

$$\textcircled{1} \quad 1^3 + 2^3 + \dots + m^3 = \frac{m^2(m+1)^2}{4} \quad \forall m \geq 1$$

BASE

$$m=1 \rightarrow 1^3 = \underbrace{1^2(1+1)^2}_4 \rightarrow 1 = \frac{1 \cdot 4}{4} \rightarrow 1=1 \quad \text{OK}$$

PASSO

$$m \quad 1^3 + 2^3 + \dots + m^3 = \frac{m^2(m+1)^2}{4}$$

$$m+1 \quad 1^3 + 2^3 + \dots + m^3 + (m+1)^3 = \frac{(m+1)^2(m+2)^2}{4}$$

$$1^3 + 2^3 + \dots + m^3 + (m+1)^3 = \frac{m^2(m+1)^2}{4} + (m+1)^3$$

$$1^3 + 2^3 + \dots + m^3 + (m+1)^3 = \frac{m^2(m+1)^2 + 4(m+1)^3}{4}$$

$$= \frac{(m+1)^2(m^2 + 4m + 4)}{4}$$

$$= \frac{(m+1)^2(m+2)^2}{4} \quad \text{OK}$$

$$= \frac{(m+1)^2(m+2)^2}{4} \quad \text{OK}$$

**2**

$$1^2 + 3^2 + \dots + (2m-1)^2 = \frac{m(2m-1)(2m+1)}{3} \quad \forall m \geq 1$$

BASE

$$m=1 \rightarrow 1^2 = \frac{1(2-1)(2+1)}{3} \rightarrow 1 = \frac{1 \cdot 1 \cdot 3}{3} \rightarrow 1=1 \quad \text{OK}$$

PASSO

$$m \rightarrow 1^2 + 3^2 + \dots + (2m-1)^2 = \frac{m(2m-1)(2m+1)}{3}$$

$$m+1 \rightarrow 1^2 + 3^2 + \dots + (2m-1)^2 + (2m+1)^2 = (m+1)(2m+1)(2m+3)$$

$$\begin{aligned}
 m+1 &\rightarrow 1^2 + 3^2 + \dots + (2m-1)^2 + (2m+1)^2 = \frac{(m+1)(2m+1)(2m+3)}{3} \\
 1^2 + 3^2 + \dots + (2m-1)^2 + (2(m+1)-1)^2 &= \frac{m(2m-1)(2m+1)}{3} + (2(m+1)-1)^2 \\
 &= \frac{m(2m-1)(2m+1) + 3(2m+2-1)^2}{3} \\
 &= \frac{m(2m-1)(2m+1) + 3(2m+1)^2}{3} \\
 &= \frac{(2m+1)(2m^2 - m + 6m + 3)}{3} \\
 &= \frac{(2m+1)(2m^2 + 5m + 3)}{3} \\
 2m^2 + 5m + 3 &= 2m^2 + 3m + 2m + 3 = m(2m+3) + (2m+3) = \\
 &= (2m+3)(m+1) \\
 &= \frac{(m+1)(2m+1)(2m+3)}{3} \quad \text{OK}
 \end{aligned}$$

(3)

$$\prod_{k=2}^m \left(1 - \frac{1}{k^2}\right) = \frac{m+1}{2m} \quad \forall m \geq 2$$

BASE

$$m=2 \rightarrow \prod_{k=2}^2 \left(1 - \frac{1}{k^2}\right) = \frac{2+1}{2 \cdot 2} \rightarrow \left(1 - \frac{1}{4}\right) = \frac{3}{4} \rightarrow \frac{3}{4} - \frac{3}{4} \quad \text{OK}$$

PASSO

$$m+1 \rightarrow \prod_{k=2}^{m+1} \left(1 - \frac{1}{k^2}\right) = \frac{m+2}{2(m+1)}$$

$$\begin{aligned}
 \prod_{k=2}^m \left(1 - \frac{1}{k^2}\right) \cdot \left(1 - \frac{1}{(m+1)^2}\right) &= \left(\frac{m+1}{2m}\right) \cdot \left(\frac{(m+1)^2 - 1}{(m+1)^2}\right) \\
 &= \underbrace{(m+1)^2 - 1}_{=} = \underbrace{m^2 + 2m + 1 - 1}_{=} =
 \end{aligned}$$

$k=2$

$$\begin{aligned}
 &= \frac{(m+1)^2 - 1}{2m(m+1)} = \frac{m^2 + 2m + 1 - 1}{2m(m+1)} = \\
 &= \frac{m^2 + 2m}{2m(m+1)} = \frac{m(m+2)}{2m(m+1)} \\
 &= \frac{m+2}{2(m+1)} \quad \text{OK}
 \end{aligned}$$

④

$$a_m = 3^m \cdot 2^m \quad \forall m \geq 3$$

$$a_1 = 1$$

$$a_2 = 5$$

$$a_m = 5a_{m-1} - 6a_{m-2}$$

BASE

$$m=3 \rightarrow a_3 = 3^3 \cdot 2^3 \rightarrow a_3 = 27 \cdot 8 = 19 \rightarrow a_3 = 19$$

$$a_3 \text{ PARTENDO DA IPOTESI: } a_m = 5a_{m-1} - 6a_{m-2}$$

$$\begin{aligned}
 &\stackrel{m=3}{\rightarrow} a_3 = 5a_{m-1} - 6a_{m-2} = 5a_2 - 6a_1 = \\
 &= 5(5) - 6(1) = 25 - 6 = 19
 \end{aligned}$$

19 = 19 | OK

PASSO

$$a_1 = 1$$

$$a_2 = 5$$

$$a_m = 5a_{m-1} - 6a_{m-2}$$

$$a_m = 3^m \cdot 2^m \quad \text{IPOTESI INDUTTIVA}$$

$$a_{m+1} = 5a_m - 6a_{m-1} \rightarrow \text{OTTENUTA DA } a_m \text{ SOSTITUENDO } m+1 \text{ AL POSTO DI } m$$

Tesi: INDUTTIVA

$$a_{m+1} = 3^{m+1} \cdot 2^{m+1}$$

$$a_{m+1} = 5a_m - 6a_{m-1} = 5(3^m \cdot 2^m) - 6(3^{m-1} \cdot 2^{m-1}) =$$

$$\begin{aligned}
 &= 5(3^m - 2^m) - (2 \cdot 3)(3^{m-1} - 2^{m-1}) = \\
 &= 5(3^m - 2^m) - 2 \cdot 3^m + 2^m \cdot 3 = \\
 &= 5 \cdot 3^m - 5 \cdot 2^m - 2 \cdot 3^m + 3 \cdot 2^m = \\
 &= 3^m(5-2) - 2^m(5-3) = \\
 &= 3^m \cdot 3 - 2^m \cdot 2 = \boxed{3^{m+1} - 2^{m+1}} \quad \text{OK}
 \end{aligned}$$

## (a) CALCOLARE MCD

## (b) IDENTITÀ DI BÉZOUT

(i)  $(1547, 560)$

(a)

$$\begin{array}{r} 1547 \\ 560 \\ \hline 927 \\ 427 \\ \hline 2 \end{array}$$

$$1547 = 560 \cdot 2 + 427$$

$$\begin{array}{r} 560 \\ 133 \\ \hline 427 \\ 1 \end{array}$$

$$560 = 427 + 133$$

$$\begin{array}{r} 427 \\ 28 \\ \hline 133 \\ 28 \\ \hline 3 \end{array}$$

$$427 = 133 \cdot 3 + 28$$

$$\begin{array}{r} 133 \\ 21 \\ \hline 28 \\ 21 \\ \hline 4 \end{array}$$

$$133 = 28 \cdot 4 + 21$$

$$\begin{array}{r} 28 \\ 7 \\ \hline 21 \\ 21 \\ \hline 1 \end{array}$$

$$28 = 21 \cdot 1 + 7$$

$$\begin{array}{r} 21 \\ 0 \\ \hline 7 \\ 7 \\ \hline 3 \end{array}$$

$$\boxed{7 = \text{mcd}}$$

(b)

$$7 = 28 - \underline{\underline{21(1)}} = \\ 28 - \underline{\underline{(133 - 28 \cdot 4)(1)}} =$$

$$28 - 133 + 28 \cdot 4 =$$

$$\underline{\underline{28 \cdot 5}} - 133 = \\ (427 - 133 \cdot 3)(5) - 133 =$$

$$427(5) - 133(15) - 133 =$$

$$427(5) - \underline{\underline{133(16)}} = \\ 427(5) - (360 - 427)(16) =$$

$$427(5) - 360(16) + 427(16) =$$

$$427(21) - 360(16) =$$

$$(1547 - 360(21))(21) - 360(16) =$$

$$1547(21) - 360(42) - 360(16) =$$

$$1547(21) - 360(58) = \boxed{7}$$

(2)

$$(-44880, 5292)$$

a

$$\begin{array}{r} 44880 \\ 2544 \end{array} \left| \begin{array}{r} 5292 \\ 8 \end{array} \right.$$

$$44880 = 5292(8) + 2544$$

$$\begin{array}{r} 5292 \\ 204 \end{array} \left| \begin{array}{r} 2544 \\ 2 \end{array} \right.$$

$$5292 = 2544(2) + 204$$

$$\begin{array}{r} 2544 \\ 96 \end{array} \left| \begin{array}{r} 204 \\ 12 \end{array} \right.$$

$$2544 = 204(12) + 96$$

$$\begin{array}{r} 204 \\ 12 \end{array} \left| \begin{array}{r} 96 \\ 2 \end{array} \right.$$

$$204 = 96(2) + 12$$

$$\begin{array}{r} 96 \\ 0 \end{array} \left| \begin{array}{r} 12 \\ 8 \end{array} \right.$$

$$\boxed{12 = MCD}$$

b

$$12 = 204 - 96(2)$$

$$= 204 - (2544 - 204(12))(2)$$

$$= 204 - 2544(2) + 204(24)$$

$$= 204(25) - 2544(2)$$

$$= (5292 - 2544(2)) \cdot 25 - 2544(2)$$

$$= 5292(25) - 2544(50) - 2544(2)$$

$$\begin{aligned}
 &= 5292(25) - \underbrace{2544}_{\text{green bracket}}(52) \\
 &= 5292(25) - (44880 - 5292(8))(52) \\
 &= 5292(25) - 44880(52) + 5292(416) \\
 &= 5292(-491) - 44880(52) = \boxed{12}
 \end{aligned}$$

1)

$$A = \{0, 1, 2, 3, 4\}$$

(a)  $E = \{(0,0), (0,1), (1,0), (1,1)\}$

(b)  $E = \{(0,0), (0,1), (1,0), (2,2), (3,3), (4,4)\}$

(c)  $E = \{(0,0), (0,1), (1,0), (1,1), (1,2), (2,1), (2,2), (3,3), (4,4)\}$

(d)  $E = \{(0,0), (0,1), (1,0), (1,1), (1,2), (2,1), (2,2), (0,2), (2,0), (3,3), (4,4)\}$

(e)  $E = \{(0,0), (0,1), (1,0), (1,1), (2,2), (3,3), (4,4), (3,4), (4,3)\}$

(a)  $E = \{(0,0), (0,1), (1,0), (1,1)\}$

RIFLESSIVA

$$\forall a \in A, aRa? \quad Sì, perché ci sono le coppie (0,0), (1,1)$$

SIMMETRICA

$$\forall a, b \in A, aRb \rightarrow bRa? \quad Sì, perché ci sono le coppie (0,1), (1,0)$$

TRANSITIVA

$$\forall a, b, c \in A, aRb, bRc \rightarrow aRc?$$

$$\text{se } 0R1 \text{ e } 1R0 \rightarrow 0R0? \quad Sì, perché esiste la coppia (0,0)$$

R è classe di equivalenza

CLASSI DI EQUIVALENZA

$$A_1 = \{0, 1\}$$

(b)  $E = \{(0,0), (0,1), (1,0), (2,2), (3,3), (4,4)\}$

### RIFLESSIVA

$\forall a \in A, aRa?$  Si, perché ci sono le coppie  $(0,0), (1,1), (2,2), (3,3), (4,4)$

### SIMMETRICA

$\forall a, b \in A, aRb \rightarrow bRa?$  No, perché manca la coppia  $(1,0)$

$R$  non è classe di equivalenza

c)  $E = \{(0,0), (0,1), (1,0), (1,1), (1,2), (2,1), (2,2), (3,3), (4,4)\}$

### RIFLESSIVA

$\forall a \in A, aRa?$  Si, perché ci sono le coppie  $(0,0), (1,1), (2,2), (3,3), (4,4)$

### SIMMETRICA

$\forall a, b \in A, aRb \rightarrow bRa?$  Si, perché abbiano le coppie  $(0,1), (1,0), (1,2), (2,1)$

### TRANSITIVA

$\forall a, b, c \in A, aRb, bRc \rightarrow aRc?$

No, perché se  $0R1, 1R2 \rightarrow 0R2$

$R$  non è classe di equivalenza

d)  $E = \{(0,0), (0,1), (1,0), (1,1), (1,2), (2,1), (2,2), (0,2), (2,0), (3,3), (4,4)\}$

### RIFLESSIVA

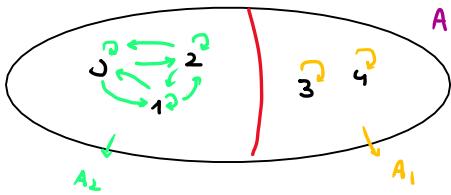
$\forall a \in A, aRa?$  Si, perché ci sono le coppie  $(0,0), (1,1), (2,2), (3,3), (4,4)$

### SIMMETRICA

$\forall a, b \in A, aRb \rightarrow bRa?$  Si, perché abbiano le coppie  $(0,1), (1,0), (1,2), (2,1), (0,2), (2,0)$

### TRANSITIVA

$\forall a, b, c \in A, aRb, bRc \rightarrow aRc?$  Si, perché in  $A_2$  tutti gli elementi sono in relazione tra loro



R è classe di equivalenza

In questo caso avremo 2 classi di equivalenza

$$A_1 = \{3, 4\} \quad A_2 = \{0, 1, 2\}$$

①

$$E = \{(0,0), (0,1), (1,0), (1,1), (2,2), (3,3), (4,4), (3,4), (4,3)\}$$

RIFLESSIVA

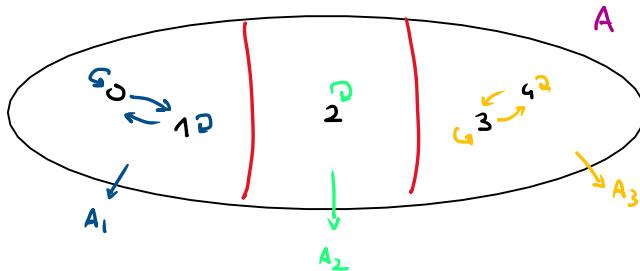
$$\forall a \in A, aRa? \quad Sì, perché ci sono le coppie (0,0), (1,1), (2,2), (3,3), (4,4)$$

SIMMETRICA

$$\forall a, b \in A, aRb \rightarrow bRa? \quad Sì, perché abbiamo le coppie (0,1), (1,0), (3,4), (4,3)$$

TRANSITIVA

$$\forall a, b, c \in A, aRb, bRc \rightarrow aRc? \quad Sì, perché gli elementi di A1 e A3 sono tutti in relazione tra loro$$



R è classe di equivalenza

2

Stabilire se R è classe di equivalenza

a)  $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x e y \text{ sono ENTRAMBI pari}\}$

RIFLESSIVA

$\forall m \in \mathbb{N}, m R_m ?$

①  $(M_{m,m}(\mathbb{R}), +)$  è un gruppo rispetto alla somma di matrici?

ASSOCIAZIONE:  $\forall A, B, C \in M_{m,m}(\mathbb{R}): (A+B)+C = A+(B+C)$

EL. NEUTRO:  $\exists A \in M_{m,m}(\mathbb{R}): A+0 = 0+A = A$  ( $0 =$  MATRICE NULLA)

EL. SOTTRATTORE:  $\forall A \in M_{m,m}(\mathbb{R}): A + (-A) = -A + A = 0$

COMMUTATIVITÀ  $\forall A, B \in M_{m,m}(\mathbb{R}): A+B = B+A$

$\rightarrow (M_{m,m}(\mathbb{R}), +)$  È GRUPPO ABELIANO

②  $(GL_m(\mathbb{R}), \cdot)$  è gruppo?

ASSOCIAZIONE:  $\forall A, B, C \in GL_m(\mathbb{R}) (A \cdot B) \cdot C = A \cdot (B \cdot C)$

EL. NEUTRO:  $\exists A \in GL_m(\mathbb{R}) A \cdot I_m = I_m \cdot A = A$  con  $I_m = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & 1 \end{pmatrix}$ , det  $I_m = 1$

$\rightarrow I_m \in GL_m(\mathbb{R})$

EL. SOTTRATTORE:  $\exists A \in GL_m(\mathbb{R}) \exists A^{-1} \in GL_m(\mathbb{R}) | A \cdot A^{-1} = A^{-1} \cdot A = I_m$

$$\text{con } \det A^{-1} = \frac{1}{\det A} \neq 0$$

COMMUTATIVITÀ  $\forall A, B \in GL_m(\mathbb{R}) A \cdot B \neq B \cdot A$

$\rightarrow (GL_m(\mathbb{R}), \cdot)$  È GRUPPO SEMPLICE

③  $(\mathbb{Z}_n, +)$  è gruppo?

ASSOCIAZIONE  $\forall [a], [b], [c] \in \mathbb{Z}_n ([a]+[b]) + [c] = [a] + [b+c]$

$$\exists \text{ EL. NEUTRO } \forall [a] \in \mathbb{Z}_m \quad [a] + [0] = [0] + [a] = [a+0] = [a]$$

$$\exists \text{ EL. SIMMETRICO } \forall [a] \in \mathbb{Z}_m \quad [a] + [-a] = [-a] + [a] = [0]$$

$$\text{COMMUTATIVITÀ} \quad \forall [a], [b] \in \mathbb{Z}_m \quad [a] + [b] = [b] + [a]$$

4  $(\mathbb{Z}_m^*, \cdot)$  È gruppo con m primo?

$$\text{ASSOCIAZIONE} \quad \forall [a], [b], [c] \in \mathbb{Z}_m^* \quad ([a] + [b]) + [c] = [a] + ([b] + [c])$$

$\exists \text{ EL. NEUTRO}$  DOBBIANO DIMOSTRARE CHE  $\forall [a] \in \mathbb{Z}_m^* \rightarrow [a]$  ha inverso

Se  $[a] \in \mathbb{Z}_m^* \rightarrow [a] \not\equiv 0 \pmod{m} \rightarrow a$  non è multiplo di m

segue che essendo m primo  $(a, m) = \begin{cases} 1 \\ m \end{cases}$

Dato che a non è multiplo di m  $\rightarrow (a, m) = 1 \rightarrow \exists x, y \in \mathbb{Z}$  tali che  $ax + my = 1$

$\rightarrow ax \equiv 1 \pmod{m} \rightarrow [ax] = [a][x] = [1] \rightarrow [a]$  ha inverso  $[x]$

5  $(\mathbb{Z}_5^*, \cdot)$  Determina gli inversi

$$\mathbb{Z}_5^* = \{[1], [2], [3], [4]\}$$

■ Sia  $GL_2(\mathbb{Z}_3)$  gruppo delle matrici invertibili:  $2 \times 2$  (det  $\neq 0$ ) a coefficienti in  $\mathbb{Z}_3$

$$\text{■ Sia } \bar{A} = \left\{ A = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{b} & \bar{c} \end{pmatrix} \mid \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_3, \det(A) = \bar{a}\bar{c} - \bar{b}^2 \neq 0 \right\}$$

(a) PROVARE CHE  $\bar{A} \leq GL_2(\mathbb{Z}_3)$

(b) PROVARE CHE  $N = \left\{ \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{b} & \bar{c} \end{pmatrix} \in \bar{A} \mid \bar{a}\bar{c} = 1 \right\}$ ,  $N \trianglelefteq A$

(c) DETERMINARE L'ORDINE DEL GRUPPO QUOTIENTE  $\bar{A}/N$ , cioè  $|\bar{A}/N|$

(a)

$$\bar{A} \leq GL_2(\mathbb{Z}_3) \iff A_1 \cdot A_2^{-1} \in \bar{A} \quad \forall A_1, A_2 \in \bar{A}$$

$$A_1 = \begin{pmatrix} \bar{a}_1 & \bar{b}_1 \\ \bar{b}_1 & \bar{c}_1 \end{pmatrix}, \det(A_1) = \bar{a}_1 \bar{c}_1 - \bar{b}_1^2 \neq 0$$

$$A_2 = \begin{pmatrix} \bar{a}_2 & \bar{b}_2 \\ \bar{b}_2 & \bar{c}_2 \end{pmatrix}, \det(A_2) = \bar{a}_2 \bar{c}_2 - \bar{b}_2^2 \neq 0$$

$$a_{11} = (-1)^{1+1} \cdot \bar{c}_2 = \bar{c}_2$$

$$a_{12} = (-1)^{1+2} \cdot \bar{b}_2 = -\bar{b}_2$$

$$a_{21} = (-1)^{2+1} \cdot \bar{b}_1 = \bar{b}_1$$

$$a_{22} = (-1)^{2+2} \cdot \bar{a}_2 = \bar{a}_2$$

$$A_2^{-1} = \frac{1}{\bar{a}_2 \bar{c}_2} \cdot \begin{pmatrix} \bar{c}_2 & \bar{b}_2 \\ -\bar{b}_2 & \bar{a}_2 \end{pmatrix}$$

$$A_1 \cdot A_2^{-1} = \frac{1}{\bar{a}_2 \bar{c}_2} \cdot \begin{pmatrix} \bar{a}_1 & \bar{b}_1 \\ \bar{b}_1 & \bar{c}_1 \end{pmatrix} \begin{pmatrix} \bar{c}_2 & \bar{b}_2 \\ -\bar{b}_2 & \bar{a}_2 \end{pmatrix} = \frac{1}{\bar{a}_2 \bar{c}_2} \begin{pmatrix} \bar{a}_1 \bar{c}_2 & \bar{a}_1 \bar{b}_2 \\ \bar{b}_1 \bar{c}_2 - \bar{c}_1 \bar{b}_2 & \bar{b}_1 \bar{a}_2 \end{pmatrix} =$$

$$= \begin{pmatrix} \cancel{\bar{a}_1 \bar{c}_2} & \bar{0} \\ \cancel{\bar{b}_1 \bar{c}_2 - \bar{c}_1 \bar{b}_2} & \cancel{\bar{b}_1 \bar{a}_2} \end{pmatrix}$$

$$\rightarrow \det(A_1 \cdot A_2^{-1}) = \det(A_1) \cdot \det(A_2^{-1})$$

$$z = \frac{a^2}{c_1 \cdot c_2} \neq 0 \quad \rightarrow \quad \boxed{\bar{A} \leq G}$$

(b)

$$N \trianglelefteq A$$

# SISTEMI DI CONGRUENZE

giovedì 2 giugno 2022 20:46

$$\left\{ \begin{array}{l} 18x \equiv 12 \pmod{30} \\ 7x \equiv 4 \pmod{9} \\ 28x \equiv 14 \pmod{98} \end{array} \right. \rightarrow \left\{ \begin{array}{l} 3x \equiv 2 \pmod{5} \\ 7x \equiv 4 \pmod{9} \\ 2x \equiv 1 \pmod{7} \end{array} \right. \quad \begin{matrix} \textcircled{a} \\ \textcircled{b} \\ \textcircled{c} \end{matrix}$$

$\textcircled{a}$   $3x \equiv 2 \pmod{5}$

$x = 4$  è soluzione

$\textcircled{b}$   $(7, 9) = 1$

$$1 = 7 \cdot x + 9 \cdot y$$

$$9 = 7 \cdot 1 + 2$$

$$7 = 2 \cdot 3 + 1$$

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

$$\begin{aligned} 7 \cdot (2 \cdot 3) &+ 7 \cdot (9 \cdot 7) \cdot 3 = \\ &= 7 \cdot 9 \cdot 3 + 7 \cdot 3 = 7 \cdot 9 + 9 \cdot (-3) \end{aligned}$$

$$7(4) \equiv 1 \pmod{9}$$

$$7(16) \equiv 4 \pmod{9}$$

$x = 16$  è soluzione

$\textcircled{c}$   $2x \equiv 1 \pmod{7}$

$x = 4$  è soluzione

$$\bar{x} = 4 \cdot 63 + 16 \cdot 35 + 4 \cdot 45 \pmod{315}$$

$$\begin{aligned} & 2 \quad 236 \bmod 315 \\ & = 47 \bmod 315 \end{aligned}$$

# DIVISIONE TRA POLINOMI

giovedì 2 giugno 2022 21:20

$\mathbb{Q}[x]$

$$a(x) = x^4 + 5x^3 + 6x + 30 \quad \text{in } \mathbb{Q}[x]$$

$$b(x) = x^3 + 6x^2 + 5x$$

$$\begin{array}{r} x^4 + 5x^3 \quad + 6x + 30 \\ \hline x^3 + 6x^2 + 5x \\ \hline -x^3 - 5x^2 + 6x + 30 \\ \hline x^3 - 6x^2 - 5x \\ \hline x^2 + 11x + 30 \end{array}$$

$$\begin{array}{r} x^3 + 6x^2 + 5x \\ \hline x^3 + 11x^2 + 30x \\ \hline -5x^2 - 25x \\ \hline -5x^2 - 55x - 150 \\ \hline 30x + 150 \end{array}$$

$$\begin{array}{r} x^2 + 11x + 30 \\ \hline x^2 + 5x \\ \hline 6x + 30 \\ \hline 6x + 30 \\ \hline 0 \end{array}$$

MCD

Resto

$$\text{MCD} = 30x + 150 = x + 6$$

$\mathbb{Z}_5[x]$

$$a(x) = x^4 + 5x^3 + 6x + 30 \quad \text{in } \mathbb{Z}_5[x]$$

$$b(x) = x^3 + 6x^2 + 5x$$

$$a(x) = x^4 + 0x^3 + x + 0$$

$$b(x) = x^3 + x^2 + 0 \cdot x$$

$x^4 + x$   
 $x^4 + x^3$   
 $- x^3 + x$   
 $x^3 - x^2$   
 $x^2 + x$

$x^3 + x^2$   
 $x^3 + x^2$   
 $x$   
 $x^2 + x$

$$\text{MCD} = x^2 + x$$

$\mathbb{Z}_2[x]$

$$a(x) = x^4 + 5x^3 + 6x + 30 \quad \text{in } \mathbb{Z}_2[x]$$

$$b(x) = x^3 + 6x^2 + 5x$$

$$a(x) = x^4 + x^3 + 0 \cdot x + 0$$

$$b(x) = x^3 + 0 \cdot x^2 + x$$

$$\begin{array}{r}
 x^4 + x^3 \\
 \underline{-} x^4 \qquad + x^2 \\
 \hline
 x^3 + x^2 \\
 \underline{-} x^3 \qquad + x \\
 \hline
 x^2 + x
 \end{array}
 \qquad
 \begin{array}{r}
 x^3 + x \\
 \hline
 x+1
 \end{array}$$

$$\begin{array}{r}
 x^3 + x \\
 \underline{-} x^3 + x^2 \\
 \hline
 x^2 + x \\
 \underline{-} x^2 + x \\
 \hline
 0
 \end{array}
 \qquad
 \begin{array}{r}
 x^2 + x \\
 \hline
 x+1
 \end{array}$$

$$\text{MCD} = x^2 + x$$

■  $f: \mathbb{C} \rightarrow \mathbb{C}$

$$z + ib \rightarrow z - ib$$

■  $\mathbb{C}$  gruppo additivo

- (a) verifica che  $f$  è unomorfismo
- (b) calcola  $\text{Ker } f$
- (c) calcola  $\text{Im } f$

(a)

$$\begin{aligned} f(z_1 + iz_1 + z_2 + ib_2) &= f(z_1 + z_2 + i(b_1 + b_2)) = \\ &= z_1 + z_2 - i(b_1 + b_2) = z_1 - ib_1 + z_2 - ib_2 = \\ &= f(z_1 - ib_1) + f(z_2 + ib_2) \end{aligned}$$

(b)

$$\text{Ker } f = \{ z = a + ib \in \mathbb{C} \mid f(z) = 0_{\mathbb{C}} \} = \{ a + ib \in \mathbb{C} \mid a \cdot ib = 0 \} = \{ z \in \mathbb{C} \mid z = 0 \}$$

$f$  è iniettiva  $\rightarrow \text{Ker } f = \{ z = 0 \}$

(c)

$$\begin{aligned} \text{Im } f &= f(\mathbb{C}) = \{ f(z) \mid z \in \mathbb{C} \} = \{ f(a+ib) \mid a+ib \in \mathbb{C} \} = \\ &= \{ a-ib \mid a, b \in \mathbb{R} \} = \{ z \mid z \in \mathbb{C} \} = \mathbb{C} \end{aligned}$$

$f$  è suriettiva  $\rightarrow \text{Im } f = \mathbb{C}$

*M*

■  $f: \mathbb{C}^* \rightarrow \mathbb{C}^*$

$$a + ib \rightarrow a - ib$$

■  $\mathbb{C}^*$  gruppo moltiplicativo

■  $\mathbb{C}^*$  gruppo moltiplicativo

- (a) VERIFICA CHE  $f$  È UNOMORFISMO
- (b) CALCOLA  $\text{Ker } f$
- (c) CALCOLA  $\text{Im } f$

(1)

$$\begin{aligned}
 f(z_1 + z_2) &= f((a_1 + ib_1) + (a_2 + ib_2)) = f(a_1 a_2 + ia_1 b_2 + ia_2 b_1 + i^2 b_1 b_2) = \\
 &= f(a_1 a_2 + ia_1 b_2 + ia_2 b_1 - b_1 b_2) = \\
 &= a_1 a_2 - b_1 b_2 - i(a_1 b_2 + a_2 b_1) = \\
 &= a_1 a_2 - b_1 b_2 - ia_2 b_1 - ia_1 b_2 = \\
 &= (a_1 a_2 - b_1 b_2) - i(a_1 b_2 + a_2 b_1) = \\
 &= (a_1 - ib_1)(a_2 - ib_2) \\
 &\cdot f(z_1) \cdot f(z_2)
 \end{aligned}$$

(b)  $\text{Ker } f = \{z = a+ib \mid f(z) = 1_{\mathbb{C}^*}\} = \{z = a+ib \mid a-ib = 1\} = \{z = 1\}$

$f$  è INIETTIVA  $\rightarrow \text{Ker } f = \{z = 1\}$

(c)  $\text{Im } f = \{f(z) \mid z \in \mathbb{C}^*\} = \{a-ib \mid a, b \in \mathbb{R}\} = \{z \mid z \in \mathbb{C}\} = \mathbb{C} \rightarrow z$  può non appartenere a  $\mathbb{C}^*$

$f$  non è SURGETTIVA  $\text{Im } f \neq \mathbb{C}^*$

(1)

Dimostrazione per induzione che  $\forall m \geq 0$ ,  $m^3 + 2m$  è un multiplo di 3

Sia  $p$  primo  $\mathbb{Z} \times \mathbb{Z}$  definisca la relazione  $\sim$

$$\forall (a,b), (c,d) \in \mathbb{Z} \times \mathbb{Z} \quad (a,b) \sim (c,d) \iff p \mid (ab - cd)$$

a) Verificare che  $\sim$  è una relazione d'equivalenza

b) Calcolare  $[ (0,0) ]$   
 $[ (1,1) ]$

### INDUZIONE

$m^3 + 2m$  è multiplo di 3 per  $m \geq 0$

### BASE

$$\text{per } m=0 \rightarrow 0=0$$

### PASSO

$$\begin{aligned} (m+1)^3 + 2(m+1) &= m^3 + 3m^2 + 3m + 1 + 2m + 2 = \\ &= (m^3 + 2m) + (3m^2 + 3m + 3) \\ &= 3t + 3(m^2 + m + 1) = 3(t + m^2 + m + 1) \quad \text{OK} \end{aligned}$$

MULTIPLO DI 3

(2)

$$(a,b) \sim (c,d) \iff p \mid ab - cd \quad p \text{ primo}$$

### RIFLESSIVA

$$(a,b) \sim (a,b) \quad ab - ab = 0 \quad \Rightarrow \quad p \mid 0$$

DEFINITO come  $p \neq 0$ 

### SIMMETRICA

$$\text{Se } (a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$$

$$p \mid ab - cd \quad \Rightarrow \quad p \mid cd - ab$$

TRANSITIVA

$$\text{se } (a,b) \sim (c,d) \text{ e } (c,d) \sim (e,f) \Rightarrow (a,b) \sim (e,f)$$

$$p \mid ab - cd$$

$$\Rightarrow p \mid (ab - cd) + (cd - ef) = ab - ef$$

$$p \mid cd - ef$$

È UNA RELAZIONE DI EQUIVALENZA

b

$$[(0,0)] = \{(a,b) \mid (a,b) \sim (0,0)\} = \{(pt,b), (a,ph) \mid t, h \in \mathbb{Z}\}$$

$$(a,b) \sim (0,0) \Rightarrow p \mid ab \Rightarrow p \mid a \circ p \mid b$$

$$[(1,1)] = \{(a,b) \mid (a,b) \sim (1,1)\} = \{(a,b) \mid ab = 1 + pt\}$$

$$(a,b) \sim (1,1) \Rightarrow p \mid ab - 1 \Rightarrow ab - 1 = pt \quad t \in \mathbb{Z}$$

$$ab = pt + 1$$

$$[(p+1,1), (pt+1,1), (1,pt+1)] \text{ POSSIBILI COPPIE}$$

$$\text{Se } A = \mathbb{Z}_5[x]. \text{ Se}$$

$$g: \mathbb{Z}_5[x] \rightarrow \mathbb{Z}_5$$

$$f(x) \rightarrow g(f(x)) = (f(x))^5$$

(a) Dimostrare che  $g$  è un omomorfismo di anelli: suriettivo

(b)  $\ker g$  è ideale primo? È massimale?

(a)  $g$  è omomorfismo di anelli se

$$\forall f(x), h(x) \in \mathbb{Z}_5[x]$$

$$g(f(x) + h(x)) = g(f(x)) + g(h(x))$$

$$g(f(x) \cdot h(x)) = g(f(x)) \cdot g(h(x))$$

$$\begin{aligned} f(x) &= a_0 + a_1 x + \dots + a_m x^m & a_i, b_i \in \mathbb{Z}_5 \\ h(x) &= b_0 + b_1 x + \dots + b_m x^m \end{aligned}$$

$$\begin{aligned} (1) \quad g(f(x) + h(x)) &= g((a_0 + b_0) + (a_1 + b_1)x + \dots) = (a_0 + b_0)^5 & \text{poiché sono in } \mathbb{Z}_5 \\ &= a_0^5 + b_0^5 \equiv \\ &= g(f(x)) + g(h(x)) \end{aligned}$$

$$\begin{aligned} g(f(x) \cdot h(x)) &= g(a_0 \cdot b_0 + (a_0 b_1 + a_1 b_0)x + \dots) = (a_0 b_0)^5 = a_0^5 b_0^5 \\ &= g(f(x)) \cdot g(h(x)) \end{aligned}$$

E' SURIETTIVA?

$$\forall \bar{a} \in \mathbb{Z}_5 \quad \exists f(x) \in \mathbb{Z}_5[x] \text{ tale che } (f(x))^5 = \bar{a}$$

$$a^5 = \bar{a}$$

(b)

$$\ker g = \{ f(x) \in \mathbb{Z}_5[x] \mid g(f(x))^5 = 0 \} \quad a_0^5 = a_0 = 0$$

$$\begin{aligned}\text{Ker } g &= \{ f(x) = a_1x + a_2x^2 + \dots + a_nx^n \mid t \in \mathbb{Z}^+, a_i \in \mathbb{Z}_5 \} \\ &= (\overline{t(x)}) = (x) = \{ x \cdot h(x) \mid h(x) \in \mathbb{Z}_5[x] \}\end{aligned}$$

Per il Teorema 1: omomorfismo

$$\mathbb{Z}_5[x]/_{\text{Ker } g(x)} \cong \mathbb{Z}_5$$

$\Rightarrow \text{Ker } g$  è un ideale massimale  $\Rightarrow$  è primo

$$\mathbb{Z} \quad a \sim b \iff \exists m, n \in \mathbb{N} \mid 5^m \cdot a = 5^n \cdot b$$

- (a) È una relazione compatibile con  $\sim$   
 (b) Determinare [1]

È UNA RELAZIONE DI EQUIVALENZA?

RIPROSSIVA

$$\forall a \in \mathbb{Z} \quad a \sim a \quad \forall m, n \in \mathbb{Z} \quad 5^m a = 5^n a$$

SIMMETRICA

$$\text{Se } a \sim b \Rightarrow b \sim a$$

$$\exists m, n \in \mathbb{Z} :$$

$$a \sim b \Rightarrow 5^m a = 5^n b \Rightarrow 5^n b = 5^m a \Rightarrow b \sim a$$

TRANSITIVA

$$a \sim b \wedge b \sim c \Rightarrow a \sim c$$

$$5^m a = 5^n b \quad 5^p b = 5^q c$$

$$\text{Se } m=p \quad 5^m a = 5^q c$$

$$\text{Se } m > p \quad 5^m b = 5^p \cdot 5^{m-p} b \quad m-p > 0$$

$$5^p b = 5^q c$$

Analogamente se  $p > m$

$$5^m b = 5^{m-p} \cdot 5^p b = 5^{m-p} 5^q c \cdot 5^{p-q}$$

È COMPATIBILE CON  $\sim$

$a \sim a' \Rightarrow ab \sim a'b'$
$b \sim b'$

$$a \sim a' \Rightarrow \exists m, n \in \mathbb{N} \mid 5^m a = 5^n a'$$

$$b \sim b' \Rightarrow \exists p, q \in \mathbb{N} \mid 5^p b = 5^q b'$$

$$5^m a \cdot 5^p b = 5^m a' \cdot 5^q b'$$

$$S^{m+p} ab \sim S^{m+p} a'b'$$

$$\Rightarrow ab \sim a'b'$$

### DETERMINATE [1]

$$[1]: \{ a \in \mathbb{Z} \mid a \sim 1 \} \Rightarrow S^m a, S^m \Rightarrow a = S^t$$

$$\in \{ S^t \mid t \in \mathbb{Z} \}$$

$$f(x) = x^5 - x^4 + x + 2 \in \mathbb{Z}_3[x]$$

$$f(\bar{x}) = 0 \quad (x - \bar{x}) \mid f(x)$$

$$\begin{array}{r|l} & x - \bar{x} \\ \hline x^5 - x^4 & + x + 2 \\ x^5 - x^4 & \\ \hline & x + 2 \\ & x - 1 \\ \hline & \bar{3} = \bar{0} \end{array}$$

$$f(x) = (x - 1)(x^4 - 1)$$

$$\text{Se } x^4 - 1 \text{ è riducibile} \Rightarrow x^4 - 1 = (x^2 + \bar{a}x + \bar{b})(x^2 + \bar{c}x + \bar{d})$$

$$x^4 - 1 = x^4 + cx^3 + dx^2 + ax^3 + ax^2 + adx + bx^2 + bcx + bd =$$

$$= x^4 + (a+c)x^3 + (d+a+c+b)x^2 + (ac+bc)x + bd$$

$$\left\{ \begin{array}{l} a+c = \bar{0} \\ d+a+c+b = \bar{0} \\ ad+bc = \bar{0} \\ bd = 1 \end{array} \right. \quad \begin{array}{l} bd = \bar{1} \\ \rightarrow \end{array} \quad \begin{array}{l} b = \bar{1} \quad d = \bar{1} \\ b = \bar{2} \quad d = \bar{2} \end{array}$$

$$\text{Se } b = d = \bar{1}$$

$$\left\{ \begin{array}{l} a+c = \bar{0} \\ ac+2 = \bar{0} \\ a+c = \bar{0} \\ bd = \bar{1} \end{array} \right. \quad \left\{ \begin{array}{l} a = -\bar{c} \\ -c^2 + 2 = 0 \end{array} \right. \quad \left\{ \begin{array}{l} c^2 = 2 \Rightarrow \text{Impossibile} \\ c \in \mathbb{Z}_3 \quad c = \bar{0}, \bar{1}, \bar{2} \end{array} \right.$$

$$\text{Se } b = d = \bar{2}$$

$$\left\{ \begin{array}{l} a+c = \bar{0} \\ ac+1 = \bar{0} \\ 2a+2c = \bar{0} \\ bd = \bar{1} \end{array} \right. \quad \left\{ \begin{array}{l} 2(a+c) = 0 \end{array} \right. \quad \left\{ \begin{array}{l} a+c = \bar{0} \\ ac+1 = \bar{0} \end{array} \right. \quad \left\{ \begin{array}{l} a = -c \\ -c^2 + 1 = \bar{0} \end{array} \right. \quad \left\{ \begin{array}{l} c^2 = \bar{1} \\ c = \bar{1} \end{array} \right. \quad \left\{ \begin{array}{l} c^2 = \bar{1} \\ c = \bar{2} \end{array} \right.$$

$$\left\{ \begin{array}{l} 2a+2c=0 \\ bd=1 \end{array} \right. \quad \left\{ \begin{array}{l} 2(a+c)=0 \\ \dots \end{array} \right. \quad \left\{ \begin{array}{l} \dots \\ \dots \end{array} \right. \quad \left\{ \begin{array}{l} \dots \\ c=2 \end{array} \right.$$

$$\text{Se } c = \bar{1} \Rightarrow a = -\bar{1} = \bar{2}$$

$$\text{Se } c = \bar{2} \Rightarrow a = -\bar{2} = \bar{1}$$

$$f(x) = x^4 + 1 = (x^2 + 2x + b)(x^2 + cx + d)$$

$$= (x^2 + 2x + 2)(x^2 + x + 2)$$

$$(x^2 + x + 2)(x^2 + 2x + 2)$$

$x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$  è riducibile!

$$\mathbb{Z}_3[x]/f(x) \quad f(x) = (x-1)(x^2 + 2x + 2)(x^2 + x + 2)$$

Non è un campo, non è un dominio d'integrità. Infatti ammette divisori dello zero

$$[(x-1) + (f(x))] [(x^2 + 2x + 2)(x^2 + x + 2) + (f(x))]$$

$$(x-1)(x^2 + 2x + 2) + (f(x)) [x^2 + x + 2 + (f(x))]$$

Sia  $(G = M_2(\mathbb{Z}), +)$  il gruppo additivo delle matrici  $2 \times 2$  con coefficienti lineari:

$$S \cap H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid a = 18k, k \in \mathbb{Z} \right\}$$

(a) Dimostrare che  $H$  è sottogruppo normale di  $G$

(b) Si consideri l'elemento  $x = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} + H$  del gruppo quoziente  $G/H$ . Calcolare il periodo di  $x$  in  $G/H$  e determinare  $k_0 < x$ .

(c) Determinare tutti i generatori di  $H$

(d) Determinare tutti i sottogruppi di  $H$

(a)  $\forall h_1, h_2 \in H \mid h_1 \cdot h_2^{-1} \in H$

$$h_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a = 18k, k \in \mathbb{Z}$$

$$h_2 = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}, \quad a' = 18t, t \in \mathbb{Z} \quad \text{det } h_2 = a'd'$$

$$h_2^{-1} = \frac{1}{a'd'} (h_2 \text{ adj})^t$$

$$a_{11} = (-1)^{1+1} \cdot d' = d'$$

$$a_{12} = (-1)^{1+2} \cdot c' = -c'$$

$$a_{21} = (-1)^{2+1} \cdot b' = -b'$$

$$a_{22} = (-1)^{2+2} \cdot a' = a'$$

$$h_2 \text{ adj} = \begin{pmatrix} d' & -c' \\ -b' & a' \end{pmatrix} \quad (h_2 \text{ adj})^t = \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix}$$

$$h_2^{-1} = \frac{1}{a'd'} \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix} =$$

$$\begin{aligned}
 h_1 \cdot h_2^{-1} &= \frac{1}{a'd'} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix} = \\
 &= \frac{1}{a'd'} \begin{pmatrix} ad' - bc' & -b'a + ba' \\ ca' - c'd & -b'c + da' \end{pmatrix} = \\
 &= \begin{pmatrix} \frac{ad' - bc'}{a'd'} & \frac{-b'a + ba'}{a'd'} \\ \frac{ca' - c'd}{a'd'} & \frac{-b'c + da'}{a'd'} \end{pmatrix} =
 \end{aligned}$$

(a)

$$\forall h_1, h_2 \in H \quad | \quad h_1 \cdot h_2 \in H$$

$$h_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a = 18k, \quad k \in \mathbb{Z}$$

$$h_2 = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}, \quad a' = 18t, \quad t \in \mathbb{Z}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a \cdot a' & b - b' \\ c \cdot c' & d - d' \end{pmatrix} \in H \quad \text{color yellow} \quad k = 18(a-a')$$

(b)

$$x = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} + H, \quad x \in G/H$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 18k & b \\ c & d \end{pmatrix}$$

$$x = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} + H$$

$$\text{Infatti } mx = qx = q \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 18 & 9 \\ 0 & 0 \end{pmatrix} \Rightarrow \text{color}(x) = m = 9$$

$$k \in \langle x \rangle = \{ 0_{G/H}, x, 2x, 3x, 4x, 5x, 6x, 7x, 8x \}$$

(c)

GENERATORI DI  $K$ 

$$\text{M di generatori} = \varphi(9) = \varphi(3^2) = 3^2 - 3 + 9 - 3 = 6$$

$$K = \langle x \rangle = \langle 1x \rangle = \langle 2x \rangle = \langle 4x \rangle = \langle 5x \rangle \cup \langle 7x \rangle = \langle 8x \rangle$$

(d)

SOTTOGRUPPI DI  $K$ 

$$\text{Divisori di } K \rightarrow 1, 3, 9$$

$$J_1 = \langle 1x \rangle = \langle x \rangle \quad \{1H\} \quad \text{BANALE}$$

$$J_3 = \langle 3x \rangle = \{H, 3x\} = \{H, 3 \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} H\} = \{H, \begin{pmatrix} 6 & 3 \\ 0 & 3 \end{pmatrix} H\}$$

$$J_9 = \langle 9x \rangle = \{H\} \quad \text{BANALE}$$

Definiamo in  $\mathbb{Z}$  la seguente relazione  $\sim$ :  $\forall a, b \in \mathbb{Z}$

$$a \sim b \Leftrightarrow \exists m, n \in \mathbb{N} \mid 5^m a = 5^n b$$

- a) Verificare che  $\sim$  è una relazione di equivalenza
- b) Dimostrare che  $\sim$  è compatibile con la moltiplicazione in  $\mathbb{Z}$   
cioè se  $a \sim a'$  e  $b \sim b'$  allora  $a \cdot b \sim a' \cdot b'$
- c) Determinare  $[1]_n$

È una relazione di equivalenza?

RIPLESSIVA

$$\forall a \in \mathbb{Z} \quad a \sim a \quad \forall m, n \in \mathbb{Z} \quad 5^m a = 5^n a$$

SIMMETRICA

$$\text{Se } a \sim b \Rightarrow b \sim a$$

$$\exists m, n \in \mathbb{Z} : \quad$$

$$a \sim b \Rightarrow 5^m a = 5^n b \Rightarrow 5^m b = 5^n a \Rightarrow b \sim a$$

TRANSITIVA

$$a \sim b \text{ e } b \sim c \Rightarrow a \sim c$$

$$5^m a = 5^n b \quad 5^p b = 5^q c$$

$$\text{Se } m=p \quad 5^m a = 5^q c$$

$$\text{Se } m > p \quad 5^m b = 5^p \cdot 5^{m-p} b \quad m-p > 0$$

$$5^p b = 5^q c$$

Analogamente se  $p > m$

$$5^m b = 5^{m-p} \cdot 5^p b = 5^{m-p} 5^q c \cdot 5^{p-q}$$

E' compatibile con.

$$\begin{array}{l} a \sim a' \\ b \sim b' \end{array} \Rightarrow ab \sim a'b'$$

$$\begin{array}{l} a \sim a' \Rightarrow \exists m, m' \in \mathbb{N} \mid s^m a = s^{m'} a' \\ b \sim b' \Rightarrow \exists p, q \in \mathbb{N} \mid s^p b = s^q b' \end{array}$$

$$s^m a \cdot s^p b = s^{m+p} a' \cdot s^q b'$$

$$s^{m+p} ab = s^{m+p} a'b'$$

$$\Rightarrow ab \sim a'b'$$

Determinare [1]

$$\begin{aligned} [1] = & \{ a \in \mathbb{Z} \mid a \sim 1 \} \Rightarrow s^m a = s^m \Rightarrow a = s^t \\ & \cdot \{ s^t \mid t \in \mathbb{Z} \} \end{aligned}$$

$$\left\{ \begin{array}{l} 3x \equiv 2 \pmod{5} \\ x \equiv 5 \pmod{13} \\ 2x \equiv 1 \pmod{7} \end{array} \right.$$

## TEOREM CHINESE DEL RESTO

$$(5, 13) = (5, 7) = (13, 7) = 1 \quad \text{IL SISTEMA AMMETTE SOLUZIONE}$$

$$N = 5 \cdot 13 \cdot 7 = 455 \quad N_1 = \frac{455}{5} = 91 \quad N_2 = \frac{455}{13} = 35 \quad N_3 = \frac{455}{7} = 65$$

SOLUZIONE

$$3x \equiv 2 \pmod{5} \rightarrow x \equiv 4 \pmod{5}$$

$$x \equiv 5 \pmod{13}$$

$$7x \equiv 1 \pmod{3} \rightarrow x \equiv 1 \pmod{3}$$

$$91x \equiv 4 \pmod{5}$$

$$x_1 \equiv 4$$

$$35x \equiv 5 \pmod{13}$$

$$35 \equiv 13 \cdot 2 + 9$$

$$13 \equiv 9 \cdot 1 + 4$$

$$9 \equiv 4 \cdot 2 + 1$$

$$1 \equiv 9 - 4 \cdot 2$$

$$\Leftarrow 9 - 2(13 - 9) \Leftarrow$$

$$\Leftarrow 9 - 2 \cdot 13 + 2 \cdot 9 \Leftarrow$$

$$\Leftarrow 3 \cdot 9 - 2 \cdot 13 \Leftarrow$$

$$\Leftarrow 3(35 - 13 \cdot 2) - 2 \cdot 13 \Leftarrow$$

$$\Leftarrow 3 \cdot 35 - 13 \cdot 6 - 2 \cdot 13 \Leftarrow$$

$$\Leftarrow 3 \cdot 35 - 8 \cdot 13 \Leftarrow$$

$$35(3) \equiv 1 \pmod{13}$$

$$35(13) \equiv 5 \pmod{13}$$

$$x_2 = 15 = 2$$

$$65x \equiv 1 \pmod{3}$$

$$x_3 = -1$$

$$N_1 x_1 + N_2 x_2 + N_3 x_3$$

$$91 \cdot 4 + 35 \cdot 2 + 65(-1) \equiv 364 + 70 - 61 \equiv 373 \pmod{955}$$

$$\text{Sia } f(x) = x^5 + x^4 + x + \bar{2} \in \mathbb{Z}_3[x]$$

a) Decomponere  $f(x)$  nel prodotto di fattori irriducibili di  $\mathbb{Z}_3[x]$

Sia  $g(x)$  il fattore irriducibile di  $f(x)$  di grado maggiore di uno su  $\mathbb{Z}_3[x]$ .  
Consideriamo  $\frac{\mathbb{Z}_3[x]}{t}$

b) Determinare l'ordine  $\left| \frac{\mathbb{Z}_3[x]}{t} \right|$

c) Determinare in  $\frac{\mathbb{Z}_3[x]}{t}$  l'inverso di  $(x + \bar{2}) + t$

a)

$$f_1(x) = x^5 + x^4 + x + \bar{2}$$

$$f_1(0) = \bar{2}$$

$$f_1(1) = \bar{1} - \bar{1} + \bar{1} + \bar{2} = \bar{0}$$

$$f_1(2) = \bar{3}\bar{2} - \bar{1}\bar{6} + \bar{2} + \bar{2} = \bar{2}$$

$$\begin{array}{r|rr} x^5 + x^4 + x + \bar{2} & x - \bar{1} \\ \underline{x^5 - x^4} & x^4 + 1 \\ \hline x + 2 & \\ x - 1 & \\ \hline -3 + \bar{0} & \end{array}$$

$$f_1(x) = (x - \bar{1})(x^4 + \bar{1})$$

$$f_2(x) = x^4 + \bar{1}$$

$$f_2(0) = \bar{1}$$

$$f_2(1) = \bar{1} + \bar{1} = \bar{2}$$

$$f_2(2) = \bar{1}\bar{6} + \bar{1} = \bar{1}\bar{7} = \bar{2}$$

$$(G = \mathbb{Z}_4 \times \mathbb{Z}_{10}, +)$$

① Determinare gli elementi di periodo 2. Esistono elementi di periodo 3?

$$\text{Se } f: \mathbb{Z}_4 \times \mathbb{Z}_{10} \rightarrow \mathbb{Z}_4 \times \mathbb{Z}_{10}$$

$$(\bar{x}_4, \bar{y}_{10}) \rightarrow 10(\bar{x}_4, \bar{y}_{10})$$

② Dimostrare che è un omomorfismo di gruppi.

③ Determinare  $\ker f$  e  $\text{Im } f$ . Determinare le cardinalità  $|\frac{\mathbb{Z}_4 \times \mathbb{Z}_{10}}{\ker f}|$

①  $(\bar{x}_4, \bar{y}_{10})$  ha periodo 2 se

$$2(\bar{x}_4, \bar{y}_{10}) = (0,0)$$

$$\begin{aligned} 2\bar{x}_4 &= \bar{0} & 2x &\equiv 0 \pmod{4} & x &\in \bar{0}, \bar{2} \\ 2\bar{y}_{10} &= \bar{0} & 2y &\equiv 0 \pmod{10} & y &\in \bar{0}, \bar{5} \end{aligned}$$

$$\cancel{(0,0)} \quad (\bar{0}, \bar{5}) \quad (\bar{2}, \bar{0}) \quad (\bar{2}, \bar{5})$$

$$|G|=m \quad \forall g \in G, \quad \text{ord } g \mid m$$

$3 \nmid 40$  quindi non esistono elementi di periodo 3

② Se  $f: \mathbb{Z}_4 \times \mathbb{Z}_{10} \rightarrow \mathbb{Z}_4 \times \mathbb{Z}_{10}$

$$(\bar{x}_4, \bar{y}_{10}) \rightarrow 10(\bar{x}_4, \bar{y}_{10})$$

$$\forall z_1, z_2 \in \mathbb{Z}_4 \times \mathbb{Z}_{10} \quad z_1 = (x, y) \quad z_2 = (\alpha, \beta)$$

$$f(z_1 + z_2) = f((x+\alpha, y+\beta)) = 10(x+\alpha, y+\beta)$$

$$= 10(x, y) + 10(\alpha, \beta)$$

$$= f(z_1) + f(z_2)$$

(3)  $\text{Im } f = \{ f((\bar{x}, \bar{y})) = 10(\bar{x}, \bar{y}) = (10\bar{x}, 10\bar{y}) = (2\bar{x}, 0) \mid \bar{x} \in \mathbb{Z}_4 \}$

$$= \{ (0, 0), (2, 0) \}$$

$$\text{Ker } f = \{ (\bar{x}, \bar{y}) \in \mathbb{Z}_4 \times \mathbb{Z}_{10} \mid f((\bar{x}, \bar{y})) = 10(\bar{x}, \bar{y}) = (2\bar{x}, 0) = (0, 0) \}$$

$$= \{ (0, 0), (2, 0) \mid x, y \in \mathbb{Z}_{10} \}$$

$$\left| \frac{\mathbb{Z}_4 \times \mathbb{Z}_{10}}{\text{Ker } f} \right| = 2 \cong \mathbb{Z}_2 \Rightarrow \text{è ciclico}$$

$$\left| \frac{\mathbb{Z}_4 \times \mathbb{Z}_{10}}{\text{Ker } f} \right| \cong |\text{Im } f|$$

$$G/N = \{ g+N \mid g \in G \} \quad g_1+N = g_2+N \Leftrightarrow g_1 - g_2 \in N$$

$$\frac{\mathbb{Z}_4 \times \mathbb{Z}_{10}}{\text{Ker } f} = \{ (\bar{x}_4, \bar{y}_{10}) + \text{Ker } f \mid \bar{x}_4 \in \mathbb{Z}_4, \bar{y}_{10} \in \mathbb{Z}_{10} \}$$

$$= \left\{ \begin{array}{l} (\bar{0}, \bar{0}) + \text{Ker } f \\ (\bar{0}, \bar{1}) + \text{Ker } f \\ \dots \\ (\bar{0}, \bar{9}) + \text{Ker } f \end{array} \right\} = \text{Ker } f$$

$$\boxed{\begin{array}{l} (\bar{1}, \bar{0}) + \text{Ker } f = (\bar{1}, \bar{1}) + \text{Ker } f \\ (\cancel{\bar{2}, \bar{0}}) + \text{Ker } f \\ (\bar{3}, \bar{0}) + \text{Ker } f \end{array}}$$

$A = \mathbb{Z}_2[x]$ . Se  $f(x) \in A$  di grado positivo

$\exists I = (f(x))$ .

Dimostrare che  $A/I$  è un campo d'ordine 4  $\Leftrightarrow f(x) = x^2 + x + 1$

Costruire se  $\exists$  un campo di 8 elementi

$A/I = \mathbb{Z}_2[x]/(f(x)) \Rightarrow$  per essere campo d'ordine 4  $\Rightarrow f(x)$  irriducibile d'grado 2

$$x^2 + ax + b \in \mathbb{Z}_2[x]$$

$$f(\bar{0}) = b \neq \bar{0} \Rightarrow b = \bar{1}$$

$$f(x) = x^2 + ax + \bar{1}$$

$$f(1) = 1 + a + 1 + 0 \Rightarrow a = \bar{1}$$

$\Rightarrow \exists$  un unico polinomio irriducibile d'grado 2  $\rightarrow x^2 + x + 1$

# TEOREMA CINESE DEL RESTO

domenica 5 giugno 2022 09:40

$$\begin{cases} 4x \equiv 3 \pmod{5} \\ 3x \equiv 2 \pmod{13} \\ 7x \equiv 1 \pmod{3} \end{cases}$$

## TEOREMA CHINESE DEL RESTO

$$(5, 13) = (5, 3) = (13, 3) = 1 \quad \text{IL SISTEMA AMMETTE SOLUZIONE}$$

$$N = 5 \cdot 13 \cdot 3 = 195 \quad N_1 = \frac{N}{5} = 39 \quad N_2 = \frac{N}{13} = 15 \quad N_3 = \frac{N}{3} = 65$$

$$4x \equiv 3 \pmod{5} \rightarrow x \equiv 2 \pmod{5}$$

$$3x \equiv 2 \pmod{13} \rightarrow x \equiv 5 \pmod{13}$$

$$7x \equiv 1 \pmod{3} \rightarrow x \equiv 1 \pmod{3}$$

$$39x \equiv 2 \pmod{5}$$

$$\lceil x_1 = 2 \rfloor \circ x_1 \equiv 3$$

$$15x \equiv 5 \pmod{13}$$

USO IL METODO DELLE DIVISIONI SUCCESSIVE

$$15 = 13 \cdot 1 + 2$$

$$13 = 2 \cdot 6 + 1$$

$$15(-6) \equiv 1 \pmod{13}$$

↓

$$15(-30) \equiv 5 \pmod{13}$$

$$1 = 13 - 6 \cdot 2 =$$

$$= 13 - 6(15 \cdot 13) = 13 - 6 \cdot 15 + 6 \cdot 13$$

$$= \lceil 13 \cdot 7 + 15 \cdot (-6) \rfloor$$

$$\lceil x_2 = -30 = 9 \rfloor$$

$$65x \equiv 1 \pmod{3}$$

$$\lceil x_3 = -1 \rfloor$$

$$N_1 x_1 + N_2 x_2 + N_3 x_3$$

$$39(-2) + 15(9) + 65(-1) = -78 + 135 - 65 = -8 \pmod{195}$$

$$\boxed{x \in 187 + t \cdot 195} \quad t \in \mathbb{Z}$$

SOSTITUZIONE

$$\begin{cases} 4x \equiv 3 \pmod{5} \\ 3x \equiv 2 \pmod{13} \\ 7x \equiv 1 \pmod{3} \end{cases}$$

(1)  
(2)  
(3)

(1)  $x \equiv 2 + 5h$

(2)  $3(2+5h) \equiv 2 \pmod{13}$

$$6 + 15h \equiv 2 \pmod{13}$$

$$15h \equiv -4 \pmod{13}$$

$$15h \equiv -2 \rightarrow h \equiv -2 + 13t, t \in \mathbb{Z}$$

$$x \equiv 2 + 5(-2 + 13t)$$

$$= 2 - 10 + 65t$$

$$= -8 + 65t$$

(3)  $7(-8 + 65t) \equiv 1 \pmod{3}$

$$-56 + 455t \equiv 1 \pmod{3}$$

$$455t \equiv 57 \pmod{3} \rightarrow 455t \equiv 0 \pmod{3}$$

$$(455, 3) = 1$$

$$455 \equiv 151 \cdot 3 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (455 - 151 \cdot 3) = \\ &= 3 - 455 + 151 \cdot 3 = \\ &= 152 \cdot 3 + 455(-1) \end{aligned}$$

$$455(-1) \equiv 1 \pmod{3}$$

↓

$$455(-57) \equiv 57 \pmod{3}$$

$$t = 3k$$

$$\begin{aligned} x &\equiv -8 + 65t \\ &\in [-8 + 195k] \end{aligned}$$

$$S_2 \subset A = M_2(\mathbb{Z}_3)$$

$$S_2 \subset B = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_3 \right\}$$

- (a) Dimostrare che  $B$  è un sottoinsieme di  $A$  ed è un campo
- (b) Dimostrare che  $B^*$  è un gruppo ciclico rispetto al prodotto
- (c) Determinare i generatori di  $B^*$

(a)  $B$  è sottoinsieme  $\Leftrightarrow A_1, A_2 \in B$

$$A_1, A_2 \in B$$

$$A_1 \cdot A_2 \in B$$

$$A_1 = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \quad A_2 = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}$$

$$A_1 \cdot A_2 = \begin{pmatrix} a \cdot c & -b \cdot d \\ b \cdot c & a \cdot d \end{pmatrix} \in B$$

$$A_1 \cdot A_2 = \begin{pmatrix} ac - bd & ad - bc \\ bc + ad & -bd + ac \end{pmatrix} \in B$$

$B$  è campo se

$$\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2 \neq 0 \text{ in } \mathbb{Z}_3$$

$$\begin{array}{lll} a=0 & b=1, 2 & a^2 + b^2 = 1 \\ a=1 & b=0, 1, 2 & a^2 + b^2 \neq 0 \\ a=2 & & a^2 + b^2 \neq 0 \end{array}$$

$\Rightarrow B = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_3 \right\}$  è un campo

(b)

$B^*$  è un gruppo cíclico  $\Rightarrow A_1 \cdot A_2 \in B^* \nabla A_1, A_2 \in B^*$

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \quad |B| = 9 \quad |B^*| = 8$$

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{matrix} a \text{ varia in } 3 \text{ modi} \\ b \text{ varia in } 3 \text{ modi} \end{matrix}$$

$B^*$  cíclico  $\Rightarrow B^* = \langle A \rangle \quad |B^*| = 8 \Rightarrow A^8 = \text{Id}$

$$\left( \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \right)^2 = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a^2 - b^2 & -2ab \\ 2ab & a^2 + b^2 \end{pmatrix} \neq \text{Id} \quad \forall a, b$$

$$B^* = \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \right.$$

In  $\mathbb{Z}_3$  sono uguali:

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \left. \right\}$$

$$\Rightarrow \left| \langle \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \rangle \right| = 8 \Rightarrow B^* = \langle \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \rangle$$

(c)

$$G = \langle a \rangle \quad |G| = m$$

$$z \langle a^k \rangle \quad (k, m) = 1 \quad m = 8 \Rightarrow k = 1, 3, 5, 7$$

$$B^* = \langle \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \rangle = \langle \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}^3 \rangle = \langle \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}^5 \rangle = \langle \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}^7 \rangle$$

$\mathbb{Z}_5[x]$ . Si considerano i polinomi  $f_1(x) = x^3 + 4x^2 + 2 \in \mathbb{Z}_5[x]$   
 $f_2(x) = x^3 + 3x + 4$

- (a) Si fattorizzino nel prodotto di pol. irriducibili
- (b) Determinare MCD ( $f_1(x), f_2(x)$ )
- (c) Verificare che  $I_1 = (f_1(x))$  e  $I_2 = (f_2(x))$  sono contenuti nello stesso ideale massimale  $M$
- (d)  $\mathbb{Z}_5[x]/M$  è un campo?

(a)

$$f_1(x) = x^3 + 4x^2 + 2 \quad f_1(0) = \bar{2}$$

$$f_1(1) = 1 + 4 + 2 = \bar{0}$$

$$f_1(2) = 8 + 16 + 2 = \bar{1}$$

$$f_1(3) = 27 + 36 + 2 = \bar{5}$$

$$f_1(4) = \bar{0}$$

$$(x - \bar{3}) \mid f_1(x)$$

$$\begin{array}{r} x^3 + 4x^2 + 2 \\ x^3 - 3x^2 \\ \hline 2x^2 + 2 \\ 2x^2 - 6x \\ \hline x + 2 \\ \end{array} \quad \begin{array}{c|l} & x - \bar{3} \\ & \hline & x^2 + 2x + 1 \end{array}$$

$\downarrow$   
 $x - \bar{3} \in \mathbb{Z}_5$

$$f_1(x) = (x - \bar{3})(x^2 + 2x + 1)$$

$$g_1(x) = x^2 + 2x + 1 \quad g_1(0) = \bar{1}$$

$$g_1(1) = \bar{4}$$

$$g_1(2) = \bar{4}$$

$$g_1(3) = 9 + 6 + 1 = \bar{1}$$

$$g_1(4) = 16 + 4 + 1 = \bar{1}$$

$$\begin{array}{r} x^2 + 2x + 1 \\ x^2 - 4x \\ \hline x + 1 \\ x - 4 \\ \hline 0 \\ \end{array} \quad \begin{array}{c|l} & x - \bar{4} \\ & \hline & x + 1 \end{array}$$

$\therefore \in \mathbb{Z}_5$

$$f_1(x) = (x - \bar{3})(x - \bar{4})(x + 1)$$

$$f_2(x) = x^3 + 3x + 4 \quad f_2(0) = \bar{4}$$

$$f_2(1) = \bar{3}$$

$$\begin{aligned}
 f_2(x) &= x^3 + 3x + 4 \\
 f_2(0) &= 4 \\
 f_2(1) &= 3 \\
 f_2(2) &= 3 \\
 f_2(3) &= 0 \\
 f_2(4) &= 0
 \end{aligned}$$

$$(x-3)(x-4) \mid f_2(x)$$

$$\begin{array}{r}
 x^2 - 4x - 3x + 12 \\
 x^2 - 2x + 2
 \end{array}$$

$$\begin{array}{r}
 x^3 + 3x + 4 \\
 x^3 - 2x^2 + 2x \\
 \hline
 2x^2 + x + 4 \\
 2x^2 - 4x + 4 \\
 \hline
 0
 \end{array}$$

$\xrightarrow{x \in \mathbb{Z}_5}$

$$f_2(x) = (x-3)(x-4)(x+2)$$

(b) MCD tra  $f_1(x)$  e  $f_2(x)$

$$\{f_1(x), f_2(x)\} = (x-3)(x+1)$$

(c)

$$I_1 = ((x-3)(x+1))^\perp \subset ((x-3)) \circ \{(x-3) \cdot h(x) \mid h(x) \in \mathbb{Z}_5[x]\}$$

$$I_2 = ((x-3)^\perp (x+1))^\perp \subset ((x+1))$$

$(x+1) = M_1$  è massimale

$$\left| \mathbb{Z}_5[x]/M_1 \right| = 5^1 = \mathbb{Z}_5$$

① Sa  $U(\mathbb{Z}_{12})$ . Studiarlo

$$|U(\mathbb{Z}_{12})| = \varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2) \cdot \varphi(3) = (2^2 - 2)(2) = 4$$

$$U(\mathbb{Z}_{12}) = \left\{ \bar{a} \in \mathbb{Z}_{12} \mid (a, 12) = 1 \right\} = \left\{ \bar{1}, \bar{5}, \bar{7}, \bar{11} \right\}$$

$$\text{o}(5) = \bar{5}^2 = \bar{25} = \bar{1}$$

$$\text{o}(\bar{5}) = 2$$

PERIODICO

$$\text{o}(\bar{7}) = \bar{7}^2 = \bar{49} = \bar{1}$$

$$\text{o}(\bar{7}) = 2$$

$$\text{o}(11) = \bar{11}^2 = 121 = \bar{1}$$

$U(\mathbb{Z}_{12})$  è ciclico? No, perché ogni elemento ha periodo 2

$|U(\mathbb{Z}_{12})| = 4$ . I sottogruppi di  $U(\mathbb{Z}_{12})$  per il teorema di Lagrange possono avere ordine 1, 2, 4

$$\begin{aligned} & \{1\} \quad (U(\mathbb{Z}_{12})), \langle \bar{5} \rangle, \langle \bar{7} \rangle, \langle \bar{11} \rangle \\ & \qquad \qquad \qquad \parallel \qquad \parallel \qquad \parallel \\ & \{\bar{1}, \bar{5}\} \quad \{\bar{1}, \bar{7}\} \quad \{\bar{1}, \bar{11}\} \end{aligned}$$

$G = \langle g \rangle \quad |G|=m \quad \forall d|m \quad \exists! \text{ un sottogruppo di ordine } \langle g^{m/d} \rangle$

②

Sa  $\varphi: \mathbb{Z}_{10} \rightarrow U(\mathbb{Z}_{12})$

$$\bar{x}_{10} \rightarrow \bar{5}^x$$

« $5$  ha periodo 2»

③  $\varphi$  è un omomorfismo di gruppi:

$$\forall \bar{x}, \bar{y} \in \mathbb{Z}_{10} \quad \varphi(\bar{x} + \bar{y}) = \varphi(\bar{x}) \cdot \varphi(\bar{y})$$

$$\varphi(\bar{x+y}) = 5^{x+y} = 5^x \cdot 5^y = f(x) \cdot f(y)$$

④  $\varphi$  è invertibile?

$$S_1, S_2 \subset \ker \varphi = \{\bar{0}\}$$

$$\ker \varphi = \left\{ \bar{x} \in \mathbb{Z}_{10} \mid f(\bar{x}) = 1 \right\} = \left\{ \bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8} \right\} \neq \{\bar{0}\}$$

Non è unisettivo

$$f(\bar{x}) = [5^x]_{12} = \bar{1}$$

$$x = \bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}$$

(c) Determinare la cardinalità  $|\mathbb{Z}_{10}/\ker \varphi|$

$$|G| = |H| \cdot |G/H|$$

Pur .l teorema di Lagrange

$$|\mathbb{Z}_{10}/\ker \varphi| = \frac{|\mathbb{Z}_{10}|}{|\ker \varphi|} = \frac{10}{5} = 2$$

$$\mathbb{Z}_{10}/\ker \varphi \cong \text{Im } \varphi$$

$$\Rightarrow |\text{Im } \varphi| = 2 \Rightarrow \varphi \text{ non è suriettiva}$$

(3)  $A = \mathbb{Q} \times \mathbb{Z}_{12}$  A è un dominio d'integrità?

$$\begin{aligned} & (\bar{0}, \bar{2}), (x, \bar{0}) \\ & (\bar{0}, \bar{2}), (\bar{0}, \bar{6}) \\ & (\bar{0}, \bar{3}), (\bar{0}, \bar{4}) \end{aligned}$$

$$\begin{aligned} & \text{Se } I = \{ (0, \bar{z}) \mid \bar{z} \in \mathbb{Z}_{12} \} \\ & J = \{ (x, 0) \mid x \in \mathbb{Q} \} \end{aligned}$$

Dimostrare che I e J sono ideali di A

$$\begin{aligned} I \text{ ideale} \Rightarrow & \forall i_1, i_2 \in I \quad i_1 - i_2 \in I \\ & \forall i \in I, \forall a \in A \quad i \cdot a \in I, a \cdot i \in I \end{aligned}$$

$$i_1 = (\bar{0}, \bar{z}_1), i_2 = (\bar{0}, \bar{z}_2) \quad i_1 - i_2 = (\bar{0}, \bar{z}_1 - \bar{z}_2) \in I$$

$$a = (x, \bar{b}), i = (\bar{0}, \bar{z}) \quad i \cdot a = (\bar{0}, \bar{z}) \cdot (x, \bar{b}) = (0, \bar{zb}) \in I$$

$$\begin{aligned} J \text{ ideale} \Rightarrow & \forall j_1, j_2 \in J \quad j_1 - j_2 \in J \\ & \forall j \in J, \forall a \in A \quad j \cdot a \in J, a \cdot j \in J \end{aligned}$$

$$j_1 = (x, \bar{0}), j_2 = (y, \bar{0}) \quad j_1 - j_2 = (x - y, \bar{0})$$

$$J_1 = (x, \bar{a}) \quad J_2 = (y, \bar{a}) \quad J_1 - J_2 = (x - y, \bar{a})$$

$$a \in (z, \bar{a}) \quad J = (x, \bar{a}) \quad a \cdot J = (z, \bar{a}) \cdot (x, \bar{a}) = (zx, \bar{a}) \in J$$

Dimostrare che  $I$  è un ideale massimale

$A/I$  è un campo

$$\varphi: \mathbb{Q} \times \mathbb{Z}_{12} \rightarrow \mathbb{Q}$$

$$(x, \bar{a}) \rightarrow x$$

È un omomorfismo di anelli

$$\ker \varphi = \{(x, \bar{a}) \in A, \varphi(x, \bar{a}) = 0\} = I$$

$$J = \{(x, \bar{a}), x \in \mathbb{Q}\}$$

$$f(x) = x^5 + x + \bar{2} \in \mathbb{Z}_3[x]$$

$$f(\bar{0}) = \bar{2}$$

$$f(\bar{1}) = \bar{1}$$

$$f(\bar{2}) = \bar{3}\bar{2} + \bar{2} + \bar{2} = \bar{3}\bar{6} = \bar{0}$$

$\Rightarrow (x - \bar{2})$  divide  $f(x)$

$$\begin{array}{r|l} x^5 + & x - \bar{2} \\ \hline x^5 - \bar{2}x^4 & x^4 + 2x^3 + x^2 + 2x \\ \bar{2}x^4 & + x + \bar{2} \\ \hline \bar{2}x^4 - 4x^3 & \\ x^3 & + x + \bar{2} \\ \hline x^2 - 2x^2 & \\ 2x^2 + x + \bar{2} & \\ \hline 2x^2 - 4x & \\ 2x + 2 & \\ \hline 2x - 4 & \\ \hline \bar{6} = \bar{0} & \end{array}$$

$$f(x) = (x - \bar{2})(x^4 + 2x^3 + x^2 + 2x + 2)$$

$$g(x) = x^4 + 2x^3 + x^2 + 2x + 2$$

$$g(\bar{0}) = \bar{2}$$

$$g(\bar{1}) = \bar{2}$$

$$g(\bar{2}) = 16 + 16 + 4 + 4 + 2 = \bar{4}2 = \bar{0}$$

$$\begin{array}{r|l} x^4 + 2x^3 + x^2 + 2x + 2 & x - \bar{2} \\ \hline x^4 - 2x^3 & x^3 + x^2 + 2 \\ \hline x^3 + x^2 + 2x + 2 & \\ x^3 - 2x^2 & \\ \hline 2x + 2 & \\ 2x - 4 & \\ \hline \bar{6} = \bar{0} & \end{array}$$

$$f(x) = (x - \bar{1})(x - \bar{2})(x^3 + x^2 + 2)$$

possiamo dire che  $\mathbb{Z}_3[x]/(f(x))$

$$\mathbb{Z}_3[x]/(x^3 + x^2 + x) \text{ campo}$$

$$\mathbb{Z}_3[x]/(f(x)) = \{ a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + (f(x)) \mid a_i \in \mathbb{Z}_3 \}$$

non danno d'integrità, infatti

$$(x - 2) + (f(x)) = (x - 2)(x^3 + x^2 + 2) + (f(x))$$

$$(x - 2)^2 + (f(x)) = (x^3 + x^2 + 2) + (f(x))$$

$$\mathbb{Z}_3[x]/(x^3 + x^2 + x) = \mathbb{I}$$

Calcolare l'inverso di  $\bar{2}x + \bar{1} = \bar{2}(x + \bar{2})$

$$(2x + 1)^{-1} = \bar{2}^{-1} (x + \bar{2})^{-1} = \bar{2} (x + \bar{2})^{-1}$$

$(x + \bar{2})$  è invertibile  $\Rightarrow (x^2 + 2x + b) + \mathbb{I} =$

$$= (x + 2)(x^2 + 2x + b) + \mathbb{I} =$$

$$= \bar{1} + \mathbb{I}$$

$$S_n \subset G = GL_2(\mathbb{R}) \quad H = \{ A \in G \mid \det A = s^m \text{ con } m \in \mathbb{Z} \}$$

Dimostrare che  $H$  è un sgl normale di  $G$

$$\forall A_1, A_2 \in H \quad A_1 \cdot A_2^{-1} \in H$$

$$\det(A_1 \cdot A_2^{-1})$$

$$= \det A_1 \cdot \det(A_2^{-1})$$

$$= \frac{\det A_1}{\det A_2} \cdot \frac{s^m}{s^t} = s^{m-t}$$

$H$  è normale se

$$\forall A \in H, \forall x \in G \quad x^{-1}Ax \in H$$

$$\det(x^{-1}Ax) = \cancel{\det(x^{-1})} \cdot \det(A) \cdot \cancel{\det(x)} = \det(A) = s^m$$

$$t = \begin{pmatrix} \sqrt[6]{s} & 3 \\ 0 & 1 \end{pmatrix} \notin H \quad \det T = \sqrt[6]{s}$$

$$tH \in G/H = \{ gH \mid g \in G \}. \text{ Calcolare il periodo}$$

$$(tH)^n = H \quad g_1H = g_2H \Leftrightarrow g_1 \cdot g_2^{-1} \in H$$

$$t^nH = H$$

$$t^n \in H$$

$$t^2 = \begin{pmatrix} \sqrt[6]{5} & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \sqrt[6]{5} & 3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \sqrt[6]{5^2} & 3\sqrt[6]{5} + 3 \\ 0 & 1 \end{pmatrix}$$

$$t^3 = \begin{pmatrix} \sqrt[6]{5^3} & * \\ 0 & 1 \end{pmatrix} \quad t^n \begin{pmatrix} \sqrt[6]{5^n} & * \\ 0 & 1 \end{pmatrix}$$

$$\cup(t), 6$$

$$G/H \quad K = \langle tH \rangle$$

Desideriamo: generatori e tutti i sgg di  $K$

### GENERATORI

$$|K|=6 \quad (tH)^m \quad (m, 6) = 1 \quad m = 1, 5$$

$$K = \langle tH \rangle = \langle t^3H \rangle$$

### SOTTOGRUPPI

ordine 1, 2, 3, 6

$$\text{ordine 2} \quad \langle (tH)^{\frac{6}{2}} \rangle = \langle t^3H \rangle$$

$$\text{ordine 3} \quad \langle (tH)^{\frac{6}{3}} \rangle = \langle t^2H \rangle$$