

CheatSheet Metodi

- Quack

Avvertenze:

Questo lavoro **NON** intende sostituire le lezioni o le esercitazioni del corso, bensì fornire un aiuto pratico, spiegando passo per passo, gli esercizi più "meccanici"/"seguenziali".

Su questi appunti **NON** ci sono esercizi su dimostrazioni.

Ringrazio @Blue3341 per la revisione sul file e per il costante aiuto in alcuni esercizi!

Indice

Congruenze Lineari	3
Teorema Cinese del Resto	5
Gruppi	6
Eulero	7
Permutazioni	9
RSA	11
Normali, Ideali	13
Polinomi	16
Codici Lineari	20
Codici Ciclici	23

Es: $23x \equiv 3 \pmod{107}$

1) La prima cosa da fare è scrivere l'equazione di Diophanto associata nella forma:

$$23x + 107y = 3$$

2) Ora devo calcolare l'gcd tra i val di x e y . Uso Euclide: scrivo il + grande dei due come l'altro $\cdot x$ + resto. Dopo scrivo l'altro come resto di prima $\cdot y$ + resto. Continuo così fino ad avere resto 0. Il primo resto $\neq 0$ è gcd. Se $\text{gcd} = 1$, sono coprimi.

$$107 = 23 \cdot 4 + 15$$

$$23 = 15 \cdot 1 + 8$$

$$15 = 8 \cdot 1 + 7$$

$$8 = 7 \cdot 1 + 1$$

$$7 = 1 \cdot 7 + 0$$

3) Confrontiamo gcd e termine noto. Se quest'ultimo è divisibile per gcd, allora l'equazione e di conseguenza la congruenza lineare ha soluzione, no altrimenti.

In questo caso abbiamo $\text{gcd} = 1$ che divide qualsiasi numero. $1 \mid 3$, ha soluzioniAltri possibili scenari: $\text{gcd} \neq 1$ $2 \mid 14$, $3 \mid 27$ ecc... $\text{gcd} \nmid$ $2 \nmid 103$, $7 \nmid 100$ 4) Se quindi $\text{gcd} \mid$, eseguiamo Bezout: poniamo il coeff maggiore = a e l'altro come b . Isoliamo i resti di Euclide

$$a = 107, b = 23$$

$$107 = 23 \cdot 4 + 15 \rightarrow 15 = 107 - 23 \cdot 4 = a - 4b$$

$$23 = 15 \cdot 1 + 8 \rightarrow 8 = 23 - 15 \cdot 1 = b - (a - 4b) = b - a + 4b = 5b - a$$

$$15 = 8 \cdot 1 + 7 \rightarrow 7 = 15 - 8 \cdot 1 = (a - 4b) - (5b - a) = a - 4b - 5b + a = 2a - 9b$$

$$8 = 7 \cdot 1 + 1 \rightarrow 1 = 8 - 7 \cdot 1 = (5b - a) - (2a - 9b) = 5b - a - 2a + 9b = 14b - 3a$$

$$7 = 1 \cdot 7 + 0$$

Continuo es: $23x \equiv 3 \pmod{107}$

5) Dopo aver trovato $\text{m.c.d.} = \dots$ con Bezout, moltiplichiamo per quel numero \bar{c} tale che ci porta al termine noto: $\text{m.c.d.} \cdot \bar{c} = t$

In questo caso, con $\text{m.c.d.} = 1$ e $t = 3$, abbiamo $\bar{c} = 3$.

Altri scenari: $\bar{c} \neq t$: $\text{m.c.d.} = 2$, $t = 14$, $\bar{c} = 7$

Dunque $1 = 14b - 3a$ diventa $3 = 42b - 9a$.

6) La soluzione sarà il coefficiente che moltiplica b . Tutte le soluzioni sono il valore di a (Non il coefficienti) che moltiplica x , $x \in \mathbb{Z}$: $\text{coeff } b + aK$, $K \in \mathbb{Z}$.

Una soluzione alla congruenza lineare è $c = 42$. Tutte le soluzioni sono $42 + 107K$, $K \in \mathbb{Z}$.

7) Possiamo verificare la validità dei valori sostituendoli nella congruenza.

$23x \equiv 3 \pmod{107}$ diventa $966 \equiv 3 \pmod{107}$, moltiplicando $107 \cdot 9 = 963$, ed effettivamente $966 \equiv 3 \pmod{963} \checkmark$

Prendiamo $K = 1$, quindi moltiplichiamo a $23(42 + 107) \equiv 3 \pmod{107}$ ovvero $3427 \equiv 3 \pmod{107}$, moltiplico (vado a tentativi) $107 \cdot 32 = 3424$, ed effettivamente $3427 \equiv 3 \pmod{3424} \checkmark$

6.3) Alternativa: se l'esercizio è solo su equazione di primo grado, allora le soluzioni dipendono dal punto 4:

• CASO 1) Se in Bezout $a = \text{coeff. } y$, allora la sol è $(x_0, y_0) = (\text{coeff. } b, \text{coeff. } a)$
e tutte le sol. saranno (x_K, y_K) dove $x_K = x_0 + \frac{a}{\text{m.c.d.}} K$, e $y_K = y_0 - \frac{b}{\text{m.c.d.}} K$

• CASO 2) Se in Bezout $a = \text{coeff. } x$, allora la sol è $(x_0, y_0) = (\text{coeff. } a, \text{coeff. } b)$
e tutte le sol. saranno (x_K, y_K) dove $x_K = x_0 + \frac{b}{\text{m.c.d.}} K$, e $y_K = y_0 - \frac{a}{\text{m.c.d.}} K$

Siamo nel caso 1. $3 = 42b - 9a$. Una soluzione è $(x_0, y_0) = (42, -9)$.

Tutte le sol sono nella forma $(x_K, y_K) = (42 + 107K, -9 - 23K)$, $K \in \mathbb{Z}$.

7) Anche in questo caso possiamo verificare

$23x + 107y = 3$ diventa $23 \cdot 42 + 107 \cdot (-9) = 3$, $966 - 963 = 3 \checkmark$

con $K = 1$ diventa $23 \cdot 149 + 107 \cdot (-32) = 3$, $3427 - 3424 = 3 \checkmark$



Metodi Cheatsheet

Teorema Cinese del Resto

Probabilità all'appello
completo: 65%

Es:
$$\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 4 \pmod{12} \\ x \equiv 2 \pmod{13} \end{cases}$$

1) Prima cosa da fare è controllare se i divisori sono coprimi: se si possa applicare T.C.R.

$$(11, 12) = 1, (12, 13) = 1, (11, 13) = 1 \quad \checkmark$$

2) Adesso calcoliamo: $N = d_1 \cdot d_2 \cdot d_3$, $N_1 = d_2 \cdot d_3$, $N_2 = d_1 \cdot d_3$, $N_3 = d_1 \cdot d_2$

$$N = 11 \cdot 12 \cdot 13 = 1716 \quad N_1 = 156 \quad N_2 = 143 \quad N_3 = 132$$

3) Eseguiamo ora la congruenza con i seguenti valori:
$$\begin{cases} N_1 y \equiv 1 \pmod{d_1} \\ N_2 y \equiv 1 \pmod{d_2} \\ N_3 y \equiv 1 \pmod{d_3} \end{cases}$$

$$\begin{cases} 156y \equiv 1 \pmod{11} \\ 143y \equiv 1 \pmod{12} \\ 132y \equiv 1 \pmod{13} \end{cases}$$
 Adesso risolviamo le congruenze:

1) $156y \equiv 1 \pmod{11}$ si può semplificare* in $2y \equiv 1 \pmod{11}$ e quindi $y \equiv 6$ (* $11 \cdot 14 = 154$, $156 - 154 = 2$, $2 \cdot 6 = 12 \equiv 1 \pmod{11}$)

2) $143y \equiv 1 \pmod{12}$ si può semplificare* in $-y \equiv 1 \pmod{12}$ e quindi $y \equiv -1$ ($12 \cdot 12 = 144$, $143 - 144 = -1$)

3) $132y \equiv 1 \pmod{13}$ si può semplificare in $2y \equiv 1 \pmod{13}$ e quindi $y \equiv 7$

4) Una soluzione è in questa forma $c = \sum_{i=1}^3 N_i y_i b_i$

Una soluzione particolare del sistema è $c = 156 \cdot 6 \cdot 3 + 143 \cdot (-1) \cdot 4 + 132 \cdot 7 \cdot 2 = 4084$

5) Tutte le soluzioni sono nella forma $c + Nk$. La minima sol. positiva la si ottiene al variare di k in \mathbb{Z} .

Tutte le soluzioni sono $4084 + 1716K$, $K \in \mathbb{Z}$. La minima soluzione la si ha con $K = 2$

$$\text{ovvero } 4084 - 3432 = 652$$

6) Anche qui possiamo verificare la validità dei nostri risultati.

$\begin{cases} 4084 \equiv 3 \pmod{11} \\ 4084 \equiv 4 \pmod{12} \\ 4084 \equiv 2 \pmod{13} \end{cases}$	$\begin{array}{r l} 4084 & 11 \\ 78 & 371 \\ 14 & \\ \hline & 3 \end{array}$	$\begin{array}{r l} 4084 & 12 \\ 48 & 340 \\ 4 & \\ \hline & \end{array}$	$\begin{array}{r l} 4084 & 13 \\ 18 & 314 \\ 54 & \\ \hline & 2 \end{array}$
$\begin{cases} 5800 \equiv 3 \pmod{11} \\ 5800 \equiv 4 \pmod{12} \\ 5800 \equiv 2 \pmod{13} \end{cases} \quad K=1$	$\begin{array}{r l} 5800 & 11 \\ 30 & 520 \\ 8 & \\ \hline & 3 \end{array}$	$\begin{array}{r l} 5800 & 12 \\ 100 & 480 \\ 4 & \\ \hline & \end{array}$	$\begin{array}{r l} 5800 & 13 \\ 60 & 446 \\ 80 & \\ \hline & 2 \end{array}$
$\begin{cases} 652 \equiv 3 \pmod{11} \\ 652 \equiv 4 \pmod{12} \\ 652 \equiv 2 \pmod{13} \end{cases}$	$\begin{array}{r l} 652 & 11 \\ 102 & 59 \\ 3 & \\ \hline & \end{array}$	$\begin{array}{r l} 652 & 12 \\ 52 & 54 \\ 4 & \\ \hline & \end{array}$	$\begin{array}{r l} 652 & 13 \\ 2 & 50 \\ 2 & \\ \hline & \end{array}$

Es. Sia G l'insieme: $G = \left\{ \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} : a, b \in \mathbb{Z}_{37}, a \neq 0 \right\}$

1) Mostrare che G è un gruppo rispetto al prodotto tra matrici.

2) Determinare n° elementi di G

3) Determinare l'inverso dell'elemento $x = \begin{pmatrix} 3 & 0 \\ 4 & 1 \end{pmatrix}$

N.B.) Le domande in questa sezione possono variare, ma spesso si chiede di dimostrare che G è gruppo, trovare degli inversi.

1) Per dimostrare che G è un gruppo rispetto al prodotto tra matrici deve soddisfare:

a) Chiusura: prese due matrici, il prodotto deve $\in G$.

Prodotto tra matrici: $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix}$ calcolo prodotto come $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$

$\forall \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} c & 0 \\ d & 1 \end{pmatrix} \in G$, $\begin{pmatrix} ac & 0 \\ bc+d & 1 \end{pmatrix} \in G$, vero perché $ac, bc+d \in \mathbb{Z}_{37}$ e $ac \neq 0$ per $a \neq 0$ e $c \neq 0$ ✓

b) Elemento neutro: deve avere mat. identitai $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$ per $a=1$ e $b=0$ ✓

c) Inversi: per ogni matrice, anche il suo inverso deve $\in G$. Calcolo l'inverso di una matrice con la seguente formula: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$\forall \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \in G$, $\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}^{-1} = \frac{1}{(a-1+b \cdot 0)} \begin{pmatrix} 1 & 0 \\ -b & a \end{pmatrix} = \frac{1}{a} \begin{pmatrix} 1 & 0 \\ -b & a \end{pmatrix} = \begin{pmatrix} 1/a & 0 \\ -b/a & 1 \end{pmatrix} \in G$, con $a \neq 0$ ✓

2) Per sapere il numero di elementi devo considerare tutte le possibilità

$|G| = 36 \cdot 37$ perché abbiamo 36 scelte per a e 37 per b

3) Calcolo le matrici inverse ricordandoci di essere in \mathbb{Z}_{37} .

$x^{-1} = \begin{pmatrix} 3 & 0 \\ 4 & 1 \end{pmatrix}^{-1}$ diventa $3^{-1} \begin{pmatrix} 1 & 0 \\ -4 & 3 \end{pmatrix}$, l'inverso di 3 in \mathbb{Z}_{37} è $[3]_{37}^{-1} x = [4]_{37}$, ovvero $x=6$

Metto $[-4]_{37}$ positivo, ovvero $[33]_{37}$ e avrò $x^{-1} = \begin{pmatrix} 6 & 0 \\ 30 & 1 \end{pmatrix}$

Es: Determinare tutti gli interi n t.c. $\varphi(n) = 16$

1) Trovo divisori

Divisori di 16: 1, 2, 4, 8, 16.

2) Tempo solo quelli che incrementati di 1 sono primi.

Le possibilità sono per p sono 2, 3, 5, 17. Dunque $n = 2^a \cdot 3^b \cdot 5^c \cdot 17^d$

3) Scriviamo allora nella formula $\varphi(n) = x^{y-1} \cdot x-1 \cdot \dots = 16$

$$\varphi(n) = 2^{a-1} \cdot 1 \cdot 3^{b-1} \cdot 2 \cdot 5^{c-1} \cdot 4 \cdot 17^{d-1} \cdot 16 = 16$$

4) Parto dal grado con base maggiore e trovo per quali valori posso ancora ottenere $\dots = 16$

In questo caso $d \leq 1$, perché con $d=1$ avrei $\dots \cdot 16 = 16$ e va bene, con $d=0$ non ho nulla

in 17 e 16 e va bene, ma con $d=2$ avrei $\dots \cdot 17 \cdot 16 = 16$, impossibile. Dividiamo i due casi:

$$\bullet d=1 \quad n = 2^a \cdot 3^b \cdot 5^c \cdot 17$$

$$\varphi(n) = 2^{a-1} \cdot 1 \cdot 3^{b-1} \cdot 2 \cdot 5^{c-1} \cdot 4 \cdot 16 = 16$$

4.1) Adesso ricavo che $c=0$, ma anche $b=0$, a può essere anche 1, in quanto quando

$a=1$ moltiplica per 1 e quindi risultato rimane lo stesso

$$\bullet c=0 \quad b=0 \quad n = 2 \cdot 17 \quad \varphi(n) = 2^{a-1} \cdot 16 = 16$$

$$\bullet a=0 \quad n = 17, \varphi(n) = 16 = 16, \text{ trovo il primo } n = 17$$

$$\bullet a=1 \quad n = 2 \cdot 17 = 34, \varphi(n) = 1 \cdot 16 = 16, \text{ trovo il secondo } n = 34$$

$$\bullet d=0 \quad n = 2^a \cdot 3^b \cdot 5^c \quad \varphi(n) = 2^{a-1} \cdot 1 \cdot 3^{b-1} \cdot 2 \cdot 5^{c-1} \cdot 4 = 16. \text{ Ricavo che } c \leq 1, \text{ perché } c=2 \text{ genera } 5 \cdot 4 = 20$$

$$\bullet c=1 \quad n = 2^a \cdot 3^b \cdot 5 \quad \varphi(n) = 2^{a-1} \cdot 1 \cdot 3^{b-1} \cdot 2 \cdot 4 = 16. \text{ Ricavo che } b \leq 1 \text{ perché } b=2 \text{ genera } 3 \cdot 2 \cdot 4 = 24$$

$$\bullet b=1 \quad n = 2^a \cdot 3 \cdot 5 \quad \varphi(n) = 2^{a-1} \cdot 1 \cdot 2 \cdot 4 = 16. \text{ Ricavo che } a \leq 3, \text{ in quanto genera } 2 \cdot 1 \cdot 2 \cdot 4 = 16$$

$$\bullet a=2 \quad n = 2^2 \cdot 3 \cdot 5 \quad \varphi(n) = 2 \cdot 1 \cdot 2 \cdot 4 = 16 \quad \text{trovo il terzo } n = 60$$

$$\bullet b=0 \quad n = 2^a \cdot 5 \quad \varphi(n) = 2^{a-1} \cdot 1 \cdot 4 = 16 \text{ da cui ricavo } a=3, \text{ in quanto genera } 2^3 \cdot 4 = 16$$

$$\bullet a=3 \quad n = 2^3 \cdot 5 \quad \varphi(n) = 4 \cdot 1 \cdot 4 = 16 \quad \text{trovo il quarto } n = 40$$

$$\bullet c=0 \quad n = 2^a \cdot 3^b \quad \varphi(n) = 2^{a-1} \cdot 1 \cdot 3^{b-1} \cdot 2 = 16. \text{ Trovo che } b \leq 1, \text{ in quanto } b=2 \text{ genera } 3 \cdot 2 = 6 \text{ e non esiste } a \text{ t.c. } 2^a \cdot 6 = 16$$

Continuo es: Determinare tutti gli interi n t.c. $\varphi(n) = 16$

$d=0$

$c=0$

$b=1$ $n=2^{\omega} \cdot 3$ $\varphi(n) = 2^{\omega-1} \cdot 2 = 16$, da cui $\omega=4$

$\omega=4$ $n=2^4 \cdot 3$ $\varphi(n) = 8 \cdot 2 = 16$ tra cui quarto $n=48$

$b=0$ $n=2^{\omega}$ $\varphi(n) = 2^{\omega-1} = 16$, da cui $\omega=5$

$\omega=5$ $n=2^5$ $\varphi(n) = 2^4 = 16$ tra cui quinto $n=32$

Le soluzioni sono 17, 34, 60, 40, 48, 32

Formule da ricordare: Eulero: $a^{\varphi(n)} \equiv 1 \pmod n$ Fermat: $a^p \equiv a \pmod p$ $a^{p-1} \equiv 1 \pmod p$
 $(a, n) = 1$ con p primo e $p \nmid a$

Es: Calcolare $98^{98989} \pmod{29}$.

1) Calcolo senza esponente

$$98 \equiv 11 \pmod{29}$$

2) Divido l'esponente per $\varphi(d)$ ovvero il primo $\leq d-1$, in questo caso 29 quindi $\varphi(29)=28$

$$\begin{array}{r|l} 98989 & 28 \\ 149 & 3535 \\ 98 & \\ 149 & \\ 9 & \end{array} \quad \text{quindi } 98989 = 3535 \cdot 28 + 9$$

3) Per Fermat avremo $(11^{28})^x \equiv 1 \pmod{29}$, quindi calcoliamo la congruenza sul resto

$$11^{98989} \pmod{29} \text{ diventa } (11^{28})^{3535} \equiv 1 \pmod{29}, 11^9 \equiv ? \pmod{29}$$

4) Risolvo a passi la congruenza sul resto

$$11^2 = 121 \equiv -5 \pmod{29}$$

$$11^4 = -5^2 = 25 \equiv -4 \pmod{29}$$

$$11^8 = -4^2 = 16 \pmod{29}$$

$$11^9 = 11^8 \cdot 11 \equiv 16 \cdot 11 = 176 \equiv 2 \pmod{29}$$

5) Conclusioni

Si conclude che $98^{98989} \equiv 2 \pmod{29}$

Es: Sia $\sigma \in S_{13}$ la permutazione

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 9 & 12 & 13 & 6 & 7 & 11 & 2 & 3 & 4 & 10 & 1 & 5 & 8 \end{pmatrix}$$

① Scrivere σ come prodotto di cicli disgiunti e determinare l'ordine.

1) Si tratta semplicemente di guardare i cicli

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 9 & 12 & 13 & 6 & 7 & 11 & 2 & 3 & 4 & 10 & 1 & 5 & 8 \end{pmatrix}$$

$$\sigma = (1, 9, 4, 6, 11)(2, 12, 5, 7)(3, 13, 8)$$

2) L'ordine è il m.c.m. delle cardinalità dei cicli.

$$|\sigma| = 5 \cdot 4 \cdot 3 = 60$$

② Posto $\tau = (9, 13, 7)(1, 12, 5, 8, 3)(11, 4, 10)(2, 6)$ in S_{13} si calcoli il prodotto $\sigma \cdot \tau$.

1) Bisogna concatenare le due permutazioni

$$\tau = \begin{pmatrix} 9 & 13 & 7 & 1 & 12 & 5 & 8 & 3 & 11 & 4 & 10 & 2 & 6 \\ 13 & 7 & 9 & 12 & 5 & 8 & 3 & 1 & 4 & 10 & 11 & 6 & 2 \end{pmatrix}$$

$$\sigma = \begin{pmatrix} 13 & 7 & 9 & 12 & 5 & 8 & 3 & 1 & 4 & 10 & 11 & 6 & 2 \\ 8 & 2 & 4 & 5 & 7 & 3 & 13 & 9 & 6 & 10 & 1 & 11 & 12 \end{pmatrix}$$

$$\sigma \cdot \tau = \begin{pmatrix} 9 & 13 & 7 & 1 & 12 & 5 & 8 & 3 & 11 & 4 & 10 & 2 & 6 \\ 8 & 2 & 4 & 5 & 7 & 3 & 13 & 9 & 6 & 10 & 1 & 11 & 12 \end{pmatrix}$$

N.B.: $\sigma \cdot \tau \neq \tau \cdot \sigma$

③ Scrivere σ^{-1} .

1) Riscrivo σ^{-1} come $\sigma^{60} \cdot \sigma^{-1}$ ovvero per σ^{ordine}

$$\sigma^{-1} = \overset{59}{\sigma} (1, 9, 4, 6, 11) \overset{59}{\sigma} (2, 12, 5, 7) \overset{59}{\sigma} (3, 13, 8)$$

2) Scrivo come 59 mod ordine

quindi per $(1, 9, 4, 6, 11)$ $59 \equiv 4 \pmod{5}$

$$\text{e ottengo } \overset{59}{\sigma} = \overset{5}{\sigma} (1, 9, 4, 6, 11)^4 \overset{3}{\sigma} (2, 12, 5, 7) \overset{2}{\sigma} (3, 13, 8)$$

3) Sposto di x posizioni: es $(3, 4, 5, 6)^3 \rightarrow (3 \overset{1}{4} \overset{2}{5} \overset{3}{6}) \rightarrow (6, 5, 4, 3)$

$$\overset{59}{\sigma} = (11, 6, 4, 9, 1)(7, 5, 12, 2)(8, 13, 3)$$

Es: Scrivere il prodotto di cicli disgiunti in prodotto di cicli disgiunti.

$$(1\ 5\ 2\ 6\ 11)(2\ 13)(5\ 11)(1\ 13\ 4\ 15\ 9\ 12) \in S_{15}$$

Riscrivo l'ultimo ciclo come permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 3 & 15 & 5 & 6 & 7 & 8 & 12 & 10 & 11 & 1 & 4 & 14 & 9 \end{pmatrix}$$

Prendo il ciclo alla sua sx e faccio il prodotto di cicli:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 3 & 15 & 5 & 6 & 7 & 8 & 12 & 10 & 11 & 1 & 4 & 14 & 9 \end{pmatrix} \begin{pmatrix} 5 & 11 \\ 11 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 3 & 15 & 11 & 6 & 7 & 8 & 12 & 10 & 5 & 1 & 4 & 14 & 9 \end{pmatrix}$$

Continuo così con tutti i cicli

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 3 & 15 & 11 & 6 & 7 & 8 & 12 & 10 & 5 & 1 & 4 & 14 & 9 \end{pmatrix} \begin{pmatrix} 13 & 2 \\ 2 & 13 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 13 & 3 & 15 & 11 & 6 & 7 & 8 & 12 & 10 & 5 & 1 & 4 & 14 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 13 & 3 & 15 & 11 & 6 & 7 & 8 & 12 & 10 & 5 & 1 & 4 & 14 & 9 \end{pmatrix} \begin{pmatrix} 2 & 11 & 6 & 5 & 1 \\ 6 & 1 & 11 & 2 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 6 & 13 & 3 & 15 & 1 & 11 & 7 & 8 & 12 & 10 & 2 & 5 & 4 & 14 & 9 \end{pmatrix}$$

Riscrivo come prodotto di cicli disgiunti

$$(1\ 6\ 11\ 2\ 13\ 4\ 15\ 9\ 12\ 5)$$

Es: Spiegazione algoritmo RSA.

Alice

1. Sceglie due numeri primi p e q grandi, interi, dispari e distinti.
Calcola $N = p \cdot q$ e $\varphi(N) = (p-1)(q-1)$
2. Sceglie un numero intero r coprimo con $\varphi(N)$.
3. Calcola con l'algoritmo di Euclide due interi s e t in modo che $rs + \varphi(N)t = 1$
4. Pubblica la coppia (N, r) mentre tiene ben segrete $p, q, \varphi(N)$ e s .

7. Riceve il messaggio a da Bob e deve ricostruire il messaggio originale, cioè b . Calcola $a^s \bmod N$ e ritrova b .

Bob

5. Vuole mandare ad Alice il messaggio b , dove b è un numero intero con $0 < b < N$.
6. Legge la coppia (N, r) che Alice ha pubblicato e calcola $a = b^r \bmod N$ e invia il numero ad Alice.

Es: Supponi che la chiave pubblica sia $(N, r) = (143, 67)$, dunque $p=11$ e $q=13$. Riceviamo il messaggio 13. Decifriamolo

1) Calcolo $\varphi(N) = (p-1)(q-1)$

$$\varphi(N) = 10 \cdot 12 = 120$$

2) Applico Euclide e Bezout a $\varphi(N)$ e r . (Euclide deve risultare = 1!)

$$(120, 67) = 1 \quad 1 = 43b - 24a$$

3) Trovo s , ovvero colui che moltiplica b .

$$13^{43} \bmod 143.$$

4) Calcolo $mex^s \bmod N$: riscrivo s in binario e creo la seguente tabella

$$43 = 101011$$

	$C_0 = 1$
1	$C_1 = 1^2 \cdot 13^1 = 13 \bmod 143$
0	$C_2 = 13^2 \cdot 13^0 = 169 \bmod 143 = 26$
1	$C_3 = 26^2 \cdot 13^1 = 878 \bmod 143 = 65$
0	$C_4 = 65^2 \cdot 13^0 = 4225 \bmod 143 = 65$
1	$C_5 = 65^2 \cdot 13^1 = 5507 \bmod 143 = 13$
1	$C_6 = 13^2 \cdot 13^1 = 2197 \bmod 143 = 52$

5) L'ultimo resto è il messaggio decifrato

Il messaggio decifrato è 52.

N.B.) In questo capitolo sono presenti molti esercizi basati su definizioni che non ho riportato. Consiglio di guardarli e cercare di capirli dall'esercitazione 10 su e-learning

1) Sia $G \in S_4$ il gruppo. $G = \{1, (12)(34), (14)(23), (13)(24), (123), (132), (124), (142), (134), (143), (234), (243)\}$

Si consideri il sottogruppo $H = \{1, (12)(34), (14)(23), (13)(24)\}$

Calcolare i laterali destri e sinistri di H in G . Verificare che $H \triangleleft G$.

Si tratta di considerare H con gli elementi di G non presenti in H .

laterali dx

$$H \cdot 1 = H \quad \text{caso base}$$

$$H \cdot (123) = \{(123), (12)(34)(123), (14)(23)(123), (13)(24)(123)\}$$

$$= \{(123), (243)^*, (134), (142)\}$$

Bisogna comporre i cicli, in questo caso avremo $(12) \rightarrow \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$, $(34) \rightarrow \begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}$
 e $(123) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, quindi avremo $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \\ 2 & 3 & 1 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ e dunque $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ ovvero (243)

$$H \cdot (132) = \{(132), (143), (124), (234)\}$$

Termino quando gli elementi appaiono tutti nei risultati.

laterali sx

$$1 \cdot H = H$$

$$(123) \cdot H = \{(123), (134), (142), (243)\}$$

$$(132) \cdot H = \{(132), (234), (143), (124)\}$$

Per verificare che $H \triangleleft G$ i laterali dx e sx devono essere uguali.

Siccome $H(123) = (123)H$ e $H(132) = (132)H$ concludiamo che $H \triangleleft G$.

2) Scrivere la tabella di Z_6/H e Z_6/K con $H = \langle [3]_6 \rangle$ e $K = \langle [2]_6 \rangle$

Controlla il gruppo, se abeliano avremo che H e K sono sottogruppi normali, dunque laterali dx = laterali sx. Troviamo i laterali.

Z_6 abeliano. $H = \langle [3]_6 \rangle$ sarà $H = \{[0]_6, [3]_6\}$ e $K = \langle [2]_6 \rangle$ sarà $K = \{[0]_6, [2]_6, [4]_6\}$.

I laterali di H sono H , $H + [1]_6 = \{[1]_6, [4]_6\}$ e $H + [2]_6 = \{[2]_6, [5]_6\}$. I laterali di K sono K e $K + [1]_6 = \{[1]_6, [3]_6, [5]_6\}$.

Ora metti i laterali su righe e colonne ed effettui i calcoli.

+	H	$H + [1]_6$	$H + [2]_6$	+	K	$K + [1]_6$
H	H	$H + [1]_6$	$H + [2]_6$	K	K	$K + [1]_6$
$H + [1]_6$	$H + [1]_6$	$H + [2]_6$	H	$K + [1]_6$	$K + [1]_6$	K
$H + [2]_6$	$H + [2]_6$	H	$H + [1]_6$			

3) Considerato il sottoanello $A = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{Q} \right\}$ di $\text{Mat}(2 \times 2, \mathbb{Q})$ provare che l'applicazione $\varphi: A \rightarrow A$, definita da $\varphi\left(\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}\right) = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ è omomorfismo di anelli. Determinare $\text{Ker } \varphi$ e $\text{Im } \varphi$.

Dobbiamo provare che $\varphi(a+b) = \varphi(a) + \varphi(b)$ e $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

$\forall \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}, \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \in A$, dobbiamo provare che

$$\varphi\left(\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} + \begin{pmatrix} x & 0 \\ y & z \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} a+x & 0 \\ c+y & d+z \end{pmatrix}\right) = \begin{pmatrix} a+x & 0 \\ 0 & d+z \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} + \begin{pmatrix} x & 0 \\ 0 & z \end{pmatrix} \quad \checkmark$$

$$\varphi\left(\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ y & z \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} ax & 0 \\ cx+dy & dz \end{pmatrix}\right) = \begin{pmatrix} ax & 0 \\ 0 & dz \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ 0 & z \end{pmatrix} \quad \checkmark$$

$$\text{Ker } \varphi = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in A : \varphi\left(\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}\right) = 0_A \right\} = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{Q} \right\} \quad \text{Ker } \varphi \text{ è ideale di } A.$$

$$\text{Im } \varphi = \left\{ \varphi\left(\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}\right) : \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in A \right\} = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{Q} \right\}. \quad \text{Im } \varphi \text{ è sottoanello di } A.$$

Concetti teorici utili per le dimostrazioni:

Per $x \in G$, scriviamo
$$x^n = \begin{cases} \underbrace{x \cdot x \cdot \dots \cdot x}_{n \text{ volte}} & \text{se } n > 0 \\ 1 & \text{se } n = 0 \\ (x^{-1})^n & \text{se } n < 0 \end{cases} \quad (n \cdot x = \underbrace{x + x + \dots + x}_{n \text{ volte}})$$

Sia G gruppo, H sottogruppo di G , $H \leq G$ sse vi è chiusura, elem. neutro e inversi.

Sia G gruppo, H sottogruppo normale di G , $H \triangleleft G$ se laterali sx = laterali dx ($xN = Nx$)

Sia G gruppo e $g \in G$. $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ si dice sottogruppo ciclico di G generato da g .

Se $G = \langle g \rangle$ si dice gruppo ciclico. Se g ha ordine finito n allora $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$

Teorema di Lagrange $n = |\langle x \rangle|$ divide $|G|$. Es: sia G gruppo di ordine $n=12$, l'ordine di un possibile sottogruppo H di G è $1, 2, 3, 4, 6, 12$. **NON** significa che esiste sicuramente sottogruppo ordine 6, ma sicuramente **NON** esistono sottogruppi di ordine 7.

Siano $(G, *)$ e (H, \circ) due gruppi. Un **omomorfismo** da G in H è un'applicazione $\varphi: G \rightarrow H$ t.c. $\forall x, y \in G$.

$\varphi(x * y) = \varphi(x) \circ \varphi(y)$. Se biettiva G e H sono **isomorfi** (\cong)

Ker $\varphi = \{x \in G : \varphi(x) = 1_H\} \leq G$ è sottogruppo normale

Im $\varphi = \{\varphi(x) : x \in G\} \leq H$ è sottogruppo.

Poiché $\text{Ker } \varphi \triangleleft G$ considero gruppo quoziente $G / \text{Ker } \varphi$, questo è **isomorfo** a **Im** φ .

Sia $(A, -, \cdot)$ anello. B si dice **sottoanello** di A se $\forall b_1, b_2 \in B$:

$$b_1 - b_2 \in B \quad (B - B \subseteq B)$$

$$b_1 \cdot b_2 \in B \quad (B \cdot B \subseteq B)$$

$$1_A \in B$$

Sia A anello. I è **ideale** ($I \triangleleft A$) se $I - I \subseteq I$ e $\forall a \in A$, $aI \subseteq I$ e $IA \subseteq I$.

Omomorfismo di anelli: $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$, $\varphi(a_1 \cdot a_2) = \varphi(a_1) \cdot \varphi(a_2)$

Es Si consideri $g(x) = x^3 + 3x^2 + x + 1$ in \mathbb{Z}_7 .

a) $g(x)$ irriducibile?

Se polinomio ha grado ≤ 3 basta verificare che non abbia radici
ovvero che per nessun valore $g(x) = 0$. Se grado > 3 bisogna controllare
che sia irriducibile, ovvero che non possa scomporlo

$$g(0)=1, g(1)=6, g(2)=2, g(3)=2, g(4)=5, g(5)=3, g(6)=2 \quad \checkmark$$

b) Si dica se $F = \mathbb{Z}_7[x]/(g(x))$ è un campo e se si determinare il numero di elementi di F .

F è campo se $g(x)$ irriducibile. n° elementi, dato \mathbb{Z}_x e pol. grado $y = x^3$.

F campo in quanto non ha radici, siamo in \mathbb{Z}_7 e $\deg(g(x))=3$, quindi $|F|=7^3$

c) Si determini se esiste l'inverso in F di $[x^2 + 6x + 6]g(x)$

① F deve essere campo e $g(x) \neq 0$

$$F \text{ campo e } [x^2 + 6x + 6]g(x) \neq [0]g(x)$$

② Applico Euclide con divisione tra polinomi su $g(x)$

$$f(x) = x^2 + 6x + 6 \quad g(x) = x^3 + 3x^2 + x + 1$$

$$\begin{array}{r|l} x^3 + 3x^2 + x + 1 & x^2 + 6x + 6 \\ -x^3 - 6x^2 - 6x & x-3 \leftarrow q \\ \hline -3x^2 - 5x + 1 & \\ +3x^2 + 18x + 18 & \\ \hline \rightarrow r & 13x + 19 \end{array}$$

③ Riporto i valori in \mathbb{Z}_7 e riscrivo $g(x)$. Applico poi Euclide su $f(x)$

$13x + 19$ in \mathbb{Z}_7 è $6x + 5$. $x-3$ in \mathbb{Z}_7 diventa $x+4$.

$$g(x) = f(x)(x+4) + 6x+5$$

$$\begin{array}{r|l} x^2 + 6x + 6 & 6x + 5 \\ / + 5x & -x - 11 \\ \hline 11x + 6 & \\ / + 55 & \\ \hline & 61 \end{array}$$

$-x-11$ diventa $6x+5$ e 61 in \mathbb{Z}_7 è 5 .

$$f(x) = (6x+3)(6x+5) + 5$$

Continuo es Si consideri $g(x) = x^3 + 3x^2 + x + 1$ in \mathbb{Z}_7 .

① Applico Bezout

$$g(x) = f(x)(x+4) + 6x+5, \quad f(x) = (6x+5)(6x+3) + 5$$

$$6x+5 = g(x) - f(x)(x+4)$$

$$5 = f(x) - (6x+5)(6x+3)$$

$$= f(x) - g(x)(6x+3) - f(x)(x+4)(6x+3)$$

$$= -g(x)(6x+3) - f(x)(6x^2+6x+6)$$

$$= +g(x)(x+4) + f(x)(6x^2+6x+6)$$

$$1 = g(x)(3x+5) + f(x)(4x^2+4x+4)$$

④ Riscrivo $6x+5$ come resto di $g(x)$

④ Raccolgo i due $f(x)$ e risolvo

④ Riscrivo $6x+3$ in $x+4$ (\mathbb{Z}_7), cambio segno

④ Divido per 5 e ottengo $1 = \dots$

⑤ Conclusione: quello che moltiplica $f(x)$ è l'inverso

$$[x^2+6x+6]^{-1}_g = [4x^2+4x+4]_g$$

d) Posto $h = 2x^2 + 2x + 1$ e $K(x) = x^3 + 3$, si scrivono in forma standard $[h(x)K(x)]_g(x)$.

Calcolo semplicemente il prodotto

$$h(x)K(x) = 2x^5 + 6x^2 + 2x^4 + 6x + x^3 + 3 = 2x^5 + 2x^4 + x^3 + x^2 - x + 3$$

Eseguo Euclide tra $h(x)K(x)$ e $g(x)$

$$\begin{array}{r|l} 2x^5 + 2x^4 + x^3 + x^2 - x + 3 & x^3 + 3x^2 + x + 1 \\ / -6x^4 - 3x^3 - 2x^2 & \\ \hline -4x^4 - 2x^3 - x^2 - x + 3 & 2x^2 - 4x + 10 \\ / +12x^3 + 4x^2 + 4x & \\ \hline 10x^3 + 3x^2 + 3x + 3 & \\ / -30x^2 - 10x - 10 & \\ \hline -27x^2 - 7x - 7 & \end{array}$$

$$\text{Risultato } h(x)K(x) = g(x)(2x^2 + x) - x^2$$

$$\text{quindi } [h(x)K(x)]_g(x) = [6x^2]_g(x)$$

Es: Si consideri in $\mathbb{Z}_5[x]$ il polinomio $g_a(x) = x^3 + ax^2 - ax + 3$.

a) $g_a(x)$ è irriducibile?

Come prima, sostituisco i valori.

$$g_a(0) = 3, g_a(1) = 4, g_a(2) = 1 + 2a, g_a(3) = a, g_a(4) = 2a + 2$$

Metto a sistema i casi con le a .

$$\begin{cases} 1 + 2a \neq 0 \\ a \neq 0 \\ 2a + 2 \neq 0 \end{cases} \rightarrow \begin{cases} a \neq 2 \\ a \neq 0 \\ a \neq 4 \end{cases}$$

Trovo i valori per cui a è riducibile o meno.

$g_a(x)$ è irriducibile per $a=1$ e $a=3$.

b) Scrivere una fattorizzazione propria per i valori in cui $g_a(x)$ è riducibile.

Prendo $g_a(x)$ to x riducibile e trovo x radice. $x - \alpha$ divide $g_a(x)$.

$a=0$, $g_0(3) = 3 \cdot 0 = 0$. Trovo $x=3$ e quindi $x-3$ divide $g_0(x)$.

$a=2$, $g_2(2) = 15 = 0$. Trovo $x=2$ e quindi $x-2$ divide $g_2(x)$.

$a=4$, $g_4(4) = 15 = 0$. Trovo $x=4$ e quindi $x-4$ divide $g_4(x)$.

Riscrivo $g_a(x)$ come $(x - \alpha)(\text{resto della divisione tra polinomi})$

$$g_0(x) = x^3 + 3 = (x-3)(x^2 + 3x + 4)$$

$$g_2(x) = x^3 + 2x^2 - 2x + 3 = (x-2)(x^2 + 4x + 1)$$

$$g_4(x) = x^3 + 4x^2 - 4x + 3 = (x-4)(x^2 + 3x + 3)$$

c) Determinare i casi in cui $\mathbb{Z}_5[x]/(g_a(x))$ ha come inverso $[x+1]g_a(x)$

Prendo i casi in cui $g_a(x)$ è irriducibile e applico Euclide.

$$a=1, g_1(x) = x^3 + x^2 - x + 3, f(x) = x + 1$$

$$\text{ottergo } g_1(x) = f(x)(x^2 - 1) + 4$$

$$\text{quindi } [x+1]^{-1}g_1(x) = [x^2 - 1]g_1(x)$$

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

$$a=3, g_3(x) = x^3 + 3x^2 - 3x + 3, f(x) = x + 1$$

$$\text{ottergo } g_3(x) = f(x)(x^2 + 2x) + 3$$

$$\text{quindi } [x+1]^{-1}g_3(x) = [x^2 + 2x]g_3(x)$$

$$\begin{array}{r|l} x^3 + 3x^2 - 3x + 3 & x + 1 \\ \hline / -x^2 & x^2 + 2x - 5 \\ \hline & 2x^2 - 3x + 3 \\ & \quad / -2x \\ \hline & \quad -5x + 3 \\ & \quad \quad / 15 \\ \hline & \quad \quad 8 \end{array}$$

Continua es: Si consideri in $\mathbb{Z}_5[x]$ il polinomio $g_a(x) = x^3 + ax^2 - ax + 3$.

Ora considero i casi in cui è riducibile e se sono coprimi esiste inverso.

In questo caso abbiamo $x+1$, quindi $x=-1$. Abbiamo verificato prima che con $a=4$ abbiamo $x=4=-1$, dunque per $a=4$ non esiste.

• $a=0$, $g_0(x) = x^3 + 3$, $f(x) = x+1$

risultava $g(x) = f(x)(x^2 + 4x + 1) + 2$

quindi $[x+1]_{g_0(x)}^{-1} = [2x^2 + 3x + 2]_{g_0(x)}$

• $a=2$, $g_2(x) = x^3 + 2x - 2x + 3$, $f(x) = x+1$

$g(x) = f(x)(x^2 + x + 2) + 1$

quindi $[x+1]_{g_2(x)}^{-1} = [4x^2 + 4x + 3]_{g_2(x)}$

Es: Si determinano tutti i polinomi grado 3 irriducibili in $\mathbb{Z}_2[x]$.

Trovo i 2^3 polinomi e escludo quelli dove $d=0$, o con monomi pari.

Con grado ≤ 3 hanno radici \rightarrow sono scomponibili.

I polinomi sono x^3 , x^3+x^2 , x^3+x , x^3+1 , x^3+x+1 , x^3+x^2+x , x^3+x^2+1 , x^3+x^2+x+1 .

Quelli irriducibili sono: x^3+x+1 , x^3+x^2+1

Variante: se grado > 3 controlleremo che non si possa scomporre anche se non ha radici.

Es: grado 4 abbiamo x^4+x^3+1 , x^4+x^2+1 , x^4+x^3+1 , x^4+x+1 , $x^4+x^3+x^2+x+1$

ma x^4+x^2+1 è riscrivibile come $(x^2+x+1)^2$ (unico polinomio in $\mathbb{Z}_2[x]$ grado 2 irriducibile)

Dunque i polinomi irriducibili in $\mathbb{Z}_2[x]$ di grado 4 sono

$$x^4+x^3+1, x^4+x^3+1, x^4+x+1, x^4+x^3+x^2+x+1$$

Es: Si costruisca un campo con 5^3 elementi

La base è p di $\mathbb{Z}_p[x]$, l'esponente il grado del polinomio irriducibile

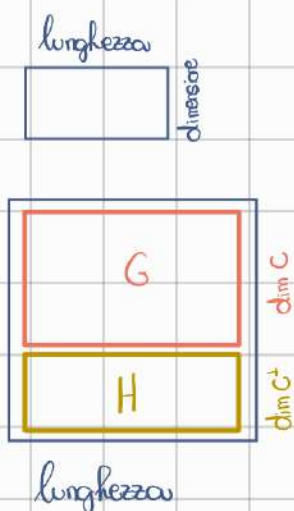
Troviamo in $\mathbb{Z}_5[x]$ il polinomio di grado 3 $g(x) = x^3+x+1$. Verifico che non ha radici.

$g(0)=1$, $g(1)=3$, $g(2)=3$, $g(3)=1$, $g(4)=4$. ✓

Matrice generatrice \rightarrow

Matrice generatrice = G

Matrice di controllo = H



$$\dim C + \dim C^\perp = \text{lunghezza}$$

Per trovare la dimensione se guardiamo G nel codice C o H nel codice C^\perp bisogna guardare solo la lunghezza. Se invece abbiamo H per C o G per C^\perp allora bisogna prendere $\text{lunghezza} - \dim C / C^\perp$.

Es. Sia C codice lineare su \mathbb{Z}_2 con matrice di controllo $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}$

1) Determinare lunghezza, dimensione, grandezza di C .

$H \in (\text{Mat}_{2 \times 5}, \mathbb{Z}_2)$, dunque lunghezza $C = 5$, dimensione è $5 - 2 = 3$, ovvero 3
e la grandezza è $2^3 = 8$ caso H su C o G su C^\perp

Es. Sia C codice lineare su \mathbb{Z}_2 con matrice generatrice $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

1) Determinare lunghezza, dimensione, grandezza di C .

$G \in (\text{Mat}_{3 \times 6}, \mathbb{Z}_2)$, dunque lunghezza $C = 6$, dimensione è $k = 3$
e la grandezza è $2^3 = 8$ caso G su C o H su C^\perp

Es. Sia C codice lineare su \mathbb{Z}_2 con matrice di controllo $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}$

1) Determinare lunghezza, dimensione, grandezza di C .

$H \in (\text{Mat}_{2 \times 5}, \mathbb{Z}_2)$, dunque lunghezza $C = 5$, dimensione è $5 - k = 2$, ovvero 3 e la grandezza è $2^3 = 8$

2) Scrivere matrice generatrice di C ed elencare gli elementi.

Prendi matrice di controllo $H = (-A^T | I_2)$, la matrice generatrice sarà $G = (I_3 | A)$

In questo caso con $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}$ avremo $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$ $3+2=5 = \text{lung.}$

N.b.: essendo in \mathbb{Z}_2 , $-A$ e A sono uguali, ma negli altri casi non lo sono

Le righe formano la base di C e gli elementi sono le comb. lineari.

In questo caso $b_1 = 10011$, $b_2 = 01001$, $b_3 = 00101$, e gli elementi sono:

$$0 = 0 \cdot b_1 + 0 \cdot b_2 + 0 \cdot b_3 \quad b_3 = 0b_1 + 0b_2 + 1b_3 \quad b_2 + b_3 = 0b_1 + 1b_2 + 1b_3 = 01100$$

$$b_1 = 1 \cdot b_1 + 0b_2 + 0b_3 \quad b_1 + b_2 = 1b_1 + 1b_2 + 0b_3 = 11001 \quad b_1 + b_2 + b_3 = 1b_1 + 1b_2 + 1b_3 = 11101$$

$$b_2 = 0b_1 + 1b_2 + 0b_3 \quad b_1 + b_3 = 1b_1 + 0b_2 + 1b_3 = 10101$$

3) Determinare dimensione ed elementi di C^\perp .

$$\dim C^\perp = n - \dim C$$

In questo caso $\dim C = 3$, mentre le colonne sono 5 quindi $\dim C^\perp = 2$

La base sono i vettori di H e gli elementi le comb. lineari.

Abbiamo dunque $b_1 = 10010$ e $b_2 = 11101$. Gli elementi sono:

$$0 = 0 \cdot b_1 + 0 \cdot b_2 \quad b_2 = 0 \cdot b_1 + 1 \cdot b_2$$

$$b_1 = 1 \cdot b_1 + 0 \cdot b_2 \quad b_1 + b_2 = 1 \cdot b_1 + 1 \cdot b_2 = 01111$$

Es. Sia C codice lineare su \mathbb{Z}_2 con matrice generatrice $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

1) Determinare lunghezza, dimensione, grandezza di C .


$G \in (\text{Mat}_{3 \times 6}, \mathbb{Z}_2)$, dunque lunghezza $C = 6$, dimensione è $k = 3$,
e la grandezza è $2^3 = 8$

2) Determinare distanza minima d di C

Ricaviamo matrice di controllo da matrice generatrice

Essendo G in forma standard in quanto $G = (I_3 | A)$, avremo $H = (-A^T | I_3)$

Troviamo che $H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$

$3+3=6$ 

Adesso controlliamo la dipendenza lineare dei vettori

Notiamo che non avendo 0, $d > 1$. Inoltre in \mathbb{Z}_2 , due vettori sono l.d. se uguali,
quindi non avendone $d > 2$. Avendo 3 righe e $d > 2$, concludiamo che $d = 3$

3) Decodificazione vettori $u = 100110$ e $v = 011101$

Data distanza minima d , allora rileva $d-1$ errori e corregge $\lfloor \frac{d-1}{2} \rfloor$ errori.

In questo caso $d = 3$ quindi C è 2-rilevatore e 1-correttore.  posso correggere

Per calcolare la sindrome di u , bisogna fare prodotto tra u e la mat.
di controllo trasposta. Ottergo vettore con lunghezza = colonne H

$$uH^T = (100110) \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} = (0, 1, 1)$$

$$vH^T = (011101) \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} = (0, 0, 0)$$

Trovo il vettore come x colonne H e l'errore sarà nella posizione col n° di colonne $\cdot x$ volte.

u è uguale a 1 volta 3° colonna di H , quindi $e = (0, 0, 1, 0, 0, 0)$.

La codifica di u è $u \cdot e = (100110) \cdot (0, 0, 1, 0, 0, 0) = (1, 0, 1, 1, 1, 0)$

Essendo invece $vH^T = 0$ e sapendo che $0 \in C$, avremo che $v \in C$ e si codifica
con v stesso.

- 1) Elenicare tutti i polinomi generatori di codici ciclici di dimensione 3 in $R_7 = \mathbb{Z}_2[x]/(x^7-1)$

Troviamo il grado del polinomio con la formula $\dim = \text{ordine } \mathbb{Z} - x$.

In questo caso il polinomio sarà di grado 4.

Le possibilità sono i polinomi di grado 4 che dividono x^7-1 .

$$\text{Avremo } p_1(t) = (t+1)(t^3+t+1) = t^4+t^3+t^2+1$$

$$p_2(t) = (t+1)(t^3+t^2+1) = t^4+t^2+t+1$$

- 2) Per ogni polinomio scrivere matrice generatrice del corrispondente codice ciclico.

La matrice avrà righe quanto la dimensione e le colonne quanto il grado pol.

La matrice sarà nella forma $\begin{bmatrix} \text{coeff. polinomio da terminare noto} \\ \text{traslo } 1 \text{ a } dx \\ \text{traslo } 2 \text{ a } dx \end{bmatrix}$

$$\text{Per } p_1 \text{ avremo } G_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \text{ mentre per } p_2 \text{ avremo } G_2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- 3) Dire se il polinomio $t+t^4+t^5+t^6$ appartiene ad uno dei codici precedenti

Scriviamolo con i suoi coefficienti.

$$\text{Abbiamo } u = 0100111 \text{ in } \mathbb{Z}_2^7$$

Cerco se esiste comb. lineare dove ottengo u .

Provo prima con G_1 . Pongo v_1 di $G_1 = 0$ perché ho 1 in 1° posizione e non va bene. Provo a vedere se $u = b_2 + b_3$ ma non lo è.

Provo adesso su G_2 . Faccio lo stesso ragionamento e trovo che $u = b_2 + b_3$. Dunque $u \in C_2$.