Fondamenti matematici per l'informatica

Mattia Marini

14 maggio 2024

Indice

Definizioni

Teoremi e Assiomi

1 Insiemistica

Definzioni di base sugli insiemi

Definizione 1: *Insieme*
Un insieme è una collezione di oggetti, detti suoi elementi. La caratteristica fondamentale di un insieme è che si possa stabilire senza ambguità se qualcosa vi appartiene o meno:

$$x \in A \text{ oppure } x \notin A$$

Quest'ultima caratteristica, sembra scontata ma non lo è. Considera il seguente insieme:

$$A = \{x | x \notin x\}$$

Questo caso è noto come il paradosso di Russel. A non può essere un insieme in quanto:

- Se $A \in A$ allora per definizione di A, $A \notin A$
- Se $A \notin A$ allora per definizione di A , $A \in A$

Definizione 2: *Insiemi uguali*
Due insiemi sono uguali se e solo se contengono gli stessi elementi. Formalmente

$$A = B \Leftrightarrow (x \in A \Leftrightarrow x \in B \; \forall x)$$

Definizione 3: *Insieme vuoto*
E' costituito dall'insieme senza alcun elemento e denotato con il simbolo $\emptyset$. Formalmente un insieme è vuoto se

$$x \notin A \ \forall x$$

Definizione 4: *Insieme contenuto*
Si dice che A è <u>contenuto</u> in B ($A \subseteq B$) se:

$$(x \in A \Rightarrow x \in B) \ \forall x$$

Si dice che A è <u>contenuto strettamente</u> in B ($A \subsetneq B$) se:

$$(x \in A \Rightarrow x \in B) \ \forall x \text{ e } A \neq B$$

Definizione 5: *Definire degli insiemi*
Abbiamo principalmente due modi di definizre degli insiemi:

- *Proprietà:* Se X è un insieme e $P(x)$ è una proprietà esprimibile sull'elemento $x \in X$ allora il seguente è un insieme:

$$\{x | x \in X \text{ e } P(x)\}$$

- *Per elenco:* possiamo elencare uno per uno gli elementi dell'insieme stesso. Questa procedura può essere vista come un iterazione sugli elementi che andranno contenuti nell'insieme stesso

$$\{1, 2, 3, \ldots, n\}$$

Definizione 6: *Operazioni su insiemi*
Se X e Y sono insiemi si costruiscono altri insiemi:

- *Intersezione* $X \cap Y = \{x \mid x \in X \text{ e } x \in Y\}$
- *Differenza* $X \backslash Y = \{x \mid x \in X \text{ e } x \notin Y\}$. Quando $Y \subseteq X$ la differenza $X \backslash Y$ viene chiamata il complemento di Y in X e viene denotata anche con $\complement_X Y$ o semplicemente con $\complement Y$ o con Y' quando non ci sia ambiguità
- *Unione* $X \cup Y = \{x \mid x \in X \text{ o } x \in Y\}$
- *Differenza simmetrica* $X \triangle Y = (X \backslash Y) \cup (Y \backslash X)$
- *Prodotto* $X \times Y = \{(x, y) \mid x \in X \text{ e } y \in Y\}$
- *Potenza* $2^X = \{x \mid x \subseteq X\}$, ossia l'insieme contenente ogni sottoinsieme

Se I è un insieme e per ogni $i \in I$ è dato un insieme X_i, si definiscono

- *Intersezione* $\bigcap_{i \in I} X_i = \{x \mid \forall i x \in X_i\}$
- *Unione* $\bigcup_{i \in I} X_i = \{x \mid \exists i x \in X_i\}$

1.1 Relazioni e funzioni fra insiemi

Definizione 7: *Relazione*
Siano X e Y insiemi si dice relazione tra X e Y, un sottinsieme $\mathcal{R} \subseteq X \times Y$. Se $\mathcal{R}$ è una relazione si scriverà anche $x\mathcal{R}y$. Una relazione tra X e se stesso, si dirà anche una *relazione binaria* su X.

Definizione 8: *Funzione parziale*
Una relazione $f \subseteq X \times Y$ si dice una funzione parziale se per ogni $x \in X$ esiste al più un $y \in Y$ tale che $(x, y) \in f$. In simboli:

$$\forall x \in X\,((x, y) \in f \,\text{e}\, (x, y') \in f) \implies y = y'$$

Si scriverà $f : X \rightharpoonup Y$ per dire che f è una funzione parziale da X a Y e in tal caso si scriverà anche $y = f(x)$ come sinonimo di $(x, y) \in f$.

Definizione 9: *Dominio e immagine*
Dominio: L'insieme $\{x \in X \mid \exists y \in Y : y = f(x)\}$ è detto il dominio di f e si denota con $\mathrm{dom}(f)$

Immagine: L'insieme $\{y \in Y \mid \exists x \in \mathrm{dom}(f) : y = f(x)\}$ è detto l'immagine di f e si denota con $\mathrm{im}(f)$.

Definizione 10: *Funzione totale*
Una funzione parziale $f : X \to Y$ si dice funzione totale o semplicemente funzione se $\mathrm{dom}(f) = X$, in tal caso si scrive

$$f : X \to Y$$

Si denota Y^X l'insieme di tutte le funzioni (totali) da X a Y, ossia $Y^X = \{f : X \to Y\}$

Definizione 11: *Iniettività, surgettività e bigettività*
Una funzione $f : X \to Y$ si dice:

- *iniettiva* se per ogni $x_1, x_2 \in X x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$
- *surgettiva* se per ogni $y \in Y$ esiste $x \in X$ tale che $f(x) = y$
- *bigettiva* se è iniettiva e bigettiva

Definizione 12: *Funzione inversa*
Sia $f : X \to Y$ una bigezione, allora esiste un'unica funzione $g : Y \to X$ tale che $f \circ g = \mathrm{id}_Y$ e $g \circ f = \mathrm{id}_X$. Tale funzione si chiama inversa *di* fe si denota con f^{-1}.

1.2 Insiemi euipotenti

Definizione 13: *Insiemi equipotenti*
Siano x e y due insiemi. Si dice che x è equipotente a Y oppure X ha la stessa cardinalità di Y se

$$\exists f : x \to y \text{ t.c. } f \text{ bigezione}$$

se due insiemi sono equipotenti si scrive informalmente che X Y

Nota bene, vale che dati tre insiemi X, Y e Z

- X è equipotente a se stesso.
- se X è equipotente a Y allora Y è equipotente a X
- se X è equipotente a Y e Y è equipotente a Z, allora X è equipotente a Z.

1.2.1 Equipotenza e numero di elementi

Cerchiamo di colegare la nozioni che due insiemi equipotenti hanno lo stesso numero di elementi

- Un insieme equipotente garantisce l'esistenza di una funzione f biettiva
- Se f è iniettiva allora ogni elemento ha una mappatura 1:1 con un elemento dell'insieme di arrivo
- Se f è surgettiva allora ogni elemento dell'insieme d'arrivo viene collegato all'insieme di inizio tramite f
- I due insiemi hanno necessariamente lo stesso numero di elementi

Teorema 1: *Cardinalità e equipotenza*
Dati due insiemi X e Y, questi sono equipotenti se e solo se la loro cardinalità è la stessa

$$X \sim Y \Leftrightarrow |X| = |Y|$$

2 Costruzione dei numeri naturali

2.1 Assiomi di Peano

Affrontiamo l'approccio assiomatico di Peano. Vediamo 4 assiomi:

- L'insieme $\mathbb{N}$ contiene almeno un elemento $0 \in \mathbb{N}$ (0 è detto zero)
- Esiste una funzione successivo $succ : \mathbb{N} \to \mathbb{N}$ iniettiva
- La funzione $succ$ ha la seguente proprietà: $succ\,(n) \subset \mathbb{N} \setminus \{0\}\ \forall n \in \mathbb{N}$
- Assioma di induzione. Sia A un sottoinsieme di $\mathbb{N}$. Supponiamo che A soddisfi le seguenti due proprietà:

- (*Base dell'induzione*) $0 \in A$
- (*Passo induttivo*) $\forall n \in \mathbb{N}\,(n \in A) \Rightarrow succ\,(n) \in A$

Allora $A = \mathbb{N}$

Inoltre ho proprietà importanti:

- Siam $n \in \mathbb{N} \setminus \{0\}$ allora $\exists! n \in \mathbb{N}$ t.c. $succ\,(m) = n$. In questo caso n è detto predecessore di m
  - Visto che $succ\,(n)$ è una funzione iniettiva, se esiste, il predecessore deve essere unico
  - Procediamo poi per assurdo ammettendo che esista un n che non abbia predecessore
    * Supponiamo che esista un $m \neq 0$ che non abbia predecessore, ossia $succ\,(n) \neq m\ \forall n \in \mathbb{N}$
    * Creo insieme A senza m:
    $$A = \mathbb{N} \setminus \{m\}$$
    * Chiaramente $0 \in A$ in quanto $m \neq 0$
    * Chiaramente $succ\,(n) \in A$ in quanto per definizione $A = \mathbb{N} \setminus \{m\}$
    * Per l'assioma di induzione quindi $A = \mathbb{N}$. Questa è tuttavia una contraddizione

Teorema 2: *Principio di induzione di prima forma*
Sia $\left\{P\,(n)_{n\in\mathbb{N}}\right\}$ una famiglia di proposizioni (affermazioni) $P\,(n)$ indicizzata su $n \in \mathbb{N}$ sulla quale valgono le seguenti proprietà:

- *(Base dell'induzione)* $P\,(0)$ è vera
- *(Ipotesi induttiva)* $\forall n \in \mathbb{N} : [P\,(n) \Rightarrow P\,(succ\,(n))]$ ossia se $P\,(n)$ è vera allora anche $P\,(succ\,(N))$ è vera.

Allora $P\,(n)$ è vera $\forall n \in \mathbb{N}$

Dimostrazione:

- Sia $A = \{n \in \mathbb{N} | P\,(n) \text{ è vera }\}$
- Sappiamo che
  - $0 \in A$ (base dell'induzione)
  - se $n \in A$ allora $succ\,(n) \in A$ quindi $A = \mathbb{N}$

Ho quindi esteso la proprietà ad ogni $n \in \mathbb{N}$ per gli assiomi di Peano

Teorema 3: *Teorema di ricorsione*
Sia X un insieme non vuoto, sia $h : \mathbb{N}_x X \to X$ una funzione (mappa) e sia $c \in X$. c è detto dato iniziale, h funzione di iterazione. Allora $\exists! f : \mathbb{N} \to x$ tale che:

$$\begin{cases} f\,(0) = c \\ \forall n \in \mathbb{N} \quad f\,(succ\,(n)) = h\,(n, f\,(n)) \end{cases}$$

Applicazioni del teorema di ricorsione

Sia $m \in \mathbb{N}$. Vogliamo formalizzare il concetto di somma a sinistra con m.

- Sia $x = \mathbb{N}$, sia $c = m$ e sia $h : \mathbb{N}x\mathbb{N} \to \mathbb{N}$ definita ponendo $h(a, b) := succ(b)$.
- Allora grazie al teorema di ricorsione $\exists! f : \mathbb{N} \to x = \mathbb{N}$ tale che :

$$\begin{cases} f(0) = c \\ \forall n \in \mathbb{N} \quad f(succ(n)) = h(n, f(n)) \end{cases}$$

f è detta somma a sinistra con m

2.2 Ordinamento di un insieme

Una volta definiza l'addizione su $\mathbb{N}$ si può definire anche l'operatore $\leq$:

Definizione 14: *Operatore minore uguale*
Siano $n, m \in \mathbb{N}$. Diremo che $n \leq m$ se esiste un k tale che

$$n + k = m$$

Si può vedere $\leq$ come un sottinsieme di $\mathbb{N} \times \mathbb{N}$ e precisamente

$$\leq = \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid \exists k \in \mathbb{N} : n + k = m\}$$

E quindi $\leq$ è una relazione (definizione 1.9) sui naturali e quello che abbiamo definito come significato di $n \leq m$ è effettivamente lo stesso che dire $(n, m) \in \leq$.

Definizione 15: *Ordinamento di un insieme*
Sia X un insieme non vuoto e sia $\leq$ una relazione binaria. $\leq$ si dice ordinamento parziale di X se:

1. *Riflessiva* $x \leq x \; \forall x \in X$
2. *Antisimmetrica* $\forall x, y \in X : (x \leq y)$ e $(y \leq x) \Rightarrow x = y$
3. *Transitiva* $\forall x, y, z \in X : (x \leq y)$ e $(y \leq z) \Rightarrow (x \leq z)$

la relazione $\leq$ si dice ordinamento parziale di un insieme. Inoltre se:

4. *Tricotomia* $\forall x, y \in X, (x \leq y)$ oppure $(y \leq x)$

Nota che è semplice dimostrare che $\mathbb{N}$ è un insieme parzialmente ordinato. Tuttavia dimostrare che è un insieme totalmente ordinato è un procedimento piuttosto tedioso.

Teorema 4: *Principio di induzione shiftato di prima forma*
Sia $\{P(m)\}_{m \geq k}$ una famiglia di proposizioni (affermazioni) indicizzate seui numeri naturali $\geq$ di un certo $k \in \mathbb{N}$ fissato. Supponiamo che:

- *Base induzione* P(k) è vera
- *Passo induttivo* $\forall n \in \mathbb{N}, n \geq k : (p(n) \Rightarrow P(n+1))$

3 Esercizi per induzione

Esercizio 2

Dimostra che

$$\sum_{k=1}^{n} 6k^2 = n\left(n+1\right)\left(2n+1\right) \tag{1}$$

- *Passo base.* Per $n = 2$ chiaramente vale:

$$\sum_{k=1}^{2} 6k^2 = \left(6 \cdot 1^2\right)\left(6 \cdot 2^2\right) = 6 + 24 = 30$$

  e anche

$$2\left(2+1\right)\left(2 \cdot 2 + 1\right) = 30$$

- *Passo iduttivo.* Assumo che l'equazione 1 sia vera per $n \geq 2$.

-

$$\begin{aligned}\sum_{k=1}^{n+1} 6k^2 &= \sum_{k=1}^{n} 6k^2 + 6\left(n+1\right)^2 \\ &= n\left(n+1\right)\left(2n+1\right) + 6\left(n+1\right)^2 = \left(n+1\right)\left(\left(n+1\right)+1\right)\left(2\left(n+1\right)+1\right)\end{aligned}$$

3.1 Cardinalità su insiemi finiti

Per ogni $n \in \mathbb{N}$, indichiamo con I_n il seguente sottoinsieme di $\mathbb{N}$:

$$I_n = \{0, 1, \ldots, n-1\}$$

Inoltre poniamo $I_0 = \emptyset$

Definizione 16: *Insieme finito*
Dato un insieme X, diciamo che X è finito se esiste un n tale che X è equipotente a I_n:

$$\exists n \in \mathbb{N} \text{ t.c. } X \sim I_n$$

se X non è finito si dice infinito

tuttavia può sorgere il dubbio se X è equipotente con solo un I_n oppure con molteplici I_n. Per risolvere questo dubbio serve il teorema dei cassetti

Teorema 5: *Teorema dei cassetti*
Siano X e Y insimemi e siano $n, m \in \mathbb{N}$ tali che:

- $n < m$
- $X \sim I_n$
- $Y \sim I_m$

Allora non esiste alcuna funzione $f : y \to x$ iniettiva (y ha più elementi)

La dimostrazione procede per induzione, indicizzando $n \in \mathbb{N}$. L'ipotesi induttiva va fatta sulla n: fissata una n, la m può essere qualsiasi numero naturale maggiore di n

- *Passo base con* $P(0)$:
  - $n = 0, m > 0$
  - $X \sim I_0 \sim \emptyset$
  - Tuttavia abbiamo dimostrato che non eisiste alcuna funzione $f : Y \to X$ che va da un insieme non vuoto ad un insieme $X = \{\emptyset\}$

  Ho quindi dimostrato che la proprietà è verificata su $P(0)$

- Assumiamo che l'ipotesi sia verificata per n, e dimostriamo che allora lo deve essere anche per $n + 1$. Per fare ciò procediamo per assurdo, supponendo che esista $f : Y \to X$ iniettiva
  - L'insieme X è in bigezione con I_{n+1}
  - Supponiamo di togliere da X l'elemento collegato dalla bigezione g fra X e I_n
  - $g(n) \notin f(y)$
    * i
  - $g(n) \notin f(y)$
    * Poichè f è iniettiva, $f^{-1}(x_n)$ sarà un singolo elemento
    * Posso rimuovere dunque sia x_n che $f^{-1}(x_n)$. Chiamo questi nuovi due insiemi X' e Y'
    * Posso considerare $f : Y' \to X'$. f è sempre iniettiva
    * Questo è tuttavia impossibile in quanto per ipotesi induttiva è stato supposto che per $n \quad \nexists f : Y \to X$ iniettiva

Posso rinforzare questa affermazione con il seguente corollario:

Teorema 6: *Colorrario a teorema dei cassetti*
Siano X e Y due insiemi e siano $n, m \in \mathbb{N}$ tali che $x \sim I_n$ e $Y \sim I_m$, allora:

$$X \sim Y \Leftrightarrow n = m$$

Dimostrazione

- $\Leftrightarrow$Se $n = m$ allora $X \sim Y$ per composizione di bigezioni
- Se $X \sim Y$ e $X \sim I_n, Y \sim I_m$, allora $I_n \sim I_m$
- Per il lemma dei cassetti, non può esistere una iniezione fra I_m e I_n se $n \neq m$. Quindi se esiste una bigezione fra questi, devono avere lo stesso numero di elementi

Definizione 17: *Cardinalità*
Dato un insieme finito X si dice che la cardinalità di X è n se

$$X \sim I_n$$

si dice informalmente che $|X| = n$, anche se il valore assoluto indicherebbe l'insieme cardinale. $|X| = I_n$ sarebbe la notazione corretta

Teorema 7:
Sia X un insieme finito e sia Y un suo sottoinsieme. Allora

$$Y \text{ è un insieme } \underline{\text{finito}} \text{ e } |Y| \leq |X|$$

Inoltre se $Y \subset X$ allora $|Y| < |X|$

Dimostrazione

Procedo per induzione indicizzando la cardinalità di X.

- Per $|X| = 0$ è verificata in quanto $|X| = I_0 = \emptyset$. L'unico sottoinsieme del vuoto è il vuoto e ha cardinalità 0
- Come in dimostrazione del teorema dei cassetti (*teo 5*)

Questo teorema ha un risvolto importantissimo, ossia che $\mathbb{N}$ è un insieme infinito.

Definizione 18: *Buon ordinamento*
Sia X un insieme e sia $\leq$ un ordinamento totale su X. Se ogni sottoinsieme non vuoto A di X ammette minimo (rispetto al $\leq$), allora $\leq$ si dice <u>buon ordinamento su X</u>. In questo $(X, \leq)$ si dice <u>insieme ben ordinato</u>

La caratteristica importante di un insieme ben ordinato è che vale su di esso un principio di induzione fortissimo: il principio di induzione di seconda forma.

Teorema 8: *Buon ordinamento dei numeri naturali*
L'insieme dei numeri naturali dotato dell'ordinamento $\leq$ standard, ovvero la coppia $(\mathbb{N}, \leq)$, è <u>ben ordinato</u>

Dimostrazionie

Sia A un sottoinsiieme di $\mathbb{N}$ <u>senza minimo</u>. Dobbiamo provare che $A = \emptyset$

- Dimostriamo per induzione che per ogni $n \in \mathbb{N}$ vale:

$$\{0, 1, \ldots, n\} \subset B := \mathbb{N} \setminus A$$

- i

3.2 La divisione euclidea

Assumiamo la conoscenza dell'insieme $\mathbb{Z} = \{\ldots - 2, -1, 0, 1, 2, \ldots, n, \ldots\}$

Teorema 9: *Esistenza ed unicità della divisione euclidea*
Siano n ed m tale che $m \neq 0$. Allora esistono e sono <u>unici</u> due interi $q, r \in \mathbb{Z}$ tali che

$$\begin{cases} n = qm + r \\ 0 \leq r \leq |m| \end{cases}$$

inoltre se $n, m \in \mathbb{N}$, $m > 0$ allora $q, r \in \mathbb{N}$

Dimostrazione esistenza

Fisso come parametro $m > 0$ e procediamo con il principio di induzione di seconda forma, usando come ipotesi induttiva che

$$P(n) = \left(\exists q, r \in \mathbb{N} \text{ t.c. } \begin{cases} n = qm + r \\ 0 \leq r < m \end{cases} \right)$$

- *Passo base* La $P(0)$ è vera con $q = r = 0$
- *Passo induttivo* Assumiano di essere in grado di saper effettuare la divisione euclidea di k per m per ogni $k < n$ (ossia avere l'esistenza e unicità di q, r). Se dimostro che ciò è possibili anche per n ho finito. Considero 4 casi:

$$\begin{array}{ll} n > 0, m > 0 & n > 0, m < 0 \\ n < 0, m > 0 & n < 0, m < 0 \end{array}$$

- $n > 0, m > 0$
  - Se $m > n$ allora basta prendere $q = 0$ e $r = n$
  - Se $n > m$ allora posso considerare la divisione fra $n-m$ e m. Questa divisione esiste per ipotesi induttiva la divisione euclidea esiste $\forall k < n$ (chiaramente $n - m < n$, visto che $m > 0$). Allora :

    $$\begin{cases} n - m = qm + r \\ 0 \leq r < m \end{cases}$$

    da cui la prima è uguale a

    $$n = m + qm + r = (q + 1)\, m + r$$

    Se ci pensi ha senso. m sta in n una volta in più $(q + 1)$
- $n < 0, m > 0$
  - Visto che $n < 0$, per quanto dimostrato fin'ora, vale che:

    $$-n = mq + r \Rightarrow n = m(-q) - r$$

  - Se $r = 0$ ho finito. Altrimenti agggiungendo e sottraendo m ottengo

    $$n = m(-q) - m - r + m = (-q - 1)\, m + m - r$$

  - Visto che per definizione $0 < r < m$, allora vale che $0 < m - r < m$
- $n > 0, m < 0$
  - Come nel caso precedente, moltiplico per -1 e mi baso su quanto già dimostrato
- $n < 0, m < 0$
  - Come nel caso precedente, moltiplico per -1 e mi baso su quanto già dimostrato

Dimostrazione unicità

Supponiamo per assurdo q ed r non siano unici. Avrei:

$$\begin{cases} n = qm + r \\ 0 \leq r < |m| \end{cases} \quad \text{e} \quad \begin{cases} n = q'm + r' \\ 0 \leq r < |m| \end{cases}$$

quindi avrò che

$$qm + r = q'm + r' \to qm - q'm = r' - r \to (q - q')\, m = r' - r$$

visto che la differenza di resti deve necessariamente essere $< |m|$ in quanto entrambi i resti sono per definizione valori positivi, vale che:

$$|(q - q')|\, |m| = |r' - r| < |m| \to |(q - q')| < 1$$

ma visto che $|q - q'| < 1$ e q e q' sono per def numeri interi, allora $q - q' = 0$, ossia $q = q'$

3.3 Scrittura dei numeri naturali in base maggiore di 2

Definizione 19: *Rappresentazione numeri naturali*
Sia $b \in \mathbb{N}$. Diremo che un numero naturale $n \in \mathbb{N}$ è rappresentabile in base b se esistono $k \in \mathbb{N}$ $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_k$ tali che :

- $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_k \in I_b$, dove $I_b = \emptyset$ se $b = 0$, $I_b = \{0, 1, \ldots, b-1\}$ se $b \geq 1$
- $n = \varepsilon_0 b^0 + \varepsilon_1 b^1 + \varepsilon_2 b^2 + \ldots + \varepsilon_k b^k = \sum_{i=0}^{k} \varepsilon_i b^i$

In questo caso $\varepsilon_0, \ldots, \varepsilon_k$ si dicono cifre di n in base b e si scrive:

$$n = (\varepsilon_0, \ldots, \varepsilon_k)_b$$

Nota che

- In base 0 non è rappresentabile nulla in quanto :

$$I_0 = \emptyset$$

- In base 1 è rappresentabile solo lo 0 in quanto :

$$I_1 = \{0\}$$

Teorema 10: *Rappresentabilità dei naturali in base b*
Sia $b \geq 2$. Allora per ogni $n \in \mathbb{N}$ esiste una succesione $\{\varepsilon_i\}_{i \in \mathbb{N}}$ tale che soddisfi le proprietà enunciate in 19 tale espressione è inoltre unica

Dimosrazione esistenza

Procedo per induzione su n:

- *Passo base* Per $n = 0$ l'hp è verificata. Basta prendere una stringa di soli 0
- *Passo induttivo di seconda forma* Prendo un $n > 0$ e assumo l'hp vera per ogni $k < n$. Assumiano di saper quindi rappresentare ogni k in base b per ogni $k < n$
  - Eseguiamo la divisione di n per b:
  $$\begin{cases} n = qb + r \\ 0 \leq r < b \Leftrightarrow r \in I_b = \{0, 1, \ldots, b-1\} \end{cases}$$
  - Dimostro che $q < n$
    - se $q = 0$ è banalmente verificata
    - Se $q \neq 0$ allora so che $q < qb$ in quanto $b \geq 2$. Allora anche $q < qb + r = n$
  - Poichè $q < n$ so che, per *hp ind* q è rappresentabile in base b, quindi
  $$n = qb + r = \left(\sum_{i=0}^{\infty} \varepsilon_i b^i\right) b + r = \left(\sum_{i=0}^{\infty} \varepsilon_i b^{i+1}\right) + r$$
  $$= \sum_{i=1}^{\infty} \varepsilon_{i-1} b^i + r$$

  Nota che ciò che ottieni è un numero rappresentato secondo le proprietà elencate in 19, in cui la $\varepsilon_0 = r$ (nella sommatoria manca la cifra $\varepsilon_0 b^0$)

Dimostrazione unicità

Procedo per induzione su n.

- *Passo base.* Per $n = 0$ l'unica rappresentazione ammessa è la stringa contenente soli zeri.
- *Passo induttivo.* Suppongo che la rappresentazione sia unica $\forall k < n$
  - Supponiamo per assurdo che esistano due rappresentazioni di n in base b
  $$n = \sum_{i=0}^{\infty} \varepsilon_i b^i = \sum_{i=0}^{\infty} \varepsilon_i' b^i$$
  - Possiamo modificare le sommatorie estraendo il termine per $i = 0$ e portando fuori un fattore b
  $$n = b \sum_{i=1}^{\infty} \varepsilon_i b^{i-1} + \varepsilon_0 = b \sum_{i=1}^{\infty} \varepsilon_i' b^{i-1} + \varepsilon_0'$$
  - Nota che ho espresso n come divisione euclidea fra n e b. Quindi per teo 9 il resto è unico $\varepsilon_0 = \varepsilon_0'$. Allora stesso modo, $q = \sum_{i=1}^{\infty} \varepsilon_i b^{i-1} = \sum_{i=1}^{\infty} \varepsilon_i' b^{i-1}$
  - Inoltre, come dimostrato precedentemente, $q < n$, quindi per hp induttiva la rappresentazione è unica, ossia $\varepsilon_i = \varepsilon_i' \quad \forall i$

4 Divisibilità

Definizione 20: *Divisibilità*
Siano $n, m \in \mathbb{Z}$. Diciamo che n divide m e scriveremo $n|m$ se

$$\exists k \in \mathbb{Z} \text{ t.c. } nk = m$$

Se ciò è falso si dice che n non divivde m e si scrive $n \not| m$

Nota che valgono le seguenti proprietà:

- $\forall n \in \mathbb{Z} \rightarrow n|0$
- $\forall n \in \mathbb{Z} \setminus \{0\} \rightarrow 0 \not| n$
- $\forall n \in \mathbb{Z} \rightarrow \begin{cases} \pm 1|n \\ \pm n|n \end{cases}$

Inoltre, se ho $n, m, q \in \mathbb{Z}$ vale che:

- $n|m$ e $m|q \rightarrow n = \pm q$
- $n|m$ e $m|n \Rightarrow n = m$ oppure $n = -m$

Definizione 21: *Massimo comune divisore*
Siano $n, m \in \mathbb{Z}$ non entrambi nulli. Si dice che un numero $d \in \mathbb{Z}$ è un massimo comune divisore(M.C.D) tra m e n se

- $d > 0$
- $d|n$ e $d|m$
- Se $c \in \mathbb{Z}$ è tale che $c|n$ e $c|m$, allora $c|d$

Come mai non possono essere entrambi nulli? In quanto la famiglia dei divisori di entrambi i numeri sarebbe tutto $\mathbb{Z}$ (ogni numero divide 0)

Teorema 11: *Esistenza ed unicità M.C.D*
Siano $n, m \in \mathbb{Z}$ non entrambi nulli. Allora

$$\exists!\,(n, m)$$

ossia esiste ed è unico l'M.C.D. fra n e m

Dimostrazione esitenza

Definiamo innanzitutto il seguente insieme S si $\mathbb{N}$:

$$S = \{s \in \mathbb{N} | s > 0, s = xn + ym\}$$

per qualche $x, y \in \mathbb{Z}$, ossia tutte le combinazioni lineari maggiori di zero fra n, m. Nota che l'insieme è non vuoto in quanto entrambi n, m sono non nulli:

$$x = n, y = m \rightarrow n^2 + m^2 > 0$$

Poichè S è un sottoinsieme non vuoto di $\mathbb{N}$, grazie al teorema del buon ordinamento, allora ammete un minimo:

$$d = min\,(S)$$

Poichè $d \in S$, vale :

$$\begin{cases} d > 0 \\ \exists x, y \in \mathbb{Z} \text{ t.c. } d = xn + ym \end{cases}$$

Nota che vale che ogni divisore comune fra n e m divide d:

- Dato c tale che $c|n$ e $c|m$, allora ho che $n = kc, m = hc$

$$d = xn + ym = xkc + yhc = c\,(xk + yh)$$

Dimostriamo ora che $d = xn + ym$ divide n e m:

- Considero la divisione euclidea tra n e d:

$$\begin{cases} n = q\,(xn + ym) + r \\ 0 \leq r < d = (xn + ym) \end{cases}$$

- Supponiamo per assurdo che $r \neq 0$, allora avrei:

$$r = n - q\,(xn + ym) = n - qxn - qym = n\,(1 - qx) + m\,(-qy)$$

  quindi $r \in S$, ma per le caratteristiche del rest della divisione euclidea $0 \leq r < d$, ossia $r < d = min\,(S)$, il che è un assurdo logico visto che $r \in S$

Analogamente si dimostra che $d|m$

Dimostrazione unicità

Per definizione un numero è M.C.D. fra m, n se è divisibile per ogni divisore comune a n, m

- Siano d, d' due M.C.M. di n, m
- Visto che $d|n, d|m$, allora è un divisore comune, quindi $d|d'$
- Al contrario, visto che $d'|n, d'|m$, allora è un divisore comune, quindi $d'|d$

Visto che $d'|d$ e $d|d'$ allora $d = \pm d'$. Per definizione, il massimo comune divisore deve essere un intero positivo, quindi da questo deriva l'unicità

Teorema 12: *Lemma utile*
Siano $c, n, m \in \mathbb{Z}$ t.c. $c|n$ e $c|m$. Per ogni $x, y \in \mathbb{Z}$ si ha:

$$c|(xn + ym)$$

4.1 Criterio d'arresto

L'M.C.D gode delle seguenti proprietà:

- Non conta il segno (posso considerare il valore assoluto dei numeri)

$$(n, m) = (-n, m) = (n, -m) = (-n, -m)$$

- Non conta l'ordine:

$$(n, m) = (m, n)$$

- L'M.C.D è il massimo fra i divisori comuni fra m e n:

$$(n, m) = max\{c \in \mathbb{Z} | c|n, c|m\}$$

- Sia $n \in \mathbb{Z} \setminus \{0\}$, vale che :

$$(n, 0) = |n|$$

> **Definizione 22:** *Coprimi*
> Siano $n, m \in \mathbb{Z}$ non entrambi nulli. Diciamo che n ed m sono coprimi se
>
> $$(n, m) = 1$$

4.2 Algoritmo di euclide per il calcolo dell'M.C.D.

Ricordiamo le 3 seguenti proprietà:

- $(n, m) = (|n|, |m|)$
- $(n, 0) = |n| \, (\forall n \in \mathbb{Z} \setminus \{0\})$
- $(n, m) = (m, n)$

L'algoritmo procede dunque nel seguente modo:

- Considero il valore assoluto di n e m
- Assumo che $n \geq m \geq 0$
- Procedo poi nel seguente modo:

M.C.D.	divisori
(n, m)	m
(m, r_1)	r_1
r_1, r_2	r_2
$\vdots$	$\vdots$
(r_{k-1}, r_k)	r_k
$(r_k, 0)$	0
r_k	/

Esempio

Calcola il M.C.D. fra 48 e 28

Sappiamo che l'M.C.D. è 4, ma procediamo con euclide ponendo $n = 48, m = 28$

Trovo M.C.D.	**Risoluzione al contrario**
$48 = 1 \cdot 28 + 20$	$20 = 48 - 1 \cdot 28$
$28 = 1 \cdot 20 + 8$	$8 = 28 - 1 \cdot 20$
$20 = 2 \cdot 8 + 4$	$4 = 20 - 2 \cdot 8$
$8 = 2 \cdot 4 + 0$	

nella risoluzione al contrario devo sostituire la linea sopra in quella sotto, trattando i numeri come variabili, quidni senza eseguire conti:

$$\begin{aligned}
4 &= 20 - 2 \cdot 8 \\
4 &= 20 - 2 \cdot (28 - 1 \cdot 20) \\
4 &= 48 - 1 \cdot 28 - 2 \cdot (28 - 1 \cdot (48 - 1 \cdot 28))
\end{aligned}$$

raccogliendo poi i 28 e i 48 ottengo chiaramente l'M.C.D. come combinazione lineare di n e m:

$$4 = 3 \cdot 48 - 2 \cdot 28$$

Teorema 13: *Implicazioni numeri coprimi*
Siano $n, m \in \mathbb{Z}$ numeri entrambi non nulli e sia $q \in \mathbb{Z}$. Supponiamo che $(n, m) = 1$ (ossia n, m sono comprimi), allora vale che:

- $n|mq \Rightarrow n|q$

- $n|q$ e $m|q$ allora $nm|q$

Dimostrazione 1

- Poichè $(n, m) = 1$ allora $\exists x, y \in \mathbb{Z}$ t.c. $xn + yn = (n, m) = 1$
- Moltiplico per q:
$$qxn + qym = q$$
ma siccome $n|mq$ allora $mq = kn$ per qualche valore di k
$$qxn + y\,(kn) = q$$
raccogliendo n ottengo
$$(qx + yk)\,n = q$$
ossia che q è divisibile per n

Definizione 23: *Numero primo*
Un numero intero $p \in \mathbb{Z}$ è detto primo se $p \geq 2$ e i suoi divisori sono tutti e soli quelli banali cioè ± 1 e $\pm p$

Teorema 14: *Corollario su numeri primi*
Sia $p \in \mathbb{Z}$ t.c. $p \geq 2$. Allora p è numero primo se e solo se possiede la segunete proprietà (detta *primalità*)

$$\forall n, m \in \mathbb{Z} : (p|nm \Rightarrow p|n \text{ oppure } p|m)$$

Ciò risulta evidente se pensi al fatto che se p è primo e $p|nm$ allora necessariamente questo deve comparire nella fattorizzazione in fattori primi da qualche parte. Questo non è necessariamente vero se p non è primo. Basti pensare a $n = 2, m = 6$

Dimostrazione

Ho due casi:

- Se $p|n$, allora palesemente è verificata la *hp*
- Se $p \not| n$ allora devo provare che $p|m$
  - Visto che $p \not| n$ e p è primo per definizione, allora $(p, n) = 1$ ossia p, n sono coprimi
  - Dunque per teorema 13 abbiamo che $n|mq \Rightarrow n|q$ se n, m coprimi. Quindi

$$p|m$$

5 Minimo comune multiplo

Definizione 24: *Minimo comune multiplo*
Siano $n, m \in \mathbb{Z}$. Un numero intero $M \geq 0$ è un m.c.m. tra n e m se

- $n|M$ e $m|m$
- Se $c \in \mathbb{Z}$ t.c. $n|c$ e $m|c$ allora $M|c$

Indicheremo l'm.c.m. fra n ed m con le parentesi quadre: $[n, m]$

Teorema 15: *Unicità m.c.m.*
Siano $n, m \in \mathbb{Z}$. Supponiamo che $M, M' \in \mathbb{Z}$ siano m.c.m. fra n e m. Allora

$$M = M'$$

Teorema 16: *M.C.D. e m.c.m.*
Siano $n, m \in \mathbb{Z}$. Allora esiste ed e unico $[n, m]$ e vede:

- $n = m = 0, [n, m] = 0$
- Se n e m non sono entrambi nulli, allora:

$$[n, m] = \frac{nm}{(n, m)}$$

Dimostrazione esistenza e unicità m.c.m.

Partiamo ponendo

$$[n,m] = M = \frac{nm}{(n,m)}$$

con $n = n'(n,m)$ e $m = m'(n,m)$. Devo dimostrare che $n|M$ e $m|M$

$$M = \frac{nm}{(n,m)} = nm' = n'm$$

dunque è evidente che $n|M$ e $m|M$.

Devo ora dimostrare che per ogni c tale che $n|c, m|c$ allora $M|c$

- Dato che c è un multiplo comune, allora $(n,m)\,|c$
- Pongo $c = c'(n,m)$, quindi

$$\begin{cases} \dfrac{n}{(n,m)} = n'|c' = \dfrac{c}{(n,m)} & \text{in quanto } n|c \\ \dfrac{m}{(n,m)} = m'|c' = \dfrac{c}{(n,m)} & \text{in quanto } m|c \end{cases}$$

- Inoltre ho che $(n', m') = \left(\frac{n}{(n,m)}, \frac{m}{(n,m)}\right) = 1$
- Allora, mettendo insieme gli ultimi tre passi ho che $n'|c', m'|c', (n', m') = 1$, allora so che

  $$n'm'|c'$$

  e dunque

  $$M = n'm'(n,m)\,|c'(n,m) = c \Rightarrow M|c \quad \forall c$$

Poiché nella dimostrazione è stato posto $M = \frac{nm}{(n,m)}$ e abbiamo dimostrato che l'M.C.D. è unico, anche M è conseguentemente unico

6 Teorema fondamentale dell'aritmetica

All'interno di questo teorema si nasconde la ragione della sicurezza della crittografia rsa

Teorema 17: *Teorema fondamentale dell'aritmetica*
Ogni numero naturale $n \geq 2$ può essere fattorizzato in numero primi, ovvero può essere scritto come prodotto di numeri primi eventualmente ripetuti:

$$n = p_1 p_2 \dots p_a, \qquad \text{dove } p_i \text{ sono primi}$$

Nota che non possiamo usare le potenze (*non ancora*)

Nota che questa scrittura è unica a meno di ordinamento

$$n = q_1 q_2 \dots q_b, \qquad \text{dove } q_i \text{ sono primi e } b \geq 1$$

allora esiste una bigezione:

$$\Rightarrow \exists \text{ una bigezione } f : \{1, \dots, b\} \to \{1, \dots, a\}$$

ossia una scrittura è semplicemente una permutazione dell'altra

Dimostrazione esistenza

Procediamo per induzione di seconda forma shiftata in 2 (dobbiamo dimostrarlo $\forall n \geq 2$). Indico con $P(n)$ la proposizione *"il numero n si può scrivere come prodotto di numeri primi eventualmente ripetuti"*

- *Caso base*: per $n = 2$ è banale, basta sceglere la stringa composta da n stesso, ossia 2
- *Passo induttivo*: considero $P(k)$ vera $\forall 2 \leq k < n$, ossia suppongo di saper fattorizzare ogni numero da 2 a $n - 1$

Ora devo dimostrare che anche n è fattorizzabile

- Se n è primo allora vale quanto esplicitato nel caso base, ossia basta prendere n stesso come fattorizzazione elementare
- Se n non è primo allora questo ammette almeno un divisore non banale, che in uanto tale deve essere diverso da 1 e n, ossia

  $$n = d_1 d_2 \text{ t.c. } d_1, d_2 \in [2, n-1]$$

  dunque per ipotesi induttiva (dato che $d_1, d_2 \in [2, n-1]$) posso fattorizzare d_1 e d_2, ottenendo quindi:

  $$n = d_1 d_2 = (p_1, \dots, p_a) \cdot (q_1, \dots, q_2)$$

Dimostrazione unicità

Supponiamo per assurdo che esista $n \geq 2$ con due fattorizzazioni

$$p_1 \dots p_a = n = q_1 \dots q_b \qquad \text{per qualche } q_1 \dots q_b, p_1 \dots p_a \text{ primi}$$

dobbiamo dimostrare che

$$a = b \qquad p_i = q_i \forall i \in \{1, \dots, a\} \qquad \text{a meno di riordinamento}$$

procediamo per induzione di prima forma su $a \geq 1$. L'ipotesi induttiva sarà la seguente:

$$P(a) = \text{ data una stringa di } a \text{ numeri primi, questa è l'unica a rappresentare } n$$

- *Caso base*: per $a = 1$ so che $n = p_1 = q_1 q_2 \dots q_b$. Supponiamo per assurdo che $b \geq 2$. Allora vale che
$$p_1 = q_1 (q_2, \dots, q_b)$$
ciò vuol dire che q_1 divide p_1, il quale è però primo. quindi $q_1 \in \{+1, -1, +p_1, -p_1\}$. L'unica alternativa possibile tuttavia è p_1 in quanto q_1 è positivo e primo. quindi ho che:
$$p_1 = p_1 (q_2, \dots, q_b)$$
tuttavia essendo $(q_2, \dots, q_b)$ maggiori o uguali a 2 l'eguaglianza risulta impossibile. Ho dimostrato che $b = a = 1$

- *Passo induttivo*: considero $p_1 \dots p_a = q_1 \dots q_b$ Ancora una volta, so che $p_a | q_1 \dots q_b$, ma essendo $q_1, \dots, q_n$ primi allora necessariamente
$$p_a | q_j \quad \text{per qualche } j$$
Divido da entrambe le parti per p_a e ottengo:
$$p_1 \cdots p_{a-1} = q_1 \cdots q_{j-1} q_{j+1} \cdots q_b$$
e ricasco nell'ipotesi induttiva in quanto ho una stringa lunga $a - 1$. In queste due stringhe ho che
$$a - 1 = b - 1, \quad p_j = p_i$$
e inorltre ho dimostrato che $p_a = p_j$

Teorema 18: *Corollario*
L'insieme dei numeri primi è infinito

Dimostrazione

Supponiamo che esistano solamente un nummero finito di primi

$$p_1 = 2, p_2 = 3, p_3 = 5, \dots, p_m$$

dimostriamo che è impossibile che di punto in bianco i numeri primi cessino di esistere

- Se i numeri primi si stabilizzassero, potremmo definire un numero specifico nel seguente modo:
$$N := (p_1 p_2 \dots p_m) + 1 \in \mathbb{N} \quad N = (2 \cdot 3 \cdot 5 \cdot 7 \dots) + 1 \geq 2$$

- Visto che N è maggiore è uguale a 2 possiamo appicare il teorema fondamentale dell'aritmetica (teo 17)

- N è quindi il prodotto di alcuni numeri primi, ovvero $\{p_1, p_2, \dots, p_m\}$. Esiste dunque $i \in \{1, \dots, m\}$ tale che $p_i | N$, ovvero se divido N per p_i ottengo resto 0. Tuttavia questo è impossibile, in quanto se torniamo alla definizione di N abbiamo che:
$$N = (p_1 p_2, \dots, p_m) + 1 = p_i (p_1, \dots p_{i-1}, p_{i+1}, p_m) + 1$$
ossia la divisione con resto fra N e p_i ha resto 1, il che è in contrasto con quanto dimostrato

7 Classi d'equivalenza e moduli

Iniziamo qui a parlare di aritmetica modulare. Innanzitutto diamo la definizione di conguità:

Definizione 25: *Congruenza*
Siano $a, b \in \mathbb{Z}$. Si dice che a è congruo a b modulo n se

$$n|a-b$$

In simboli si scrive che $a \equiv b \mod n$

Nota che questa affermazione equivale a dire che a, b divisi per n danno lo stesso resto. Valgono quindi le seguenti proprietà:

- *Riflessiva* $a \equiv a \mod n$
- *Simmetrica* $a \equiv b \mod n \Leftrightarrow b \equiv a$
- *Transitiva* $A \equiv b \mod n$ e $b \equiv c \mod n \Leftrightarrow a \equiv c \mod n$

Le proprietà risultano evidenti se si pensa alla congruenza in modulo n come il fatto che a e b danno lo stesso resto divisi per n

La relazione di congruenza è detta d'equivalenza in quanto è riflessiva, simmetrica e transitiva:

Definizione 26: *Relazione d'equivalenza*
Una relazioe $\mathcal{R}$ su X si dice d'equipotenza se:

- E' *riflessiva* ossia $\forall x \in X \quad x\mathcal{R}x$
- E' *simmetrica* ossia $\forall x, y \in X \quad x\mathcal{R}y \Rightarrow y\mathcal{R}x$
- E' *transitiva* ossia $\forall x, y, z \in X \quad x\mathcal{R}y$ e $y\mathcal{R}z \Rightarrow x\mathcal{R}z$

Data una relazione di equivalenza e un insieme, si può creare una classe contenente tutti gli elementi che soddisfano tale relazione. Tale classe è detta classe di equivalenza.

Definizione 27: *Classe d'equivalenza*
Siano X un insieme, $\sim$ una relazione d'equivalenza su X e $x \in X$. Si chiama Classe d'equivalenza di x in X rispetto a $\sim$, l'insieme:

$$[x]_\sim \{y \in X | y \sim x\}$$

ossia l'insieme costituito da tutti gli elementi di X che soddisfano $x \sim y$

Definizione 28: *Insieme quoziente*
Siano X un insieme e $\sim$ una relazione di equivalenza su X. L'insieme costituito da tutte le classi d'equivalenza si chiama insieme quoziente di X modulo $\sim$ e si denota con il simobolo $X/\sim$:

$$X/\sim = \{[x]_\sim x \in X\}$$

Ci sono tre importanti proprietà delle classi d'equivalenza:

- Una classe di eqiuvalenza $[x]$ contiene sempre x stesso $\forall x \in X \quad x \in [x]$
- Due classi sono uguali se e solo se $\forall x, y \in X \quad [x] = [y] \Leftrightarrow x \sim y$
- $\forall x, y \in X \quad [x] \cap [y] \neq \emptyset \Rightarrow [x] = [y]$

Dimostrazione

1. Per la proprietà riflessiva di $\sim$ $x \sim x$, quindi $x \in [x]_\sim$
2. Doppia inplicazione
   - $\Leftarrow$: $y \in [y]$, ma essendo $[y] = [x]$ allora appartiene anche a $[x]$. Visto che appartiene ad $[x]$, per definizione $x \sim y$
   - $\Rightarrow$: Per ogni $z \in [x]$ vale che $z \sim x$ per def. Dato che $x \sim y$, allora $z \sim x \sim y \Rightarrow z \sim y$. Ogni z che sta in $[x]$ sta anche in $[y]$. Posso fare il ragionamento al contrario dimostrando che $[x] = [y]$
3. Se $z \in [y] \cap [x]$ allora $z \sim x$ e $z \sim y$. Per la proprietà transitiva $x \sim y$. Per proprietà 2 allora $[x] = [y]$

Nota che l'insieme quoziente su X è un insieme delle parti di X

Pensa che :

- Ogni suo insieme è disgiunto, per la proprietà 3
- L'unione di ogni insieme appartenente a $X/\sim$ da X, in quanto nel peggiore dei casi, per proprietà 1, ogni insieme $[x]$ sarebbe un singoletto contenente x stesso
- Ogni insieme $[x]$ è non vuoto in quanto contiene almeno x stesso

7.1 Classi di congruenza

Una classi di congruenza su $\mathbb{Z}$ è un insieme contenente tutti i numeri interi che danno lo stesso resto divisi per n.

Definizione 29: *Classe di congruenza*
Siano $a, n \in \mathbb{Z}$. Si chiama classe di congruenza di a modulo n l'insieme dato da:

$$[a]_n = \{x \in \mathbb{Z} | x \equiv a \mod n\}$$

Indicheremo con $\mathbb{Z}/n\mathbb{Z}$ l'insieme dato da tutte le classi di congruenza di modulo n:

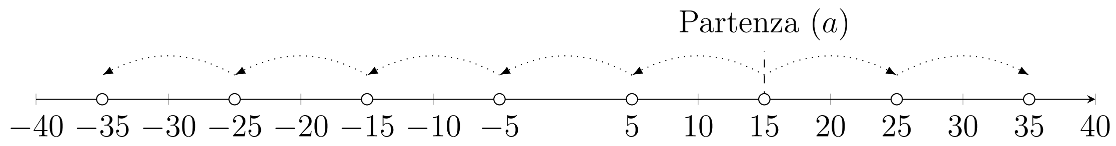
$$\mathbb{Z}/n\mathbb{Z} = \{[a]_n \, | a \in \mathbb{Z}\}$$

Per visualizzare una *classe di congruenza* si può usare un metodo efficace per costruirne una:

- Prendi l'asse dei numeri interi $\mathbb{Z}$
- Prendi a su tale asse

- Segna ogni punto a distranza di kn rispetto ad a, ossia i punti $a + kn$

Classe $[15]_1$ 0



Questo "processo costruttivo intuitivo" può essere formalizzato come segue:

$$x \equiv a \mod n \Leftrightarrow n|\,(x-a) \Leftrightarrow \exists k \in \mathbb{Z} : x - a = kn \Leftrightarrow \exists k \in \mathbb{Z} : x = a + kn$$

quindi

$$[a]_n = \{aj + kn | k \in \mathbb{Z}\}$$

> Osservazione: la classe $[a]_n$ è la <u>classe di equivalenza</u> rispetto alla relazione di equivalenza di modulo n, mentre $\mathbb{Z}/n\mathbb{Z}$ è <u>l'insieme quoziente</u> di $\mathbb{Z}$ rispetto a tale relazione

Valgono di conseguenza le tre proprietà già enunciate e dimostrate:

- $\forall a \in \mathbb{Z} \quad a \in [a]_n$
- $\forall a, b \in \mathbb{Z} \quad [a]_n = [b]_n \Leftrightarrow a \sim b$
- $\forall a, b \in \mathbb{Z} \quad [a]_n \cap [b]_n \neq \emptyset \Rightarrow [a]_n = [b]_n$

7.2 Numero classi congruenza

Innanzitutto va esplicitata una proposizione intuitiva:

> **Teorema 19:** *Resto classi di congruenza*
> Se $n > 0$ e rè il resto della divisione euclidea di a per n allora.
>
> $$a \equiv r \mod n$$

Ciò è molto importante quando si parla di classi di equivalenza: se $r = \text{ resto}\,(a/n)$ allora

$$[a]_n = [r]_n$$

E' intuitivo pensare che le classi di congruenza di modulo n siano esattamente n.

$$\boxed{\mathbb{Z}/n\mathbb{Z} \text{ ha } \underline{\text{esattamente}}\ n \text{ elementi}}$$

Formalmente, ciò si dimostra nel modo seguente:

- Dato un $n \in \mathbb{Z}$ avrò esattamente n possibili resti e dunque n <u>classi di congruenza</u>:

  $$[0,]_n, [1]_n, \ldots, [n-1]$$

- Queste classi non possono essere le stesse, in quanto dati h, k distinti, i quali possono assumere il valore di ongi possibile resto, ho che:
  - $0 \leq h < k < n$
  - La differenza $k - h$ è al più $n - 1$, in quanto questi variano in $[0, m)$, quindi $n \not| (k - h) \Rightarrow k \neq h \mod n$. Per questa ragione $[h]_n \neq [k]_n$

7.3 Somma e prodotto di classi di congruenza

E' possibile definire somma e prodotto di classi di congruenza: questo ci è estremamente utile in quanto possiamo eseguire operazioni in $\mathbb{Z}/n\mathbb{Z}$, il quale è un insieme limitato.

Definizione 30: *Somma e prodotto di classi di congruenza*

- La *somma* è così definita:
$$[a]_n + [b]_n = [a+b]_n$$
- Il *prodotto* è così definito:
$$[a]_n \, [b]_n = [ab]_n$$

Questo ha senso in quanto permette di operare con numeri $< n$. Questa definizione equivale con le seguenti proprietà:

- $a \mod n + b \mod n = (a+b) \mod n$
- $(a \mod n)\,(b \mod n) = (ab) \mod n$

D'ora in poi, quando si parlerà di classi di congruenza, si useranno le seguenti notazioni, tutte equivalenti:

$$3 + 3 \equiv 0 \mod 6$$
$$[2]_6 + [3]_6 = [0]_6$$
$$3 + 3 = 0 \text{ in } \mathbb{Z}/6\mathbb{Z}$$

7.4 Proprietà operazioni su classi di congruenza

- $([a] + [b]) + [c] = [a] + ([b] + [c])$
- $([a][b])[c] = [a]([b][c])$
- $[a] + [b] = [b] + [a]$
- $[a][b] = [b][a]$
- $[a] + [0] = [a]$
- $[a] + [-a] = [0]$
- $[a][1] = [a]$
- $[a]([b] + [c]) = ([a][b]) + ([a][c])$

Osservazione

L'esercizio precedente, mostra che le operazioni tra classi di congruenza godono delle stesse proprietà di cui godono le operazioni tra interi. Attenzione però a due importanti differenze: *somma e moltiplicazione di interi non nulla può essere nulla*

$$2 \cdot 3 = 0 \text{ in } \mathbb{Z}/6\mathbb{Z}$$

$$\underbrace{1+1+\cdots+1}_{n\text{-volte}} = 0 \text{ in } \mathbb{Z}/n\mathbb{Z}$$

7.5 Teorema cinese del resto

Teorema 20: *Teorema cinese del resto*
Siano $n, m > 0$ e siano $a, b \in \mathbb{Z}$. Consideriano:

$$\begin{cases} x \in \mathbb{Z} \\ x \equiv a \mod n \\ x \equiv b \mod m \end{cases} \Leftrightarrow \begin{cases} [x]_n = [a]_n \\ [x]_m = [b]_m \end{cases}$$

Tale sistema è detto sistema delle congruenze. Indichiamo con S l'insieme delle soluzioni di tale sistema

$$S = \{x \in \mathbb{Z} | x \equiv a \mod n \text{ e } x \equiv b \mod m\}$$

Allora so che :

- Il sistema ha soluzione se e solo se

$$(n, m) \,| a - b$$

- Il sistema ha insieme delle soluzioni uguale a

$$S = [c]_{[n,m]} \to c + k\,[n, m]$$

Dimostrazione condizione affinchè esistano soluzioni

- **Dimostrazione** $\Leftarrow$
  - Sappiamo che $(n, m)\,| a - b$
  - Sappiamo che l'M.C.D. può essere scritto come combinazione lineare:

$$(n, m) = xn + ym \quad \text{per qualche } x, y \in \mathbb{Z}$$

  - Quindi $xn + ym | a - b \to k\,(xn + ym) = a - b$
  - Ottengo la seguente eguaglianza:

$$kxn + kym = a - b$$

  quindi se definisco la quantità c come segue:

$$c = b + (kx)\,n = a + (-ky)\,m$$

  avrò che c soffisfa il sistema di congruenze

- **Dimostranzione** $\Rightarrow$
  - Visto che c è una soluzione del sistema ho che
$$c = a + xn = b + ym$$
  - Giro l'uguaglianza:
$$a - b = ym - xn$$
  - Noto che $(n, m) \,| ym - xn$ e dunque anche $a - b$

Dimostrazione forma insieme delle soluzioni

Devo ora dimostrare che se ho delle soluzioni, queste stanno in $[c]_{[n,m]}$ e che, viceversa, ogni elemento di $[c]_{[n,m]}$ sta nelle soluzioni $S = \{x \in \mathbb{Z} | x \text{ risolve il sistema } \}$. In poche parole devo dimostrare la reciproca inclusione degli insiemi:

$$S = \{x \in \mathbb{Z} | x \text{ risolve il sistema } \} \text{ e } [c]_{[n,m]}$$

- **Dimostrazione** $\Rightarrow$:
  - Considero due soluzioni generiche:
$$c = kn + a = hm + b$$
$$c' = k'n + a = h'm + b$$
  - Considero la differenza delle soluzioni nei due modi seguenti:
$$c - c' = kn + a - k'n - a = n\,(k - k') \Rightarrow n|\,(c - c')$$
$$c - c' = hm + b - h'm - b = m\,(h - h') \Rightarrow m|\,(c - c')$$
  - Detto ciò, per definizione, l'm.c.m. fra n, m è il multiplo comune che didive tutti gli altri multipli comuni di n, m. Per questo
$$[n, m]\,|c - c' \Rightarrow c \equiv c' \mod [n, m]$$
  - Vista l'arbitrarietà nella scelta di c', posso affermare che ogni soluzione $\subseteq [c]_{[n,m]}$
- **Dimostrazione** $\Leftarrow$
  - Considero un generico elemento di $c' \in [c]_{[n,m]}$. Questo elemento avrà forma del tipo:
$$c' = c + h\,[n, m]$$
  - Dimostro che $c' \equiv a \mod n$:
$$c \equiv a \mod n \quad \text{in quanto } c \text{ è soluzione}$$
$$h\,[n, m] \equiv 0 \mod n \quad \text{in quanto } [n, m] \text{ è multiplo di } n$$
    quindi per proprietà dei moduli
$$c' \equiv a \mod n$$
  - Lo stesso discorso può essere fatto per m dimostrando che $c' \equiv b \mod m$

Esercizio interessante

Dimostra che un numero n è divibile per 3 se e solo se la somma delle sue cifre è divisibile per 3:

$$3|n \Leftrightarrow 3|\left(\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_k\right)$$

dove ε_k è la k-*esima* cifra.

- Scriviamo n nel seguente modo:

$$n = \sum_{i=0}^{i=k} \varepsilon_i 10^k$$

- Sottraiamo e sommiamo 1 nel seguente modo:

$$n = \sum_{i=0}^{i=k} \varepsilon_i \left(10^k - 1 + 1\right) = \sum_{i=0}^{i=k} \varepsilon_i \left(10^k - 1\right) + \varepsilon_i = \left[\sum_{i=0}^{i=k} \varepsilon_i \left(10^k - 1\right) + \sum_{i=0}^{i=k} \varepsilon_i\right]$$

- Se ora dimostro che $10^k - 1$ è sempre divisibile per 3 sono a cavallo. Intuitivamente ha senso, basti pensare che

$$\begin{aligned} 10^2 - 1 &= 99 \\ 10^3 - 1 &= 999 \\ 10^4 - 1 &= 9999 \\ &\vdots \end{aligned}$$

  Formalmente, tuttavia la dimostrazione procede nel seguente modo:

  - Scrivo 10 come 9+1
  $$10^k - 1 = (9+1)^k - 1$$
  ed applico il binomio di newwtoon per eseguire la potenza:
  $$(9+1)^k - 1 = \left[\sum_{i=0}^{i=k} \binom{k}{i} \cdot 9^i \cdot 1^{k-i}\right] - 1$$
  - Per ogni termine della sommatoria, avrò un fattore che è una potenza di 9, quindi ogni fattore è divisibile per 3, ad eccezione del termine per $i = 0$, il quale è uguale ad 1
  - La sommatoria è dunque uguale a, considerando che il primo termine è 1:
  $$\left[1 + \sum_{i=1}^{i=k} \binom{k}{i} \cdot 9^i \cdot 1^{k-i}\right] - 1 = \sum_{i=1}^{i=k} \binom{k}{i} \cdot 9^i \cdot 1^{k-i}$$
  - Dunque ogni termine della sommatoria contiene una potenza di 9. <u>L'intera sommatoria è divisibile per 3</u>
  $$10^k - 1 = \sum_{i=1}^{i=k} \binom{k}{i} \cdot 9^i \cdot 1^{k-i} \Rightarrow 3|10^k - 1$$

- Ritornando alla dimostrazione di prima, ho che
$$n = \left[\sum_{i=0}^{i=k} \varepsilon_i \left(10^k - 1\right) + \sum_{i=0}^{i=k} \varepsilon_i\right]$$
Ma abbiamo dimostrato che la sommatoria a sinistra è divisibile per 3, dunque la somma delle sommatorie sarà divisibile per 3 se e solo se anche la sommatoria di destra è divisibile per 3. La sommatoria di destra è la somma delle cifre di n

In maniera analoga potremmo dimostrare che
$$9|n \Leftrightarrow 9|\left(\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_k\right)$$
o che
$$11|n \Leftrightarrow 11|\left(\varepsilon_0 - \varepsilon_1 + \ldots + (-1)^k \varepsilon_k\right)$$

7.6 Esempio esercizio con teorema cinese del resto

Si determinino tutte le soluzione del seguente sistema di congruenze:
$$\begin{cases} x \equiv 33 \mod 77 \\ x \equiv -2 \mod 56 \end{cases}$$
si dimostri inoltre che tutte le soluzioni sono divisibili per 11

Segui questi passi

- Verifica che il sistema sia compatibile verificando che $(n, m)\,|a - b$
- Trova una soluzione particolare:
  - Lancia Euclide e trova (n, m) come combinazione lineare di n, m
  - Visto che il sistema è compatibile, sappiamo che $(n, m)\,|a - b \to a - b = k\,(n, m) = kn + km$
  - Girando quest'ultima equazione è evidente che
  $$c = a - kn = b + km$$
  è una soluzione
- Trova classe soluzioni sapendo che se c è solzuione, allora $S = [c]_{[n,m]}$

Compatibilità

- Secondo il teorema cinese del resto il sistema è compatibile se e solo se :
$$(n, m)\,|a - b \to (77, 55)\,|35$$
- Trovo (n, m) tramite euclide:
$$\begin{aligned} 77 &= 1 \cdot 56 + 21 \\ 56 &= 2 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + \underbrace{7}_{\text{M.C.D.}} \\ 14 &= 2 * 7 + 0 \end{aligned}$$
- Visto che $(m, n) = 7|35$ il sistema è compatibile

Soluzione particolare

Per trovare una soluzione particolare del sistema devo applicare la sostituzione arritroso di euclide:

$$\begin{aligned} 77 &= 1 \cdot 56 + 21 \\ 56 &= 2 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 * 7 + 0 \end{aligned} \qquad \begin{aligned} 21 &= 77 - 1 \cdot 56 \\ 14 &= 56 - 2 \cdot 21 \\ 7 &= 21 - 1 \cdot 14 \end{aligned}$$

$$7 = 21 - 14 = 21 - [56 - 2 \cdot 21] = (77 - 1 \cdot 56) - [56 - 2 \cdot (77 - 56)] = -4 \cdot 56 + 3 \cdot 77$$

Dunque, ho che

$$\begin{aligned} 33 - (-2) = 5 \cdot 7 &= 5 \cdot (-4 \cdot 56 + 3 \cdot 77) \\ &= -20 \cdot 56 + 15 \cdot 77 \end{aligned}$$

Girando l'equazione ottengo che

$$c = 33 + (-15) \cdot 77 = -2 + (-20 \cdot 56) = -1122$$

Insieme soluzioni

Dato che

$$S = [c]_{[m,n]}$$

è subito fasso dato che :

$$[56, 77] = \frac{56 \cdot 77}{(77, 56)} = 616$$

allora

$$S = [c]_{[77,56]} = [-1122]_{616} = \{-1122 + k \cdot 616 | k \in \mathbb{Z}\}$$

8 Inversi modulari

Definizione 31: *Inverso modulare*
Sia $x \in \mathbb{Z}$. Diremo che a è <u>invertibile</u> *modulo* n se esiste un $x \in \mathbb{Z}$ tale che $ax \equiv 1 \mod n$. x è detto <u>inverso</u> di a *modulo* n

Teorema 21: *Condizione invertibilità modulare*
a è <u>invertibile</u> *modulo* n se e solo se:

$$(a, n) = 1$$

Una proprietà importante dei numero invertibili modulo n è la seguente. Se u è invertibile, allora

$$ux = uy \Leftrightarrow x = y$$

in quanto

$$ux = uy \to u^{-1}ux = u^{-1}uy \to x = y$$

Nota che questo non è necessariamente vero se u non è primo:

$$3 \cdot 2 \equiv 2 \cdot 0 \mod 6 \text{ tuttavia } 2 \neq 0 \mod 6$$

Dimostrazione

- $\Rightarrow$
  - Se $(a, n) = 1$ allora per teorema **??**, posso scrivere l'M.C.D. come combinazione lineare:
  $$(a, n) = 1 = ax + ny$$
  - Se applico il modulo da entrambe le parti ottengo che $ax \equiv 1 \mod n$
  $$[1]_n = [ax + ny]_n = [ax]_n + [ny]_n = [ax]_n + [0]_n = [ax]_n$$
- $\Leftarrow$
  - Se x è un inverso di $a \mod n$, allora $ax \equiv 1 \mod n$
  - Ciò vuol dire che $ax = nk + 1$ ossia $n|ax - 1$
  - Dunque $ax - 1 = nk \rightarrow 1 = ax - nk$
  - Per teorema **??**, $(a, b) = 1 \Leftrightarrow 1 = xa + yb$

Teorema 22: *Unicità inverso modulare*
Siano x, y due inversi di $a \mod n$, allora $x = y \mod n$. La classe che costituisce l'insieme degli inversi modulari verrà denotata con
$$[a]_n^{-1}$$

NB: più che l'unicità, questo teorema sancisce il fatto che gli inversi modulo n costituiscano una classe di congruenza

Dimostrazione

- Tengo in mente che $[ax]_n = [1]_n$ in quanto x è inverso di $a \mod n$Tengo in mente che $[ax]_n = [1]_n$ in quanto x è inverso di $a \mod n$
- Applico proprietà moduli:
$$[y]_n = [1]_n [y]_n = ([a]_n [x]_n) [y]_n = [x]_n ([a]_n [y]_n) = [x]_n [1]_n = [x]_n$$

8.1 Sistemi lineari

Possiamo "generalizzare" quanto affermato per gli inversi modulari, tramite il segtuente teorema:

Teorema 23: *Sistemi lineari modulari*
Siano $a, b \in \mathbb{Z}$, allora esiste un intero x tale che:
$$ax \equiv b \mod n$$
se e solo se $(a, n) | b$. Se x_0 è soluzione del sistema, allora l'insieme delle soluzioni è dato da:
$$[x_0]_{n'} = \{x0 + kn' | k \in \mathbb{Z}\} \qquad \text{con } n' = \frac{n}{(a, n)}$$

Dimostrazione

- $\Rightarrow$
  - Se esiste una soluzione x tale che $ax \equiv b \mod n$ allora $n|ax-b$ per definizione
  - Per questa ragione $ax - b = kn \rightarrow b = ax - kn$
  - Visto che tali combinazioni lineari sono tutti e soli i multipli di (a, n) allora $(a, n)\,|b$
- $\Leftarrow$
  - Sappiamo che $(a, n)\,|b$
  - Scriviamo (a, n) come combinazione lineare: $(a, n) = xa + yn$
  - Visto che $(a, n)\,|b$ allora $b = k\left((a, n)\right) = k\left(xa + yn\right)$
  - Giro equivalenza $b = kxa + kyn \rightarrow kyn = b - kxa$
  - Cio significa che $b - kxa = kyn$ è divisibile per n, dunque kx è una soluzione

Dimostrazione insieme soluzioni

- $\Rightarrow$
  - Se $x_1 \in [x_0]_{n'}$ allora $x_1 = x_0 + k\frac{n}{(a,n)}$
  - Se moltiplico per a da entrambe le parti ottengo: $ax_1 = ax_0 + a\frac{kn}{(a,n)}$ ossia $ax_1 - ax_0 = a\frac{kn}{(a,n)}$
  - Cio significa che $n|ax_1 - ax_0$, ossia, per definizione, $ax_1 \equiv ax_0 \mod n$
  - Visto che per ipotesi x_0 è una soluzione dell'equazione, allora $ax_1 \equiv ax_0 \equiv b \mod n$. Per proprietà transitiva $ax_0 \equiv ax_1 \mod n$
- $\Leftarrow$
  - Siano x_1 e x_2 due soluzioni
  - Avrò che $n|\left(ax_1 - ax_2\right) = kn$ per definzione di congruenza modulare
  - Avrò dunque che $\frac{a}{(a,n)}\left(x_1 - x_2\right) = k\frac{n}{(a,n)} = kn'$
  - Quindi $n'|\frac{a}{(a,n)}\left(x_1 - x_2\right)$. Tuttavia è impossibile che $n'|\frac{a}{(a,n)}$. L'unica opzione è che
$$n'|x_1 - x_2, \text{ ossia } x_1 \equiv x_2 \mod n'$$

Nota bene: la prima parte della dimostrazione ci da un algoritmo per ricavare una soluzione particolare del sistema

In particolare, per trovare una soluzione particolare bisogna:

- Calcolare (a, n)
- Per teo **??**, $(a, n) = \alpha a + \beta n$
- Se il sistema ha soluzioni, allora $(a, n)\,|b$ (vedi teo 23)
- Dunque $(a, n) = \alpha a + \beta n|b \rightarrow k\left(\alpha a + \beta n\right) = b$
- Girando l'equazione ottengo che $k\beta n = b - k\alpha a$. Di conseguenza $k\alpha$ è una soluzione

8.2 Esempi calcolo inversi modulari

Esercizio 1

Si dica se 21 è invertivile $\mod 30$ e in caso affermativo calcolare tutti gli interi inversi di 21 $\mod 30$

- Uso il teorema ?, per il quale a è invertibile $\mod b \Leftrightarrow (a,b) = 1$

$$(21,30) = 3 \rightarrow \text{ non è inveritibile}$$

Esercizio 2

Si dica se 11 è invertibile $\mod 30$ e in caso affermativo calcolare tutti gli inveri inveri di 11 $\mod 30$

- Visto che 11 è un numero primo e 11 non divide 30, allora

$$(11,30) = 1 \rightarrow \text{ sono comprimi}$$

- Applichiamo *Euclide* a 11 e 30:

$$\begin{aligned} 30 &= 2 \cdot 11 + 8 \\ 11 &= 1 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned} \qquad \begin{aligned} 8 &= 30 - 2 \cdot 11 \\ 3 &= 11 - 1 \cdot 8 \\ 2 &= 8 - 2 \cdot 3 \\ 1 &= 3 - 1 \cdot 2 \end{aligned}$$

sostituendo a ritroso ottengo che:

$$(11,30) = 1 = 11 \cdot 11 - 4 \cdot 30$$

- Applico il modulo da entrambe le parti:

$$[(11,30)]_{30} = [1]_{30} = [11 \cdot 11 - 4 \cdot 30]_{30} = [11 \cdot 11]_{30} = [11]_{30} \cdot [11]_{30}$$

quindi in questo caso l'inverso modulare di 11 in modulo 30 è 11

Eserzicio 3

Calcola $[8]_{35}^{-1}$

- E' invertibile:

$$(8,35) = 1 \rightarrow \text{ sono coprimi}$$

- *Euclide:*

$$\begin{aligned} 35 &= 4 \cdot 8 - 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned} \qquad \begin{aligned} 3 &= 35 - 4 \cdot 8 \\ 2 &= 8 - 2 \cdot 3 \\ 1 &= 3 - 1 \cdot 2 \end{aligned}$$

quindi risolvendo arritroso:

$$(8,35) = 1 = 3 \cdot 35 - 13 \cdot 8$$

- Applico modulo da entrambe le parti:

$$[(8,35)]_{35} = [1]_{35} = [3 \cdot 35 - 13 \cdot 8]_{35} = [-13 \cdot 8]_{35} = [-13]_{35} \cdot [8]_{35}$$

quindi l'inverso modulare di 8 in modulo 35 è -13

8.3 Classi invertibili

Definizione 32: *Insiemi classi invertibili*
Dato $n \in \mathbb{N} > 0$ indichiamo con $(\mathbb{Z}/_{n\mathbb{Z}})^*$ l'insieme di tutti gli interi modulo n, cioè $[a]_n \in \mathbb{Z}/_{n\mathbb{Z}}$ che siano invertibili in $\mathbb{Z}/_{n\mathbb{Z}}$

Teorema 24: *Classi invertibili modulo numero primo*
Se p è un numero primo, allora l'insieme delle classi invertibili modulo p è costituito da tutte le classi modulo p, tranne $[0]_p$:

$$(\mathbb{Z}/_{p\mathbb{Z}})^* = \mathbb{Z}/_{p\mathbb{Z}} \setminus \left\{[0]_p\right\}$$

- $[0]_p \notin (\mathbb{Z}/_{p\mathbb{Z}})$ in quanto non può esistere un $x \in \mathbb{Z}$ tale che :

$$[x]_p \cdot [0]_p = [1]_p$$

- Ogni altra classe $[c]_p$ è invertibile in quanto (c,p) e sempre 1 in quanto:
  - $c < p$
  - p è primo

Teorema 25: *Invertibilità prodotto*
Siano $u, v \in \mathbb{Z}/_{n\mathbb{Z}}$ allora $uv \in \mathbb{Z}/_{n\mathbb{Z}}$

Un'importantissima conseguenza di questo teorema è il fatto che la funzione $L_u : \mathbb{Z}/^*_{n\mathbb{Z}} \to \mathbb{Z}/^*_{n\mathbb{Z}}$ che manda $x \in \mathbb{Z}/^*_{n\mathbb{Z}}$ in ux è una bigezione.

- u è invertibile in quanto $u \in \mathbb{Z}/^*_{n\mathbb{Z}}$
- $L_u(x_1) = L_u(x_2)$ significa che $ux_1 = ux_2$. Visto che u è invertibile, questo è vero se e solo se $x_1 = x_2$ vedi questa proprietà

Definizione 33: *Phi di eulero*
Detiniamo la funzione $\phi : \mathbb{N} \setminus \{0\} \to \mathbb{N}$, detta *"phi" di Eulero*,

$$\phi(n) := |\{a \in \mathbb{Z} | 1 \le a \le n, (a,n) = 1\}|$$

ossia il numero di numeri comprimi con n compresi fra 1 e n

Proprietà 1

- $\phi(1) = |\{1\}| = 1$
- $\phi(2) = |\{1\}| = 1$
- $\phi(4) = |\{1, 3\}| = 2$
- $\phi(8) = |\{1, 3, 5, 7\}| = 4$

allora viene da chiedersi se sia vero che $\phi(ab) = \phi(a)\phi(b)$. Tale proprietà viene detta moltiplicatività. La risposta, tuttavia è no.

$$\phi(2 \cdot 4) = \phi(8) = 4$$

$$\phi(2)\phi(4) = 1 \cdot 2 = 2 \neq 4$$

tuttavia vale la seguente proprietà importantissima:

$$\boxed{\text{La } \phi \text{ di } \textit{Eulero} \text{ è moltiplicativa per coppie di numeri comprimi}}$$

quindi vale che

$$\phi(ab) = \phi(a)\phi(b) \Leftrightarrow a, b \text{ comprimi}$$

tale proprietà si dimostra con il teorema cinese del resto in modo molto elegante

Proprietà 2

$$\boxed{\phi(p^m) = p^m - p^{m-1} \text{ se } p \text{ è un numero primo}}$$

$$\begin{aligned}
\phi(p^m) &= |\{a \in \mathbb{Z} | 1 \leq a \leq p^m, (a, p^m) = 1\}| \\
&= |\{a \in \mathbb{Z} | 1 \leq a \leq p^m, (a, p) = 1\}| \\
&= |\{1, 2, \ldots, p^m\} \setminus \{a \in \mathbb{Z} | 1 \leq a \leq p^m, (a, p) \neq 1\}| \\
&= \left|\{1, 2, \ldots, p^m\} \setminus \left\{1 \cdot p, 2 \cdot p, \ldots, p^{m-1} \cdot p\right\}\right| \\
&= p^m - p^{m-1}
\end{aligned}$$

Teorema 26: *Teorema di Fermat-Eulero*
Sia $u \in \mathbb{Z}/_{n\mathbb{Z}}^*$, allora $u^{\phi(n)} = 1$ (in $\mathbb{Z}/_{n\mathbb{Z}}$)

Dimostrazione

Come enunciato qui, la funzione $L_u(x) = ux$ è una bigezione. Dunque procedo così

- Siano $x_1, \ldots, x_k$ gli elementi di $\mathbb{Z}/_{n\mathbb{Z}}^*$
- Visto che L_u è una bigezione, se applico tale funzioni a tutti gli elementi dell'insieme su cui è definita, allora otterrò sempre lo stesso insieme come immagine:

$$x_1 x_2 \ldots x_k = ux_1 ux_2 \ldots ux_k = u^k x_1 x_2 \ldots x_k$$

- $u^k = 1$ per soddifare l'eguaglianza. Tuttavia vale anche che $u^k = u^{\phi(n)}$ in quanto $\phi(n) = |\mathbb{Z}/_{n\mathbb{Z}}^*|$

Nota che se p è primo, allora $x^{p-1} = x^{\phi(p)} = 1$ in $\mathbb{Z}/_{p\mathbb{Z}}$, in quanto $\phi(p) = p - 1$ (*tutti* i numeri minori di p sono comprimi con p se p è primo)

Teorema 27: *Phi di eulero numeri comprimi*
La *phi di Eulero* è moltiplicativa solo per coppie di numeri comprimi:

$$\phi(ab) = \phi(a)\phi(b) \Leftrightarrow a, b \text{ comprimi}$$

Osservazine 2

Calcoliamo $\phi(p^m)$ dove p è un numero primo:

- Per definzione:
$$\phi(p^n) = |\{x \in \mathbb{Z} | 1 \leq z \leq p^m, (a, p^m) = 1\}|$$
- I divisori di p^m saranno solamente $p^1, p^2, \ldots, p^m$
- Per questa ragione posso calcolare la phi di Eulero nel seguente modo: i

Teorema 28: *Formula generale calcolo ϕ di eulero*
Sia $n \geq 2$. Se $n = p_1^{m_1} p_2^{m_2}, \ldots, p_k^{m_k}$ dove $p_1, p_2, \ldots, p_k$ sono comprimi a due a due e $m_1, \ldots, m_k > 0$ allora

$$\begin{aligned}\phi(n) &= \phi\left(p_1^{m_1} p_2^{m_2}, \ldots, p_k^{m_k}\right) = \phi\left(p_1^{m_1}\right)\phi\left(p_2^{m_2}\right)\ldots\phi\left(p_k^{m_k}\right) \\ &= \left(p_1^{m_1} - p_1^{m_1-1}\right)\left(p_2^{m_2} - p_2^{m_2-1}\right)\ldots\left(p_k^{m_k} - p_k^{m_k-1}\right)\end{aligned}$$

8.4 Crittografia RSA

Tutto ciò dimostrato finora serve a dimostrare il teorema alla base della crittografia RSA.

Teorema 29: *Teorema base crittografia RSA*
Sia c coprimo con $\phi(n)$, allora l'applicazione $C : \mathbb{Z}/_{n\mathbb{Z}}^* \to \mathbb{Z}/_{n\mathbb{Z}}^*$ definita da $x \to x^c$ è invertibile e la sua inversa è data da $D(x) = x^d$

$$C(x) = x^c \qquad D(x) = C^{-1}(x) = x^d$$

dove d è l'inverso modulo $\phi(n)$ di c, ossia $cd \equiv 1 \mod \phi(n)$

Dimostrazione

- Visto che vale $cd \equiv 1 \mod \phi(n)$ allora $cd = k\phi(n) + 1$
- Avrò che
$$D(C(x)) = (x^x)^d = x^{cd} = x^{k\phi(n)+1} = \left(x^{\phi(n)}\right)^k \cdot x = x \cdot 1^k = x$$

- Lo stesso idendico ragionamento può essere fatto per provare che $C(D(x)) = x$

Esempio

Si calcolino tutte le soluzioni dell'equazione:

$$x^{11} \equiv 35 \mod 38$$

Devo verificare due condizioni per poter applicare la Crittografia RSA. Se questa non è applicabile diventa difficilissimo trovare l'insieme delle soluzioni

- $(35, 38) = 1$ in quanto 35 deve appartenere a $\mathbb{Z}/^{*}_{n\mathbb{Z}}$. ✓
- $(11, \phi(38)) = 1$
  - Calcolo $\phi(38)$ tramite proprietà di ϕ di Eulero:

    $$\phi(38) = \phi(2 \cdot 19) = \phi(2) \cdot \phi(19) = 1 \cdot 18 = 18$$

  - $(11, 18) = 1$ ✓

Ora tengo in considerazinoe il teorema fondamentale della crittografia RSA. Data $C(x) = x^{11}$ e $D(x) = C^{-1}(x) = x^d$ so che

$$C(x) = 35$$

quindi applicando l'inversa trovo x:

$$C(x) = x^{11} = 35 \to D(35) = x$$

quindi mi rimane solo da calcolare l'inverso di $c \mod \phi(n)$

$$(11, 18) = 1 = 5 \cdot 11 - 3 \cdot 18$$

ora trovo l'inverso di $c = 11$

$$[1]_{\phi(18)} = [5 \cdot 11 - 3 \cdot 18]_{\phi(38)} = [5 \cdot 11]_{\phi(38)} = [5]_{\phi(38)} [11]_{\phi(38)}$$

quindi 5 è l'inverso di 11 $\mod \phi(38)$. L'insieme delle soluzioni è dato da $[35^5]_{38}$. Per ridurre al rappresentante canonico, posso o eseguire il conto, oppre procedere come segue:

$$\left[35^5\right]_{38} = [35]_{38}^5 = \left[-3^5\right]_{38} = [-243]_{38} = [23]_{38}$$

Esempio 2

Si risolva la seguente equazione:

$$x^9 \equiv 49 \mod 60$$

- $(49, 60) = 1$. ✓
- $(9, \phi(60)) = (9, 16) = 1$. ✓

L'inverso modulare di 9 è 9 stesso. L'insieme delle soluzioni è:

$$S = \left[49^9\right]_{60}$$

9 Grafi

Definizione 34: *2-sottoinsieme*
Dato un insieme V, indichiamo con

$$\binom{V}{2} := \left\{A \in 2^V \,|\, |A| = 2\right\}$$

ossia tutti gli insiemi di due elementi che si possono costruire da V. Un sottoinsieme contenente n elementi viene detto *n-sottoinsieme*

Teorema 30: *Cardinalità 2-sottoinsieme*
Considero un 2-sottoinsieme $\binom{V}{2}$. Allora

$$\left|\binom{V}{2}\right| = \binom{|V|}{2} = \frac{|V|\left(|V| - 1\right)}{2}$$

Possiamo ora dare definizione formale di grafo:

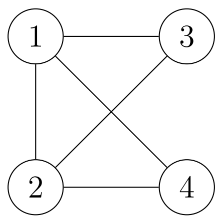
Definizione 35: *Grafo*
Un grafo G è una coppia ordinata (V, e), dove V è un insieme non vuoto, detto insieme dei vertici di G, mentre e è un sottoinsieme di $\binom{V}{2}$. ϵ è detto insieme dei lati di G

Spesso indicheremo con $V\left(G\right)$ l'insieme dei vertici, mentre $E\left(G\right)$ l'insieme dei lati

Esempio

$$G\left(V, e\right)$$

$$V = \{1, 2, 3, 4\} \quad e = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}\}$$



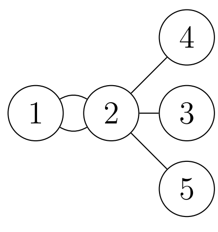


Figura 1: Questo non è un grafo

9.1 Sottografi

Definizione 36: *Sottografo*
Siano $G = (V, E)$ e $G' = (V', E')$ due grafi. Diciamo che G' è un sottografo di G se $V' \in V$ e $E' \subset E$

Definizione 37: *Sottografo indotto*
Siano $G = (V, E)$ un grafo. Diciamo che G' è un sottografo di G indotto da V'

$$G[V'] = \left(V', E \cap \binom{V'}{2}\right)$$

9.2 Morfismi di grafi

Definizione 38: *Morfismo di grafo*
Siano $G(V, E)$ e $G' = (V', E')$. Una $f : V \to V'$ una funzione iniettiva si dice morfismo da G in G' se preserva i lati

Definizione 39: *Isomorfismo di grafo*
Siano $G(V, E)$ e $G' = (V', E')$. Una $f : V \to V'$ una funzione iniettiva si dice isomorfismo da G in G' se:

- f è bigettiva
- f è un morfismo
- $f^{-1} : V(G') \to V(G)$ è un morfismo

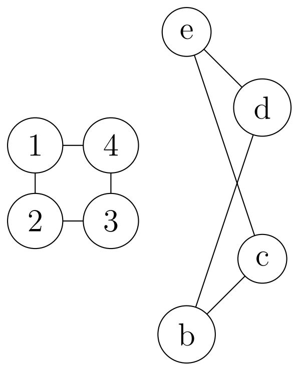
se esiste un isomorfismo da G e G' allora sono isomorfi. Scriveremo che $G \cong G'$

Teorema 31: *Condizione isomorfismo*
Sia $G = (V, E)$ e $G' = (V', E')$ e sia $f : V \to V'$. Allora f è un isomorfismo da G in G' se e solo se:

- f è bigettiva
- $f(E) = E'$

Dimostrazione

Chiaramente la prima proprietà coincide con la prima. La seconda proprietà afferma che f è un morfismo.



$$f : V \to V'$$
$$1 \to d \qquad \{1,2\} \to \{d,b\} \in E'$$
$$2 \to b \qquad \{2,3\} \to \{b,c\} \in E'$$
$$3 \to c \qquad \{3,4\} \to \{c,e\} \in E'$$
$$4 \to e$$

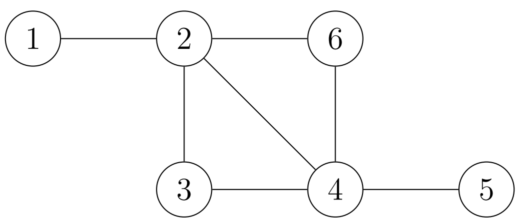
Quindi f è bigettiva

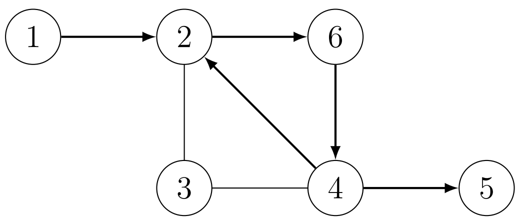
Quindi preserva i lati

Definizione 40: *Passeggiate cammini e cicli*
Sia $G\,(V, E)$ un grafo. Una successione finita ordinata $(v_0, v_1, \dots, v_n)$ si verdici di G si dice:

- Passeggiata se $n = 0$ oppure $n \geq 1$ e $\{v_i, v_{i+1}\} \in E \quad \forall i \in \{0, \dots, n-1\}$
- Cammino se è una passeggiata in G, ma non si ritorna mai sullo stesso vertice
- Ciclo se è una passeggiata in G e:
  - $n \geq 3$
  - $v_n = v_0$
  - $(v_0, \dots, v_{n_1})$ è un cammino

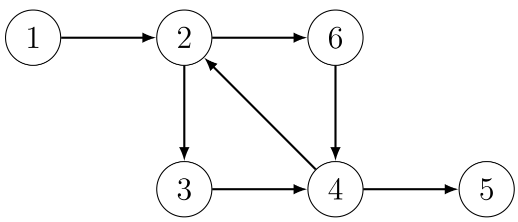
Esempio





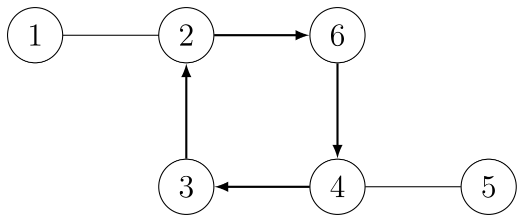
Cammino di lunghezza 5

$C\,(1, 2, 6, 4, 5)$



Passeggiata di lunghezza 8

$P\,(1, 2, 6, 4, 2, 3, 4, 5)$



Ciclo di lunghezza 4

$C\,(2,6,4,3)$

Definizione 41: *Confiungibilità*
Sia $G=(V,E)$ un grafo e siano $v,w\in V$. Diciamo che v è <u>congiungibile</u> a w in G per cammini (o per passeggiate), se esiste una cammino (o una passeggiata) che parte da v e finisce in w.

$$\exists\,(v_0,\ldots,v_n)\ \text{ t.c. } v_0=v \text{ e } v_n=w$$

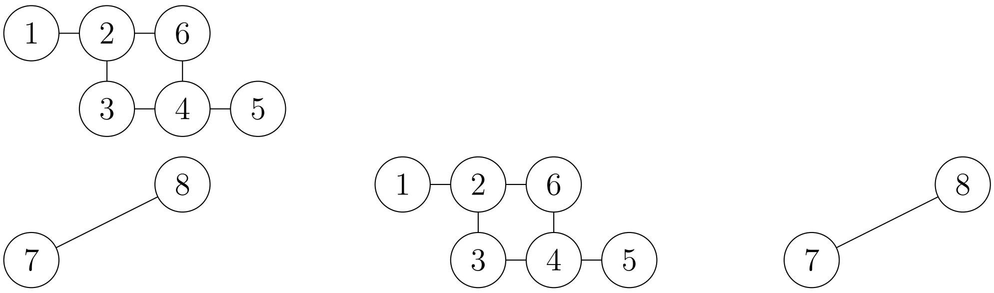
Teorema 32: *Congiungibilità per cammino o passeggiata*
Se v e w sono congiungiungibili <u>per passeggiate</u> in G, allora lo sono <u>anche per cammini</u> e viceversa

Dimostrazione

- Se v e k sono congiungibili per cammini, allora lo sono anche per passeggiate in quanto un cammino è una passeggiata
- Viceversa, se v e k sono congiungibili in passeggiata, posso scegliere la passeggiata più corta, evitando di ritornare sui miei passi
  - Seleziono il seguente insime:
    $$\mathcal{P}:=\{Q|Q \text{ è una passeggiata in } G \text{ da } v \text{ a } w\}$$
    nota che $P\neq\emptyset$ in quanto per hp esiste una passeggiata da v e w
  - Definiamo anche il seguente insieme:
    $$\mathcal{A}:=\{l\,(Q)\in\mathbb{N}|Q\in\mathcal{P},l\,(Q)=n \text{ lati persorsi durante la passeggiata } Q\}$$
    Per lo stesso motivo di prima, anche $\mathcal{A}\neq\emptyset$
  - Grazie al teorema del buon ordinamento $\exists p_0=min\,(\mathcal{A})$
  - Dimostriamo che p_0 è un cammino
    * Supponiamo per assurdo che p_0 non sia un cammino.
    * Se p_0 non fosse un cammino allora potrei risparmiare lunghezza"tagliando la parte di cammino" che riporta allo stesso vertice
    * Tuttavia così facendo otterrei una passeggiata più corta di p_0, che per definizione è la passeggiata più corta di $\mathcal{A}$, i che è un assurdo logico

> **Definizione 42:** *Grafi connessi*
> Sia $\sim$ una relazione di equivalenza tale che
>
> $$v \sim w \text{ se } v \text{ è connesso a } w$$
>
> detta $[c]_\sim$ la classe dei vertici che soddisfano la relazione $\sim$ a partire da c, allora il sottografo indotto dai vertici di una tale classe è detto grafo delle componenti connesse. Se un grafo ha una sola classe è detto grafo connesso. In caso contrario è detto grafto sconnesso

Esempio



$G\,(V, E)$ $\qquad$ $G\,[V_1]$ $\qquad$ $G\,[V_1]$

Figura 2: A sinistra G, a destra i sottografi connessi di G

$$[1]_\sim = \{1, 2, 3, 4, 5, 6\} = V_1$$
$$[7]_\sim = \{7, 8\} = V_2$$

9.3 Grafi 2-connessi e hamiltoniani

Definiamo innanzitutto delle operazioni sui grafi:

Definizione 43: *Operazioni sui grafi*
Sia $G = (V, E)$ un grafo, definiamo alcuni grafi costruiti a partire da G :

- *Cancellazione di un lato* se $e \in E$ denotiamo
$$G - e = (V, E \backslash \{e\})$$
- *Aggiunta di un lato* se $e \in \left(\begin{array}{c} V \\ 2 \end{array} \right) \backslash E$ denotiamo
$$G + e = (V, E \backslash \{e\})$$
- *Cancellazione di un vertice* se $v \in V$ denotiamo
$$G - v = (V \backslash \{v\}, \{e \in E \mid v \notin e\})$$
- *Divisione di un lato* se $e = \{u, v\} \in E$ denotiamo
$$G\%e = (V \cup \{z\}, E \backslash \{e\} \cup \{\{u, z\}, \{v, z\}\})$$
essendo $z \notin V$.

Definizione 44: *Grafo 2-connesso*
Una grafo F si dice 2-connesso se ha almeno tre vertici e
$$\forall v \in V(G) \quad G - v \text{ è connesso}$$
ossia qualsiasi vertice io tolga ottengo un grafo connesso

Definizione 45: *Grafo hamiltoniano*
Sia G un grafo. Un ciclio in G che attraversa tutti i vertici di G è detto ciclo hamiltoniano in G. Se G ammette almeno un ciclo hamiltoniano, allora G è detto grafo hamiltoniano

Nota che un grafo hamiltoniano è sempre anche 2-connesso

9.4 Gradi di un vertice e teoremi correlati

Definizione 46: *Grafo finito*
Un grafo si dice finito se il suo numero di vertici è finito

Nota che un grafo finito ha anche un numero di lati finito. Tuttavia un grafo con numero finito di lati può essere anche infinito

Definizione 47: *Grado di un vertice*
Sia $G = (V, f)$ un grafo finito e sia $v \in V$. Definiamo il grado $deg_G(V)$ di $v$in G ponendo:

$$deg_G(v) = |\{e \in E\}|v \in e|$$

intuitivamente indica il numero di lati che escono da v

Teorema 33: *Somma dei gradi*
Sia $G = (V, f)$ un grafo finito. Allora vale che

$$\sum_{v \in V} \deg_G(v) = 2|E|$$

Intuitivamente, ogni volta che aggiungo un lato, ogni lo score dei due vertici che collega si alzerà di 1 per ogni vertice.

Dimostrazione

Definisco innanzitutto la matrice di adiacenza nel seguente modo:

$$m_{ij} = \begin{cases} 1 & \text{se } v_i \in e_j \\ 0 & \text{se } v_i \notin e_j \end{cases}$$

immaginati di avere sulla ascisse il vertice e sulle ordinate il lato. Se in posizione (i, j) c'è un 1, vuol dire che il j-esimo lato è collegato all'i-esimo vertice

- Immagina di sommare tutti gli uni presenti in matrice.
- Puoi procedere sommando prima colonne e poi righe o viceversa. La somma è chiaramente uguale
$$\sum_{i=1}^{n}\left(\sum_{j=1}^{k} m_{ij}\right) = \sum_{j=1}^{k}\left(\sum_{i=1}^{n} m_{ij}\right)$$
assumendo che vi siano n vertici e k lati
- La quantità a sinistra è pari alla somma dei gradi (fisso un vertice e conto quali lati lo contengono)
- La quantità della sommatoria interna a destra è sempre pari a 2 (fisso un lato e contro quanti vertici lo contengono, sempre 2). Visto che la sommatoria esterna varia da 1 a k, dove k è il numero dei lati, allora la quantità di destra è pari a $2|E|$
$$\sum_{i=1}^{n} \deg(v_i) = 2|E|$$

Teorema 34: *Teorema delle strette di mano*
Il numero di vertici di grado dispari in un grafo finito è pari

Dimostrazione

Consideriamo i due insiemi contenenti i vertici pari e dispari:

$$P := \{v \in V | \deg_G(v) \text{ è pari } \} \qquad D := \{v \in V | \deg_G(v) \text{ è dispari } \}$$

ora so che la somma di questi gradi sarà uguale alla somma di tutti i gradi:

$$\sum_{v \in P} \deg_G(v) + \sum_{v \in D} \deg_G(v) = \sum_{v \in V} \deg_G(v) = \underbrace{2|E|}_{\text{teo 33}}$$

A questo punto , girando l'uguaglianza ottengo che :

$$\sum_{v \in D} \underbrace{\deg_G(v)}_{\text{dispari}} = \overbrace{\sum_{v \in P} \deg_G(v)}^{\text{pari}} + \overbrace{2|E|}^{\text{pari}}$$

- Il membro di destra è pari (somma di numeri pari è pari)
- La somma di numeri dispari è pari se e solo se il numero di numeri dispari è pari

Definizione 48: *Foglia*
Sia $G = (V, E)$ un grafo . Un vertice $v \in V$ si dice foglia di G se

$$deg(v) = 1$$

Teorema 35: *Foglie in grafo 2 connesso*
Sia $G = (V, E)$ un grafo 2-connesso. Allora G non ha foglie

Dimostrazione

Supponiamo per assurdo che esista una foglia di G, ossia $\exists v \in V$ t.c. $deg(v) = 1$. Se considero il grafo $G - w$ dove $w \in \{w, v\}$, allora chiaramente ottengo un grafo sconnesso

Teorema 36: *Foglie grafo hamiltoniano*
Se $G = (V, E)$ è un grafo hamiltoniano allora non ha foglie

Dimostrazione

Il fatto che un grafo sia hamiltoniano implica che sia $2 - connesso$, allora per teo 35 ho che il grafo non ha foglie

Nota che non è vero che se un grafo è connesso e senza foglie allora è 2-connesso o hamiltoniano

Categorie di grafi

Teorema 37: *Proprietà grafi isomorfi*
Siano G e G' grafi finiti. Supponiamo $G \cong G'$. Allora valgono:

- $\text{Score}(G) = \text{Score}(G')$
- G e G' hanno lo stesso numero di componenti connesse
- G è 2-connesso $\Leftrightarrow G'$ è 2 connesso
- G è hamiltoniano $\Leftrightarrow G'$ è hamiltoniano
- G e G' hanno lo stesso numero di sottografi che sono 3-cicli, 4-cicli,...

9.5 Verificare se uno score esiste o meno

Osservazione

Se conosco lo score di un grafo allora conosco anche il numero di vertici e lati:

- Il numero di vertici è il numero di entrate nello score
- La somma delle entrare dello score è il numero di lati presenti

Teorema 38: *Condizione esistenza score 1*
Sia $d = (d_1, d_1, \ldots, d_n) \in \mathbb{N}^n$ con $n \geq 1$ con $d_1 \leq d_2 \leq \ldots \leq d_n$ lo score di un grafo. Se

$$d_n > n - 1$$

non può essere lo score di alcun grafo

- Se la n-upla è lunga n, allora vuol dire che il grafo ha n vertici
- Ogni vertice può essere collegato con al massimo $n - 1$ vertici

Nota che se ho uno score con 0:

$$d = (0, 0, 0, 1, 1, 2, 2, 2, 3, 4, 9)$$

in questo caso lo score è lungo $n = 11$ dunque non posso provare l'inesistenza dello score dato che $9 \not\geq 11$. Tuttavia posso considerare lo score senza gli 0, in quanto ogni vertice con grado 0 non è collegato a nulla. Dato che lo score

$$d = (1, 1, 2, 2, 2, 3, 4, 9)$$

non esiste, allora non esiste nemmeno lo score iniziale

Teorema 39: *Condizione esistenza score 2*
Siano $h, k \in \mathbb{N} \setminus \{0\}$, sia $n := h + k$ e sia $d \in \mathbb{N}^n$ tale che :

$$d = \left(\underbrace{d_1, d_2, \ldots, d_h}_{h \text{ volte}}, \underbrace{n-1, n-1, \ldots, n-1}_{k \text{ volte}}\right)$$

allora se $d_1 < k$, allora $\nexists G$ con score d

Dimostrazione

Supponiamo per assurdo che eiste $G(V, E)$ con score d. Se ho k vertici collegati a $n-1$ vertici, ossia a tutti, non posso avere nemmeno un vertice che non sia collegato ad almeno k vertici

Esempio

Considera la stringa:

$$d = (0, 0, 0, 2, 3, 3, 3, 3, 3, 3, 4, 10, 10, 10)$$

quindi $n = 14$

- Metodo 1: non posso dire nulla in quanto $d_1 = 10 \not\geq n - 1 = 14$
- Tutta via posso trimmare via gli zero davanti e appricare il metodo 3

$$d' = (2, 3, 3, 3, 3, 3, 3, 4, 10, 10, 10)$$

Teorema 40: *Condizione esitenza score 3*
Sia $n \in \mathbb{N}$ e $n \geq 3$, sia $d = (d_1, \ldots, d_n) \in \mathbb{N}^n$ tale che

$$d_1 \leq d_2 \leq \ldots \leq d_n$$

e sia $L \in \mathbb{N}$ definita ponendo

$$L = |\{i \in \{1, 2, \ldots, n-2\} \, | d_i \geq 2\}|$$

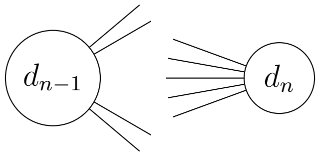
ossia calcolo quante entrate nello score sono maggiori o uguali a 2, eccetto le ultime 2. Allora se

$$L < d_{n-1} + d_n - n$$

allora non esiste un grafo con tale score

L'idea intuitiva è la seguente:

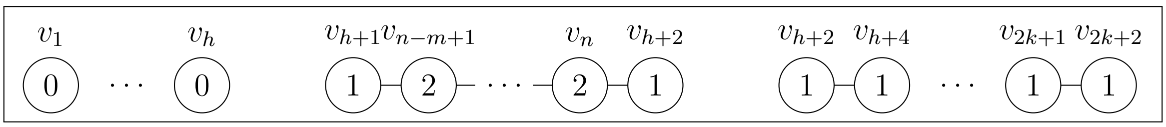
- Immaginati di porre gli utlimi due vertici dello score d_{n-1}, d_n
- A questo punto i lati che escono da questi devono confluire in alcuni vertici, ma se questi sono troppo pochi allora ci devono essere alcuni vertici collegati da entrambi d_{n-1} e d_n



Teorema 41: *Condizione esitenza score 4*
Se il vettore $d \in \mathbb{N}^n$ possiede un numero dispari di componenti dispari allora non può essere lo score di un grafo, grazie al lemma delle strette di mano

Teorema 42: *Prerequisito teorema dello score*
Sia $n \in \mathbb{N} \setminus \{0\}$ e sia $d = (d_1, \dots, d_n) \in \mathbb{N}^n$ tale che $d_1 \leq d_2 \leq \dots \leq d_n \leq 2$. Valgono le seguenti:

- Se $d = (0, 0, \dots, 0, 2)$ oppure $d = (0, 0, \dots, 2, 2)$ allora non esiste
- Se $d = (0, \dots, 0)$ p $d = (\underbrace{0, \dots, 0}_{n-m \text{ volte}}, \underbrace{2, \dots, 2}_{m \text{ volte}})$ allora esiste. In quest'ultimo caso basta prendere un m ciclo e $n - m$ vertici non collegati a nulla
- Se compare almeno una volta 1, allora se compare un numero di volte dispari il grafo non esiste (*teo delle strette di mano*). Supponiamo di avere un numero pari di uni:
$$d = (\underbrace{0, \dots, 0}_{h \text{ volte}}, \underbrace{1, 1}_{2 \text{ volte}}, \underbrace{1, \dots, 1}_{2k \text{ volte}}, \underbrace{2, \dots, 2}_{m \geq 0})$$



Grafo "canonico" dell'ultimo punto

Teorema 43: *Teorema dello score*
Sia $n \in \mathbb{N}$ con $n \geq 2$ e sia $d = (d_1, \dots, d_n) \in \mathbb{N}^n$ tale che $d_1 \leq \dots \leq d_n \leq n - 1$. Definiamo il vetore $d' = \left(d'_1, \dots, d'_{n-1} \in \mathbb{N}^{n-1}\right)$, togliendo l'ultimo elemento di d in modo tale che:
$$d'_i = \begin{cases} d_i & \text{se } i < n - d_n \\ d_i - 1 & \text{se } i \geq n - d_n \end{cases}$$
per $i \in \{1, \dots, n-1\}$. Allora
$$d \text{ esiste} \Leftrightarrow \text{esiste } d'$$

Nota che il teorema può essere applicatore iterativamente su anche su d' finche non otteniamo uno score banale.

Esempio

Consideriamo lo score

$$(2, 2, 2, 2, 3, 3, 3, 5, 6)$$

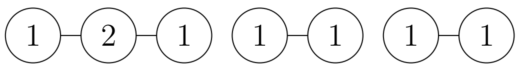
Score	Dati
$(2, 2, \underbrace{2, 2, 3, 3, 3, 5}_{\text{range}}, 6)$	$n = 9, n - d_m = 3$
$(2, 2, 1, 1, 2, 2, 2, 4)$ $(1, 1, 2, \underbrace{2, 2, 2, 2}_{\text{range}}, 4)$	$n = 8, n - d_m = 4$
$(1, 1, 2, 1, 1, 1, 1)$ $(1, 1, 1, 1, 1, 1, 2)$	Ottengo score banale

Come visto in teo 42 esiste un grafo con score $(1, 1, 1, 1, 1, 1, 2)$, allora posso affermare che ne esiste uno con score $(2, 2, 2, 2, 3, 3, 3, 5, 6)$. Posso ora costruire un grafo con quest'ultimo score procedendo così:

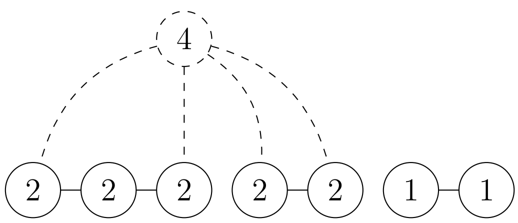
- Nella tabella ho ottenuto i seguenti score secondo l'algoritmo dello Score:

$$d = (2, 2, 2, 2, 3, 3, 3, 5, 6)$$
$$d' = (1, 1, 2, 2, 2, 2, 2, 4)$$
$$d'' = (1, 1, 1, 1, 1, 1, 2)$$

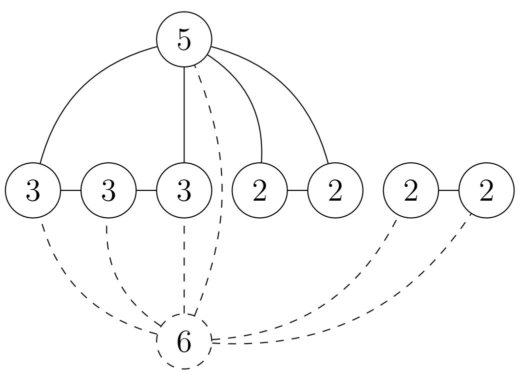
- Disegno grafo canonico dell'ultimo score:



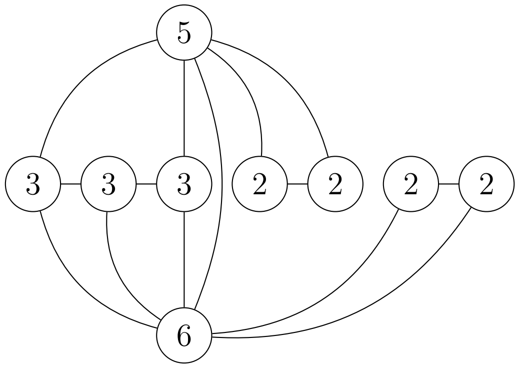
- Aggiungo il vertice che ho tolto nell'ultimo passaggio. Lo collego in maniera tale da riscostruire le differenze con l'ultimo score



- Ripeto iterativamente:



- Il grafo ottenuto tramite la ricostruzione arritrovo e quindi il seguente:



10 Esercizi

10.1 Esercizio induzione

Dimostrare per induzione su $n \geq 0$ che vale la proprietà:

$$\sum_{k=0}^{n} k!k = (n+1)! - 1 \quad \forall n > 0$$

- *Caso base*

$$\sum_{k=0}^{0} k!k = 1 - 1 \rightarrow \ \checkmark$$

- *Passo induttivo* suppongo la proprietà vera per $n-1$:

$$n!n+\sum_{k=0}^{n-1} k!k = n!n+[(n-1+1)!-1] = n!n+[n!-1] = n!\,(n+1)-1 = (n+1)!-1$$

10.2 Alberi e foreste

Definizione 49: *Alberi e foreste*
Un grafo si dice <u>albero</u> se è un grafo <u>connesso senza cicli</u>. Una <u>foresta</u> è un grafo <u>senza cicli</u>

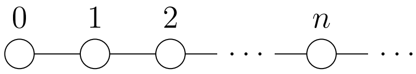
Nota che un grafo è una foresta solo se le sue componenti connesse sono tutte alberi

Teorema 44: *Caratterizzazione alberi*
Sia $T = (V, E)$ un grafo (non necessariamente finito). Le seguenti affermazioni sono equivalenti:

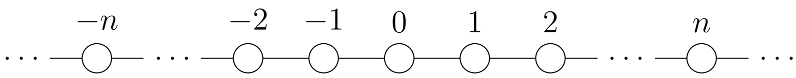
- T è un albero
- Per ogni $v, v' \in V$, esiste un unico cammino in T che congiunge v a v'
- T è connesso ma $\forall e \in E$ il grafo $T - e$ è sconnesso
- T non ha cicli e $\forall e \in \binom{V}{2} \setminus E$ il grafo $T + e$ ha almeno un ciclo

Teorema 45: *Foglie e alberi*
Sia T un albero finito avente almeno due vertici. Allora T possiede almeno due foglie

Nota che il teorema è falso per i grafi non finiti:



oppure



Teorema 46: *Formula di eulero per gli alberi*
Sia $T\,(V, E)$ un grafo finito e connesso. Allora

$$T \text{ è un albero } \Leftrightarrow |V| = |E| + 1$$

Dimostrazione $\Rightarrow$

Procediamo per induzione su $|V| \geq 1$

- *Base induzione* $V = 1$, non può avere lati dunque vale l'hp ✓
- *Ipotesi induttiva* un albero con n vertici soddisfa la hp, ossia vale che $|V| = |E| + 1$
  - So che ogni albero con $|V| \geq 2$ ha almeno due foglie
  - So che se tolgo una foglia ad un albero questo rimane un albero
  - Dunque tolgo una foglia all'albero T, ricadendo nell'ipotesi induttiva

$$|V\,(T - v)| - 1 = |E\,(T - v)|$$

  - Tuttavia, rimuovendo una foglia tolgo a T un vertice e un lato, dunque vale che

$$|V\,(T - v)| = |V\,(T)| - 1 \qquad |E\,(T - v)| = |E\,(T)| - 1$$

  - Sostituendo nella prima equazione, ottengo che

$$|V\,(T)| - 1 = |E\,(T)|$$

Dimostrazione $\Leftarrow$

Procediamo per induzione su $|V| \geq 1$

- *Base induzione* $V = 1$ chiaramente verificata come prima ✓
- *Ipotesi induttiva* un grafo finito per cui vale $|V| = |E| + 1$ è un albero

- Devo dimostrare che il grafo ha almeno una foglia: supponiamo per assurdo che non la abbia

$$2|V| - 2 = \underbrace{2(|V| - 1)}_{\text{per hp}} = \overbrace{2 \cdot |E| = \sum \deg(v)}^{\text{teo somma gradi}} \underbrace{\geq 2|V|}_{\text{no foglie}}$$

- Tuttavia si noti come si è ottenuto un assurdo logico in quanto se confrontiamo il membro di estrema sinistra con quello di estrema destra otteniamo che

$$2|V| - 2 \geq 2|V|$$

l'assunzione falsa è che non esistano foglie

- Dunque considero il grafo $T - v$ dove v è la foglia di cui abbiamo dimostrato l'esistenza
- Mi basta dimostrare che aggiungendo v a $T - v$ non introduco cicli:
  * v è una foglia, quindi un ciclo non può passare per una foglia
  * Dato che per hp induttiva $T - v$ è un albero, non ha cicli
  * Per questa ragione anche T non ha cicli, quindi T è connesso e senza cicli, ossia un albero

Quest'ultimo teorema ha un importante corollario:

Teorema 47: *Corollario 1 a teorema di Eulero per i grafi*
Sia $n \in \mathbb{N} \setminus \{0\}$ e sia $d = (d_1, \ldots, d_n) \in n\mathbb{N}^n$. Allora esiste un albero con score d se e soltanto se è soddisfatta la relazione di eulero:

$$|V| - 1 = |E| = \frac{1}{2}\sum_{i=1}^{|V|} d_i$$

Forzatura alla disconnessione

Teorema 48: *Corollario 2 a teorema di Eulero per i grafi*
Sia $n \in \mathbb{N} \setminus \{0\}$ e sia $d(d_1, \ldots, d_n) \in \mathbb{N}^n$. Se vale

$$|E| = \frac{1}{2}\sum_{i=1}^{n} d_i < n - 1$$

allora tutti i grafi che hanno score uguele a d sono sconnessi

Informalmente, pensa che per un albero vale la relazione di Eulero, ossia $|E| = v - 1$. Se a questo albero tolgo un qualsiasi lato ottengo un grafo sconnesso, dunque se $|E| < v - 1$ ho un grafo sconnesso

Forzatura alla connessione

Teorema 49: *Forzatura alla connessione*
Sia $n \in \mathbb{N} \setminus \{0\}$ e sia $d\left(d_1, \ldots, d_n\right) \in \mathbb{N}^n$ tale che $d_1 \leq \ldots\ldots \leq d_n$. Se vale

$$d_1 + d_n \geq n - 1$$

allora tutti i grafi con score d sono connessi

10.3 Albero di copertura

Definizione 50: *Albero di copertura, spanning tree*
Sia G un grafo. Un sottografo T di G si dice albero di copertura di G se

$$T \text{ è un albero e } V\left(T\right) = V\left(G\right)$$

Nota che se G ammette almeno un albero di copertura, allora G è conneso

Teorema 50: *Esistenza albero di copertura*
Sia G un grafo finito e connesso. Allora

$$G \text{ ammette almeno un albero di copertura}$$

Dimostrazione

Iniziamo considerando l'insieme di tutti i sottografi di G

$$\mathcal{C} := \{C | C \text{ è un sottografo connesso di } G \text{ con } V\left(C\right) = V\left(G\right)\}$$

nota che $\mathcal{C}$ non è vuoto in quanto contiene almeno G stesso.

Considero l'insieme contentente tutti i i possibili numeri di lati di un sottografo di G:

$$\mathcal{S} := \{n \in \mathbb{N} | n = \left|E\left(C\right)\right| \text{ per qualche } C \in \mathcal{C}\}$$

anche questo insieme conterrà al minimo il numero di lati di G stesso.

Considero ora $\overline{C}$, ossia il sottografo di G con il numero minimo di lati. Supponiamo per assurdo che questo non sia un albero. Se $\overline{C}$ non fosse un albero, allora esisterebbe almeno un lato che, tolto, lascerebbe $\overline{C}$ connesso. Questo è tuttavia impossibile in quanto togliendo un lato otterrei un altro grafo connesso con meno lati di $\overline{C}$, ma per definizione $\overline{C}$ è il sottografo di G con meno lati

11 Riassunto teoremi importanti

1. Esistenza e unicità divisione euclidea

   - *Esistenza:* induzione su n, distinguo casi $(n > 0, m > 0)$, $(n < 0, m > 0)$, $(n < 0, m < 0)$, $(n > 0, m < 0)$

- *Unicità:* pongo $n = qm + r = q'm + r'$ e dimostro che $(q - q')\, m < 1$

2. Rappresentazione in base arbitraria maggiore o uguale a 2
   - *Esistenza:* induz su n. Divido per base b, applico hp ind su q e manipolo sommatoria
   - *Unicità:* induz su n. Rappresento n come sommatoria, la manipolo fino ad ottenere divisione euclidea

3. Esistenza e unicita del M.C.D
   - *Esistenza:* considero il minimo d delle combinazioni lineari $xn+ym$. Dimostro che il resto della divisione fra n e d deve essere 0, altrimenti apparterrebbe a S e sarebbe $< d$, il che è assurdo
   - *Unicità:* dimostro che due $M.C.D.$ si dividono reciprocamente, e sono dunque uguali

4. Esistenza e unicità del m.c.m
   - *Esistenza:* considera $\frac{nm}{(n,m)}$. Considera c multiplo comune, e dimostra che, posto $n = n'\,(n,m)\,, m = m'\,(n,m)$
     - $n'|c'$, $m'|c'$
     - $(n', m') = \left(\frac{n}{(n,m)}, \frac{m}{(n,m)}\right) = 1$
     - $M|c$
   - *Unicità:* per via dell'unicità dell'M.C.D. segue l'unicità di $M = \frac{nm}{(n,m)}$

5. Teorema fondamentale dell'artimetica (fattorizzazione in fattori primi)
   - *Esistenza:* induzione su $n \geq 2$. Distinguo se n è primo o meno e divido se non lo è
   - *Unicità* induzione su lunghezza stringa a. Applico ipotesi induttiva dopo aver diviso da entrambe le parti per q_i

6. Teorema cinese del resto
   - *Condizione soluzioni:* sfrutto il fatto che $(n, m) = xn + ym$
   - *Forma soluzioni:*
     - $\Rightarrow$ esprimo differenza soluzioni c, c' in due modi e ottengo che $c' - c$ è un multiplo comune, ossia $[n, m]\,|c' - c$
     - $\Leftarrow$ se $c' \in [c]_{[n,m]}$ allora $c' = c + k\,[n, m]$, ossia risolve entrabe le congruenze

7. Teorema di Fermat-Eulero (potenza di intero invertibile per $\phi\,(n)$)
   - Dimostro che la moltiplicazione di invertibili è una bigezione e la applico sul prodotto di tutti gli elementi: $x_1 \dots x_k = u^k x_1 \dots x_k$
   - $k = \phi\,(n)$

8. Teorema crittografia RSA

- $x^{cd} = x^{k\phi(n)+1}$

9. Equivalenza fra congiungibilità per passeggiate e per cammini(la relazione di congiungibilità è una relazione di quivalenza)
   - Un cammino è una passeggiata quindi se è congiungibile per passeggiata lo è anche per cammino
   - Consiidero insieme delle passeggiate e considero elemento più corto. Dimostro che è un cammino
10. Relazione fra somma dei gradi e numeri di lati in un grafo
    - Considero matrice di adiacenza ed equiparo somma prima per righe e po per colonne alla somma prima per colonne e poi per righe
11. Teorema delle strette di mano
    - Sommatoria di gradi pari e dispari $= 2|E|$
    - Somma di n numeri dispari è pari $\Leftrightarrow n$ è pari
12. Teorema di eulero per gli alberi
    - $\Rightarrow$ tolgo una foglia (la cui esistenza è garantita) e ricado in hp induttiva
    - $\Leftarrow$
      - Dimostro che se vale $|V| - 1 = |E| + 1$ allora ho almeno una foglia
      - Dimostro che aggiungendo quella foglia v al grafo $T - v$, (il quale è un albero per hp ind), allora ottengo un albero
13. Teorema di esistenza albero di copertura per grafi connessi e finiti
    - Considero insieme dei sottografi connessi di G che hanno gli stessi vertici di G
    - Considero grafo con numero minore di lati. Questo deve essere un albero altrimenti esisterebbe almeno un lato che tolto lascerebbe il grafo connesso