Queste a loro volta possono essere ri-scritte} \\ \text{con la notazione iniziale } ax \equiv b \pmod{N} \end{array}$$

$a' \equiv b' \pmod{N'}$

A questo punto, avendo finito i divisori,  $a'$  sarà coprimo di  $N'$  ovvero  $\text{MCD}(a', N') = 1$  per cui si può risolvere con la scorsa tecnica

ESEMPIO 1: Date le congruenze  $6x \equiv 10 \pmod{33}$ , risolvere l'equazione.

- Determino se  $a$  è invertibile:  $33/6 \rightarrow 33 = 5 \cdot 6 + 3 \pmod{6}$   $\text{MCD}(33, 6) = 3$   $a$  non è invertibile. Procedo...
- Determino se  $d=3$  è divisore di  $10$ :  $3 \nmid 10$   $3$  non è div. di  $10$ . Non risolv.

ESEMPIO 2: Date le congruenze  $9x \equiv 12 \pmod{51}$ , risolvere l'equazione:

- Determino se  $a$  è invertibile:  $51/9 \rightarrow 51 = 5 \cdot 9 + 6$   $\text{MCD}(9, 51) = 3$  non è invertibile Procedo...
- Determino se  $d \mid b$ :  $12/3 \in \mathbb{Z}$  è divisore. Divido tutti i termini per  $d$ :

$$9x \equiv 12 \pmod{51} \Rightarrow 9x + g \cdot 51 = 12 \Rightarrow \frac{9x}{3} + g \cdot \frac{51}{3} = \frac{12}{3} \Rightarrow 3x + g \cdot 17 = 4$$

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

-  $17/3$ :  $17 = 5 \cdot 3 + 2$  \* Bezout  $z = 6 \cdot 3 - 17 \cdot 1$

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

$$\begin{aligned} z &= 1 \cdot 2 + 1 \\ &= 2 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} z &= 17 - 5 \cdot 3 \Rightarrow 1 = 3 - 1 \cdot (17 - 5 \cdot 3) \\ 1 &= 3 - 17 + 5 \cdot 3 \end{aligned}$$

L'inverso di  $a' = \overline{6}$

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

$x = \overline{24} \Rightarrow \overline{24} \in \mathbb{Z}_{17}$  · Elencandole sarebbero

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

$\left[ \begin{array}{c} \overline{7} \\ \hline \overline{51} \end{array} \right], \left[ \begin{array}{c} \overline{24} \\ \hline \overline{51} \end{array} \right], \left[ \begin{array}{c} \overline{41} \\ \hline \overline{51} \end{array} \right]$  gli altri fanno opp. sempre a uno dei 3

# DISCRETA: ARITMETICA • ARITMETICA 6

**TEOREMA DI EULER >**  $a, n \in \mathbb{Z} \wedge n \geq 2 \wedge \text{MCD}(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

Dati  $z$  numeri interi  $a, N \in \mathbb{Z}$ , in cui  $N \geq 2$ , allora la classe di resto del primo elevato a  $\varphi(N)$ , ovvero della cardinalità del gruppo moltiplicativo in  $N$  è uguale a  $\bar{1}$

**TEOREMA DI FERMAT >**  $a, p \in \mathbb{Z} \wedge p \geq 2 \wedge \text{MCD}(a, p) = 1 \wedge p \text{ è primo} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

Il teorema di Fermat è un caso particolare del Teorema di Euler che descrive la cardinalità di  $N$  primi.

Se ciò è vero, allora basterà elevare  $a$  al numero primo-1 per ottenere  $\bar{1}$ .

## CASI D'USO >

I due Teoremi sono utili quando:

- Si vogliono calcolare le ultime  $N$  cifre di un num. molto grosso.
- Quel'è il resto dato dalla div. del num per un certo

**ESEMPIO 1:** "Determinare le ultime  $z$  cifre del numero  $17^{894283}$ " cioè equivalenti a dire quanto vale  $17^{894283} \pmod{10^z}$

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

$$100 \text{ non è primo per cui lo si scomponete } \varphi(100) = \varphi(5^2) \cdot \varphi(2^2) \Rightarrow 5 \cdot 4 \cdot 2 - 1 = 40$$

- Si scomponete la potenza facendo in modo che sia multiplo di  $\varphi(100)$

$$894283 / 40 \rightarrow 22357 \cdot 40 + 3 \text{ per cui } 17^{894283} \equiv 17^3 \pmod{100}$$

- Si riscriva la potenza affinché rientri nel T. Euler  $a^{\varphi(100)} \equiv 1 \pmod{100}$

$$17^{22357 \cdot 40 + 3} \equiv (17^4)^{22357} \cdot 17^3 \pmod{100}$$

$$\text{per cui } 17^3 \equiv 1 \cdot 17^3 \pmod{100} \Rightarrow 1513 \text{ da cui per cento}$$

da dove ultime  $z$  cifre  $13$

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

**ESEMPIO 2:** "Determinare la cifra finale di  $3^{405041} + 7^{448065}$

- Si calcola  $\varphi(10)$ :  $10$  non è primo:  $\varphi(10) = \varphi(2) \cdot \varphi(5) \Rightarrow 10 \equiv 4 \pmod{10}$

- Si scompongono le potenze di entrambi i numeri

$$405041 / 4 \cdot 226260 \cdot 4 + 1$$

$$448065 / 4 \cdot 112016 \cdot 4 + 1$$

- Si riscrivono le potenze

$$405041 = 3^{226260 \cdot 4 + 1}$$

$$226260 \quad \text{MCD}(3, 10) = 1$$

$$3^{448065} = 7^{112016 \cdot 4 + 1}$$

$$(3^4)^{112016} \cdot 3 = 3 \pmod{10}$$

$$7^{448065} = 7^{112016 \cdot 4 + 1}$$

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

$$\text{MCD}(7, 10) = 1$$

$$\text{quindi } 3^{405041} + 7^{448065} = 3 + 7 \pmod{10}$$

$$= 10 \pmod{10} = 0 \text{ cifra finale}$$

**ESEMPIO 3:** "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  $N$

- $\text{MCD}(3, 27) = 3 \cdot 3 + 0 = 3$  non si può usare Euler

Si pos comunque risolvere tramite le potenze di  $3$

$$3^2 = 9 \pmod{27} \quad 3^3 = 27 \pmod{27} \text{ allora } 3^{12007} = 3^{12004+3} = 3^{12004} \cdot 3^3 \Rightarrow 3^{12004} \cdot 3^3 \equiv 0 \pmod{27}$$

- $\text{MCD}(5, 27) = 5 \cdot 5 + 2 = 1$  ok Euler

$$5^{12} = 2 \cdot 2 + 1$$

$$2^{11} = 2 \cdot 1 + 0$$

- Risoluzione  $S$ :  $36184 / 18 = 24 \cdot 18 + 4 \quad 5 = 5 \Rightarrow (5^{18})^2 \cdot 5^4 \equiv 5^4 \pmod{27}$

$$\text{quindi } 0 + 5^4 \pmod{27} : 025 \pmod{27} \text{ quindi } 3^{12007} + 5^{36184} \equiv 0 \pmod{27}$$