Matematica Discreta

▾ Insiemi e simboli

Simboli

Connettivi logici $\neg \quad \wedge \; \vee \quad \rightarrow \leftrightarrow$
Quantificatori
$\exists$ quant. esistenziale $\exists$! "esiste ed è unico" $\forall$ quant. universale

Insiemi

INSIEME: collezione di **elementi** distinti (diversa) e deve essere ben definito (dobbiamo essere in grado di stabilire se un oggetto appartiene o meno nell'insieme)

TIPI RAPPRESENTAZIONE:

1. Elencazione (A={1,2,3})
2. Per caratteristica ($A = \{a \in X | P(a)\}$)
3. diagrammi di Venn

INSIEMI NUMERICI

Naturali $\mathbb{N}$ $\subset$ Interi $\mathbb{Z}$ $\subset$ Razioni $\mathbb{Q}$ $\subset$ Reali $\mathbb{R}$ + Irrazionali $\mathbb{R} \backslash \mathbb{Q}$

- $\mathbb{Q}$ (insieme quoziente (ovvero insieme classi equivalenza) frazioni)
- $\mathbb{R}$ (esp. decimaleinfinita, finita o aperiodica ‼ possono avere 2 esp. decimali)
- $\mathbb{C} = \{a + bi | a \in R, b \in R, i^2 = -1\}$

Cardinalità, insieme vuoto

|A|= numero di elementi di A (se sono in numero finito).

$\emptyset = \{\}$ è l'insieme (‼ unico in quanto = a tutti quelli senza el.) che non contiene elementi

Inclusione

$A \subseteq B$ **incluso in senso lato** (possono coincidere)
$A \subset B$ **incluso strettamente** (A≠B)

PRINCIPIO DOPPIA INCLUSIONE:

$$A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$$

Insieme delle parti

INSIEMI PARTI P(A): è l'insieme dei sottoinsimi di A (‼ |P(A)|=2^|A|)

$$P(A) = \{S | S \subseteq A\}$$

▾ Operazione su insiemi

Operazioni tra insiemi

INTERSEZIONE: (sono gli elementi sia di A che di B)

$$A \cap B = \{\, c | c \in A \wedge c \in B\}$$

Due insiemi A, B si dicono **DISGIUNTI** se:
$A \cap B = \emptyset$

UNIONE: (elementi di entrambi gli insieme)
$A \cup B = \{\, c | c \in A \vee C \in B\}$

DIFFERENZA (o COMPLEMENTARE di B in A): elementi che stanno in A ma non B$A \backslash B = C_A^{"}(B) = \{a \in A \wedge a \notin B\}$

Proprietà delle operazioni tra insiemi (+morgan)

Commutativa: [1]
$A \cap B = B \cap A$
$A \cup B = B \cup A$

Associativa: [2]

$A \cap (B \cap C) = (A \cap B) \cap C$
$A \cup (B \cup C) = (A \cup B) \cup C$

Distributiva [3]
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (D1)

Es

- An insieme multipli di n

  $n \in N \quad A_n = \{a \in \mathbb{Z} | a = kn, k \in \mathbb{Z}\}$
  $\cup_{n \in \mathbb{N}} A_n = \mathbb{Z}$ (n appartiene a N va sotto) (è unione ti tutti
  $\cap_{n \in \mathbb{N}} A_n = \{0\}$ (non insieme vuoto)

  Dimostro 1) usando definizione di uguale
  $\cup_{n \in \mathbb{N}} A_n \subseteq \mathbb{Z}$ $A_n \subseteq \mathbb{Z}$ per ogni n (è prodotto di N e Z)
  $\mathbb{Z} \subseteq \sum_{n \in \mathbb{N}} A_n$ in quanto $A_1 = \mathbb{Z}$

Dati due insiemi A, B [+] (se **intersezione** è uno ⇒ **sottoinsieme**)
$A \cap B = A \Leftrightarrow A \subseteq B$
$A \cup B = A \Leftrightarrow B \subseteq A$ (D2, D3)

LEGGE DI DE MORGAN [4]
$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ (si scambiano quando distribuisco per la differenza)

Dim:

- Distributività (usando distributività dei connettivi)

  $x \in A \cap (BUC) \Leftrightarrow x \in A \wedge x \in (B \cup C) \Leftrightarrow x \in A \wedge (x \in B \vee x \in C)$
  $\Leftrightarrow (x \in A \wedge x \in B) v (x \in A \wedge x \in C) \Leftrightarrow (A \cap B) \cup (A \cap C)$

- Morgan (usando de morgan operatori logici)

  $x \in A \setminus (B \cup C) \Leftrightarrow x \in A \wedge \neg (x \in B \vee x \in C)$
  $\Leftrightarrow x \in A \wedge (x \notin B \wedge x \notin C)$
  $\Leftrightarrow (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)$
  $\Leftrightarrow (A/B) \cap (A/C)$

Ricoprimenti, partizioni e insieme quoziente

RICOPRIMENTO: di X è una famiglia di sottoinsiemi di X
$A_i \subseteq X (i \in I)$ tali che $\cup_{i \in I} A_i = X$

PARTIZIONE: di X è una famiglia di sottoinsiemi di X $A_i \subseteq X (i \in I)$ t.c.

- $\cup_{i \in I} A_i = X$ (è un ricoprimento)
- $A_i \neq \emptyset \quad \forall i \in I$ (non sono vuoti)
- $A_i \cap A_j = \emptyset \quad \forall i, j \in I, i = j$ (sono separati)

INSIEME QUOZIONTE: è l'insieme dei sottoinsiemi di X facenti parte della partizione.

$$Q = \{A_i, i \in I\}$$

Es.

- i numeri pari e dispari formano famiglia parzione di $\mathbb{Z}$ →Q={{pari}, {dispari}}
- $X = \left\{ \frac{a}{b} | a \in \mathbb{Z}, b \in \mathbb{Z} - \{0\} \right\} = \mathbb{Q}$

  a/b e c/d stanno nello stesso insieme se a*d=b*c (le due frazioni sono equivalenti)

  Ogni elemento della partizione è una classe di equivalenza della frazione ([1/2] indica di quale è rappresentante).
  $Q = \mathbb{Q}$

Prodotto cartesiano

PRODOTTO CARTESIANO AxB è l'insieme: (‼️ $|A \times B| = |A| \times |B|$)

$$A \times B = \{ (a, b) | a \in A, b \in B\}$$

Insieme di coppie ordinate→ non commutativo

$A = \{x, y\}$ $B = \{x, \beta, \gamma\}$

$A \times B = \{(x,\alpha), \ldots, (y,\gamma)\}$

▾ Induzione

Assiomi peano sui numeri naturali

Assiomi Peano (1889):

1. $0 \in \mathbb{N}$
2. $\forall n \in \mathbb{N}, \exists s(n) \in \mathbb{N}$ "successore di n"
3. se $m, n \in \mathbb{N}, m \neq n \Rightarrow s(m) \neq s(n)$ (successori diversi)
4. $\forall n \in \mathbb{N}(0 \neq s(n))$ (0 è minimo)
5. se $U \subseteq \mathbb{N}$ è tale che $0 \in U, \forall n \in U(s(n) \in U) \Rightarrow U = \mathbb{N}$

Induzione e ricorsione (grazie a quinto assioma)

DIMOSTRAZIONE PER INDUZIONE: sia P(n) una proposizione è vera $\forall n \in \mathbb{N}$ se:

- **Passo base:** P(0) è vero
- **Passo induttivo:** $\forall n \in \mathbb{N} \quad P(n) \Rightarrow P(n+1)$

💡 Es.

▾ Dimostro che la somma dei primi numeri è n(n+1)/2

$P(n) : \sum_{k=0}^{n} k = \frac{(n+1)\,n}{2}$

- P(0)=0 $P(n) : \sum_{k=0}^{0} k = \frac{(0+1)\,0}{2}$=0 (vero)
- P(n)⇒P(n+1) P(n+1)=P(n)+(n+1) (vero ⇒ cvd)

$P(n) : \sum_{k=0}^{n} k = \frac{(n+z)(n+1)}{2} = \frac{n^2+3n+2}{2} = P(n) + (n+1)$

▾ P(x) ha cardinalità 2^|A| (per ogni sottoinsieme di y-1 esistono 2 sottinsiemi in y)

- $|x| = 0 \Rightarrow |P(x)| = 2^0 = 1 \qquad P(\emptyset) = \{\emptyset\}$ (vera)
- $|x| = n, |P(x)| = 2^n$ vogliamo mostrare $|y| = n+1 \Rightarrow |P(y)| = 2^{n+1}$
  $y = \{y_1, y_{2,\ldots,} y_{n+1}\}$ considero $|y \backslash \{y_{n+1}\}| = n \ \rightarrow |P(y \backslash \{y_{n+1}\})| = 2^n$

  Sia ora $S \subseteq \{y - \{y_{n+1}\}\}$ allora $S \subseteq y \quad S \cup \{y_{n+1}\} \subseteq y \ \ ma \ \ S \cup$
  $\{y_{n+1}\} \subseteq y \backslash \{y_{n+1}\}$

  Per ogni S ottengo due diversi sottoinsiemi di Y (con o senza ultimo).
  Allora $|p(y) = 2, |P(y - \{g_{n+1}\})| = 2 * 2^n = 2^{n+1}$

RICORSIONE: Anche le definizione ricorsive si basano sul principio d'induzione.

💡 Es.

▾ n!

oppure $n! = \prod_{k=1}^{n} k$

$$\begin{cases} 0! = 1 \\ (n+1)! = (n+1) \cdot n! \quad \forall n \in \mathbb{N} \end{cases}$$

▾ Funzioni

Funzioni e grafici

Le funzioni sono morfismi (leggi che ci permettono di passare da ente a altro) tra insiemi.

FUNZIONI: Una funzione f da un insieme A, detto dominio, ad un insieme B, detto codominio, è una legge che associa ad ogni elemnto a∈A uno e un solo elemento f(a)∈B.
f:A→B a→f(a) $\forall a \in A \quad \exists! f(a) \in B$ (unica immagine)

GRAFICO (univoco): di una f:A→B è il sottoinsieme (gamma) $\Gamma \subseteq A \times B$ dato da:

$$\Gamma = \{(a,b) \in A \times B | b = f(a)\}$$

FUNZIONI NOTEVOLI

1. Identità id_A : A→A a→a
2. Dati A e B e fissato elemento $b \in B$, possiamo definire la funzione costante fb: A→b $\forall a \in A \ \ f(a) = b$
3. Dati A e B consideriamo il prodotto cartesiano AxB, la proiezione su A $\pi_A : A \times B \rightarrow A \quad (a,b) \rightarrow a$
4. Dati $S \subseteq A$, inclusione $i : S \rightarrow A \quad s \rightarrow s$ (≠ da identità in quanto

cambia dominio)

5. Successioni: è una funzione di dominio e codominio $\mathbb{N}$
   $f:\mathbb{N}\to\mathbb{N} \qquad n\to f(n) \qquad f(0), f(1), f(2)\dots$
6. Operazioni: Es. una operazione binaria su A è una funzione: (es. +((m,n))=m+n
   $f: A\times A\to A$

💡 Es.

- U={esseri umani} f:"x ama y" (non è unica immagine oppure 0 ⇒ no funzione)
- $\mathbb{R}$ x→$\sqrt{x}$ (restringo dominio ⇒ ‼cambio la funzione (dominio è parte integrante))
- f:R→R x→x^2 g:Z→Z x→x^2 SONO DIVERSE FUNZIONI
- f:{1,2}→R x→x^2-2x+1 g:{1,2}→R x→$\log_2(x)$ SONO STESSA FUNZ.

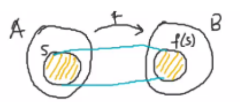
Immagini e controimmagini (come funzioni)

IMMAGINE: Data una funzione f:A→B, f(S) è immagine di S tramite f

f:P(A)→P(B) $\quad S\subseteq A->f(S)=\{b\in B|\exists a\in S, f(a)=b\}$

CONTROIMMAGINE: $f^{-1}(T)$ è controimmagine di T tramite f

$f^{-1}:P(B)\to P(A) \qquad T\subseteq B\to f^{-1}(T)=\{a\in A|f(a)\in T\}$



Come casi speciali abbiamo (per un elemento)
$a\in A \quad f(\{a\})=f(a)$ immagine di a
$b\in B \quad f^{-1}(\{b\})=f^{-1}(b)=\{a\in A|f(a)=b\}$ controimmagine di b

Funzioni iniettiva, suriettiva e biettiva

Una funzione f:A→B si dice:

1. **iniettiva:** se $a_1\neq a_2\in A => f(a_1)\neq f(a_2)$
2. **suriettiva:** se $\forall_{b\in B}, \exists_{a\in A}|f(a)=b$
3. **biettiva:** se è iniettiva e biettiva

💡 Es. $f:\mathbb{Z}\to\mathbb{Z} \quad n\to 2n$ iniettiva $\qquad f:\mathbb{Z}\to\mathbb{N} \quad n\to|n|$ suriettiva
$f:\mathbb{Z}\to\mathbb{Z} \quad n\to n^2$ nessuna delle due $\qquad$ ‼Dipende da dominio e codominio

PROP 1: f:A→B è iniettiva
$\leftrightarrow \quad \forall b\in B\left|f^{-1}(b)\right|\leq 1 \quad \leftrightarrow \quad f(a_1)=f(a_2)\to a_1=a_2$

PROP 2: f:A→B è suriettiva allora: $\quad \forall b\in B\left|f^{-1}(b)\right|\geq 1$

COROLLARIO: f:A→B è biettiva allora: $\quad \forall b\in B\left|f^{-1}(b)\right|=1$

A Dim:

- Se f non è iniettiva (verifico che $\neg A\equiv\neg B$)
  $\exists a_1\neq a_2\in A\Rightarrow f(a_1)=f(a_2) \quad se \quad |f^{-1}(f(a_1))|\geq 2$
  (se non iniettiva maggiore di 2 controimmagini e viceversa)
  $a1, a2\in A|f(a1)=f(a2) \quad se \quad f^{-1}(f(x1))|\leq 1 => a_2=a_1$
  (in quanto se minore di 1 ⇒ sono uguali controimmagini)

Composizione

COMPOSIZIONE: date f:A→B, g:B→C la funzione composta è (‼non commutativa) :
$g\circ f: A\to C \qquad a\to g(f(a))$

Associatività: $\quad h\circ g\circ f=(h\circ g)\circ f=h\circ(g\circ f)=h(g(f(x)))$

Compos. con Id: $\quad f\circ Id_A=Id_A\circ f=f$

PROP 1: Dato f:A→B g:B→C

1. Se f,g sono iniettive/suriettive/biettive ⇒ la **composta è altrimenti**

PROP 2: f:A→B g, B→C

1. Se $g \circ f$ è iniettiva ⇒ f **è iniettiva** (prima applicata)
2. Se $g \circ f$ è suriettiva ⇒g **è suriettiva** (seconda applicata) ??????

Dimostrazioni

- 1a (tolgo iniettive)

  Consideriamo gof(a1)=gof(a2)

  - ⇒ f(a1)=f(a2) in quanto g iniettiva
  - ⇒ a1=a2 in quanto f iniettiva ⇒ **cvd. (iniettiva)**
- 2a (uso suriettività per sostituire b=g(a))

  Vogliamo mostrare $\forall_c \exists_{a\in A}[g(f(a)) = c]$

  - Poichè g è suriettiva $\forall_c \exists_{b\in B}[g(b) = c]$
  - Poichè f è suriettiva $\forall_b \exists_{a\in A}[g(a) = b]$
    - $=> \quad \forall_c \exists_{a\in A}[g(b) = g(f(a)) = c]$ **cvd (sostiduendo b=g(a)**
- 1b (ad f compongo a sinistra g)

  Dato f(a1)=f(a2)

  - compongo con g g(f(a1))=g(f(a2))
  - a1=a2 x iniettività gof **cvd**
- 2b (gof(a)=c → g(b)=c)

  In quanto gof suriettiva $\forall_c \exists_{a\in A}[g(f(a)) = c]$

  ⇒$\forall_c \exists_{a\in A}[g^{-1}(c) \neq \emptyset]$ ⇒ **è suriettica cvd**

Esempio chiarificatore proprietà

- Composta n→(n,n) (m,n)→n
  - $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N} \quad n \to (n, n)$ (uguali)
  - $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad (m, n) \to n$ (quella di destra)
  - gof è biettiva (identià)
    - f è iniettiva **cvd**
    - g è suriettiva **cvd**

PROP: Date f,g $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ (!! penso ai domini)

Inverse e prop.

INVERSA: f:A→B g:B→A si dicono inverse tra loro se:
$g \circ f = id_A \quad f \circ g = id_B$ (!! devono valere entrambe)

PROP: Se f e $g = f^{-1}$ → f e g entrambe biezioni.

TEOREMA: Se f:A→B è una funzione biettiva ⇒ $\exists!\ f^{-1} : B \to A$

Dim:

- Prop

  Se $gof = id_A$ ⇒ f è iniettiva e g è suriettiva
  Se $fog = id_B$ ⇒ g è iniettiva e f è suriettiva
- Teorema

  Dato $b \in B$, poichè f è biettiva $|f^{-1}(b)| = 1$, possiamo scrivere $|f^{-1}(b)| = \{a\}$
  Possiamo dunque **scrivere** una funzione g:B→A tale che g(b)=a.

  Verifichiamo che g è inversa di f:
  $gof \quad a \to f(a) \in B \to a$ ⇒ idA
  $fog \quad b \to a \to b$ ⇒ idB (in quanto a sta nella controimmagine di b)

  Unicità: (qualunque inverse sono uguali per catena identità)
  Sia h:B→A un'altra funzione inversa i f.
  Allora $h = h\ o\ id_B = h\ o(fog) = (hof)og = id_A\ o\ g = g$

- Combinatorica

Combinatoria ed equipollenza

COMBINATORICA: è una branca della matematica che si occupa di problemi di conteggio su insiemi finiti.

!? 1.significato insieme è finito ? 2. sign. contare ? 3.sign. stesso numero di elementi ?

3) **EQUIPOLLENZA:** 2 insiemi X, Y si dicono equipollenti se esiste una

funzione biettiva
f:X→Y ↔ |X|=|Y|

E' una "**buona**" nozione in quanto riflessiva, simmetrica e transitiva (⇒rel. equivalenza)

Def. insieme infinito e prop. su finitit

PROP: Se $X \subseteq Y$ allora |X|≤|Y|
‼ Però è possibile $X \subset Y$ che |X|=|Y|

INSIEME INFINITO: Se è equipollente ad un suo sottoinsieme proprio.
INSIEME FINITO: Se non è infinito.

Es.

- $f : \mathbb{N} \to \mathbb{N} \backslash \{0\}$ n→n+1 ⇒ secondo la definizione $|\mathbb{N}| = |\mathbb{N} \backslash \{0\}|$
- $f : \mathbb{Z} \to 2\mathbb{Z}$ n→2n ⇒ secondo la definizioni $|\mathbb{Z}| = |2\mathbb{Z}|$

PROP: Sia A un insieme finito e f:A→A, allora le seguenti affermazioni sono equivalenti:
1. f è iniettiva 2. f è suriettiva 3. f è biettiva

Dim: (attraverso circolo 1→2→3→1)

- A→f(A) e inversa a caso è iniettiva

1→2 suppongo f iniettiva. Allora f(A) è un sottoinsieme di A equipollente ad A (in quanto biettiva, ovvero iniettiva e suriettiva per il cambio di codominio). Ma poichè A non è infinito ⇒ f(A)=A ⇒ f è suriettiva

2→3 f:A→A suppongo suriettiva e definiamo $g : A \to A$ $a \to a' \in f^{-1}(a)$ (esiste per suriettivita e scelta a caso tra quelle presenti) Dati $a_1 \neq a_2 \in A$ $f^{-1}(a1) \cap f^{-1}(a2) = \emptyset$ allora g è iniettiva e, per [1→2] biettiva

3→1 ovvia

Nuberabili e contabilità con In

Teorema (senza dim): definiamo degli insiemi: $I_0 = \emptyset$ $In = \{1, 2, ..., n\}$ $\forall n >= 1$
1) $\forall n \in \mathbb{N}$ I_n è finito
2) Se m≠n allora I_m, I_n non sono equipollenti
3) Se m≤n allora $|I_m| \leq |I_n|$
4)Ogni insieme finito è equipollente a un certo I_n.
(si può definire cardinalità/contare con questo)
5)Per ogni insieme infinito X si ha $|X| \geq |\mathbb{N}| = \aleph_0$ (aleph zero)
(N è l'infinito più piccolo a parimerito)

Es. imp(vedi logica) $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{Q}| \leq |R| = |P(\mathbb{N})|$

Principio cassetti e inclusione esclusione

Parleremo sempre di insiemi finiti in questi capitoli

PRINCIPIO DEI CASSETTI (/gabbie e piccioni): se vogliamo mettere n piccioni in k<n gabbie ci sarà almeno in una gabbia che contiene più di un piccione.
$|X| < |Y|$ ↔ $\neg \exists f : X \to Y$ iniettiva

PRINCIPIO INCLUSIONE ESCLUSIONE: A e B, $|A \cap B| = k \leq \min\{|A|, |B|\}$
$|A \cup B| = |A| + |B| - |A \cap B|$ (tolgo intersezione)

3 iniemi(applicando 2 volte su): (Elementi - intersezioni 2 a due + intersezione di tutto)
$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cup C| - |A \cup C| + |A \cap B \cap C|$

Es. 90 superano fisica, 120 Chimica e 48 entrambe. Chi supera una=162 =90+120-48

- Quanti numeri primi tra 6 e 40

X={6,7,...,40} quali tra questi sono primi = non div 2,3,5 (7 solo da 49 in avanti)

|X|=40-6+1=35

$A=\{n\in X|n=2k\ \ n\in\mathbb{N}\}$ 17.5 ⇒18 (parto con pari)
$B=\{n\in X|n=3k\ \ n\in\mathbb{N}\}$ 11.6⇒ 12 (parto con 6)
$C=\{n\in X|n=5k\ \ n\in\mathbb{N}\}$ 7

|unione|=(18+12+7)-(6+4+2)+(1)=25+1=26
|C(unione)|=35-26=9

Prodotto cartesiano e metodo scelte successive

PRODOTTO CARTESIANO:
$$A_1\times A_2\times ...\times An=\{(a_1,...,a_n)|a_i\in A_i,\ 1\leq i\leq n\}$$

📢 $(A\times B)\times C$ $\quad A\times B\times C$ ‼️non sono uguali ma posso fare biezione

PROP: dati n insiemi A1,..., An finiti, $|A_1\times ...\times A_n|=\prod_{i=1}^{n}|A_i|$

🅰 Dim per induzione
- PASSO BASE (n=2): $|A\times B|=|A|*|B|$
- PASSO INDUTTIVO (come se fosse 2 insiemi)

💡 Es. numero pasti completi diversi=360 se: 6 antipasti, 4 primi, 5 secondi, 3 dolci

Disposizioni entrambe

DISPOSIZIONI CON RIPETIZIONE: $D'_{n,k}\ \ n,k\in\mathbb{N}$ sono sequenze con k elementi (eventualmente ripetuti) presi in un insieme di n elementi.
$$D'_{n,k}=n^k$$

Oss: Questo valore corrisponde al numero di funzioni $f:I_k\to I_n$ (per ogni k ho n poss.)
In generale dati due insiemi A, B $\mathfrak{f}_{A,B}=\{\text{funzioni}\ \ A\to B\}\ \ \ |\mathfrak{f}_{A,B}|=|B|^{|A|}$.

- 0^0=1 unica $f:\emptyset\to\emptyset$ in quanto unica funzione è identità

💡 Es. ‼️**Rivalutazione P(A):** $X_s:A\to\{0,1\}\quad |P(A)|=|\{0,1\}|^{|A|}=2^{|A|}$

DISPOSIZIONI SEMPLICI: $D_{n,k}$ sono sequenze di k el. distinti in insieme di n elementi :
Se k>n allora $D_{n,k}$ =0 (impossibile per principio piccionaia), altrimenti (n*...*(n-k+1)):
$$D_{n,k}=\frac{n!}{(n-k)!}$$

Oss: Questo valore corrisponde al numero di funzioni iniettive $f:I_k\to I_n$. (per distinti)
In generale dati A, B $\mathfrak{f}_{A,B}=\{\text{funzioni iniettive}\ \ A\to B\}\ \ \ |\mathfrak{f}_{A,B}|=D_{|B|,|A|}$.

Permutazioni e anagrammi

PERMUTAZIONI: sono tutti i possibili riordinamenti di un insieme di n elementi (o di I_n).
$$P_n=D_{n,n}=n!$$

Oss: Questo valore corrisponde al numero di funzioni biettive $f:I_k\to I_n$. (per 1 a 1).
+ quindi 0! =1 in quanto unica funzione biettiva di vuoto in sè è identità

ANAGRAMMI CON RIPETIZIONI: In generale se n, ci sono k lettere ripetute rispettivamente r1,.... rn allora il numero di anagrammi:
$$\text{n di anagrammi}=\frac{n!}{r_1!\cdot r_2!\cdot...\cdot r_k!}$$

💡 Es. anagrammi:
1. Numero di anagrammi (anche senza senso) della parola AMORE 5! =120
2. anag. MATEMATICA MMAAATTEIC (10!)/(3!*2!*2!)= 10!/24= 151200

Combinazioni semplici e con ripetizione

COMBINAZIONI SEMPLICI: $C_{n,k}$ sono raccolte di k elementi distinti presi da un insieme di n elementi [Se k>n allora $C_{n,k}=0$] (‼ non conta ordine)

$$C_{n,k}=D_{n,k}/P_k=\binom{n}{k}=\frac{n!}{(n!)(n-k)!}$$

Oss: Sono tutti i possibili sottoinsiemi di cardinalità k in un insieme di cardinalità n

Es. scegliere 3 cifre tra 0 a 9 = 9!/(6!*3!)=84

Dim: su I_n (stelle e barre)

ooo||o|o|o → [(n-1)+k]! / [k! (n-1)!] (numero totale permutazione)

COMBINAZIONI CON RIPETIZIONI: sono raccolte di k elementi anche ripetuti provenienti da un insieme di n elementi. (‼ quanti di ogni elemento prendere)

$$C'_{n,k}=\binom{n+k-1}{n-1} \quad n,k\geq 1$$

Es. Numero di monomi non simili tra loro di grado 9 ci sono nelle variabili w, x, y, z $\binom{9+4-1}{4-1}=\binom{12}{3}=220$

Coefficiente binomiale e sue proprietà

COEFFICIENTE BINOMIALE: si indica $\binom{n}{k}=\frac{n!}{(n!)(n-k)!}=C_{n,k}$

Ricordando che sono i sottoinsiemi di cardinalità k in un insieme di cardinalità n:

$\binom{n}{0}=1 \quad S\subseteq I_n \quad |S|=0 <=> S=\emptyset$ (solo insieme vuoto da 0)

$\binom{n}{1}=n \quad S\subseteq I_n \quad |S|=1 <=> S=\{x\}$ (n insiemi da 1)

$\binom{n}{k}=\binom{n}{n-k} \quad f:P(I_n)\to P(I_n) \quad S\to I_n\backslash S$ biezione tra I_k, I_{n-k}

Es. ‼2 **rivisitazione di P(A)**: $|P(I_n)|=\sum_{k=0}^{n}\binom{n}{k}$ k cardinalità S

FORMULA DI STIEFEL: $\binom{n}{k-1}+\binom{n}{k}=\binom{n+1}{k}$ 1≤k≤n

Per costruire tartaglia

Triangolo di Pascal-Tartaglia

TRIANGOLO DI PASCAL-TARTAGLIA: (riga colonna) oppure somma dei 2 sopra

1	$\binom{0}{0}$
1 1	$\binom{1}{0}$ $\binom{1}{1}$
1 2 1	$\binom{2}{0}$ $\binom{2}{1}$ $\binom{2}{2}$
1 3 3 1	$\binom{3}{0}$ $\binom{3}{1}$ $\binom{3}{2}$ $\binom{3}{3}$
1 4 6 4 1	$\binom{4}{0}$ $\binom{4}{1}$ $\binom{4}{2}$ $\binom{4}{3}$ $\binom{4}{4}$
1 5 10 10 5 1	$\binom{5}{0}$ $\binom{5}{1}$ $\binom{5}{2}$ $\binom{5}{3}$ $\binom{5}{4}$ $\binom{5}{5}$

FORMULA DEL BINOMIO DI NEWTON: per $n\in\mathbb{N}$ $(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$

Es. ‼2b **rivisitazione di P(A):** $2^n=(1+1)^n=\sum_{k=0}^{n}\binom{n}{k}1^k1^{n-k}=\sum_{k=0}^{n}\binom{n}{k}$

▾ Permutazioni

Rivalutazione permutazioni e prop. Sn

DEF: $S_X=\{f|f:X\to X \ \ biettiva\}$ (cons. le permutaz. come le f. biettive)

Se $X=In=\{1,2,...,n\}$ usiamo $S_n=S_{I_n}$ (es. S_3= {f. biettive $I_3\to I_3$})

PROP: Sia X insieme finito, con |X|=n. Allora c'è una biezione $f : S_X \to S_n$ tale che per $\sigma, \pi \in S_X$, vale $f(\sigma \circ \pi) = f(\sigma) \circ f(\pi)$ (mantiene composizione dopo biezione)

PROPRIETA' Sn:

1. $id_{I_n} : I_n \to I_n \ \ id_{I_n}(x) = x \quad id \in S_n => Sn \neq \emptyset$ (mai vuota)
2. Se $\sigma, \pi \in S_n => \sigma, \pi \ \ sono\ biezioni => \sigma \circ \pi\ è\ biezione => \sigma \circ \pi \in S_n$
   (composte)
3. Se $\sigma \in S_n => \sigma\ \ è\ biettiva => inverti. => \sigma^{-1}\ \ è\ biettiva => \sigma^-1 \in S_n$
   (inverse)
4. $|Sn| = n!$ (da combinatoria)

NOTAZ.: nella pratica per descrivere un elemento di Sn, useremo:

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix}$$ (‼️non da perm se ripetuti o assenti)

Composizione e inversa

COMPOSTA: $\sigma, \pi \in S_n$, la composta $\sigma \circ \pi$ si ottiene: (‼️non comm. , esegue da destra)

$$\sigma \circ \pi : \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(\pi(1)) & \sigma(\pi(2)) & \sigma(\pi(3)) & \sigma(\pi(4)) \end{pmatrix}$$

💡 Es.

▾ Con tutti i passaggi

$$S_5 \quad \sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \ \pi : \begin{pmatrix} 1 & 2 & 3 & 2 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$$

$$\pi \circ \sigma \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$$

INVERSA: Data $\sigma \in S_n$, l'inversa σ^{-1} si ottiene (scambio righe e rioridino):

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix} \ \sigma^{-1} : \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Per verificare che è inversa faccio $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = Id$

Cicli e periodo e inversa

CICLO: $\sigma \in S_n$ si dice ciclo se $\exists \{x1, x2, ...x_l\} \subseteq I_n \quad l \leq n$ (**lunghezza ciclo**) t.c.:

$$\begin{cases} \sigma(x_1) = x_2, \ \sigma(x_2) = x_3, \ \ldots, \ \sigma(x_i) = x_1 \\ \sigma(k) = k \qquad \forall k \neq x_i \end{cases}$$ (‼️n girano tra loro e resto x=x)

NOTAZ. compatta: $\pi = (x_1\ x_3\ x_5\ ...\ x_7\ x_4)$ (x1 →x3 x1 immaagine in x3,...)

OSS: Il punto di partenza di un ciclo non è rilevante (Es. (1 3 7 4)=(3 7 4 1)=...)

PERIODO: Data una permutazione π, si dice periodo di π il numero:

$$per(\pi) = \min\{k > 0 \quad t.c. \quad \pi^k = id\}$$

PROP: se π è un ciclo di lunghezza l (quelli scambiati), allora $per(\pi) = l$

INVERSA: L'inversa di un ciclo è il **ciclo** che si ottiene **invertendo** l'ordine degli elementi.

$$\pi = (x1, x2, ...xl) \quad \pi^{-1} = (xl, ...x2, x1)$$

🅰️ Dim imp:

- Periodo   E' min e vale per tutti $(\pi = (x_1, x_2, \dots, x_l))$

  SOLO DOPO ALMENO L

  $x_1 \overset{\pi}{-} > \pi(x_1) = x_2 \neq x_1 \dots$

  $x_l \overset{\pi}{-} \pi(x_1) = \pi^l(x_1) = x_1$

  VALE PER TUTTI

  $\pi^l(x_i) = \pi^\ell\left(\pi^{i-1}(x_1)\right) = \pi^{l+i-1}(x_1) = \pi^{i-1}\left(\pi^l(x_1)\right) = \pi^{i-1}(x_1) = x_i$

- Inversa   faccio composizione destra e sinistra e ottengo Id

Cicli disgiunti e essenzialmente univoca strittura permutazione

> **CICLI DISGIUNTI:** Due cicli $\sigma = (x1, x2, \dots xl)$ e $\pi = (y1, y2, \dots, ym)$ si dicono disgiunti se $\{x1, x2, \dots xl\} \cap \{y1, y2, \dots, ym\} = \emptyset$ (non hanno el. in comune)

> **PROP**: cicli disgiunti (π, σ) commutano quindi $\sigma \circ \pi = \pi \circ \sigma$

Dim imp:

- Una non agisce su elementi altro

  UNO NON TOCCA L'ALTRO (e viceversa)

  $xi(1 \leq i < l) : (\sigma \circ \pi)(xi) = \sigma(xi)\ (\pi \circ \sigma)(xi) = \pi(x_{i+1}) = x_{i+1}$

  NON TOCCATI DA ENTRAMBI RESTANO UGUALI

Es.

- Es. di non disgiunti (seguendo percorso da destra a sinistra)

  (1 3 4 7) (2 6 4) (5 1 2)

  il 5 va in 1 che va in 3   il 3 va in 4 , 4→2 2→5 ⇒ (5342),....

> **PROP**: Ogni permutazione π si scrive in modo essenzialmente unico (in quanto posso commutare ordine) come composizione di cicli a due a due disgiunti
> $$\pi = c_1 \circ c_2 \circ \dots \circ c_r$$

Dim imp:

- Tolgo un ciclo alla volta

  1-**FACCIO PARTIRE CICLO SE NON TUTTI FERMI**

  $Se\ \ \forall x \in In\ \ \ \pi(x) = x => \pi = id$

  $se\ \ \exists x \in I_n | \pi(x) \neq x,$

  2-**CONTINUO E SI RIPETE**

  $Pongo\ \ x_1 = x, \pi(x_1) = x_2, \dots, \pi^i(x_1) = x_{i+1}$

  Perchè In è finito, ad un certo punto gli elementi si ripetono cioè esite il più piccolo l t.c $x_{l+1} = xj$ per qualche $1 \leq j \leq l.$

  3-**DICO CHE NON PUO' ESSERE ALTRO CHE x1 (altrimenti non iniettiva)**

  4-**TOLGO ELEMENTI DI CICLO E RIPETO**

  5-**TERMINAZIONE DEL PROCESSO**→Avviene in quanto In è finito

Tipo permutazione e periodo

> **TIPO PERMUTAZIONE:** data una permutazione $\sigma = c_1 \circ \dots \circ c_r$ dove $c_1 \circ \dots \circ c_r$ sono cicli disgiunti di lunghezza rispettivavente (le ho ordinate in quanto disgiunte):
> $$l_1 \geq l_2 \geq \dots \geq l_r,\ \ \sigma \text{ si dice di tipo } (l_1,\ l_2, \dots, l_r)$$

l1+l2+...+lr≤n in quanto disgiunti e viceversa posso scrivere permutazione di quel tipo

Es. imp (su come calcolare)

- Partizioni **(dato numero →numero di tipi)**→no formula

  n = 4 Quanti tipi ci sono in S_4?
  (4) (3) = (3,1) (2,2) (2) = (2,1,1) (1,1,1,1) = id

  n = 5 Quanti tipi ci sono in S_5?
  (5) (4) = (4,1) (3,2) (3) = (3,1,1) (2,2) = (2,2,1) (2) = (2,1,1,1) (1,1,1,1,1) = id

- **Permutazioni di un certo tipo** (dato tipo e Sn→permutazione)
  - Scelgo un ciclo $D_{12,5} = 12!/7!$
  - Ma non conta inizio quindi /5 → 12!/(7!*5)
  - Ripeto per tutti

$$\frac{12!}{5\cdot \cancel{7!}}\cdot\frac{\cancel{7!}}{3\cdot\cancel{4!}}\cdot\frac{\cancel{4!}}{2\cdot 2!}=\frac{12!}{5\cdot 3\cdot 2\cdot 2!}$$

- Problemi ↑ se **ln=lm** (⇒ faccio i calcoli a mano)

  (2,2) in S5

  - Devo ancora divedere 2!

Es. Quante permutazioni di tipo $(6,6,6,5,5,2,2,2,2)$ ci sono in S_{40}?

Sono $$\frac{40!}{6^3 5^2\cdot 2^4\cdot 4!\ 3!\cdot 2!\cdot 4!}$$

retta riordinamenti

PERIODO PERMUTAZIONE: di $\sigma = c_1 \circ .... \circ c_r$ cicli disgiunti di $(l_1, ..., l_r)$, allora:

$$per(\sigma) = mcm(l_1, ...l_r)$$ (dipende solo dal tipo)

Dim imp:

- Con solo 2 elementi (vale solo perchè disgiunti)

  $\sigma = c_1 \circ c_2 \ \ disgiunti \ \ (l1, l2)$

  DIVIDO PER OGNUNA (e poi ordino in quanto disgiunti)

  $$\sigma^k = (c_1\cdot c_2)^k = \underbrace{(c_1\cdot c_2)\cdot(c_1\cdot c_2)\cdot \dots \cdot(c_1\cdot c_2)}_{k \text{ volte}} = c_1^k\cdot c_2^k$$

  IN QUANTO DISTINDI⇒ COMPONENTI DEVONO ESSERE ID

  $$\sigma^k = id \iff c_1^k = id \ \ e \ \ c_2^k = id$$

  ⇒ k è multiplo di l1 e di l2 ⇒ mcm(l1,l2)

Scambi e parità e scrittura non univoca

Usati in quanto pochi: |Sn|=n! vs $\binom{n}{2}$ scambi ma posso ottenere ogni permutazioni

SCAMBIO: è un ciclo di lunghezza 2

OSS: se s è uno scambio $s \circ s = s^2 = id \quad \Rightarrow s = s^{-1}$ (scambio è suo opposto)

PROP: Un ciclo di lunghezza *l* è una composizione di *l*-1 scambi (non disgiunti)

Dim: $(x_1\ x_2\ ...\ x_l) = (x_1\ x_l)(x_1\ x_{l-1})...(x_1\ x_2)$ e calcolo

COROL: Ogni permutazione si può scrivere come composizione di scambi. (Dim: permutazione→cicli→scambi) (‼ma scomposiz. in scambi non unica (es. id))

Parità

PARITA': Una composizione di scambi $s_1 \circ ... \circ s_j$ si dice pari se j è pari.

TEOREMA: Data π, ogni sua scomposizione in scambi ha la stessa parità.

Se *c* è un ciclo di lunghezza *l*, la sua parità è pari se *l* è dispari. (!! non viceversa)

Se σ è permutazione qualsiasi la scompongo in cicli $\sigma = c_1 \circ ... \circ c_r$ calcolo:

$$(l_1 - 1) + ...(l_r - 1) = l_1 + ... + l_r = p$$ (basta calc numero di cicli pari)

- Aritmetrica

Aritmetica

ARITMETICA: è lo studio delle proprietà dell'insime dei numeri interi relativi $\mathbb{Z}$, rispetto alle operazioni di addizione e moltiplicazione.

Addizione e gen. additiva

> Proprietà facili (!! $(\mathbb{Z}, +, 0)$è gruppo abeliano):
>
> - Associativa $\forall x, y, z \in \mathbb{Z} \ \ (x + y) + z = x + (y + z)$
> - Elemento neutro $\exists 0 \in \mathbb{Z} | \forall x \in \mathbb{Z} \quad x + 0 = 0 + x = x$
> - Opposto $\forall x \in \mathbb{Z} \, \exists -x \in \mathbb{Z} \quad x + (-x) = (-x) + x = 0$
> - Commutativa $\forall x, y \in \mathbb{Z} \ \ x + y = y + x$

> $\mathbb{Z}$ è "generato additivamente" da 1 (ogni numero ottenuto da somma di 1 e opposto)

Moltiplicazione +generazione moltiplicamente+ distributiva

> Proprietà facili (!! $(\mathbb{Z}, *, 1)$ monoide commutativo):
>
> - Associativa $\forall x, y, z \in \mathbb{Z} \ \ (x * y) * z = x * (y * z)$
> - Elemento neutro $\exists 1 \in \mathbb{Z} | \forall x \in \mathbb{Z} \quad x * 1 = 1 * x = x$
> - Commutativa $\forall x, y \in \mathbb{Z} \ \ x * y = y * x$
> - Gli inversi non garantiti (solo +-1)

> Per "generare $\mathbb{Z}$ moltiplicamente" abbiamo bisogno di tutti i numeri primi, oltre che 0,+-1.

> Distributiva (tra addizione e moltiplicazione): $\forall x, y, z \in \mathbb{Z} x * (y + z) = x * y + x * z$

!!Una struttura come $(\mathbb{Z}, +, *, 0, 1)$ con le proprietà date → anello commutativo unitario

Divisibilità e prop.

> **DIVISIBILITA'**: Dati $a, b \in \mathbb{Z}$ diciamo che "a divide b", scritto a|b se:
>
> $$\exists k \in \mathbb{Z} \ | \ b = a * k$$

💡 Es. 2|6 vero 6|9 falso -4|12 vero (!!al contrario divisione)

> **PROP 1** facili:
>
> - +-1 divide tutto $\forall n \in \mathbb{Z} \ \ + -1 | n$
> - 0 è diviso da tutto $\forall n \in \mathbb{Z} \ \ n | 0$

> **PROP 2**: Siano $a, b, k \in \mathbb{Z}$
>
> 1. Se $k | a \wedge k | b => k | (a + b)$
> 2. se $k | a \wedge k | (a + b) => k | b$

Dim facili:

▾ 1-2 (sostituzione)

1) Sia k t.c. $k|a$ e $k|b$, allora $a = k \cdot \alpha$, $b = k \cdot \beta$ per qualche valore $\alpha, \beta \in \mathbb{Z}$.
Ma allora $a + b = k\alpha + k\beta = k(\alpha + \beta) \Rightarrow k | (a+b)$.

2) Sia k t.c. $k|a$ e $k|(a+b)$, allora $a = k\alpha$, $a + b = k \cdot \sigma$ per qualche $\alpha, \sigma \in \mathbb{Z}$.
Ma allora $b = (a+b) - a = k \cdot \sigma - k\alpha = k(\sigma - \alpha) \Rightarrow k|b$.

Divisori, MCD

> **INSIEME DIVISIORI:** Dato un certo $n \in \mathbb{Z}$, denotiamo $Dn = \{d \in \mathbb{Z} \ \ t.c. \ \ d | n\}$ l'insieme dei divisori di n (notazione non standard).

> **OSS** su grandezza:
>
> - se n=0, allora $D_0 = \mathbb{Z}$
> - se n≠0, allora D_n è finito (se d|n⇒ |d|<|n|) e non vuoto (+-1|n)

> **MCD(a,b):** è il massimo tra l'intersezione dei divisori di a e b con a,b≠0
>
> $$MCD(a, b) = max(D_a \cap D_b)$$

> **OSS:** questo valore esiste sempre ed è ≥ 1 (in quanto ogni numero ha almeno 1)

Divisione euclidea e proprietà base algoritmo

> **TEOREMA:** Dati $a, b \in \mathbb{Z}$ (b≠0), esistono!!unici 2 numeri $q, r \in \mathbb{Z}$ (quoziente e resto) t.c.:
>
> $$a = bq + r \quad e \quad 0 \leq r < |b|$$

A Dim

- Esistenza (su a,b≥0)(induzione forte e differenza con b per avere stesso resto)

  PASSO BASE 0=0*b+0

  PASSO INDUTTIVO

  Ipotesi induttiva: $\forall \alpha < a \exists q', r' \ t.c. \ \alpha = b * q' + r' \ \ e \ \ 0 \leq r' < b$

  - **Se a<b** ⇒ a =b*0+a
  - **se a≥b**⇒ $\alpha = a - b < a$ e per hp su alpha ⇒ricavo $a = b(q' + 1) + r'$

- Esistenza in vari segni (cambio segno e sistemo semplicemente)
- Unicità (sottraggo 2 esistenti e ottengo che b divide r-r' ⇒r-r'=0 ⇒ q-q'=0)

  PER ASSURDO a=qb+r=q'b+r' che soddisfano ipotesi

  SOTTRAGGO E OTTENGO CHE R UGUALI E POI Q UGUALI

  Suppongo r>r' (se necessario scambio) ⇒0=(q-q')b+(r-r')

  ⇒ -(q-q')b=r-r' ⇒ b|(r-r') ma r e r' <b⇒ **r=r'** **⇒ q-q'=0**

Algoritmo euclideo

> **PROP:** Dati $a, b, q, r \in \mathbb{Z} \ \ t.c. \ \ a = bq + r$ allora i divisori comuni ad *a* e *b* = quelli di b e r
>
> MCD(a, b)=MCD(b, r)

A Dim imp ma facile

- Pongo a e b come d per qualcosa e ottengo r=d*... (+ viceversa)

  SE D DIVIDE A E B ALLORA DIVIDE R

  Sia d in Z t.c. d|a e d|b. Allora $\exists \alpha, \beta \ \ t.c. \ \ a = d\alpha \ \ e \ \ b = d\beta$

  $d\alpha = dq\beta + r \Rightarrow r = d(\alpha - q\beta)$⇒ d|r

  SE D DIVIDE B E R ALLORA DIVIDE A

  $a = d(\beta q + \gamma)$ (dove $\gamma = r/d \wedge \beta = b/r$)

> **ALGORITMO EUCLIDEO** (più efficiente): Partiamo da $a, b \in \mathbb{Z}$ con b≠0 e procediamo ($a = bq + r, \ \ 0 \leq r < |b|$) con la divisione euclidea e per la proposizione precedente sappiamo che il MCD tra *a* e *b* è uguale MCD tra *b* e *r*. Ripeto il tutto su b,r e continuo così. Costruiamo così una successione di quozionti q1,q2,... e resti r1,r2,... con le proprietà
>
> 1. MCD(a, b)=MCD(b, r)= MCD(r, r1)=...=MCD(rn,rn+1)=... (**stesso mcd**)
> 2. $|b| > r > r_1 > r_2 >, \ldots > r_n > \ldots \geq 0$ (**termina per minimo**)
>
> Ma allora $r_{n-1} = r_n * q_{n+1} + 0$ $\Rightarrow MCD(a, b) = MCD(r_n, 0) = r_n$

Esempio

- MCD(2702,324)

  Esempio : MCD(2702, 324) = ? $\quad a = 2702 \quad b = 324$

  $2702 = 324 \cdot \underbrace{8}_{q} + \underbrace{110}_{r}$

  $324 = 110 \cdot \underbrace{2}_{q_1} + \underbrace{104}_{r_1}$

  $110 = 104 \cdot \underbrace{1}_{q_2} + \underbrace{6}_{r_2}$

  $104 = 6 \cdot \underbrace{17}_{q_3} + \underbrace{2}_{r_3} \quad \Rightarrow MCD(2702, 324) = 2$

  $6 = 2 \cdot 3 + \underbrace{0}_{r_4}$

  $2702 : 324 = 8$ q
  2592
  110 r

Identità di Bézout e quando esiste

> **TEOREMA**(no dim): Siano $a, b \in \mathbb{Z}$ e d=MCD(a, b). Allora esiste (!!non unici) $x, y \in \mathbb{Z}$
>
> t.c. $ax + by = d$

> **COROLLARIO**: Dati $a, b, c \in \mathbb{Z}$, l'equazione
>
> $ax + by = c$ ha soluzioni $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ sse.
>
> MCD(a, b)|c

Esempio chiarificatori

- Uso esempio prima (ricavo i resti e sostituisco a raffica)

  SCARTO ULTIMA E ESEGUO AL CONTRARIO

Vediamo l'applicazione all'esempio precedente. "Invertiamo" i risultati delle divisioni:

$$\begin{aligned}
2 &= 104 - 6 \cdot 17 &\longrightarrow\quad 2 &= 104 - (110 - 104) \cdot 17\\
6 &= 110 - 104 & &= 104(1+17) - 110 \cdot 17 = 104 \cdot 18 - 110 \cdot 17\\
104 &= 324 - 2 \cdot 110 & &= (324 - 2 \cdot 110) \cdot 18 - 110 \cdot 17 = 324 \cdot 18 - 110 \cdot (2 \cdot 18 + 17)\\
110 &= 2702 - 8 \cdot 324 & &= 324 \cdot 18 - 110 \cdot 53\\
& & &= 324 \cdot 18 - (2702 - 8 \cdot 324) \cdot 53 =\\
& & &= 324 \cdot (18 + 8 \cdot 53) - 2702 \cdot 53 =
\end{aligned}$$

$$\boxed{2 = 324 \cdot \underline{442} - 2702 \cdot 53}$$

- Esempio (!!non unici→ infiniti)

  POSSO TROVARNE INFINITI

  ES. 9 6 MCD(9,6)=3

  → tutte sol. equazione diofantea 6x+9y=3

- Corollario

  Es: $2702x + 324y = 4$ ha soluzioni? Sì perché $\mathrm{MCD}(2702, 324) = 2 \mid 4$

  Per trovare x e y basta moltiplicare per 2 l'identità di Bézout

  Es: $2702x + 324y = 3$ no

Notazione posizionale

DEF: La scrittura di $n \in \mathbb{N}$ in base b >1 è la stringa di cifre n=$c_s c_{s-1} \ldots c_1 c_0 [b]$ dove

n=$c_s * b^0 + c_{s-1} * b^1 + \ldots + c_1 b^{s-1} + c_0 b^s$

💡 Es.

- Che cosa significa $1238 = 8 * 10^0 + 3 * 10^1 + 2 * 10^2 + 1 * 10^3$
- Con divisione euclidea (~binario)

$$\begin{aligned}
1238 &= 123 \cdot 10 + \boxed{8}\\
123 &= 12 \cdot 10 + \boxed{3}\\
12 &= 1 \cdot 10 + \boxed{2}\\
1 &= 0 \cdot 10 + \boxed{1}
\end{aligned}$$

Primi/irriducibili e teorema fondamentale aritmetrica

DEF: Un numero **!!**$n \in \mathbb{Z} \setminus \{0, +-1, -1\}$, si dice

- **irriducibile** se n=a*b $(a, b \in \mathbb{Z}) \Rightarrow a = \pm 1 \vee b = \pm 1$ (diviso solo da 1 e sè)
- **primo** se n|ab $(a, b \in \mathbb{Z}) \Rightarrow n|a \vee n|b$ (div un fattore)

TEOREMA: $n \in \mathbb{Z} \setminus \{0, +-1, -1\}$ è primo sse. è irriducibile. (equiv. in Z!! non altri)

A Dim

- Irriducibile → primo (o n|a o per Bézout n|b)

  N IRRIDUCIBILE (mcd=1, Bézout)

  Suppongo n|ab:

  - Se **n|a ⇒ finito**
  - altrimenti poiché è irriducibile ⇒ MCD(a, n)=1
    - $ax + ny = 1$ → per l'idenità di Bézout
    - Moltiplico per b e sost. ab=nk (x hp)→ $b = (ba)x + (bn)y = (nk)x + (bn)y = n(kx + by)$
    - ⇒ **n|b ⇒ n è primo**

- Primo → irriducibile (deve dividere uno ⇒ n=kab⇒ k e b=+-1)

  "solo se". Sia n primo e valga $n = a \cdot b \Rightarrow n \mid a \cdot b \Rightarrow$ poiché n primo $n \mid a \vee n \mid b$.

  Supponiamo $n \mid a \Rightarrow a = n \cdot k$ $(k \in \mathbb{Z}) \Rightarrow \cancel{n} = a \cdot b = \cancel{n} k b \Rightarrow 1 = k \cdot b \Rightarrow k = b = \pm 1$

TEOREMA: Ci sono infiniti numeri primi.

A Dim per assurdo imp:

- Preso un qualsiasi insieme finito posso trovare altro primo (+ primo o contrad. est.)

  IDEA

  Sia $S = \{p_1, p_2, \ldots, p_n\}$ un insieme finito di numeri primi. Vogliamo mostrare che esiste sempre un numero primo diverso dai precedenti o dai loro opposti.

PRODOTTO +1 (primo o riducibile (nuovo primo o contraddizione 2 forme)

Considero $\alpha = p_1 * p_2 * ... * p_n + 1$

- Se alpha è primo o riducibile e Se $q \notin S$ ⇒ **finito**
- riducibile e se $q \in S \Rightarrow \alpha = p_i * k$ $1 = p_i * k - (\alpha - 1)$ $= p_i * (k - (\alpha - 1)/p_i)$ **⇒pi invertibile ASSURDO pi è primo**

TEOREMA FONDAMENTALE ARITMETICA: $n \in \mathbb{Z} \setminus \{0, +-1, -1\}$ si fattorizza in modo (essenzialmente (per ordine)) unico come prodotto di primi positivi:

$$n = +- p_1 * p_2 * .... * p_n (p_i > 0)$$

Dim imp: per positivi (per negativi basta cambiare segno) ⇒ n≥2

- Esistenza (induzione forte → o primo o divisione in 2 sotto se) usa irr.

  PASSO BASE

  n=2 → p1=2

  PASSO INDUTTIVO (primo o non primo)

  supponiamo l'enunciato valido $\forall x \in \mathbb{Z}, \ 2 \leq x < n$

  - Se n è primo ⇒ n è irriducibile ⇒ p1=n fine
  - Se n non è primo ⇒ è riducibile n=a*b a, b≠+-1
    - Applico ipotesi induttiva su a o b ⇒ poi moltiplico → **fine**

- Unicità (elimino elementi uguali fino ad ottenere 1=1 ⇒ coincide) usa primo

  CANCELLO ELEMENTO A VOLTA (<= deve dividere qualcosa ma primo ⇒ =)

  Sia n=p1*p2*...*ps=q1*q2...*qt (suppongo s≤t (al massimo inverto))

  - p1|q1*q2*...*qt=n ⇒ poiché p1 è primo $\exists q_i \ t.c. \ p1|qi$
  - Ma qi è irriducibile⇒ p1=qi e riordinando ottengo p1=q1 quindi tolgo p1 e q1 dalla serie

  IMPOSSIBILITA' $1 = q_s....q_{t+1}$ 1 = prodotto primi

- Aritmetrica modulare

Modulo, partizione e insieme quoziente

CLASSI DI RESTO MODULO N: Dato $N \in \mathbb{N} \setminus \{0\}$ detto modulo e defininiamo gli insiemi:

$A_0 = \{n \in \mathbb{Z} | \exists k \ \ t.c. \ \ n = q * N\}$, (divisibili, resto 1,... resto N-1)

$A_1 = \{n \in \mathbb{Z} | \exists k \ \ t.c. \ \ n = q * N + 1\}$,...,

$A_{N-1} = \{n \in \mathbb{Z} | \exists k \ \ t.c. \ \ n = q * N + (N-1)\}$

Useremo anche la scrittura in termini di rappresentanti delle classi (fa parte e rappres.) $\mathbb{Z}_N = \{[0]_N, [1]_N, ...[N-1]_N\}$ dove $[i]_N = A_i$ =!!$\bar{i}$ (se è chiaro chi è N)

PROP: Gli insieme $A_0, A_1, ..., A_n$ formano una partizione di $\mathbb{Z}$

L'INSIEME DELLE CLASSI DI RESTO MODULO N: è l'insieme quoziente della partizione appena vista dato un certo N. $\mathbb{Z}_N = \{A_0, ...A_{N-1}\}$

Dim imp:

- Non vuoti (i)- disgiunti - ricoprimento (divisione euclidea)
  - Non vuoto $\forall i, 0 \leq i < N-1 \quad i \in A_i$
  - Disgiunti <=resto divisione euclidea è unico
  - ricoprimento <=$\forall n \in \mathbb{Z} \quad \exists! q, r | n = q * N + r \quad 0 \leq r < N$

Es.

- N=3 (classi 0 mod 3, 1 mod 3, 2, mod 3 + !!attenzione ai negativi)

  Esempio: N=3 $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ è un rappresentante.

  $[0]_3 = A_0 = \{n \in \mathbb{Z} | \exists q \in \mathbb{Z} \ t.c. \ n = q \cdot 3\} = \{ ..., -6, -3, 0, 3, 6, 9, ...\}$ classe 0 modulo 3

  $[1]_3 = A_1 = \{n \in \mathbb{Z} | \exists q \in \mathbb{Z} \ t.c. \ n = q \cdot 3 + 1\} = \{ ..., -5, -2, 1, 4, 7, ..., 19, ...\}$ classe 1 mod 3

  $-5 = \underbrace{(-2)}_{q} \cdot 3 + \underbrace{1}_{r}$

- Stessa classe

  Es: $[3]_7 \stackrel{?}{=} [10]_7$ Sì, perché $10 = 1 \cdot 7 + \underbrace{3}_{r}$

  $[111]_{34} = [5702]_{34}$?

Stessa classe

> **Lemma (o prop.)**: Diciamo che "x è congruo a y modulo N" e scriviamo $x \equiv y \mod N$
>
> $$[x]_N = [y]_N <=> N|(x-y)$$

Dim:

- Due sensi

  DA STESSA CLASSE (ricavo differnza resti =0)

  Supponiamo [x]N=[y}N. Allora $\exists q, q', r \in \mathbb{Z}, 0 \le r < N | x = qN + r \ e \ y = q'N + r$ allora x-y=(q-q')N $\Rightarrow$ N|x-y

  DA DIV A CLASSE (da differenza e euclideo ricavo resto uguale)

  Supponiamo che N|x-y. Allora $\exists q \in \mathbb{Z} \quad x - y = N * q$ quindi $x = N * q + y$.

  Ora grazie alla divisone euclidea ottengo y=q'N+r. Ma allora sostituisco e x=(q+q')N+r $\Rightarrow y, x \in [r]_N$

Addizione e prop. e generazione additiva

> **ADDIZIONE**: $\mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N \quad (\overline{a}, \overline{b}) \to \overline{a+b}$

Dim di essere "ben posta" (ovvero che immagine sia univocamente determinata):

- a' e b' li scrivo in base ad a e b ($\Rightarrow$scrivo a'+b' in base a+b $\Rightarrow$ [a'+b']=[a+b])

  USO DIFFERENZA

  Sia $[a]_N = [a']_N \ e \ [b]_N = [b']_N$. Ciò vuol dire che
  - $\exists h \in \ | a' - a = hN => a' = hN + a,$
  - $\exists k \in \mathbb{Z} | b'b = kN => b' = hN + b$

  OTTENGO DIFFERENZA TRA SOMME (è = Nq)

  Ora $a' + b' = (hN + a) + (kN + b) = (h + k)N + (a + b)$

  $\Rightarrow (a' + b') - (a + b) = (h + k)N \Rightarrow [a' + b']_N = [a + b]_N$

> **PROPRIETA'**: dell'addizione in $\mathbb{Z}_N \ (N \in \mathbb{N}, N \ge 2)$
>
> 1. **associativa**: $\forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_N \quad (\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$
> 2. **commutativa**: $\forall \overline{a}, \overline{b} \in \mathbb{Z}_N : \overline{a} + \overline{b} = \overline{b} + \overline{a}$ infatti
> 3. **el. neutro:** $\forall \overline{a} \in \mathbb{Z}_N : 0 + \overline{a} = \overline{a}$ infatti $0 + \overline{a} = \overline{0 + a} = \overline{a} = \overline{a}$
> 4. **opposto:** $\forall \overline{a} \in \mathbb{Z}_N \exists b \in \mathbb{Z}_N \ \ t.c. \overline{a} + \overline{b} = \overline{0}$ basta prendere $\overline{a} = -\overline{b}$

2 cose da notare

- "dim" (passando da $\mathbb{Z}$)

  ASSOCIATIVA

  Infatti passando da $\mathbb{Z}$, si ha:
  $(\overline{a} + \overline{b}) + \overline{c} = (\overline{a + b}) + \overline{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \overline{a} + (\overline{b} + \overline{c})$

  ALTRO

  Si fa lo stesso per il resto (ovvero converto in tutto sotto overline e poi uso proprietà addizione in $\mathbb{Z}$

- !! tabella additiva (con ogni possibile combinazione in incrocio)→diagonali

  Costruiamo la tabella additiva di $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$:

  in $\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

  ci dice che $\overline{1} + \overline{3} = \overline{0}$ in $\mathbb{Z}_4$
  cioè $\overline{3} = -\overline{1}$ in $\mathbb{Z}_4$

- !!Opposto sembra particolare (-n diventa un numero positivo per modulo)

  Esempio : $\mathbb{Z}_{12}$. Consideriamo $\overline{7}$. Il suo opposto è $\overline{-7} = \overline{5}$.
  Infatti $7 + 5 = 12 \Rightarrow 7 + 5 \equiv 0 \mod 12 \Rightarrow \overline{7} + \overline{5} = \overline{0}$

> **PROP:** $\overline{a}$ genera additivamente $\mathbb{Z}_N$ <=> MCD(a,N)=1

Esempio esplicativo

- Genera additivamente e non

  ES GENERAZIONE

  $\overline{1}$ "genera additivamente" tutto $\mathbb{Z}_N$, infatti $\forall \overline{r} \in \mathbb{Z}_N (0 \le N) \quad r = \overline{1} + ... + \overline{1}$

  ES NON GENERAZIONE

$\overline{2} \in \mathbb{Z}_4$ in quanto 2+2=0 e 2+0 =2...

A Dim imp:

- ▾ Se a genere additivamente (deve essere 1 per certo k $\Rightarrow$ uso bezout)

  A DEVE ESSERE 1 PER UN CERTO K (1 genera tutto vedi esempio)

  Se $\overline{a}$ genera $\mathbb{Z}_N \Rightarrow \exists k | \overline{a} + ... + \overline{a} = 1$ (devo ottenere 1 per fare tutto)

  cioè $\overline{a + ... + a} = \overline{1} \Rightarrow \underline{a + ... + a - 1 = h * N}$ (per prop. moduli)

  USO BEZOUT

  Da ciò ottengo ka-hN=1

  $\rightarrow$Per l'identità di Bézout, ciò succede solo se MCD(a,N)=1

- ▾ Se MCD(a,N)=1 (inverso proc.)

  BEZOUT

  Se MCD(a,N)=1, per Bezout $\exists x, y \in \mathbb{Z} | ax + Ny = 1$

  $\Rightarrow ax = 1 - Ny$

  OTTENGO CHE AK E' 1 $\Rightarrow$ GENERA ADDITIVAMENTE

  $\Rightarrow ax \equiv 1 \mod N \Rightarrow \overline{a} + ... + \overline{a} = \overline{1}$

Prodotto e divisori di 0 e invertibili

MOLTIPLICAZIONE: $\mathbb{Z}_N \times \mathbb{Z}_N \rightarrow \mathbb{Z}_N (\overline{a}, \overline{b}) \rightarrow \overline{ab}$

A Dim ben postezza (non ha due immagini)

- ▾ (Come somma)

  COME SOMMA (USO DIFFERENZA)

  Siano $a, a', b, b' \in \mathbb{Z} | \overline{a} = \overline{a'} \wedge \overline{b} = \overline{b'}$ (li prendo uguali in modulo N)

  $\exists h \in \mathbb{Z} | a - a' = hN$

  $\exists k \in \mathbb{Z} | b - b' = kN$

  $\Rightarrow ab = (a' + hN)(b' + kN)$

  ARRIVO A MODULO

  $\Rightarrow ab - a'b' = N(a'k + b'h + hkN)$

PROPRIETA': (dim come prima passando da $\mathbb{Z}$) $\rightarrow$ è monoide commutativo

1. **associativa**: $\forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_N \quad (\overline{a} * \overline{b}) * \overline{c} = \overline{a} * (\overline{b} * \overline{c})$
2. **commutativa**: $\forall \overline{a}, \overline{b} \in \mathbb{Z}_N \quad \overline{a} * \overline{b} = \overline{b} * \overline{a}$
3. **elemento neutro**: $\forall \overline{a} \in \mathbb{Z}_N \quad \overline{a} * \overline{1} = \overline{a}$

Inoltre vale la proprietà:

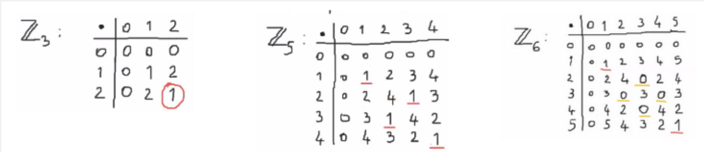
- **distributiva**: $\forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_N \quad (\overline{a} + \overline{b}) * \overline{c} = \overline{a} * \overline{c} + \overline{b} * \overline{c}$

  ($\Rightarrow \mathbb{Z}_N$ è quindi anello communtativo unitario come $\mathbb{Z}$)

  facoltativo

Es.

- ▾ !!Tabelle moltiplicative (-1 invertibile + zeri e uni)



$\mathbb{Z}_3$:

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_5$:

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_6$:

•	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- $\mathbb{Z}_3$: In questo caso 2 è invertibile e il suo inverso è 2
- $\mathbb{Z}_5$: 1234 invertibili con 1 3 2 4
- $\mathbb{Z}_7$: 1 e 5 invertibili + 0 strano (hanno divisori non banali con 6)

Divisore di 0 e invertibile

DIVISORI DI 0: $\overline{a} \in \mathbb{Z}_N, \overline{a} \neq \overline{0}$ si dice divisore di 0 se $\exists \overline{b} \in \mathbb{Z}_N, \overline{b} \neq \overline{0}$ tale che:

$$\overline{a} * \overline{b} = \overline{0}$$

TEOREMA: Sia $\overline{a} \in \mathbb{Z}_N, \overline{a} \neq \overline{0}$

1. $\overline{a}$ è invertibile ($\overline{a} * \overline{x} = \overline{1}$) <=> MCD(a,N)=1
2. $\overline{a}$ è divisore di zero ($\overline{a} * \overline{x} = \overline{0}$) <=> MCD(a,N)>1

COROL: p è primo allora $\forall a \in \mathbb{Z}_p, \overline{a} \neq \overline{0} \quad \exists \overline{b} \in \mathbb{Z}_p | \overline{a} * \overline{b} = \overline{1}$

A Dim imp:

- Dim p.1 (bezout)

PARTO DA MCD (uso Bezout e arrivo a prodotto (dimostrando entrambe))

Sia MCD(a,N)=1 per Bezout ax+Ny=1 <=>ax-1=-Ny

<=> $\overline{a} * \overline{x} = \overline{1}$ <=> è invertibile

- Dim p.2 (a=dh e N=dk e inverso per assurdo)

PARTE 1

Sia d=MCD(a,N)>1, allora $\exists h, k \in \mathbb{Z} | a = dh, N = dk$ (con 0<k<N)
(esiste fattore per arrivare ad *a e N)*

Considero il prodotto ak=dhk=h(dk)=hN (per MCD su)

allora $\overline{a} * \overline{k} = \overline{0}$ (con k≠0 (per su)⇒ divisore 0)

PARTE 2 (per assurdo)

⇒ $\overline{a}$ è divisore di zero.
Viceversa, se $\overline{a}$ è divisore, allora non è invertibile, infatti, se lo fosse, esisterebbe $\overline{x}$ t.c.
$\overline{a} \cdot \overline{x} = \overline{1} \Rightarrow \overline{a} \cdot \overline{x} \cdot \overline{k} = \overline{k} \Rightarrow (\overline{a} \cdot \overline{k}) \cdot \overline{x} = \overline{k} \Rightarrow \overline{0} = \overline{k}$ ASSURDO
⇒ $\overline{a}$ non è invertibile ⇒ MCD(a,N) ≠ 1 ⇒ > 1. ☒

<=ak=0 xchè divisore di zero (ma k=0 e k≠0 per definizione)

Es.

- $\mathbb{Z}_{79}$ (!!per trovare inverso uso Bezout+ come si fa)

Inverso di 22 esiste ma chi è.

DEVO TROVARE MCD

79=22*3+13

22=13*1+9

13=9*1+4

9=4*2+1

4=1*4+0

ESEGUO AL CONTRARIO (in base a resto)

1=9-2*4

4=13-9*4

9=22-13*1

13=79-22*3

SOSTITUISCO (tutto deve essere uguale a 1)

$1 = 9 - 2 \cdot (13 - 9) = 3 \cdot 9 - 2 \cdot 13$
$= 3 \cdot (22 - 13) - 2 \cdot 13 = 3 \cdot 22 - 5 \cdot 13$
$= 3 \cdot 22 - 5 \cdot (79 - 3 \cdot 22) = 18 \cdot 22 - 5 \cdot 79$
$1 = 79 \cdot (-5) + 22 \cdot 18$

22*18=Nq+1 $\Rightarrow 22 * 18 \equiv 1 \mod 79 => \overline{22} * \overline{18} = \overline{1}$

- $\mathbb{Z}_{27}$

a=10 MCD(10,27)=1

$$27 = 10 \cdot 2 + 7$$
$$10 = 7 \cdot 1 + 3$$
$$7 = 3 \cdot 2 + 1$$

$$1 = 7 - 3 \cdot 2$$
$$3 = 10 - 7 \cdot 1$$
$$2 = 27 - 10 \cdot 2$$

$$1 = 7 - (10 - 7 \cdot 1) \cdot 2 = -2 \cdot 10 + 3 \cdot 7$$
$$= -2 \cdot 10 + (27 - 10 \cdot 2) \cdot 3 = 3 \cdot 27 - 8 \cdot 10$$

RISULTATO

$\overline{-8} = \overline{27 - 8} = \overline{19}$

Congruenze lineari

> **OSS:** L'equazione $ax \equiv b \mod N$ (x incognita) ha soluzioni
> sse. ha soluzioni (($(x, k) \in \mathbb{Z} \times \mathbb{Z}$ che soddisfi) $ax - kN = b$

> **PROP:** L'equazione $ax \equiv b \mod N$ ha soluzioni sse. MCD(a,N)|b

💡 Es.

▾ "Dim" osservazione

LATO 1

Se $\exists(x,k) \in \mathbb{Z} \times \mathbb{Z} | ax - kN = b \Rightarrow ax - b = KN \Rightarrow ax \equiv b \mod N$

LATO 2

Viceversa se $ax \equiv b \mod N \Rightarrow \exists k \in \mathbb{Z} | ax - b = kN \Rightarrow ax - kN = b$

▾ Esempio 1 (come scrivere insieme soluzioni)

12x=10 mod 25 o 12x+25y=10 mcd(12,25)=1

BEZOUT

25-12*2=1 25*1 -2*12=1 (x10) → **12**(-20)**+25***10 =**10**

⇒ a=-20=5

SOLUZIONI

Insieme soluzioni $S = \{n \in \mathbb{N} | n \equiv 5 \mod 25\} = [5]_{25}$

- 9x=14 mod 24 MCD(9,24)=3 ⇒ 3 non divide 14 ⇒ NO SOLUZIONI

SCHEMA RIASSUNTIVO: $ax \equiv b \mod N$

1. Si calcola d=MCD(a,N)
   - Se non è vero che d|b allora ci fermiamo ⇒ non ci sono soluzioni
2. In base a d procedo
   - Se d=1 basta trovare $c \in \mathbb{Z} | \overline{a} \cdot \overline{c} = \overline{1}$ (con Bezout) e moltiplico per b (trovo inversa e moltiplico per b)
   - ‼Se d>1 bisogna dividere (*) per d ⇒ $a/d \cdot x \equiv b/d \mod N/d$ poi rieseguo punto precedente

Invertibili e chiusura a moltiplicazione

INSIEME INVERTIBILI $\mathbb{Z}_N^\times$: il sottoinsieme di $\mathbb{Z}_N$ dato dagli elementi invertibili.

OSS: E' sott. proprio, non nullo di $\mathbb{Z}_N$ $(0 \notin \mathbb{Z}_N^\times,\ 1 \in \mathbb{Z}_N^\times\ \forall N > 2)$

PROP: se $\overline{a}, \overline{b}$ sono invertibili in $\mathbb{Z}_N \Rightarrow$

$\overline{ab}$ è invertibile [$\mathbb{Z}_N^\times$ è **chiuso rispetto alla moltiplicazione** (oper. interna)]

▾ Infatti (associativa)

$(\overline{b^{-1}} * \overline{a^{-1}}) * (\overline{a} * \overline{b}) = \overline{b^{-1}} * (\overline{a^{-1}} * \overline{a}) * \overline{b} = \overline{b^{-1}} * \overline{b} = 1$

Funzione di eulero

FUNZIONE EULERO: Si dice ϕ di Eulero la funzione $\phi : \mathbb{N} \backslash \{0\} \to \mathbb{N}$ tale che:

$$\phi(n) = |\{r \in \mathbb{N} | 1 \leq r \leq n \wedge MCD(r,n) = 1\}| = |\mathbb{Z}_N^\times|$$

(cardinalità invertibili o coprimi minori di n)

OSS 1: Se n è primo $\phi(n) = n - 1$ (‼conta 1)

PROP 2: Se $p \in \mathbb{N}$ è primo, $k \in \mathbb{N} \backslash \{0\} \Rightarrow \phi(p^k) = p^{k-1}(p-1) = p^k - p^{k-1}$

🅰 Dim:

▾ Trovo i non coprimi (che sono multipli di $p \Rightarrow p^{k-1}$)

DIVISORI SONO POTENZA P

Sia $1 \leq r \leq p^k$ e MCD (r, p^k)≠1, allora $\exists j 1 \leq j \leq k | MCD(r, p^k) = p^j$

PRENDO TUTTI I MULTIPLI DI P MINORI DI K

Quindi p*1 , p*2,..., p*p, (p+1)*p,..., p^k=p^k-1*p

- Prendo quindi p^{k-1} valori =|non coprimi|

TROVO CARDINALITA' COPRIMI (per differenza)

Gli elementi di $|\mathbb{Z}_N^\times| = p^k - p^{k-1} = p^{k-1}(p-1)$

LEMMA 3: Siano $m, n \in \mathbb{N} \backslash \{0\}$ t.c. MCD(m,n)=1. Allora

$f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n \qquad [a]_{mn} \to ([a]_m, [a]_n)$

è una biezione che preserva i prodotti (cioè $f([a]_{mn} * [b]_{mn}) = f([a]_{mn}) * f([a]_{mn})$.

LEMMA 4: f(come sopra) si restringe ad una $f : \mathbb{Z}_{mn}^{\times} \to \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$

COROL: $|\mathbb{Z}_{mn}^{\times}| = |\mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}| = |\mathbb{Z}_m^{\times}| * |\mathbb{Z}_n^{\times}|$

PROP 5: Siano $m, n \in \mathbb{N} \backslash \{0\}$ con MCD(m,n)=1. allora $\phi(m,n) = \phi(m) * \phi(n)$

Dim:

- L3-ben definita (a-b=kmn)

$f(a) - f(b) =$ $\qquad a = b \bmod mn$

$([a]_m, [a]_n) - ([b]_m, [b]_n) =$ $\qquad a - b = k\,mn$

$([a-b]_m, [a-b]_n) =$

$([kmn]_m, [kmn]_n) = (0,0) = 0$

$\hookrightarrow f(a) = f(b)$

- L3-preserva i prodotti (omomorfismo)

$f([a]_{mn}) \cdot f([a]_{mn}) =$

$([a]_m, [a]_n) \cdot ([b]_m, [b]_n) =$

$([ab]_m, [ab]_n) \overset{def}{=}$

$f([ab]_{mn}) = f([a]_{mn} \cdot [b]_{mn})$

- L3-Biettiva (a-b mod m n ⇒ a-b mod mn | stessa cardinalità)

INIETTIVA (ricavo differenza a-b in m e n ⇒ a=b mod mn)

Siano $[a]_{mn}, [b]_{mn}$ tali che f([a])=f([b]) ovvero **([a]m, [a]n)=([b]m, [b]n)**

Allora $\begin{cases} \exists h \in \mathbb{Z} | a - b = hm \\ \exists h' \in \mathbb{Z} | a - b = h'n \end{cases}$

M DIVIDE H' ⇒ m*k=h' e sostituisco

quindi hm=h'n, ma MCD (m,n)=1⇒ m|h' cioè $\exists k \in \; |h' = km$

allora $a - b = h'n = kmn \Rightarrow [a]_{mn} = [b]_{mn}$

SURIETTIVA (stessa cardinalità e iniettiva ⇒ suriettiva)

$|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m| * |\mathbb{Z}_n| = |\mathbb{Z}_m \times \mathbb{Z}_n|$

E' iniettiva su due A, B di stessa cardinalità ⇒ è suriettiva ⇒ è biettiva

- L4-mn→m-n (invertibili) e viceversa (passando da cartesiano) manda inv in inv

PASSO 1 (invert. cartesiano sse. invert. elementi)

1) gli invertibili in $\mathbb{Z}_m \times \mathbb{Z}_n$ sono del tipo $(\bar{a}, \bar{a}')$ dove $\bar{a} \in \mathbb{Z}_m^{\times}$, $\bar{a}' \in \mathbb{Z}_n^{\times}$ infatti se $(\bar{a}, \bar{a}')$ è invertibile $\exists (\bar{b}, \bar{b}') \in \mathbb{Z}_m \times \mathbb{Z}_n$ t.c. $(\bar{a}, \bar{a}') \cdot (\bar{b}, \bar{b}') = (\bar{1}, \bar{1})$ cioè $\begin{cases} \bar{a} \cdot \bar{b} = \bar{1} \text{ in } \mathbb{Z}_m \\ \bar{a}' \cdot \bar{b}' = \bar{1} \text{ in } \mathbb{Z}_n \end{cases}$
Perciò $(\mathbb{Z}_m \times \mathbb{Z}_n)^{\times} = \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$.

PASSO 2 ([a]mn invert. ⇒ [a]m e [a]n invert.)

2) Se $\bar{a} \in \mathbb{Z}_{mn}^{\times}$ allora $\exists \bar{b} \in \mathbb{Z}_{mn}^{\times}$ t.c. $\bar{a} \cdot \bar{b} = \bar{1}$ in $\mathbb{Z}_{mn}$, ma allora $f(\bar{a} \cdot \bar{b}) = f(\bar{1}) = (\bar{1}, \bar{1})$
Poiché f preserva i prodotti $f(\bar{a} \cdot \bar{b}) = f(\bar{a}) \cdot f(\bar{b}) = (\underset{\text{in } \mathbb{Z}_m}{\bar{a}}, \underset{\text{in } \mathbb{Z}_n}{\bar{a}}) \cdot (\bar{b}, \bar{b}) = (\bar{1}, \bar{1})$
ma allora $\begin{cases} \bar{a} \cdot \bar{b} = \bar{1} \text{ in } \mathbb{Z}_m \\ \bar{a} \cdot \bar{b} = \bar{1} \text{ in } \mathbb{Z}_n \end{cases} \Rightarrow \bar{a} \in \mathbb{Z}_m^{\times}$ e $\bar{a} \in \mathbb{Z}_n^{\times}$. (Invertibili vanno in invertibili

passando da f(a*b)=f(1)=(1,1) mantiene prodotti

PASSO 3 inverso passo 2

Viceversa, sia $(\bar{a}, \bar{a}') \in \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$, vogliamo mostrare che $f^{-1}(\bar{a}, \bar{a}')$ è invertibile
Sia $(\bar{b}, \bar{b}')$ l'inverso di $(\bar{a}, \bar{a}')$, cioè $(\bar{a}, \bar{a}')(\bar{b}, \bar{b}') = (\bar{1}, \bar{1})$.
Ora $f^{-1}(\bar{a}, \bar{a}') \cdot f^{-1}(\bar{b}, \bar{b}') = f^{-1} f (f^{-1}(\bar{a}, \bar{a}') \cdot f^{-1}(\bar{b}, \bar{b}')) = f^{-1}(f f^{-1}(\bar{a}, \bar{a}') \cdot f f^{-1}(\bar{b}, \bar{b}')) =$
$= f^{-1}((\bar{a}, \bar{a}') \cdot (\bar{b}, \bar{b}')) = f^{-1}((\bar{1}, \bar{1})) = \bar{1}$.

Quindi $f^{-1}(\bar{a}, \bar{a}')$ è invertibile $\boxtimes$

PROP 6: usare la fattorizzazione in prodotti primi per calcolare $\phi(n) \forall n \in \mathbb{N} \backslash \{0\}$

Sia $n = p_1^{e_1} * p_2^{e_2} * ... * p_r^{e_r}$ Allora $\phi(n) = \prod_{i=1}^{r} [p_i^{e_i - 1} * (p_i - 1)]$

Teorema di eulero

> **TEOREMA DI EULERO** (dell'aritmetrica modulare): Sia $a \in \mathbb{Z} | MCD(a, N) = 1$
> Allora $a^{\phi(n)} \equiv 1 \mod N$ (‼️vedo dim in gruppi)

> **PICCOLO TEOREMA DI FERMAT**: Sia $a \in \mathbb{Z}$, p primo.
> Allora $a^{p-1} \equiv 1 \mod p$

💡 Es.

▾ 5^864735 mod 42

Esempi di applicazione.

1) Calcolare il resto della divisione di 5^{864735} per 42.

$\phi(42) = (2-1)(3-1)(7-1) = 12$

$864735 = 72061 \cdot 12 + 3$

$5^3 \mod 42 \qquad 125 \% 42 = -1 = 41$

$864735 = 12 \cdot \underbrace{72061}_{q} + \underbrace{3}_{r}$ ma allora $5^{864735} = 5^{12 \cdot 72061 + 3} = (5^{12})^{72061} \cdot 5^3$

in mod 42 → 5^12=1

▾ Resto divisione 30 di 7^4106+11^2171

Entrambi sono coprimi

$4106 = 8 \cdot 513 + 2 \qquad 2171 = 8 \cdot 271 + 3$

$[7^{4106}]_{30} = [7^8]_{30}^{513} \cdot [7^2]_{30} = [1]_{30}^{513} \cdot [49]_{30} = [19]_{30}$

$[11^{2171}]_{30} = [11^8]_{30}^{271} \cdot [11^3]_{30} = [1]_{30}^{271} \cdot [1331]_{30} = [11]_{30}$

$[19]_{30} + [11]_{30} = [0]_{30}$

$7^{4106} + 11^{2171} \equiv 19 + 11 \equiv 30 \equiv 0 \mod 30$

▾ Resto 6^755 mod 62 (!!controllo se coprimi→ non vale altrimenti)

3) Calcolare il resto della divisione di 6^{755} per 62.

Problema: $MCD(6, 62) = 2 \neq 1$ Però: $6 = 2 \cdot 3$

$3^{755} \cdot 2^{755}$

$\phi(62) = (31-1)(2-1) = 30$

$755 \% 30 = 5$

$3^5 \% 62 = 243 \mod 62 = -5 = 57$

$2^6 = 2$

$2^{755} = 2^{750} \cdot 2^5 \mod 62$

$[2^6]^{125} \cdot 2^5 \mod 62$

$[2^{130}]_{62} = [2^6]^{21} \cdot 2^4$

$2^{25} = [2^6]^4 \cdot 2$

$2^5 = 32$

$32 \cdot 57 =$

26

Criteri di divisibilità

> Sia $n \in \mathbb{N}$ la cui notazione in base 10 è $n = c_r c_{r-1} ... c_0$ sulla base di ciò ricaviamo i criteri seguenti:
>
> 1. $2 | n \quad sse. \quad 2 | c_0$ (in quanto [10]_2=[0]_2)
> 2. $5 | n \quad sse. \quad 5 | c_0$
> 3. $3 | n \quad sse. \quad 3 | (c_0 + c_1 + ... + c_r)$ (in quanto [10]_3= [1]_3)
> 4. $9 | n \quad sse. \quad 9 | (c_0 + c_1 + ... + c_r)$
> 5. $11 | n \quad sse. \quad 11 | (c_0 - c_1 + ... + (-1)^r c_r)$ (segni alterni 1 -1 resto)

- Infatti
  1. $\forall k \geq 1 \;\; 2|10^k \;\; \Rightarrow [10]_2 = [0]_2$
     Quindi $[n]_2 = [c_0]_2 + [c_1]_2[0]_2 + ... + [c_r]_2[0]_2 = [c_0]_2$
  2. "
  3. $\forall k \geq 1 \;\; 10^k \mod 3 = 1 \;\; \Rightarrow [10]_3 = [1]_3$
     Quindi $[n]_3 = [c_0]_3 + [c_1]_3[1]_3 + ... + [c_r]_3[1]_3 = [c_0]_3 + ... + [c_r]_3$
  4. "
  5. infatti $[10]_{11} = [-1]_{11}$ $\quad [100]_{11} = [1]_{11}$ $\rightarrow$ così per tutti
     (IMMAGINE EXTRA)

$$[n]_{11} = [c_0 + c_1 \cdot 10 + \ldots + c_r \cdot 10^r]_{11} = [c_0]_{11} + [c_1]_{11} \cdot \underset{[-1]_{11}}{\underset{\shortparallel}{[10]_{11}}} + \ldots + [c_r]_{11} \cdot \underset{[(-1)^r]_{11}}{\underset{\shortparallel}{[10^r]_{11}}} = [c_0] - [c_1] + \ldots + (-1)^r [c_r]$$

- Gruppi

Gruppi

> **DEF:** Sia $(A, *)$ una coppia formata da un insieme A e una operazione binaria su A:
> $$* : A \times A \to A \qquad (a_1, a_2) \to a_1 * a_2$$ (‼️devo contr. ben definita e interna)

> **DEF:**
> 1. Se $*$ è associativa, $(A, *)$ si dice **semigruppo;**
> 2. Se l'operazioni $*$ è associativa ed esiste un elemento neutro $e \in A$allora si dice
> $(A, *, e)$ si dice **monoide;**
> 3. Se $(A, *, e)$ è un monoide e $\forall a \in A \exists b \in A | a * b = e$ (inverso),
> $(A, *, e)$ si dice **gruppo;**
> 4. Se $(A, *, e)$ è un gruppo e l'operazione $*$ è commutativa, $(A, *, e)$ si dice **gruppo alebiano.**

📢 Notazioni importanti

- Un gruppo con $(G, *, e)$ può essere indicato solo con $(G, *)$.
- in questa notazione ‼️le potenze sono n volte operazione
  - es. in $(\mathbb{Z}, +, 0)$ $\qquad x^3 = x + x + x = 3x$

> Dati 2 gruppi $(G, *, e)$ e $(H, \square, i)$ allora $G \times H$ è ancora un gruppo.
> (faccio componente per componente (inverso,...))

💡 Esempi compatti ma importanti

- Quali insiemi che conosciamo già
  1. (N, +, 0) ⇒**monoide (commutativo)**
  2. (Z/Q/R, +, 0) sono **gruppi abeliani**
  3. (N\{0}, +) è **semigruppo** (manca neutro)
  4. $(P(X), \cap, X)$, è assoc., c'è el. neutro X, no inverso **monoide comm.**
  5. $(F_x, \circ)$ (‼️monoide (è ass., neutro (Id) ma non inverso)// se biettive→gruppo)
  6. $X^{<\mathbb{N}}$ e concatenzaione (**monoide** (ass., neutro, ma non inverso))
  7. $(\mathbb{Z}_N, +)$ **gruppo abeliano** (è ass., commutativa, netutro (0), inverso (-n))
- $(\mathbb{N} \backslash \mathbb{Z} \backslash \mathbb{Z}_N \backslash \mathbb{Q}, \cdot, 1)$ monoide (0 non inver) $(\mathbb{Q}^\times \backslash \mathbb{R}^\times \backslash \mathbb{Z}^\times \backslash \mathbb{Z}_N^\times, \cdot, 1)$ ‼️gruppo ab.

  DEFINIZIONI INVERTIBILI
  - $(\mathbb{Q}^\times = \mathbb{Q} \backslash \{0\}, \cdot, 1)$ è gruppo $\qquad \rightarrow$ Stessa cosa per **R**
  - $Z^\times = \{\pm 1\}$
  - $N^\times = \{1\}$ $\qquad \rightarrow$ insiemi banale
  - $\mathbb{Z}_N^\times$ insiemi invertibili

Proprietà e asimmetria

> **OSS:** neutro e inverso sono di per sè asimmetrici (se * non è commutativa → si può parlare di elemento neutro e inverso a sinistra o a destra)
> + ma con "elemento neutro"/"inverso" si intende da entrambi i lati

💡 Es.

- $(\mathbb{Z}, -)$ ha elemento neutro solo a destra⇒non ha "elemento neutro"(=da entrambi)
- In $(F_{\mathbb{Z}}, \circ)$

  Ovverso insieme di funzioni da $\mathbb{Z} \to \mathbb{Z}$

  Se prendo per esempio $f : \mathbb{Z} \to \mathbb{Z}$ n→ 2n

  - ha inverso sinistro $g : \mathbb{Z} \to \mathbb{Z}$ $\quad n \to \begin{cases} n/2 \; se \; n \; pari \\ 0 \; se \; n \; dispari \end{cases}$
  - ma non è anche inverso destro

PROP: Sia (G,*) (‼non necessariamente gruppo):

1. Se esiste un elemento neutro per * allora è unico
2. Se (G, *, e) è monoide ⇒ se $g \in G$ ha inverso, allora l'inverso è unico
3. Se $g, h \in G$ hanno inversi, allora $(g * h)^{-1} = h^{-1} * g^{-1}$ (inversi scamb. di ordine)
4. Se $g \in G$ ha inverso, allora $\forall h1, h2 \in G : i) g * h1 = g * h2 <=> h1 = h2$
   $i) h1 * g = h2 * g <=> h1 = h2$

COROL: se (G,*, e) è un gruppo, le proprietà 2)3)4) valgono per ogni scelta di g, h

Dim:

- 1)Siano e, e' due elementi neutri: e=e*e' e'=e*e' (in quanto neutri)⇒ e=e'
- 2)Siano h, h' due inversi di g (g*h=h*g=e, g*h'=h'*g=e, uso associatività)

  Allora h=h*e = h*(g*h')=(h*g)*h' = e*h'=h'
- 3) $(h^{-1} * g^{-1}) * (g * h) = e$ ⇒ associat. elimino in mezzo +viceversa
- 4) A) $g * h1 = g * h2 <=> h1 = h2$ (moltiplico a sinistra per g^{-1}) +viceversa

Es. "moltiplicando o dividendo ambo i membri di eq. n≠0 si ottiene una eq.equivalente"
$\leftarrow (R^{\times} = R - \{0\}, *, 1)$ è un gruppo quindi valgono le leggi di cancellazione

Sottogruppi e in Z

SOTTOGRUPPO (H≤G): Sia (G, *, e) un gruppo e $H \subseteq G$ t.c. (H, *, e) è un gruppo.

(‼deve essere stesso * ed *e*)

PROP 1:

1. $e \in H$ (elemento neutro) ⇒ un sottogruppo non è mai vuoto
2. $\forall h, h' \in H \;\; h * h' \in H$ (operazione interna \ chiusa rispetto a *)
3. $\forall h \in H \;\; h^{-1} \in H$ (inverso di ognuno è interno)

PROP 2: Sia (G,*, e) un gruppo e $\emptyset \neq H \subseteq G$, allora: (criterio sottogruppo)

H è sottogruppo di G sse. $\forall h1, h2 \in H \;\; h1 * h2^{-1} \in H$

Dim:

- ⇒ è ovvia
- <= (divido in 3 parti inverso prima)

  Poichè $H \neq \emptyset \;\; \exists h \in H$

  1. Applicando h1=h2=h $\quad h * h^{-1} = e \Rightarrow e \in H$ **(elemento neutro)**
     - Se un solo elemento finito qui
  2. h1=e h2=h ottengo $e * h^{-1} = h^{-1} \in H$ **(inverso)**
  3. h1=h h2=$(h')^{-1}$ con h, h' in H $\quad h * ((h')^{-1})^{-1} = h * h' \in H$ **(interna)**

Es.

- Non esempi (imp il 3)

  Non esempi: 1) $(\mathbb{Z}, +, 0)$ $\quad S = \{1, 2, 3\}$ non è un sottogruppo, perché $0 \notin S$.
  $\mathbb{Z} \setminus \{0\}$ " per lo stesso motivo.

  2) $(\mathbb{N}, +, 0)$ non è un sottogruppo di $(\mathbb{Z}, +, 0)$ ... mancano gli inversi.

  3) $(S_3, \circ, id_{I_3})$ $\quad H = \{id, (12), (13)\}$ non è un sottogruppo perché non è chiuso rispetto all'operazione: $(12) \circ (13) = (1\,3\,2) \notin H$

- Esempi
  1. per ogni gruppo (G,*,e) ci sono 2 sottogruppi banali: {e}, G
  2. Gruppi

$$(\mathbb{Z},+,0) \leq (\mathbb{Q},+,0) \leq (\mathbb{R},+,0)$$

$$3)\ (\{+1,-1\},\cdot,1) \leq (\mathbb{Q}^\times,\cdot,1) \leq (\mathbb{R}^\times,\cdot,1)$$

PIU' DIFFICILE (operazione su permutazione → pari)

4) $(S_n,\circ,id_{I_n})$ possiamo considerare il sottoinsieme $A_n=\{\sigma\in S_n \mid \sigma \text{ è pari}\}$
È un sottogruppo ?

PERCHE' (id=0 scambi)

Sì, perché : 1) esiste l'elemento neutro : $id \in A_n$
2) $\forall \sigma\in A_n \Rightarrow \sigma^{-1}\in A_n$
3) $\forall \sigma,\tau\in A_n \Rightarrow \sigma\circ\tau \in A_n$ (pari + pari = pari)

SOTTOGRUPPI DI Z (teorema): i sottogruppi di $(\mathbb{Z},+0)$ sono tutti e soli:

$$n\mathbb{Z}=\{m\in\mathbb{Z}|m=n\cdot k,\ \ con\ \ k\in\mathbb{Z}\}$$

A Dim

▾ 2 $\subseteq$ (n minimo e non esiste più piccolo)

CASO BANALE ($0\mathbb{Z}=\{0\}$)

Sia ora H sottogruppo di $(\mathbb{Z},+,0)$. Se $H=\{0\}$ allora $H=0\cdot\mathbb{Z}$

$n\mathbb{Z}\subseteq H$ **(pos e neg→ min pos e gruppo ⇒ cvd)**

Se invece $H\neq\{0\}$, allora $\exists h\in\mathbb{Z}$ tale che $h\neq 0$ e $h\in H$. Inoltre, poiché H è un gruppo, $-h\in H$, quindi H ha almeno un elemento positivo (h o $-h$).
Siano $H^+=H\cap(\mathbb{N}\setminus\{0\})=\{h\in H \mid h>0\}\neq\emptyset$ e $n=\min H^+$.
Poiché H gruppo ed $n\in H \Rightarrow n\mathbb{Z}\subseteq H$ sono i multipli di n, che sta in H

$H\subseteq n\mathbb{Z}$ **(divisione euclidea →resto tra min h+ e 0⇒0 ⇒ qn)**

Sia ora $h\in H$. Per la divisione euclidea, $\exists q,r\in\mathbb{Z}$, $0\leq r<n$ tali che:
$h=q\cdot n+r$ ovvero $r=\underbrace{h}_{\in H}-\underbrace{qn}_{\in H}$
Perciò $r\in H$. Ma poiché $0\leq r<n$ ed n è il minimo tra gli elementi positivi di H, non può che essere $r=0 \Rightarrow h=qn\in n\mathbb{Z}$.
Il ragionamento vale $\forall h\in H \Rightarrow H\subseteq n\mathbb{Z} \Rightarrow H=n\mathbb{Z}$. ⊠

Omomorfismi + nomenclatura

➕ OMOMORFISMO⇒ funzione tra strutture con la stessa forma (‼non solo ai gruppi)

OMOMORFISMO: Siano $(G,\cdot),(H,*)$ due gruppi. Un omomorfismo da G a H è funzione

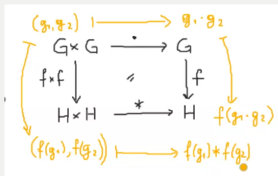
$$f:G\to H \qquad t.c. \qquad \forall g_1,g_2\in G \quad f(g_1\cdot g_2)=f(g_1)*f(g_2)$$

NOMENCLATURA:

1. **monomorfismo**: se è iniettivo
2. **epimorfismo**: se è suriettivo
3. **isomorfismo**: se è biettivo
4. **endomorfismo**: se la strut. di partenza è uguale a quella di arrivo (‼anche operaz.)
5. **automorfismo**: se è endomorfismo, biettivo

💡 Esempi chiarificativi ma compattati imp

▾ Immagine esplicativa



▾ -

▼ 1-2 (funzione costante a el. neutro) (identità →banale)

ESERCIZIO 1

1) $(G,\cdot)$, $(H,*)$. Sia e_H l'elemento neutro di H.

$f: G \longrightarrow H$, $g \longmapsto e_H$ costante è un omomorfismo :

$\forall g \in G \; f(g)=e_H$

2 PERCORSI:

- $f(g_1 \cdot g_2) = e_H$ (in quanto f(g)=eH)
- f(g_1)*f(g_2)=e_H*e_H=e_H

ESERCIZIO 2

$(G,\cdot)$ gruppo . $id_G : G \longrightarrow G$ è un omomorfismo

E' sempre g1*g2.

▼ 3-4(x→nx, n fisso <=distributiva) (x→x^2 in $(\mathbb{R}^\times,\cdot)$)

ESERCIZIO 3

3) $(\mathbb{Z},+)$, $n \in \mathbb{N}$ fissato. $f: \mathbb{Z} \longrightarrow \mathbb{Z}$, $x \longmapsto n \cdot x$ è un omomorfismo

$$f(x_1+x_2) = n\cdot(x_1+x_2) \underset{\text{propr. distributiva}}{=} nx_1 + nx_2 = f(x_1)+f(x_2)$$

ESERCIZIO 4

4) $(\mathbb{R}^\times,\cdot)$ $f: \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto x^2$ è un omomorfismo da $(\mathbb{R}^\times,\cdot)$ in sé stesso perché $f(x\cdot y) = (xy)^2 = x^2y^2 = f(x)f(y)$

▼ 5 (x→x^2 in $(\mathbb{R}^\times,+)$ <= non vale)

ESERCIZIO 5

$(\mathbb{R},+)$ $f: \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto x^2$ non è un omomorfismo da $(\mathbb{R},+)$ in sé stesso

Per esempio: f(1)+f(2)=1+4 ≠ 9=f(1+2) cvd

▼ 6-7 (f(x)=2^x →$(\mathbb{R},+)$ a $(\mathbb{R}^\times,\cdot)$) (viceversa con dom. ridotto)

ESERCIZIO 6

5) $(\mathbb{R},+) \xrightarrow{f} (\mathbb{R}^\times,\cdot)$, $x \longmapsto 2^x$ è un omomorfismo perché $\forall x,y \in \mathbb{R}$ $f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x)\cdot f(y)$

ESERCIZIO 7 (proprietà logaritmo)

$((0,+\infty),\cdot) - f^{-1} - > (\mathbb{R},+)$ $\quad x - f^{-1} - > log_2(x)$

6) $((0,+\infty),\cdot) \xrightarrow{f^{-1}} (\mathbb{R},+)$, $x \longmapsto \log_2 x$ è un omomorfismo perché $\forall x,y \in (0,+\infty)$

$$f^{-1}(x\cdot y) = \log_2 xy \underset{\text{proprietà dei logaritmi}}{=} \log_2 x + \log_2 y = f^{-1}(x) + f^{-1}(y)$$

▼ 8 $((S_n,\circ) - sg > (\{\pm1\},\cdot)$ da il segno di parità)

ESEMPIO 8 (· è una moltiplicazione)

7) $n \in \mathbb{N}$ fissato $(S_n,\circ) \xrightarrow{sg} (\{\pm1\},\cdot)$, $\sigma \longmapsto sg(\sigma)$ $\quad sg(\sigma) = \begin{cases} 1 & \text{se } \sigma \text{ è pari} \\ -1 & \text{se } \sigma \text{ è dispari} \end{cases}$

Siano $\sigma,\tau \in S_n$ $\quad sg(\sigma\circ\tau) = ?$

1) Se σ,τ pari $\sigma\circ\tau$ è pari $sg(\sigma\circ\tau)=1$
2) Se σ,τ dispari $\sigma\circ\tau$ è pari $sg(\sigma\circ\tau)=1$
3) Se σ,τ sono una pari e una dispari allora $\sigma\circ\tau$ dispari $\Rightarrow sg(\sigma\circ\tau)=-1$

$$\left.\begin{array}{l} 1)\; sg(\sigma)\cdot sg(\tau) = 1\cdot1 = 1 \\ 2)\; sg(\sigma)\cdot sg(\tau) = (-1)(-1) = 1 \\ 3)\; sg(\sigma)\cdot sg(\tau) = -1\cdot1 = -1 \end{array}\right\}$$ coincidono con i precedenti $\Rightarrow$ sg è un omomorfismo

▼ 9 non esempi

ESEMPIO 9

- Seno

$(\mathbb{R},+) \longrightarrow (\mathbb{R},+)$, $x \longmapsto \sin x$ non è un omomorfismo

Per esempio: $x = \frac{\pi}{2}$, $y = \frac{\pi}{4}$ $\quad \sin x + \sin y = 1 + \frac{1}{\sqrt{2}}$

$\sin(x+y) = \frac{1}{\sqrt{2}}$

- Costante non a elemento neutro

g) $(\mathbb{Z},+) \xrightarrow{f} (\mathbb{Z},+)$ non è un omomorfismo

$x \longmapsto 1$ $x=0,\ y=1$ $f(0+1)=f(1)=1$

$\forall x \in \mathbb{Z}\ f(x)=1$ • $f(0)+f(1)=1+1=2$

▼ $f:(0,+\infty),\cdot \to (\mathbb{R},+)$ è un isomorfismo (ovvero sono isomorfi →stessa cosa)

$f:((0,+\infty),\cdot) \longrightarrow (\mathbb{R},+)$ è un isomorfismo.

$x \longmapsto \log_2 x$

Proprietà

PROP: f è un omorfismo, allora valgono (‼ altrimenti non omomorfismo) :

1. $f(e_G) = e_H$ (preservano el. neutro)
2. $\forall g \in G \quad f(g)^{-1} = f(g^{-1})$ (preservano inverso)
3. $\forall g \in G, \forall n \in \mathbb{Z}, f(g)^n = f(g^n)$ (preservano potenze)
4. Se G1≤G, allora f(G1)≤H (preservano sottogruppi)
5. Se H1≤H, allora $f^{-1}(H_1) \leq G$ (inverso)

A Dim imp: (specialmente 4-5)

- 1) neutro (cancellazione) f(eG)=f(eG*eG)=f(eG)*f(eG) ⇒ f(eG) è el. neutro =eH
- 2) Inverso eH=f(eG)=$f(g*g^{-1}) = f(g)*f(g^{-1})$ $\Rightarrow f(g^{-1}) = f(g)^{-1}$

▼ 3) Potenze (induttivo)

SE N=0

$g^0 = e_G \quad f(g^0) = f(e_G) = e_H = f(g)^0$

SE N=1

$n=1 \quad f(g^1) = f(g) = f(g)^1$

PASSO INDUTTIVO (con n in zeta c'è lo risparmia ma se voglio es)

hp: $f(g^n) = f(g)^n$

$$f(g^{n+1}) = f(g^n \cdot g) \underset{f\text{ omom.}}{=} f(g^n) * f(g) \underset{\text{hp induttiva}}{=} f(g)^n * f(g) = f(g)^{n+1}$$

▼ 4) - (prop. omomorfismi e porto dentro)

Siano $h_1, h_2 \in f(G_1)$. Dobbiamo mostrare che $h_1 * h_2^{-1} \in f(G_1)$

$h_1 * h_2^{-1} = f(g_1) * f(g_2)^{-1} = f(g_1) * f(g_2^{-1}) = f(g_1 \cdot g_2^{-1}) \Rightarrow h_1 * h_2^{-1} \in f(G_1)$

sta in $f(G_1) \Rightarrow \exists g_1 \in G_1$ t.c. $h_1 = f(g_1)$
(lo stesso per h_2)

▼ 5) Stessa cosa ma al contrario (poi applico f-1)

Siano $g_1, g_2 \in f^{-1}(H_1)$. Allora $\exists h_1, h_2 \in H_1$ t.c. $f(g_1) = h_1$, $f(g_2) = h_2$

$f(g_1 \cdot g_2^{-1}) = f(g_1) * f(g_2^{-1}) = f(g_1) * f(g_2)^{-1} = h_1 * h_2^{-1} \in H_1 \Rightarrow g_1 \cdot g_2^{-1} \in f^{-1}(H_1)$

Kernel

KERNEL(/NUCLEO): dato $f:(G,\cdot) \to (H,*)$ omorfismo, il kernel è:

$$Ker(f) = \{g \in G \ \ t.c. f(g) = e_H\} = f^{-1}(e_H)$$

TEOREMA: f omorfismo è iniettivo sse. $Ker(f) = \{e_G\}$

A Dim:

▼ (iniettiva (immagini ≤1) e assurdo (due immagini puntano a stesso ⇒ a+b^-1=eH))

⇒ **(se iniettivo per definizione ≤1 e deve essere $f(e_G) = e_H$)**

<= **(2 immagini uguali f(g1)=f(g2)⇒ f(g1*g2^-1)=e))**

Dim: "solo se": Sia f iniettivo, allora $|f^{-1}(e_H)| \leq 1$ e poiché $f(e_G) = e_H \Rightarrow Ker(f) = f^{-1}(e_H) = \{e_G\}$.
"se": Sia $Ker(f) = \{e_G\}$ e siano $g_1, g_2 \in G$ tali che $f(g_1) = f(g_2)$. Allora $f(g_1 g_2^{-1}) = f(g_1) * f(g_2^{-1}) =$
$= f(g_1) * f(g_2)^{-1} = f(g_1) * f(g_1)^{-1} = e_H$, quindi $g_1 g_2^{-1} \in Ker(f) \Rightarrow g_1 g_2^{-1} = e_G \Rightarrow g_1 g_2^{-1} g_2 = g_2 \Rightarrow g_1 = g_2$ ☒

Laterali e Lagrange

DEF: $(G,\cdot)$ è un gruppo, H≤G, fissato $g \in G$, si dice:

1. **Laterale sinistro** di H definito da g il sottoinsime:
$$g \cdot H = \{g \cdot h | h \in H\} \subseteq G$$
2. **Laterale destro:** di H definito da g il sottoinsime:

$$H \cdot g = \{h \cdot g | h \in H\} \subseteq G$$

Es.

- $(\mathbb{Z}, +)$ $\underline{H = n\mathbb{Z}}$ fissiamo $k \in \mathbb{Z}$ $\underline{=[k]_n}$

  COMMUTATIVO

  (Laterali destri e sinistri concidono per commutativa)

  LATERALE DESTRO PER ESEMPIO

  $H + k = n\mathbb{Z} + k = \{..., -n + k, k, n + k, 2n + k, ...\}$
  $= \{x \equiv k \mod n | x \in \mathbb{Z}\}$=

  ESEMPIO NUMERICO

  $\underline{n=5}$ $H = 5\mathbb{Z}$ $k=1$ $5\mathbb{Z}+1 = \{ ..., -9, -4, 1, 6, 11, ...\}$

  E' la classe $[1]_5$ (1 modulo 5)

  $k=-3$ $5\mathbb{Z}-3 = \{ ..., -8, -3, 2, 7, ...\} = [-3]_5 = [2]_5$

- $G = (S_3, \circ)$ $H = \{id, (12)\}$ g=(1,2,3) <u>(‼non sottogruppo o simmetrico)</u>

  LATERALE SINISTRO $g \circ H$ → non sottogruppo

  $g \circ H = \{(1, 2, 3) \circ id, (1, 2, 3)(1, 2)\} = \{(1, 2, 3), (1, 3)\}$

  LATERALE DESTRO $H \circ g$ → non sottogruppo

  $g \circ H = \{id \circ (1, 2, 3), (1, 2)(1, 2, 3)\} = \{(1, 2, 3), (2, 3)\}$

PROP: Sia $(G, \cdot)$ è gruppo e H ≤ G. Allora vale: <u>(‼vale anche per lat. destri)</u>

1. $\forall g \in G,\quad f : H- > g \cdot H \quad f(h) = g \cdot h$ <u>è una biezione</u>
2. $\forall g_1, g_2 \in G \quad g_1H = g_2H \quad sse. \quad g_2^{-1}g_1 \in H$
3. i laterali sinistri di H formano una <u>partizione di G.</u>

Dim anche su <u>infiniti</u>:

- 1) Leggi canc. e definizione gH (ovvio)

  INIETTIVA (leggi cancellazione)

  se <u>f(h)=f(h')</u> $g \cdot h = g \cdot h'$ → moltiplico <u>per g^{-1}</u> → <u>h=h'</u>

  SURIETTIVA (per definizione gH)

  se $x \in gH$ allora <u>$\exists h \in H | x = g \cdot h$ =f(h)</u>

- 2) Cancellazione<u>($g_2^{-1}g_1H = H$)</u> e poi <u>xH=H <=> $x \in H$</u>

  PUNTO 0 (cancellazione)

  $g_1H = g_2H \quad >> \quad g_2^{-1}g_1H = H \quad chiamo \;\; g_2^{-1}g_1 = x$

  PUNTO 1 ($xH = H <=> x \in H$)

  - se xH=H prendo <u>h sinistra come $x * e_G = x \in H$</u>
  - <u>se $x \in H$ ovvio</u>

- 3)Non vuoto (H biez), Ricoprim. (eH*g) partizione (assurdo $h_2h_1^{-1}$ →prop.2)

  I LATERALI SONO IN BIEZIONE CON H ⇒ NON VUOTI

  - H è un sottogruppo quindi $e_g \in H$

  RICOPRIMENTO (per $e_G \in H * g$)

  $\forall g \in G, g \in gH$ in quanto $e_G \in H \;\; e \;\; g = g * e_g$

  DISGIUNTI (assurdo →due modi→ esterni per inversi)

  se non disgiunti $\exists g \in g1H \cap g_2H$ ⇒$\exists h_1, h_2 \in H | g = g_1h_1 = g_2h_2$

  <u>(appartiene a entrambi per assurdo ⇒ due modi per scriverlo)</u>

  $\Rightarrow g_2^{-1}g_1h_1 = g_2^{-1}g_2h_2 \quad => \quad g_2^{-1}g_1h_1 = h_2h_1$

  ⇒ per teorema 2 sono uguali

TEOREMA LAGRANGE: Sia $(G, \cdot)$ un gruppo ‼<u>finito</u> e H ≤G e ⇒
⇒ d|n dove |H|=d, |G|=n

Dim:

- Faccio <u>partizioni</u> (s<n) e <u>$|g_iH| = d$ ⇒ n=sd</u>

  PARTIZIONO

  Abbiamo visto (proposizione precedente) che i laterali sinistri di H formano una partizione di G. $G = g_1H \cup .... \cup g_sH$ (e inter. nulla

PER INCLUSIONE ESCLUSIONE (SENZA INTERSEZIONI)

$n = |G| = |g_1H| + ... + |g_sH|$ (per biezione con H e finiti)

$|g_iH| = d \quad \Rightarrow$ **n=d+d+.....+d (n volte)=sd**

Es.

- 1 $(\mathbb{Z}_5, +)$, ha ordine 5 primo $\Rightarrow$ solo sottogruppi banali
- 2 $(S_4, \circ)$ $|S_4| = 4! = 24$ (‼non nec. esiste sottogruppo H per ogni divisore)

  ESEMPIO

  $H_1 = \{id, (1\,2)\} \leq S_4 \quad H_2 = \{id, (123), (132)\} \leq S_4 \quad \dots$

  Per esempio, non ci sono sottogruppi di ordine 8.

Sottogruppi ciclici

SOTTOGRUPPO CICLICO generato da $g \in G$: H= $< g >= \{g^n | n \in \mathbb{Z}\}$

(H è **generato** da g(/g è **generatore** di H))

Dim:

- E' sottogruppo g^{r-s}

  Siano $g^r, g^s \in <g> \Rightarrow g^r \cdot (g^s)^{-1} = g^r \cdot g^{-s} = \underbrace{g\, g \cdots g}_{r \text{ volte}} \cdot \underbrace{g^{-1} g^{-1} \cdots g^{-1}}_{s \text{ volte}} = g^{r-s} \in <g>$

OSS:

1. $(G, \cdot)$ gruppo, $g \in G$ <g> è sempre **abeliano**: $g^r \cdot g^s = g^{r+s} = g^s \cdot g^r$
   a. Anche se non è G (‼)
   b. **quindi** $(H, \cdot)$ non abeliano $\Rightarrow$ non può essere ciclico
2. Un gruppo ciclico può avere **più generatori**

Es.

- $(\mathbb{Z}_5, +) \rightarrow \mathbb{Z}_5 =< \bar{2} >=< \bar{1} >$ (‼generatore gruppo ciclico non è unico)
- $(S_n, \circ)$ non è ciclico per n>2 in quanto non abeliano

Funzione epsilon (ϵ)

FUNZIONE EPSILON: fisso $g \in G$ (gruppo). Epsilon è ‼l'epimorfismo

$\epsilon : (\mathbb{Z}, +) \rightarrow < g > \qquad k \rightarrow g^k$

PROP: qualunque omomorfismo $f : (< g >, \cdot) \rightarrow (H, *)$ è determinato solo da f(g).

"Dim":

- Epsilon è infatti epimorfismo

  OMOMORFISMO (immagine somma è prodotto immagini)

  $\varepsilon(r+s) = g^{r+s} = g^r \cdot g^s = \varepsilon(r) \cdot \varepsilon(s)$

  SURIETTIVO

  $\forall x \in < g > x = g^k$ per qualche $k \in \mathbb{Z}$, ma allora $x = \epsilon(k) \Rightarrow$ suriettiva

- "dim" prop chiarificatrice

  L'immagine di qualunque elemento di G è determinata dall'immagine del generatore (g).
  Infatti se $x \in G \Rightarrow x = g^k$ per qualche $k \in \mathbb{Z}$, quindi:

  $f(x) = f(g^k) = f(g)^k$

‼ f(g) non può essere scelta a piacere

- Es. $f : (G, \cdot) \rightarrow (\mathbb{Z}, +)$ con |G|>0

  SVOLGIMENTO (n=|G| volte somma)

  Allora $n \cdot f(g) = f(g^n) = f(e_G) = 0$

  $\Rightarrow$ f(g)=0 (esiste un solo omorfismo)

  $\Rightarrow$f(g^k)=0^k=0

  L'UNICO OMOMORFISMO E' IL BANALE CHE MANDA TUTTO IN 0

- Metodo quando trovato uno per trovare altri ‼

2. Il calcolo diretto delle potenze $[2]_{11}^k$ mostra che $[2]_{11}$ genera $\mathbb{Z}_{11}^\times$. Dunque i generatori sono le potenze $[2]_{11}^k$ con $\mathrm{MCD}(k, 10) = 1$, ovvero

$$[2]_{11}, \quad [2]_{11}^3 = [8]_{11}, \quad [2]_{11}^7 = [7]_{11}, \quad [2]_{11}^9 = [6]_{11}.$$

Es.

- 3) $(\mathbb{Q}^\times, \cdot)$ -1 ha periodo 2
- $f : (\mathbb{Z}_6, +) \to (\mathbb{Z}_4, +) \quad (\mathbb{Z}_6 =< 1 >)$ ricavare possibili basi

  IN 2 BASI DIVERSE

  Allora $6 \cdot f(\bar{1}) = f(6 \cdot \bar{1}) = f(\bar{0}) = \bar{0}$ → base 6
  $6 \cdot f(\bar{1}) = 4f(\bar{1}) + 2f(\bar{1}) = 2f(\bar{1})$ → base 4

  $\Rightarrow 2 \cdot f(\bar{1}) = \bar{0}$ in $\mathbb{Z}_4 \Rightarrow f(\bar{1})$ può essere $= \bar{0}$
  oppure $= \bar{2}$

OSS A: 2 casi possibili

1. ϵ è anche **iniettiva** ⇒ è un isomorfismo, in simboli $(\mathbb{Z}, +) \cong \ (< g >, \cdot)$ e le potenze di g sono tutte distinte tra loro (g^r≠g^s) ⇒ <g> è infinito
2. ϵ **non è iniettiva** ⇒ esiston k potenze dist.: $< g >= \{e_G, g, g^2, ..., g^{k-1}\}$ e poi ripete

PERIODO: si dice periodo di g in G l'ordine |<g>|=n

OSS B:

1. g ha **periodo 1** <=> $g = e_G$
2. g ha **periodo infinito** => ϵ è iniettiva $\Rightarrow < g > \cong \ \mathbb{Z}$
3. Possono esistere elementi di **periodo finito** dentro **gruppi infiniti.**
4. Se **<g> è infinito** $\Rightarrow g^k$ ha periodo infinito ‼ $\forall k \neq 0$ (tutte potenze ≠e_G)
5. **Lagrange**

Dim oss A2:

- -(⇒ esiste $g^k = e_G$ min → divisione → k potenze e poi ripete)

  ESISTE $g^k = e_G$ min

  $\Rightarrow \exists s, t (s \neq t) \in \mathbb{Z} | \epsilon(s) = \epsilon(t)$, cioè $g^s = g^t$ suppongo s>t. Allora moltiplico per g^{-t} ottengo $g^{s-t} = e_G$. $\exists k \in \mathbb{N} \backslash \{0\} | g^k = e_G$. Sia $n = min\{k \in \mathbb{N} \backslash \{0\} | g^k = e_G\}$

  DIVISIONE EUCLIDEA (minimo 0≤r<n)

  Ora $\forall k \in \mathbb{Z}$, possiamo svolgere la divisione euclidea per n e otteniamo k=qn+r con 0≤r<n. Allora:

  $$g^k = g^{q \cdot n + r} = g^{qn} \cdot g^r = (\underbrace{g^n}_{e_G})^q \cdot g^r = (e_G)^q \cdot g^r = e_G \cdot g^r = g^r$$

  OSS: $g^r = e_G$ sse. r=0 (perchè r<n ed n è il min(+) con quella proprietà)

  CONCLUSIONE

  Esistono r potenze distinte di g

  $< g >= \{e_G, g, g^2, ..., g^{n-1}\}$ e poi si ripetono

Teorema di eulero (di nuovo)

PROP: Sia $(G, \cdot)$ un gruppo con |G|=n finito $\Rightarrow \forall g \in G \quad g^n = e_G$(in sottogruppo)

TEOREMA EULERO (ripasso): Dati $a \in \mathbb{Z}, N \in \mathbb{N}$, N≥2, MCD (a,N)=1
Allora $a^{\phi(N)} \equiv 1 \mod N$

Dim:

- PROP (d|n x lagrange → n=dk e $g^n = g^d k = e_G^k$)

  DIVIDE D|N g non è detto che sia generatore ma sappiamo che

  <g> ≤G $\Rightarrow \exists k \in \mathbb{Z} \ t.c. \ | < g > | \cdot k = n$

  $g^n = g^{dk} = (g^d)^k = e_G^k = e_G$ (perchè d è periodo <g>)

- TEOREMA - Considero $a \in (\mathbb{Z}_N^\times, \cdot)$→ prop prima

  PARTENZA (se invertibile *a* gruppo N)

  Premessa: sia $(\mathbb{Z}_N^\times, \cdot, 1)$ un gruppo abeliano.

  - ⇒ uso preposizione di prima $\forall \bar{a} (\bar{a}^{|\mathbb{Z}_N^\times|} = \bar{a}^{\phi(N)} \equiv 1 \mod N)$