

CORTEZIONE • 1

MCD - CASO D'USO >

"Sia $n > 0$ numero intero, Spiegare perché $\text{MCD}(n, n+3)$ può essere solo 1 o 3"

3.) Definirlo Tramite Euclide

$n+3 = q \cdot n + r$ Per def. $r \leq d$ quindi $3 \leq n$

3.a) Calcolo i casi in cui $n \geq 3$

$$n = x \cdot 3 + y \quad \text{Sempre per def } y < 3$$

$$\begin{array}{l} \text{3.a.1)} \\ \text{3.a.2)} \\ \text{3.a.3)} \end{array} \quad \begin{array}{l} y=2 \\ y=1 \\ y=0 \end{array}$$

$$n = x \cdot 3 + 2 \rightarrow \begin{array}{l} \text{MCD} \\ \text{MCD} \end{array} \quad 3 = 1 \cdot 2 + \underline{1} \rightarrow 1 = 2 - 1 \cdot 0$$

$$\begin{array}{l} \text{3.a.2)} \\ \text{3.a.3)} \end{array} \quad \begin{array}{l} y=1 \\ y=0 \end{array}$$

$$n = x \cdot 3 + \underline{1} \rightarrow \begin{array}{l} \text{MCD} \\ \text{MCD} \end{array} \quad 3 = 3 \cdot 1 + 0$$

$$\begin{array}{l} \text{3.a.3)} \\ \text{3.b.1)} \end{array} \quad \begin{array}{l} y=0 \\ n=3 \end{array}$$

$$n = x \cdot \underline{3} + 0 \rightarrow \begin{array}{l} \text{MCD} \\ \text{MCD} \end{array}$$

3.b) Calcolo i casi per cui $n \leq 3$

$$\begin{array}{l} \text{3.b.1)} \\ \text{3.b.2)} \\ \text{3.b.3)} \end{array} \quad \begin{array}{l} n=3 \\ n=2 \\ n=1 \end{array}$$

$$6 = 2 \cdot \underline{3} + 0 \quad \text{MCD}$$

$$5 = 2 \cdot 2 + \underline{1} \quad \text{MCD}$$

$$5 = 2 \cdot 2 + \underline{1} \rightarrow 2 = 2 - 1 \cdot 0$$

$$4 = 4 \cdot 1 + 0 \quad \text{MCD}$$

$$4 = 4 \cdot \underline{1} + 0$$

2) Elenco i numeri distinti di MCD = {1, 3}

METODO ALTERNATIVO >

1. Dato $d = \text{MCD}(a, b)$ allora $d \mid b-a$

Sostituire b e a coi membri

$$d = \text{MCD}(n, 3+n) \rightarrow d \mid (3+n)-n \rightarrow d \mid 3$$

2. Elencare i divisori del numero trovato

3 è primo, gli unici divisori sono 3 e 1

ELLENCO PRIMI > 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43
47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

CONCETTO • 2

CONVERGENZA NUM IN BASE X >

1. Dividere il num fin quando ha quoziente = 0

NB: Per ogni divisione,
Tracciare il resto.

2. Il nuovo numero sarà
composto dai resti:

basso \rightarrow alto

sx \rightarrow dx

ES: "Converti 15407 in base 8"

$$15407 \div 8 = 1925 \text{ resto } 7$$

$$1925 \div 8 = 240 \text{ resto } 5$$

$$240 \div 8 = 30 \text{ resto } 0$$

$$30 \div 8 = 3 \text{ resto } 6$$

$$3 \div 8 = 0 \text{ resto } 3$$

$$15407 = [3607]_8$$

SEMPLIFICAZIONE INSIEMI DIVISORI >

Dati due insiemi che definiscono degli insiemi divisibili per un num, la loro intersezione è equivalente all'insieme di elementi divisibili per l'mcm

Dato $a, b \in \mathbb{N}$ $Y = \{y \in \mathbb{N} \mid a \mid y\}$ $W = \{w \in \mathbb{N} \mid b \mid w\}$

$$Y \cap W = \{n \in \mathbb{N} \mid \text{mcm}(a, b) \mid n\}$$

ES: "Definire Intersezione tra elementi divisibili per 2 e per 3"

$$Y = \{n \in \mathbb{N} \mid 2 \mid n\} \quad W = \{n \in \mathbb{N} \mid 3 \mid n\} \quad Y \cap W = \{n \in \mathbb{N} \mid 6 \mid n\}$$

CARDINALITÀ DI ELEMENTI DIVISORI >

Dati due insiemi che definiscono degli insiemi divisibili per un num, la sua cardinalità è equivalente alla cardinalità del totale / Divisore intersezione

Dato $a, b \in \mathbb{N}$ $Y = \{y \in \mathbb{N} \mid a \mid y\}$ $W = \{w \in \mathbb{N} \mid b \mid w\}$

$$|Y \cap W| = \left[\frac{\text{tot}}{\text{mcm}(a, b)} \right] \quad |W| = \left[\frac{\text{tot}}{a} \right] \quad |Y| = \left[\frac{\text{tot}}{b} \right]$$

ES: "Quanti sono gli elementi da 1 a 15 div per 3?" $\left[\frac{15}{3} \right] = 5$

PERMUTAZIONI

2

APPLICAZIONE DI 1 PERM > IN:

1. Disporre gli elementi da 1 a n
2. Dato il ciclo, applicare la trasformazione: $(1,2) \Rightarrow \begin{pmatrix} 1 & \dots \\ 2 & \dots \end{pmatrix}$
3. Riscrivere il ciclo
4. (opt): Ri-applicare alg. su nuova riga

$S_n \rightarrow$ Insieme di perm. di len: n
 IN: $\pi \in S_4 \quad \pi = (1,2,3)(4,5)$
 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 4 & 6 & 7 \end{pmatrix} \xrightarrow{\text{1° ciclo}} \xrightarrow{\text{2° ciclo}} \xrightarrow{\text{Non compiono restano uguali}}$
 $(1,2,3)(4,5) \quad \textcircled{3}$

in basso se si ha bisogno di ri-applicare più volte perm. differenti

APPLICARE POTENZA PERM >

0. ? SE l'esponente == 0?

0.T ALLORA $\sigma^0 = id$ FWE

0.F Proseguire

1. ? SE l'esponente < 0?

1.T ALLORA $\sigma^{-n} = \sigma^{-1} \cdot \sigma^n$ ovvero

si effettuerà prima σ^{-1} e poi
si applicherà σ^n con l'esponente
 $\sigma^{-1} = C_1^{-1} \cdot C_2^{-1} \cdots C_n^{-1}$

ovvero scrivere i cicli nel
verso opposto

1.F Proseguire

2. $\sigma^n = C_1^n \cdot C_2^n \cdots C_m^n$ ovvero

riscrivere i cicli skippingo

n elementi es: $(1,2,3)^2 = (1,3,2)$

N.B.: Se la dimensione del ciclo

è uguale a n si annulla

$(1,2,3)^3 = id$

$\sigma^0, \sigma^n, \sigma^{-n}$

ES dato $\sigma = (1,2,3)(4,8)(12,13,14) \in S_14$
calcolare σ^2, σ^3

- $\sigma^0 = id_{S_{14}} \rightarrow 0.T$

1,2,3

$$\begin{aligned} - \sigma^2 &= (1,2,3)^2(4,8)^2(12,13,14)^2 \\ &= (1,3,2)(4,2,4,13) \end{aligned}$$

$$\begin{aligned} - \sigma^3 &= \sigma^2 \cdot \sigma^1 \Rightarrow \sigma^1 = (1,2,3)^{-1}(4,8)^{-1}(12,13,14)^{-1} \\ &= (1,3,2)(8,4)(12,14,13) \end{aligned}$$

$$\begin{aligned} \sigma^3 &= (1,3,2)^3(4,8)^3(12,13,14)^3 \\ &= (8,4) \quad (\text{8}) \end{aligned}$$

PERMUTAZIONI

2

- CICLI NON DISGIUNTI \rightarrow CICLI DISGIUNTI > In: $\pi \in S_n$ $\pi = (\dots)$
1. min = Numero più piccolo nei cicli di π
 2. scrivere min nel primo ciclo
 3. Percorrere da dx \rightarrow sx cercando min
 4. s = numero dopo min nel 1° ciclo trovato
 5. SE Ripeti ricerca (s) \Rightarrow nei cicli a sx
 - S.T Scrivere s nel ciclo
 - S.F S'è scritto trovato, DO(s).
 - S.E S'è un num del ciclo scritto attualmente non scritto e chiudere il ciclo
 6. DO(z) con min = prossimo num. minimo che non appare nei cicli disgiunti

ES: $\pi \in S_7$ find(x,y)

$$\pi = (1,2,4)(2,7)(4,5)$$

$$\min(\pi) = \frac{1}{\text{ciclo}} \quad w=1(1)$$

$$\text{find}(1,1) = (2,3) \quad 3=3 \rightarrow w=2(1,2)$$

$$\text{find}(2,2) = \emptyset, \text{find}(2,2) = (2,3), \text{find}(2,3) = \emptyset \quad w=7(1,2,7)$$

$$\text{find}(3,1) = \emptyset, \text{find}(3,2) = (2,3), \text{find}(2,3) = (4,5) \quad w=4(1,2,7,4)$$

$$\text{find}(4,1) = (5,6), \text{find}(5,2) = \emptyset, \text{find}(5,3) = \emptyset \quad w=5(1,2,7,4,5)$$

$$\text{find}(5,1) = (4,1), \text{find}(4,2) = \emptyset, \text{find}(4,3) = 1 \quad w=1(1,2,3,4,5)$$

TIPO PERM \Rightarrow IN: $\pi \in S_n$ π è rapp come cicli disgiunti
 OUT: n-upla contenente per ogni ciclo di π la cardinalità.
ES: $\pi \in S_7$ $\pi = (1,2,3)(5,6)$ $\text{Tipo}(\pi) = [3,2]$

PERIODO \Rightarrow IN: $\pi \in S_n$ π è rapp. come cicli disgiunti
 OUT: $n \in \mathbb{Z}$ pari a m.c.m (elem. del tipo)
ES: $\pi \in S_6$ $\pi = (1,2,3)(5,6)$ $\text{Tipo}(\pi) = [3,2]$ $P(\pi) = \text{mcm}(3,2) = 6$
NB: I periodi fatti da numeri primi sono formati da più cicli disgiunti con quell'esatto periodo.
ESS: "Elenca una $\pi \in S_n$ di periodo 13" $\rightarrow 13$ è primo \Leftrightarrow non si può fare!

PARITÀ \Rightarrow IN: $\pi \in S_n$ π è rapp. come cicli disgiunti
 OUT: P se pari, D=dispari: Somma di parità invertite partendo dal $\text{Tipo}(\pi)$ $\overset{\text{D.P.}}{\text{Parity}} = P + D = D$
ES: $\pi \in S_7$ $\pi = (1,2,3)(5,6)$ $\text{Tipo}(\pi) = [3,2]$ Parity = $P + D = D$

PERMUTAZIONI • 3

CALCOLARE PER QUALI n σ^k è ciclo \Rightarrow IN: σ in cicli disgiunti
 1. Trovare il tipo(σ)
 [vedere step dedicato]

2. Partire definendo che

$$\sigma = C_n \cdot C_m \dots \rightarrow \sigma^k = C_n^k \cdot C_m^k \dots$$

3. σ^k è ciclico se quando applicato rimane solo 1 ciclo

ES: Dato σ con $\text{Tipo}(\sigma) = (3, 5)$ per quali $k > 0$ è ciclo?

So che $\sigma = C_3 \cdot C_5$ quindi

$$\sigma^k = C_3^k \cdot C_5^k$$

è ciclico se sse $C_3^k = \text{id}$ V $C_5^k = \text{id}$ rimane solo 1 ciclo
 sse $k \mid 3$ V $k \mid 5$

$\pi \in S_n$, Periodo(π) \rightarrow Tipi(π)

1. Definite l'eq: Periodo(π) = mcm(Tipi(π))

2. I tipi saranno l'unione:

- Calcolo di 1 num
È equivalente a Periodo(σ)
- Calcolo di 2 num
È equivalente a scegliere $x, y \in \mathbb{N}$ che soddisfino $\frac{x \cdot y}{\text{MCD}(x, y)} = \text{Periodo}(\sigma)$

- Calcolo di 3+ num
Provate a generare dei tipi aumentando il num di x e y generate prima.

Sono accettate tutte quelle che hanno somma $\leq n$

CARDINALITÀ DEI CICLI

1. Seguire la formula

$$\text{Card}(\ell) = n \cdot (n-1) \cdot (n-2) \cdots n-k \cdot \frac{1}{\ell}$$

In cui:

- ℓ è la lunghezza desiderata
- k è sinonimo di ℓ

IN: - σ in cicli disgiunti
- Periodo(σ)

ES: Dato $\sigma \in S_{12}$ con Periodo(σ) = 10, Trovare i Tipi(σ)

$$10 = \text{mcm}(\text{Tipi}(\sigma))$$

- Con 1 num $\rightarrow 10$
- Con 2 num

$$\frac{x \cdot y}{\text{MCD}(x, y)} = 10 \rightarrow x=2 \ y=5 \quad \text{MCD}(2, 5)=1$$

$$\frac{5 \cdot 2}{1} = 10$$

- Con 3+ num Espando $x \cdot y$
 $1 \cdot 2 + 2 \cdot 5 = \times, 2 \cdot 2 + 1 \cdot 5 = q \checkmark$
 $3 \cdot 2 + 1 \cdot 5 = \cancel{11} \checkmark, 4 \cdot 2 + 5 = \cancel{13} \times$

Sono quindi: $\{(10), (5, 2), (5, 2, 2), (5, 2, 2, 2)\}$

ES: Quanti cicli di Lunghezza 3 si possono formare in S_{12} ?

$$= \frac{12 \cdot 11 \cdot 10}{3}$$

PERMUTAZIONI

1

CARNALITÀ DELLE PERMUTAZIONI

0.? SE Ci sono ripetizioni nel Tipo(π)

O.T Moltiplicare le cardinalità dei cicli [vedere parte]

Che andrà moltiplicata per
 $\frac{1}{j!}$ j = Numero di ripetizioni

FWE

O.F Moltiplicare le cardinalità dei cicli [vedere parte]

FWE

- IN: • $\pi \in S_n$ disgiointi
• $Tipo(\pi)$

Esercizio: Quante sono le permutazioni in S_{12} dato che
Tipi $(4, 3, 3, 2)$

Il Tipo fornito ha ripetizioni O.T

$$\frac{12 \cdot 11 \cdot 10 \cdot 0}{4} \cdot \frac{8 \cdot 7 \cdot 6}{3} \cdot \frac{5 \cdot 4}{2} \cdot \frac{1}{2!}$$

Viene peso 1 volte il 3 si ripete 2 volte.

ES 2 "Quante sono le permutazioni in S_{12} del tipo $(4,3,2)$?"

$$= \frac{32 \cdot 14 \cdot 10 \cdot 9}{4} \cdot \frac{8 \cdot 7 \cdot 6}{3} \cdot \frac{5 \cdot 4}{2}$$

GRUPPI

2

FUNZ. EULERO $\varphi(n) > \times \varphi(0) \times \varphi(n), n < 0$

Describe la cardinalità del gruppo moltiplicativo \mathbb{Z}_n^*

O. CASE SU n

O.A n primo \wedge ha grado 1
 $\varphi(n) = n-1$

O.B n primo \wedge ha grado ≥ 2
 $\varphi(n^k) = n^{k-1} \cdot (n-1)$

O.C SE $\varphi(a \cdot b)$ \wedge a, b sono coprimi ($\text{MCD}(a,b)=1$)
 $\varphi(a^n \cdot b^m) = \varphi(a^n) \cdot \varphi(b^m)$

O.ELSE Scomporre il numero nei primi e ripetere.

ES1: "Calcolare $\varphi(35)$ "

$$\begin{aligned}\varphi(35) &= \varphi(5 \cdot 7) \quad \text{MCD}(5,7)=1 \\ &= \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 24\end{aligned}$$

ES2: "Calcolare $\varphi(36)$ "

$$\begin{aligned}\varphi(36) &= \varphi(3^2 \cdot 2^2) = \text{MCD}(3,2)=1 \\ &= \varphi(3^2) \cdot \varphi(2^2) = 3 \cdot 2 \cdot 2 \cdot 1 = 12\end{aligned}$$

ES3: "Calcolare $\varphi(1485)$ "

$$\begin{aligned}\varphi(1485) &= \varphi(3^3 \cdot 5 \cdot 11) \quad \text{MCD}(3,5,11)=1 \\ &= \varphi(3^3) \cdot \varphi(5) \cdot \varphi(11) = 3^2 \cdot 2 \cdot 4 \cdot 10 = 720\end{aligned}$$

GENERATORI GRUPPI CICLICI (PERM)

1. Calcolare Periodo(σ)

Vedere sezione I

2. $\langle \sigma \rangle$ sarà l'insieme di σ^n con esponente incrementata da 0... $p-1$ in cui
 $p = \text{Periodo}(\sigma)$

IN: • $\sigma \in S_n$

$$\bullet \sigma = c_1 \cdot c_2 \cdots c_n$$

ES "dato $\sigma = (1,3,5,6)(2,4) \in S_8$
definire $\langle \sigma \rangle$ "

Calcolo Periodo(σ) = 4 [I]

$$\langle \sigma \rangle = \{ \text{id}, \sigma, \sigma^2, \sigma^3 \}$$

INTERSEZIONE GRUPPI CICLICI (PERM)

1. PER OGNI α permutazione

data:

• determinarlo come $\langle \alpha \rangle$
[generatori gruppi ciclici]

2. L'intersezione saranno le permutazioni comuni

IN: • $\sigma, \beta \dots \in S_n$

$$\bullet \sigma, \beta \dots = c_1 \cdot c_2 \cdots c_n$$

ES: "Dati $\sigma = (1,3,5,6)(2,4) \in S_8$
 $\beta = (1,5)(3,6)(2,7,4) \in S_8$ calcolare $\langle \sigma \rangle \cap \langle \beta \rangle$ "

$$\langle \sigma \rangle = \left[\begin{smallmatrix} \text{generatori} \\ \text{gruppi} \end{smallmatrix} \right] = \text{id}, \sigma, \sigma^2, \sigma^3$$

$$\langle \beta \rangle = \left[\begin{smallmatrix} \text{ciclici} \end{smallmatrix} \right] = \text{id}, \beta, \beta^2, \beta^3, \beta^4, \beta^5$$

$$\sigma^2 = (1,5)(3,6) \quad \sigma^3 = (1,6,5,3)(2,4)$$

$$\beta^3 = (1,5)(3,6) \quad \beta^4 = (2,4,7)$$

$$\langle \sigma \rangle \cap \langle \beta \rangle = \{ \text{id}, (1,5)(3,6) \}$$

CARDINALITÀ DI GENERATORI (CLASSI RESIDUO) > IN: $\{n\}$ numeri, Z_n

1. Elencare il numero di elementi

possibili prima di superare Z_n . Sarà il periodo2. I generatori saranno $\mathcal{C}(\text{periodo})$ ES: "Dato $H = \{5^k \mid k \in \mathbb{N}\}$ in Z_{60} , calcolare il num. di generatori."1. elenco H

$$H = \left\{ \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{6}{5}, \frac{7}{5}, \frac{9}{5}, \frac{11}{5}, \frac{13}{5}, \frac{17}{5}, \frac{19}{5}, \frac{21}{5}, \frac{23}{5}, \frac{27}{5}, \frac{29}{5}, \frac{31}{5}, \frac{33}{5}, \frac{37}{5}, \frac{39}{5}, \frac{41}{5}, \frac{43}{5}, \frac{47}{5}, \frac{49}{5}, \frac{51}{5}, \frac{53}{5}, \frac{57}{5}, \frac{59}{5} \right\}$$

Periodo (H) = 12In quanto $\sum 12 = 60 = 5$

2. Calcolo cardinalità

$$\mathcal{C}(12) = \mathcal{C}(2^3 \cdot 3) = 2 \cdot 1 \cdot 2 = 4$$

ELEMENTI CON INVARIATO (PERM) >

1. Sono tutti gli elementi che al dato elemento come input hanno quel preciso risultato

IN: $H = \{g \in G \mid g(1)\}$ ES: "Dato $G = \{(1,2)(3,4,5,6), (5,6,2)\}$ in S_6 , e $H = \{g \in G \mid g(1)=1\}$ descrivere H "Solo $(5,6,2)$ manda 1 int.

HA GENERATORI? (PERM) >

1. Ha generatori SE tutti gli elementi sono rappresentabili come g^n ovvero la potenza di un membro.ES: "Dato $G = \{(1,2,3,4,5,6), (3,5,7)\}$ ha generatori?"

$$(1,2,3,4,5,6)^2 = (1,5)(3,7). \text{ Siccome ha solo questi 2 allora ogni } g \in G \text{ è } g^n \text{ quindi SI}$$

STABILIRE CICLICITÀ TRAMITE Periodo (PERM) > IN: $G \subseteq S_n$

1. Trovare le cardinalità dei

gruppi $|G|$ 2. Se esiste almeno 1 elemento con periodo $(g) = |G|$ [periodo perm] allora è ciclicoES: Dato il sottogruppo di S_6

$$G = \{(1,2)^i (3,4,5,6)^j \mid 0 \leq i \leq 1, 0 \leq j \leq 3\}$$

id $0 \leq j \leq 3$ è ciclico?"

$$= \{ (1,2)^0 (3,4,5,6)^0, (1,2)^1 (3,4,5,6)^0, (1,2)^0 (3,4,5,6)^1, \\ (1,2)^1 (3,4,5,6)^1, (1,2)^0 (3,4,5,6)^2, (1,2)^1 (3,4,5,6)^2, (1,2)^0 (3,4,5,6)^3, (1,2)^1 (3,4,5,6)^3 \}$$

Non ci sono elementi con periodo 8!

DETERMINARE ORDINE DA $\mathbb{Z}_n \times \mathbb{Z}_m$

1. Dividere per ogni membro della tupla

1.A $a \cdot x \equiv 0 \pmod{n} \rightarrow$ Ordine solo \mathbb{Z}_n 1.B $b \cdot x \equiv 0 \pmod{m} \rightarrow \mathbb{Z}_m$ 2. Sarà $\text{lcm}(r_1, r_2)$ in cui r_1 ed r_2 sono i risultati delle congruenze

NB: Come nell'esempio, se si risolve e l'elemento non è invertibile sarà il più piccolo n nel nuovo insieme fatto lo 0.

IN: $\langle (a, b) \rangle$ in cui $a \in \mathbb{Z}_n \wedge b \in \mathbb{Z}_m$

ES: "Si consideri il gruppo $\mathbb{Z}_{24} \times \mathbb{Z}_{30}$ determinare gli ordini di $\langle (6, 5) \rangle$ e $\langle (5, 6) \rangle$ "

- Per $\langle (6, 5) \rangle$ $6x \equiv 0 \pmod{24}$ $\frac{6x}{6} \equiv 0 \pmod{24}$ $\text{lcm}(24, 6) = 6$ $x = 0 \pmod{4}$ ma 6 lo

$= \{0, 4, 8, 12, 16, 20\}$

 $\rightarrow u$ è il più piccolo lato &

$\underline{5x \equiv 0 \pmod{30}}$

$30 = 6 \cdot 5 + 0 \quad \text{lcm}(5, 30) = 5$

ma 5 lo quindi $\frac{5x}{5} \equiv 0 \pmod{30}$

$= \{0, 5, 10, \dots\}$ $x \equiv 0 \pmod{6}$

Quindi il risultato sarà

$\text{lcm}(6, 5) = \underline{30}$ e ordine

(che soddisfano condizione)

ELENCARE / CONTARE CLASSI DI RESTO > IN: $\bar{k} \pmod{\mathbb{Z}_n}$, cond = \bar{k}

1. Partendo dalla condizione,

generare tutti gli elementi fino a quando non si trova l'identità.

ES: "Dare quante sono le classi $\bar{x} \in \mathbb{Z}_n$ tali che $\bar{s} = \bar{x}$ per qualche

$\bar{x} \in \mathbb{N}$

$$\begin{aligned}\bar{s}^0 &= \bar{1} & \bar{s}^1 &= \bar{s} & \bar{s}^2 &= \bar{s}s \\ \bar{s}^3 &= \bar{s}s^2 & \bar{s}^4 &= \bar{s}^2s & &= \bar{s}s \\ &= \bar{q} & \bar{s}^5 &= \bar{s}^4s & &= \bar{q}s \\ && & & &= \bar{q}s\end{aligned}$$

Quindi sono $\underline{5}$

CICLICITÀ $\mathbb{Z}_m \times \mathbb{Z}_n \Rightarrow$ lo sono se $\text{MCD}(m,n)=1$

CICLICITÀ $\mathbb{Z}_n \times \mathbb{Z} \Rightarrow$

GENERATORI EXP $\mathbb{Z}_m \times \mathbb{Z}_n >$

- Sono tutte le tuple (α_m, β_n) in cui i rappresentanti sono co-primi con la base del modulo:

$$(\alpha_m, \beta_n) \rightarrow \text{MCD}(\alpha, m) = \text{MCD}(\beta, n) = 1$$

- Scegliere degli α, β arbitrari per cui valga la formula.

ELENCARE ELEMENTI INVERTIBILI $(\mathbb{Z} \times \mathbb{Z}_m)^*$

- Il gruppo moltiplicativo rispetto al prodotto si propaga:

$$(\mathbb{Z} \times \mathbb{Z}_m)^* = \mathbb{Z}^* \times \mathbb{Z}_m^*$$

- Definire gli elementi invertibili dei singoli insiemi:

- $\mathbb{Z}^* = \{ \pm 1 \}$
- $\mathbb{Z}_n^* = \{ z \in \mathbb{Z} \mid 1 \leq z \leq m \wedge \text{MCD}(z, m) = 1 \}$

Per \mathbb{Z}_n^* , una soluzione più veloce è scomporre n nei suoi fattori primi:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$$

Gli elementi invertibili saranno tutti i numeri da 1 a $n-1$ che non sono divisibili per i coefficienti p_1, \dots, p_r

ES: "Dato $\mathbb{Z} \times \mathbb{Z}_{12}$, calcolare gli invertibili rispetto al prodotto componente per componente"

Propago gruppo molt: $(\mathbb{Z} \times \mathbb{Z})^* = \mathbb{Z}^* \times \mathbb{Z}_{12}^*$

Calcolo i singoli:

$$\mathbb{Z}^* = \{ \pm 1 \}$$

$$\mathbb{Z}_{12}^* = \{ z \in \mathbb{Z} \mid 1 \leq z \leq 12 \wedge \text{MCD}(z, 12) = 1 \} = \{ \pm 1, \pm 5, \pm 7, \pm 11 \}$$

$$\text{MCD}(12, 1) = 1 \vee, \text{MCD}(12, 2) = 2x$$

$$\text{MCD}(12, 3) = 3x, \text{MCD}(12, 4) = 4x$$

$$\text{MCD}(12, 5) = 1 \vee, \text{MCD}(12, 6) = 6x$$

$$\text{MCD}(12, 7) = 1 \vee, \text{MCD}(12, 8) = 4x, \text{MCD}(12, 9) = 3x$$

$$\text{MCD}(12, 10) = 2x, \text{MCD}(12, 11) = 1 \vee \text{MCD}(12, 12) = 12x$$

Soluzione alternativa per \mathbb{Z}_{12}

$$12 = 3 \cdot 2^2 \quad \text{Tutti gli } n \text{ da } 1 \text{ a } 12 \text{ in cui } 3 \nmid n \text{ e } 2 \nmid n$$

$$1, 5, 7, 11$$