

$(\mathbb{Z}_7^*, \cdot)$

generatore

ordine degli elementi

$\langle [2]_7 \rangle$

$$\mathbb{Z}_7^* = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$$

$[1]_7$  è l'elemento neutro della struttura  $(\mathbb{Z}_7^*, \cdot)$   
e quindi non può essere un generatore

Vediamo se  $[2]_7$  è un generatore di  $(\mathbb{Z}_7^*, \cdot)$

$$[2]_7^2 = [4]_7$$

$$[2]_7^3 = [8]_8 = [1]_8 \quad \text{perché } 8 \equiv 1 \pmod 7 \quad (8-1=7 \text{ multiplo di } 7)$$

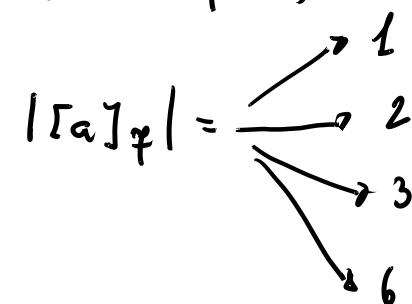
e quindi  $|[2]_7| = 3$  perché  $3 = \min \{ h \in \mathbb{N}^* : [2]_7^h = [1]_8 \}$

$|[2]_7| \neq |\mathbb{Z}_7^*| = 6$  e quindi  $[2]_7$  non è un generatore  
di  $(\mathbb{Z}_7^*, \cdot)$

Vediamo se  $[3]_7$  è un generatore di  $(\mathbb{Z}_7^*, \cdot)$

$$[3]_7^2 = [9]_7 = [2]_7 \quad 9-2=7 //$$

$$[3]_7^3 = [27]_7 = [6]_7 \quad 27-6=21 //$$



(possiamo affermare che  $[3]_7$  è un generatore di  $(\mathbb{Z}_7^*, \cdot)$  perché  
 $|[3]_7| \neq 1, |[3]_7| \neq 2, |[3]_7| \neq 3$ )

$$[3]_7^4 = [3]_7^3 \cdot [3]_7 = [6]_7 \cdot [3]_7 = [18]_7 = [6]_7 \quad 18 - 6 = 12 \quad //$$

$$[3]_7^5 = [3]_7^4 \cdot [3]_7 = [6]_7 \cdot [3]_7 = [12]_7 = [5]_7 \quad 12 - 5 = 7 \quad //$$

$$[3]_7^6 = [3]_7^5 \cdot [3]_7 = [5]_7 \cdot [3]_7 = [15]_7 = [1]_7 \quad \text{perché} \quad 15 - 1 = 14 \quad \text{multiplo} \\ \text{di } 7$$

$|[3]_7| = 6 \Rightarrow [3]_7$  è generatore di  $(\mathbb{Z}_7^*, \cdot)$

$(G, \cdot)$  gruppo ciclico finito       $|G| = n$   
 di generatore di  $(G, \cdot)$        $G = \{g^0 = 1_G, g, g^2, \dots, g^{n-1}\}$

$\forall a \in G \quad \exists h \in \mathbb{N} \quad 0 \leq h \leq n-1 \quad \text{tale che} \quad a = g^h$

$$|a| = |g^h| = \frac{n}{\text{M.C.D.}(h, n)}$$

$$|[1]_7| = 1$$

$$|[2]_7| = |[3]_7^2| = \frac{6}{\text{M.C.D.}(2, 6)} = \frac{6}{2} = 3 \quad //$$

$$|[3]_7| = 6$$

$$|\mathbb{[4]}_7| = |\mathbb{[3]}_7^4| = \frac{6}{M.C.D.(4,6)} = \frac{6}{2} = 3$$

$$|\mathbb{[5]}_7| = |\mathbb{[3]}_7^5| = \frac{6}{M.C.D.(5,6)} = \frac{6}{1} = 6 \quad [\mathbb{5}]_7 \text{ generator}$$

$$|\mathbb{[6]}_7| = |\mathbb{[3]}_7^3| = \frac{6}{M.C.D.(3,6)} = \frac{6}{3} = 2$$

$$\langle \mathbb{[2]}_7 \rangle = \{ \mathbb{[2]}_7, \mathbb{[2]}_7^2 = \mathbb{[4]}_7, \mathbb{[2]}_7^3 = \mathbb{[1]}_7 \} =$$

$$= \underbrace{\{ \mathbb{[1]}_7, \mathbb{[2]}_7, \mathbb{[4]}_7 \}}$$

$$\langle \mathbb{[6]}_7 \rangle = \{ \mathbb{[6]}_7, \mathbb{[6]}_7^2 = \mathbb{[36]}_7 \xrightarrow{36-1=35} \mathbb{[1]}_7 \} = \underbrace{\{ \mathbb{[1]}_7, \mathbb{[6]}_7 \}}$$

$$\langle \mathbb{[1]}_7 \rangle = \{ \mathbb{[1]}_7 \}$$

$$\begin{cases} 3x \equiv 2 \pmod{5} \\ 3x \equiv 6 \pmod{3} \\ x \equiv 3 \pmod{2} \end{cases}$$

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

$x = 4$  è una soluzione perché  $3 \cdot 4 - 2 = 12 - 2 = 10$  multiplo di 5

$$x = x_0 + mh \quad h \in \mathbb{Z}$$

$$x = 4 + 5h \quad h \in \mathbb{Z}$$

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

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

con il teorema cinese del resto

$$R = 5 \cdot 3 \cdot 2 = 30$$

$$R_1 = 6$$

$$R_2 = 10$$

$$R_3 = 15$$

$$R_1 x \equiv 4 \pmod{5}$$

$$6x \equiv 4 \pmod{5} \quad x_1 = 4$$

$$R_2 x \equiv 2 \pmod{3}$$

$$10x \equiv 2 \pmod{3} \quad x_2 = 2$$

$$10 \cdot 2 - 2 = 18 \pmod{3}$$

$$R_3 x \equiv 3 \pmod{2}$$

$$15x \equiv 3 \pmod{2}$$

$$x_3 = 1$$

$$15 \cdot 1 - 3 = 12 \pmod{2}$$

$$\bar{x} = R_1 x_1 + R_2 x_2 + R_3 x_3 = 6 \cdot 4 + 10 \cdot 2 + 15 \cdot 1 = 24 + 20 + 15 = 59$$

$$X = 59 + Rk = 59 + 30k$$

$$k \in \mathbb{Z}$$

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

$x_0 = 4$  è una soluzione

$$\text{M.C.D.}(3,5) = 1 \quad \bar{m} = \frac{m}{1} = 5$$

$$\text{tutte le soluzioni} \quad x = 4 + \bar{m}h = 4 + 5h \quad h \in \mathbb{Z}$$

Soluzioni tutte congrue tra loro mod 5.

$$-1$$

$$4$$

$$9$$

$$14$$

$$19$$

---

$$3x \equiv 6 \pmod{9}$$

$$\text{M.C.D.}(3,9) = 3$$

3 soluzioni non congrue tra loro mod 9

$$x = 2 + \bar{m}h = 2 + 3h \quad h \in \mathbb{Z}$$

$$\begin{array}{c|c|c} -7 & -4 & -1 \\ 2 & 5 & 8 \\ 11 & 14 & 17 \end{array}$$

$$\begin{array}{c} \textcolor{red}{a} \\ \textcolor{blue}{b} \\ \hline 105x + 75y = 30 \\ \hline \end{array}$$

$$\begin{array}{cc|c} 105 & 5 & 5 \\ 21 & 3 & 3 \\ 7 & 1 & 1 \\ \hline 1 & & 1 \end{array} \quad \begin{array}{cc|c} 75 & 5 & 5 \\ 15 & 3 & 3 \\ 3 & 1 & 1 \\ \hline 1 & & 1 \end{array} \quad 30 = 2 \cdot 3 \cdot 5$$

$$\bar{a} = \frac{a}{d} = \frac{105}{15} = 7$$

$$\bar{b} = \frac{b}{d} = \frac{75}{15} = 5$$

$$\text{M.C.D.}(a, b) = \text{M.C.D.}(105, 75) = 15$$

$15 \mid 30 \Rightarrow$  ci sono soluzioni

$$4x + 5y = 2$$

$$x = 1 \quad y = -1$$

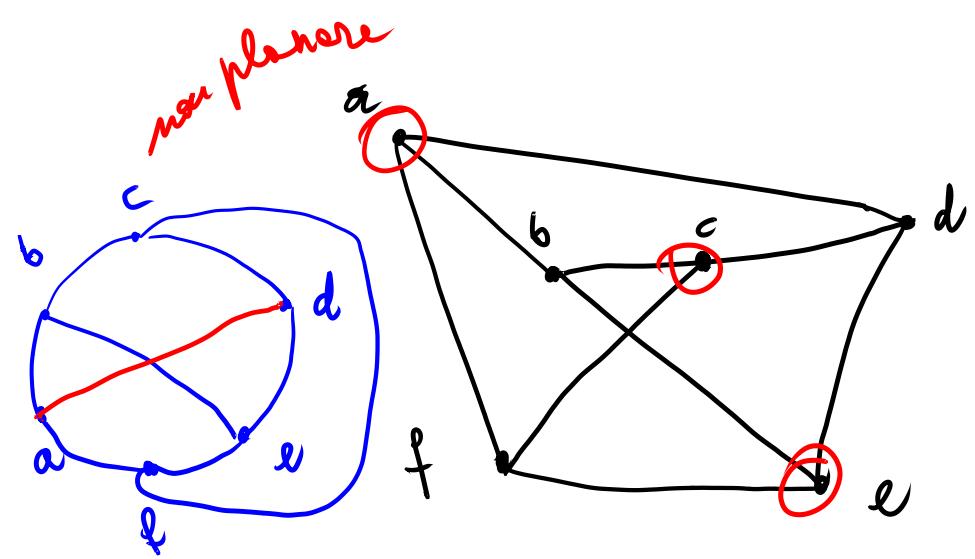
$$7 \cdot 1 + 5(-1) = 7 - 5 = 2$$

una soluzione è  $(1, -1)$ .

$$\bar{a} = 7 \quad \bar{b} = 5$$

$$(1 + 5h, -1 - 7h) \quad h \in \mathbb{Z}$$

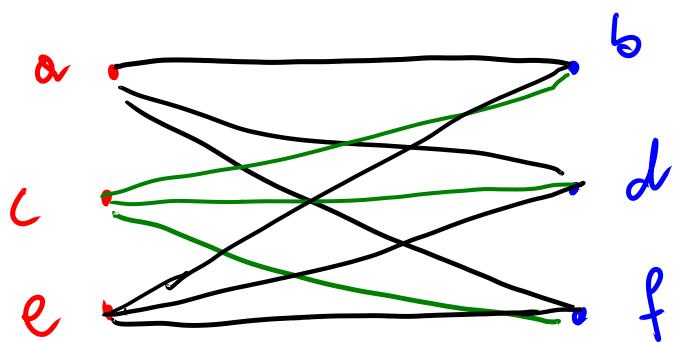
tutte le soluzioni.



~~ab  
bc  
cd  
ef  
ad  
be  
cf  
ef~~  
camino o circuito Eul.

bipartito (completo)  
plenare

- (a) Non esiste un cammino o un circuito Euliano perché ci sono più di 2 vertici dispari
- (b) Poiché non ci sono circuiti di lunghezza dispari, il grafo è bipartito



bipartito completo

$K_{3,3}$

- (c) Non è plenare poiché è  $K_{3,3}$ .

$$\oplus : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

$$x \oplus y = x + y + 1$$

$(\mathbb{Z}, \oplus)$  è un gruppo abeliano

$\mathbb{N}, \mathbb{D}, \mathbb{P}$  sottogruppi

elem neutro  $e \in \mathbb{Z}$  tale che  $\forall x \in \mathbb{Z}$

$$e \oplus x = x \oplus e = x$$

$$e \oplus x = x \Leftrightarrow e + x + 1 = x \Leftrightarrow e = -1$$

$-1$  è l'elemento neutro di  $(\mathbb{Z}, \oplus)$

$-1 \notin \mathbb{N}$  allora  $\mathbb{N}$  non è sottogruppo

d<sup>a</sup> contrapposizione dei sottogruppi  $(G, \cdot)$

$$SG_1) \quad 1_G \in H$$

$$SG_2) \quad \underbrace{\forall a, b \in H}_{a \cdot b^{-1} \in H}.$$

$-1 \notin \mathbb{P}$  e quindi  $\mathbb{P}$  non è un sottogruppo di  $(\mathbb{Z}, \oplus)$

$$-1 \notin \mathbb{D}$$

$$\forall x, y \in \mathbb{D} \quad x \oplus y \in \mathbb{D}$$

$$\exists h, k \in \mathbb{Z} \text{ tali ch } x = 2h + 1 \quad y = 2k + 1$$

$$x \oplus y = x + y + 1 = (2h + 1) + (2k + 1) + 1 = 2h + 2k + 2 + 1 = \\ = 2(h + k + 1) + 1$$

quindi  $\exists t = h + k + 1 \in \mathbb{Z}$  tali ch  $x \oplus y = 2t + 1$   
e quindi  $x \oplus y \in \mathbb{D}$ .

Calcoliamo l'opposto di un elemento  $x \in \mathbb{Z}$

$$\text{cerchiamo } x' \in \mathbb{Z} \text{ tali ch } x \oplus x' = x' \oplus x = -1$$

$$x \oplus x' = -1 \Leftrightarrow x + x' + 1 = -1 \Leftrightarrow x' = -2 - x$$

$$\text{Se } x \in \mathbb{D} \text{ allora } \exists h \in \mathbb{Z} \text{ tali ch } x = 2h + 1$$

$$\text{allora } x' = -2 - x = -2 - (2h + 1) = -2 - 2h - 1 =$$

$\underbrace{\qquad\qquad\qquad}_{\text{dispari}} = - \underbrace{(2(L+h)+1)}_{\text{dispari}}$  opposto di un numero dispari  
rispetto a + che è dispari

$$= -2 - 2h - 2 + 1 = -4 - 2h + 1 = 2(-2 - h) + 1$$

$$\exists s = -2 - h \in \mathbb{Z} \text{ tali ch } x' = 2s + 1 \text{ per cui } x' \in \mathbb{D}$$

SG<sub>1</sub>)  $\mathbb{D} \neq \emptyset$  (abbiamo visto che  $-1 \in \mathbb{D}$ )

SG<sub>2</sub>)  $\forall x, y \in \mathbb{D} \quad x \oplus y \in \mathbb{D}$

SG<sub>3</sub>)  $\forall x \in \mathbb{D} \quad \underbrace{x' \in \mathbb{D}}_{\text{opposto di } x \text{ rispetto a } \oplus} \quad$

Cerchiamo, se esiste, la matrice inversa

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$$

A è invertibile se ha range 2

$$\left( \begin{array}{cc} 2 & -1 \\ 1 & 1 \end{array} \right) \xrightarrow{R_2 - \frac{1}{2}R_1} \left( \begin{array}{cc} 2 & -1 \\ 0 & \frac{3}{2} \end{array} \right)$$

$$1 - \frac{1}{2}(-1) = 1 + \frac{1}{2} = \frac{3}{2}$$

Matrice a scale

2 pivot e quindi la matrice ha range 2: è invertibile

$$\left( \begin{array}{cccc} 2 & -1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) \xrightarrow{\frac{1}{2}R_1} \left( \begin{array}{cccc} 1 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) \xrightarrow{R_2 - R_1}$$

$$\begin{pmatrix} 1 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{3}{2} & -\frac{1}{2} & 1 \end{pmatrix} \xrightarrow{\frac{2}{3} \cdot R_2} \begin{pmatrix} 1 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 1 & -\frac{1}{3} & \frac{2}{3} \end{pmatrix} \quad R_1 + \frac{1}{2} R_2$$

$$\begin{pmatrix} 1 & 0 & \frac{1}{3} & \frac{1}{3} \\ 0 & 1 & -\frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

$$\frac{1}{2} - \frac{1}{6} = \frac{3-1}{6} = \frac{2}{6} = \frac{1}{3}$$

$$\frac{2}{3} \cdot \frac{1}{2} =$$

$$A^{-1} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

$$\begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

OK.

Altre metode

$A$  è invertibile  $\Leftrightarrow \det A \neq 0$

$$\begin{vmatrix} 2 & -1 \\ 1 & 1 \end{vmatrix} = 2 \cdot 1 - (1) \cdot (-1) = 2 + 1 = 3 \neq 0$$

$$\text{Agg}(A) = \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}^t = \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}$$

$$A^{-1} = \frac{1}{\det(A)} \text{Agg}(A) = \frac{1}{3} \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \end{pmatrix}.$$

$$B = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ -1 & 1 & 1 \end{pmatrix}$$

$B$  è invertibile se il range di  $B$  è 3

$$\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ -1 & 1 & 1 \end{pmatrix} \xrightarrow{R_3 + R_1} \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

matrice a scale  
3 pivot

Il range di  $B$  è 3

$$\begin{pmatrix} 1 & -1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ -1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{R_3 + R_1} \begin{pmatrix} 1 & -1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 & 0 & 1 \end{pmatrix} \xrightarrow[R_3]{\frac{1}{2}} \begin{pmatrix} 1 & -1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} \xrightarrow{R_1 - R_3} \begin{pmatrix} 1 & 0 & 0 & -\frac{1}{2} & 1 & -\frac{1}{2} \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}$$

$$B^{-1} = \begin{pmatrix} -\frac{1}{2} & 1 & -\frac{1}{2} \\ 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}$$

$$B \cdot B^{-1} = I_3$$

Altre metodi di soluzione

$$B = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ -1 & 1 & 1 \end{pmatrix}$$

$$\begin{vmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ -1 & 1 & 1 \end{vmatrix} = 1 \cdot \begin{vmatrix} 1 & 1 \\ -1 & 1 \end{vmatrix} = 1 \cdot (1 \cdot 1 - (1) \cdot (-1)) = 2 \neq 0$$

La matrice B è invertibile

$$\text{Agg } B = \begin{pmatrix} |1 & 0| & |0 & 0| & |0 & 1| \\ |-1 & 1| & |1 & 1| & |-1 & 1| \\ |1 & 1| & |1 & 0| & |1 & -1| \end{pmatrix}^T = \begin{pmatrix} 1 & 0 & 1 \\ -2 & 2 & 0 \\ -1 & 0 & 1 \end{pmatrix}^T$$

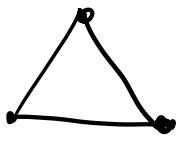
$$= \begin{pmatrix} 1 & -2 & -1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

$$B^{-1} = \frac{1}{\det B} \text{Agg}(B) = \frac{1}{2} \begin{pmatrix} 1 & -2 & -1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix} =$$

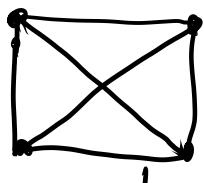
$$= \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}$$



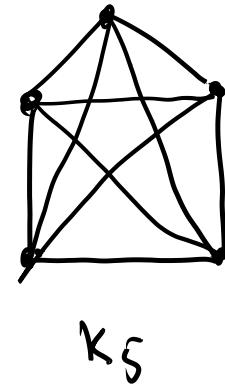
$K_2$



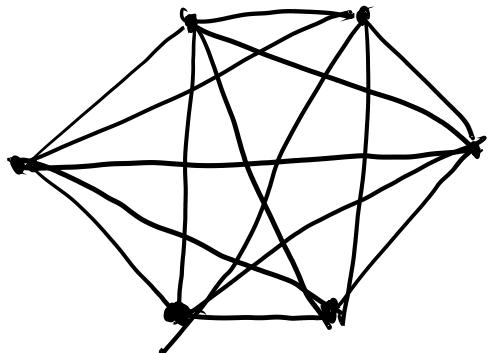
$K_3$



$K_4$



$K_5$



$K_6$