Dimostrazioni Matematica Discreta

In questo file ci sono solo le cose dimostrate: le definizioni e tutti i teoremi, lemmi e proposizioni che non sono stati dimostrati non ci sono.

Quelle che c'erano sulle slide sono copiate pari pari dalle slide con alcune aggiunte di spiegazioni tra parentesi per parti che io ho trovato complicate da capire, le altre dagli appunti presi a lezione e/o dalle videolezioni.

1 Insiemi discreti e loro proprietà

Tutte le dimostrazioni di questo argomento sono contenute nelle slide (il primo file).

Dalla slide 15 del file 1:

Proposizione 1. *Se X e Y sono insiemi finiti, con $\#X = n$, $\#Y = m$ e $X \cap Y = \emptyset$, allora $(X \cup Y) = n + m$.*

Dimostrazione. Per ipotesi esistono due funzioni biettive $f : X \to N_n$ e $g : Y \to \mathbb{N}_m$. Per dimostrare la proprietà occorre costruire una funzione biettiva $h : X \cup Y \to \mathbb{N}_{n+m}$.

Ad esempio, $\forall c \in X \cup Y$, si può porre:

$$h(c) = \begin{cases} f(c) & \text{se } c \in X \\ g(c) + n & \text{se } c \in Y \end{cases}$$

□

Dalla slide 16 del file 1:

Proposizione 2. *Se X è finito con $\#X = n$ ed Y è numerabile, con $X \cap Y = \emptyset$, allora $\#(X \cup Y)$ è numerabile.*

Dimostrazione. Per ipotesi esistono due funzioni biettive $f : X \to \mathbb{N}_n$ e $g : Y \to \mathbb{N}$. Per dimostrare la proprietà occorre costruire una funzione biettiva $h : X \cup Y \to \mathbb{N}$.

Ad esempio, $\forall c \in X \cup Y$, si può porre:

$$h(c) = \begin{cases} f(c) & \text{se } c \in X \\ g(c) + n & \text{se } c \in Y \end{cases}$$

□

Dalla slide 17 del file 1:

Proposizione 3. *Se X e Y sono insiemi numerabili, allora anche $X \cup Y$ è numerabile.*

Dimostrazione. Senza perdere di generalità, supponiamo che $X \cap Y = \emptyset$. Per ipotesi esistono due funzioni biettive $f : X \to \mathbb{N}$ e $g : Y \to \mathbb{N}$. Per dimostrare la proprietà occorre costruire una funzione biettiva $h : X \cup Y \to \mathbb{N}$.

Ad esempio, $\forall c \in X \cup Y$, si può porre:

$$h(c) = \begin{cases} 2f(c) - 1 & \text{se } c \in X \\ 2g(c) & \text{se } c \in Y \end{cases}$$

□

Dalle slide 19 (enunciato), 20 e 21 (dimostrazione) del file 1:

Proposizione 4. *Se $\{A_i \ / \ i \in \mathbb{N}\} = \{A_1, A_2, ..., A_i, ...\}$ è un insieme numerabile di insiemi numerabili, si ha che*

$$\#(\bigcup_{i \in N} A_i) = \#\mathbb{N}$$

Dimostrazione. Senza perdere di generalità, supponiamo che gli insiemi siano fra loro disgiunti: $A_i \cap A_j = \emptyset, \forall i \neq j$.

Per dimostrare la tesi, utilizziamo il *procedimento diagonale di Cantor*, enumerando per righe gli elementi di ciascun insieme:

$$\begin{array}{lcccccc} A_1: & a_{11} & a_{12} & a_{13} & ... & a_{1h} & ... \\ A_2: & a_{21} & a_{22} & a_{23} & ... & a_{2h} & ... \\ A_3: & a_{31} & a_{32} & a_{33} & ... & a_{3h} & ... \\ \vdots & ... & & & & & \\ A_i & a_{i1} & a_{i2} & a_{i3} & ... & a_{ih} & ... \\ \vdots & & & & & & \end{array}$$

Consideriamo le diagonali $D_1, D_2, ..., D_k, ...$, ove

$$D_k = \{a_{ij} \ / \ i + j = k + 1\}$$

(N.B.: sono le diagonali parallele alla diagonale secondaria, o al forward slash /)

Per dimostrare che $\#(\bigcup_{i \in \mathbb{N}} A_i)$ è numerabile, occorre costruire un'applicazione biunivoca

$$h : \bigcup_{i \in \mathbb{N}_n} A_i \to \mathbb{N}$$

Scorrendo ogni diagonale a partire dall'elemento che sta nell'insieme con indice maggiore *(in questo modo si scorre dal basso all'alto, e quindi da sinistra a destra, N.B.: in questo modo il j-esimo elemento della diagonale è quello che si trova sulla colonna j-esima, ovvero il j-esimo elemento di un certo insieme)*, incontrerò l'elemento a_{ij} come j-esimo elemento della diagonale a cui esso appartiene, ovvero come j-esimo elemento della diagonale D_{i+j-1}. *(l'indice della diagonale si ricava dalla formula usata per definire le diagonali)*

Osservando che $\#D_k = k$, si ha che *(tra parentesi mia aggiunta per maggiore chiarezza, questa somma sarebbe il numero di elementi che si trovano lungo tutte le diagonali precedenti alla diagonale $i + j - 1$, che sarebbe quella in cui si trova l'elemento a_{ij})*:

$$\sum_{k=1}^{i+j-2} \#D_k (= \sum_{k=1}^{i+j-2} k) = \frac{(i+j-2)(i+j-1)}{2}$$

Si ottiene così un'applicazione biunivoca $h : \bigcup_{i \in \mathbb{N}_n} A_i \to \mathbb{N}$ definita, $\forall a_{ij} \in \bigcup_{i \in \mathbb{N}_n} A_i$, da:

$$h(a_{ij}) = j + \frac{(i+j-2)(i+j-1)}{2}$$

(come quando si indicizza una matrice allocata contiguamente in C, ma stavolta con righe di lunghezza variabile: l'indice è la somma degli elementi nelle diagonali precedenti+l'indice lungo la diagonale in cui si trova l'elemento cercato).

*(**mia osservazione:** credo che gli $\mathbb{N}_n$ nelle unioni dovrebbero essere $\mathbb{N}$, essendo unioni di un insieme numerabile (e non finito) di insiemi.)*

□

slide 24 e 25 (in corsivo e tra parentesi sono aggiunte mie che mi aiutano a capire meglio):

Teorema 1. *(Teorema di Cantor-Bernstein-Schroeder)*

Se $\exists f : A \to B$, f iniettiva, ed $\exists g : B \to A$, g iniettiva, allora $\exists h : A \to B$, h biunivoca.

Dimostrazione. Poiché f e g sono iniettive, si ha:
$\#A = \#f(A)$ con $f(A) \subseteq B$ e $\#B = \#g(B)$ con $g(B) \subseteq A$.
Da $g(B) \subseteq A$ e $f(A) \subseteq B$, segue

$$g(f(A)) \subseteq g(B) \subseteq A$$

Inoltre:

$$\#g(f(A)) = \#f(A) = \#A$$

Per il lemma precedente *(che era il "teorema dei carabinieri" con i sottoinsiemi dicendola da ingegneri e non da matematici, ovvero se $g(f(A)) \subseteq g(B) \subseteq A$ e la cardinalità degli estremi è uguale, cioè $\#g(f(A)) = \#A$, allora hanno tutti e tre la stessa cardinalità, ovvero anche $\#g(B) = \#A$)*, si ha allora: $\#g(B) = \#A$. Poiché per ipotesi $\#g(B) = \#B$, resta dimostrato che $\#A = \#B$, ovvero che esiste una funzione $h : A \to B$ biunivoca. □

slide 26 (enunciato ed inizio dimostrazione) e 27 (fine dimostrazione):

Teorema 2. *(Teorema di Cantor)*
Se A è un insieme numerabile, allora $\mathcal{P}(A)$ ha cardinalità strettamente maggiore di A:

$$\#A \leq \#\mathcal{P}(A), \text{ con } \#A \neq \#\mathcal{P}(A)$$

Dimostrazione. (**Parte 1**: dimostrazione che $\#A \leq \#\mathcal{P}(A)$)
Per dimostrare che $\#A \leq \mathcal{P}(A)$, basta osservare che la applicazione $f : A \to \mathcal{P}(A)$ definita, $\forall a \in A$, da:

$$f(a) = \{a\}$$

è iniettiva.
Vogliamo ora dimostrare che, se A è numerabile, $\#A \neq \#\mathcal{P}(A)$, ovvero che $\mathcal{P}(A)$ NON è numerabile.
(**Parte 2**: dimostrazione che $\#A \neq \#\mathcal{P}(A)$)
Procediamo con una dimostrazione per assurdo.
Sappiamo che $\mathcal{P}(A)$ è in corrispondenza biunivoca con le successioni a valori in $\{0, 1\}$; allora, se $\mathcal{P}(A)$ fosse numerabile, sarebbe possibile elencare tutte le successioni a valori in $\{0, 1\}$:

$$\begin{array}{lccccccc}
\mathbf{s_1}: & s_{11} & s_{12} & s_{13} & \dots & s_{1n} & \dots \\
\mathbf{s_2}: & s_{21} & s_{22} & s_{23} & \dots & s_{2n} & \dots \\
\mathbf{s_3}: & s_{31} & s_{32} & s_{33} & \dots & s_{3n} & \dots \\
\vdots & \dots & & & & & \\
\mathbf{s_j}: & s_{j1} & s_{j2} & s_{j3} & \dots & s_{jn} & \dots \\
\vdots & & & & & &
\end{array}$$

Consideriamo ora la successione a valori in $\{0, 1\}$

$$\bar{\mathbf{s}} = \bar{s}_1\bar{s}_2\bar{s}_3 \dots \bar{s}_j \dots \text{ ove } \bar{s}_j \neq s_{jj}$$

(in altre parole: prendiamo una successione che ha il primo valore diverso da s_{11}, il secondo da s_{22}, ecc., visto che si parla di successioni a valori in {0,1} banalmente $\bar{s}_1 = 0$ se $s_{11} = 1$ e $\bar{s}_1 = 1$ se $s_{11} = 0$, e lo stesso andando avanti con gli indici).
Poiché $\bar{\mathbf{s}}$ è diversa da ciascuna delle successioni $\mathbf{s_j}$, $\forall j \in \mathbb{N}$, si arriva ad un assurdo. Quindi, l'insieme delle successioni a valori in $\{0, 1\}$ non può essere numerabile; e (quindi) nemmeno $\mathcal{P}(A)$.

□

2 Relazioni di equivalenza

Anche per questo argomento, le dimostrazioni sono tutte contenute nel file di slide numero 2.
Dalle slide 7 e 8:

Proprietà 1. *(Proprietà delle classi di equivalenza)*

- $\forall a \in A, a \in [a]$.
- $\forall a, b \in A, a \in [b] \implies [b] = [a]$.
- $\forall a, b \in A, [a] = [b]$ *oppure* $[a] \cap [b] = \emptyset$.

Dimostrazione. (punto per punto)

- È conseguenza diretta della proprietà riflessiva.
- Poiché $a \in [b]$, $a\mathcal{R}b$. Se $x \in A$, $x \in [a]$, allora $x\mathcal{R}a$; per la proprietà transitiva segue $x\mathcal{R}b$, ovvero $x \in [b]$. Resta così dimostrato che $[a] \subseteq [b]$.

  Analogamente, se $y \in A, y[b]$, allora $y\mathcal{R}b$; per la proprietà di simmetria, $a\mathcal{R}b \implies b\mathcal{R}a$, per cui la transitività assicura $y\mathcal{R}a$, ovvero $y \in [a]$. Resta cosı dimostrato che $[b] \subseteq [a]$, e quindi $[b] = [a]$
- Se $\exists c \in [a] \cap [b]$, si ha $c \in [a]$ e $c \in [b]$, ovvero $c\mathcal{R}a$ e $c\mathcal{R}b$. Applicando la proprietà di simmetria a $c\mathcal{R}a$ si ottiene $a\mathcal{R}c$, per cui la proprietà transitiva assicura $a\mathcal{R}b$, ovvero $a \in [b]$. La seconda proprietá implica $[a] = [b]$. Quindi, se due classi hanno un elemento in comune, le due classi coincidono.

□

Dalla slide 15 (non enunciata esplicitamente, ma dimostrata):

Proprietà 2. $\equiv_n$ *è una relazione di equivalenza*

Dimostrazione. Verifichiamo le tre proprietà:

- *Riflessività*:: $\forall x \in \mathbb{Z}, x \equiv_n x$ è verificato, perché $x - x = h \cdot n$, prendendo $h = 0 \in \mathbb{Z}$.
- *Simmetria:* se $x \equiv_n y$, per definizione, $\exists h \in \mathbb{Z}$ tale che $x - y = h \cdot n$. Per dimostrare che $y \equiv_n y$, devo trovare $h' \in \mathbb{Z} / x - y = h' \cdot n$. Basta prendere $h' = -h$.
- *Transitività:* se $x \equiv_n y$ e $y \equiv_n z$, allora $\exists h \in \mathbb{Z} / x - y = h \cdot n$ ed $\exists h' \in \mathbb{Z} / y - z = h \cdot n$. Sommando membro a membro, si ottiene $x - z = (h + h')n$; poiché $h + h' \in \mathbb{Z}$, segue $x \equiv_n z$.

□

Dalla slide 18:

Proposizione 5. *L'insieme delle classi resto modulo n è costituito da:*

$$\mathbb{Z}_n = \{[0], [1], [2], ..., [n-1]\}.$$

Dimostrazione. Per ogni $x \in \mathbb{Z}$, la divisione euclidea per n assicura che $\exists q, r \in \mathbb{Z}, 0 \leq r < n$ tali che $x = q \cdot n + r$, ovvero $x - r = q \cdot n$. Quindi, $x \equiv_n r$, da cui $[x] = [r]$, con $r \in \{0, 1, ..., n-1\}$.
Occorre ora provare che le n classi $[0], [1], [2], ..., [n-1]$ sono a due a due disgiunte, ovvero che

$$\forall r, s \in \mathbb{Z}, 0 \leq r < s < n \implies [r] \neq [s].$$

Per assurdo suppongo $[r] = [s]$; ciò significherebbe che $\exists h \in \mathbb{Z} \ / \ s - r = h \cdot n$. Per ipotesi $s > r$, per cui $0 < s - r < n$; quindi, $s - r$ non può essere multiplo intero di n. □

3 Numeri interi e teoria della divisibilità

Questo argomento è diviso nei file numero 3 e numero 4.

3.1 File 3

Le tre proprietà sono dimostrate nelle slide, i teoremi successivi solo a lezione (quindi le dimostrazione sono tratte dagli appunti).

Dalla slide 11 del file 3:

Proprietà 3. *(Transitività della divisibilità)*

Se $n|m$ e $m|q$, allora $n|q$.

Dimostrazione. Per ipotesi: $\exists h \in \mathbb{Z} \ / \ m = hn$ e $\exists h' \in \mathbb{Z} \ / \ q = h'm$. Sostituendo la prima relazione nella seconda si ottiene $q = h'hn$. Poiché $h'h \in \mathbb{Z}$, si conclude che $n|q$. □

Dalla slide 12 del file 3:

Proprietà 4. *Se $n|m$ e $m|n$, allora $m = \pm n$.*

Dimostrazione. Per ipotesi: $\exists h \in \mathbb{Z} \ / \ m = hn$ e $\exists h' \in \mathbb{Z} \ / \ n = h'm$. Sostituendo la prima relazione nella seconda si ottiene $n = h'hn$, ovvero $n(1 - h'h) = 0$.

Essendo $\mathbb{Z}$ dominio di integrità, segue che o $n = 0$ (e allora anche $m = 0$) o $h'h = 1$.

Da $h'h = 1$ ricaviamo che h ammette inverso h', da cui o $h = h' = 1$ o $h = h' = -1$ (in $\mathbb{Z}$, gli unici elementi che ammettono inverso sono 1 e -1).

Segue così o $m = n$ o $m = -n$. □

Dalla slide 13 del file 3:

Proprietà 5. *Se d e d' sono due massimi comuni divisori tra a e b, allora $d' = \pm d$.*

Dimostrazione. Se d è un massimo comune divisore, $\forall d' \in Z$ tale che $d'|a, d'|b \implies d'|d$.

Poichè anche d' è un massimo comune divisore, valgono $d'|a$ e $d'|b$, per cui $d'|d$.

Analogmente, si dimostra $d|d'$; segue quindi $d' = \pm d$. □

Dalla slide 14 del file 3:

Teorema 3. *(Esistenza ed unicità del MCD)*

Dati $a, b \in Z$ non entrambi nulli, allora $\exists! MCD(a, b)$.

Inoltre, $\exists \alpha, \beta \in \mathbb{Z}$ tali che

$$MCD(a, b) = a\alpha + b\beta \text{ (identità di Bezout).}$$

Dimostrazione. considero combinazioni lineari a coefficienti interi di a e b che diano risultato positivo:

$$S = \{x \cdot a + y \cdot b \ / \ x, y \in \mathbb{Z}, x \cdot a + y \cdot b > 0\}$$

è un sottoinsieme di $\mathbb{N}$.

Inoltre, si osserva che non è vuoto, perché almeno uno tra a e b non è nullo, infatti supponendo $a \neq 0, sign(a) \cdot a + 0 \cdot b = |a| \subset S$

Si assume che esista un elemento

$$d = \min S$$

Da dimostrare che $d = MCD(a, b)$

visto che $d = \min S$, il fatto che d appartenga ad S implica che $\exists \alpha, \beta \in \mathbb{Z} : d = \alpha \cdot a + \beta \cdot b$ (ovvero l'identità di Bezout).

Da dimostrare che $d|a, d|b$ e che gli altri divisori comuni dividano d.

Consideriamo la divisione euclidea tra a e d, allora

$$\exists q, r \in \mathbb{Z}, 0 < r < d : a = q \cdot d + r$$

Quindi

$$r = a - q \cdot d = a - q(\alpha \cdot a + \beta \cdot b) = (1 - q \cdot \alpha) \cdot a + (-q \cdot \beta) \cdot b$$

Ovvero r si scrive come combinazione lineare intera di a e b, ovvero "assomiglia a quelli che stanno dentro S", più precisamente $r > 0 \implies r \in S$, ciò è assurdo perché $r < d$ e $d = \min S$

quindi r deve essere uguale a 0, cioè $a = q \cdot d$, cioè $d|a$

Da dimostrare $\forall d' \in \mathbb{Z} : d'|a, d'|b \implies d'|d$

$$d = \min S \implies d \in S \implies \exists \alpha, \beta \in \mathbb{Z} : d = \alpha \cdot a + \beta \cdot b$$

Visto che $d'|a$ si scrive a come $d' \cdot h$, e visto che $d'|b$ si scrive b come $d' \cdot k$, quindi:

$$d = \alpha \cdot d' \cdot h + \beta \cdot d' \cdot k = (\alpha \cdot h + \beta \cdot k) \cdot d' \in Z \implies d'|d$$

□

Dalla slide 15 del file 3:

Teorema 4. *Siano $a, b \in \mathbb{Z}$, con $|a| \geq |b| > 0$. Se $a = bq + r$ è la divsione euclidea fra a e b, allora:*

$$\{c \in \mathbb{Z} \ / \ c|a, c|b\} = \{c \in \mathbb{Z} \ / \ c|b, c|r\}$$

quindi

$$MCD(a, b) = MCD(b, r)$$

Dimostrazione. considero $c \in \mathbb{Z} : c|a, c|b$. Voglio provare che $c|b$ e $c|r$.

Per ipotesi $c|a$, ovvero $\exists h \in \mathbb{Z} : a = c \cdot h$, e anche $c|b$, ovvero $\exists k \in \mathbb{Z} : b = c \cdot k$.

poiché $a = bq + r$, segue che $r = a - b \cdot q = c \cdot h - c \cdot k \cdot q = c \cdot (h - k \cdot q)$, con $h - k \cdot q \in \mathbb{Z}$, quindi $c|r$

quindi tutti i divisori comuni di a e b sono anche divisori di r (e quindi comuni ad r e b): l'insieme di sinistra nell'uguaglianza nella tesi è contenuto in quello di destra ($\{c \in \mathbb{Z} \ / \ c|a, c|b\} \subseteq \{c \in \mathbb{Z} \ / \ c|b, c|r\}$).

Resta da dimostrare che $\{c \in \mathbb{Z} \ / \ c|b, c|r\} \subseteq \{c \in \mathbb{Z} \ / \ c|a, c|b\}$

Per ipotesi $c|b$, ovvero $\exists h \in \mathbb{Z} : b = c \cdot h$, e anche $c|r$, ovvero $\exists k \in \mathbb{Z} : r = c \cdot k$.

poiché $a = bq + r$, segue che $a = c \cdot h \cdot q + c \cdot k = c \cdot (hq + k)$ con $(hq + k) \in \mathbb{Z}$, quindi $c|a$

quindi ($\{c \in \mathbb{Z} \ / \ c|b, c|r\} \subseteq \{c \in \mathbb{Z} \ / \ c|a, c|b\}$) □

Dalla slide 20 del file 3:

Teorema 5. *(Esistenza soluzioni di equazioni diofantee)*
L'equazione diofantea $ax + by = c$ con $a, b, c \in \mathbb{Z}$ ammette soluzioni (intere) se e solo se $MCD(a, b)|c$. Inoltre, se $(\bar{x}, \bar{y})$ è una soluzione, allora esistono infinite soluzioni:

$$Sol = \{(\bar{x}, \bar{y}) + k\frac{(-b, a)}{MCD(a, b)} \ / \ k \in \mathbb{Z}\}$$

Dimostrazione. **condizione necessaria e sufficiente**
Prima parte: **Ipotesi**: ha soluzione, **Tesi**: $MCD(a, b)|c$
Per ipotesi esiste $(\bar{x}, \bar{y}) \in Z \times Z : a\bar{x} + b\bar{y} = c$
chiamiamo $d = MCD(a, b)$, quindi sappiamo che $d|a$, $d|b$, cioè:

- $\exists h \in Z : a = dh$
- $\exists k \in Z : b = dk$

quindi $dh\bar{x} + dk\bar{y} = c$, cioè $d(h\bar{x} + k\bar{y}) = c$ con $h\bar{x} + k\bar{y} \in Z$ quindi $d|c$
Seconda parte: **Ipotesi**: $MCD(a, b)|c$, **Tesi**: ha soluzione
Per l'identità di Bezout, $MCD(a, b) = d = \alpha \cdot a + \beta \cdot b$
per ipotesi, $\exists h \in Z : c = dh$
Perciò $c = (\alpha \cdot a + \beta \cdot b) \cdot h = (\alpha \cdot h) \cdot a + (B \cdot h)b$, ovvero $(\alpha \cdot h, \beta \cdot h)$ è soluzione dell'equazione diofantea.
Dimostrata la condizione necessaria e sufficiente, ci occupiamo dell'insieme delle soluzioni.*(Questo credo conti come un cenno, non come una dimostrazione, non credo la chieda, anche dalla videolezione mi sembra solo un cenno)*
Come noto dall'algebra lineare (ad es., teorema 6.12 del libro di Geometria della prof. Casali), le soluzioni di un sistema lineare si ottengono come la somma di una particolare soluzione del sistema e delle soluzioni del sistema lineare omogeneo associato.
L'equazione omogenea associata $ax + by = 0$ ha come soluzione $(-b, a)$, e tutti i suoi multipli interi la soddisfano. Però, non è detto che sia la più piccola coppia che soddisfa l'equazione, ovvero che $-b$ ed a non siano coprimi. Per questo, le soluzioni dell'omogenea associata sono $\{k\frac{(-b,a)}{MCD(a,b)} / k \in \mathbb{Z}\}$. □

3.2 File 4

Dalla slide 3:
Proprietà 6. *Due interi consecutivi sono sempre coprimi*

Dimostrazione. Si utilizza l'algoritmo di Euclide delle divisioni successive tra $n + 1$ ed n.
$n + 1 = 1 \cdot n + 1$
$n = n \cdot 1 + 0$
L'ultimo resto non nullo era 1, quindi $MCD(n + 1, n) = 1$

□

Proprietà 7. *Due dispari consecutivi sono sempre coprimi*

Dimostrazione. Si utilizza l'algoritmo di Euclide delle divisioni successive tra $2n + 1$ e $2n - 1$.
$2n + 1 = 1 \cdot (2n - 1) + 2$
$2n - 1 = (n - 1) \cdot (2) + 1$
$2 = 2 \cdot 1 + 0$

L'ultimo resto non nullo era 1, quindi $MCD(2n+1, 2n-1) = 1$

□

Proprietà 8.

$$\forall a, b \in \mathbb{Z} - \{0\}, \frac{a}{MCD(a,b)} \text{ e } \frac{b}{MCD(a,b)} \text{ sono coprimi}$$

Dimostrazione. Per l'identità di Bezout

$$\exists \alpha, \beta \in \mathbb{Z} \text{ tali che } MCD(a,b) = \alpha \cdot a + \beta \cdot b$$

Dividendo per $MCD(a,b)$

$$1 = \alpha \cdot \frac{a}{MCD(a,b)} + \beta \cdot \frac{b}{MCD(a,b)}$$

entrambi i numeri sono divisibili per il loro massimo comune divisore, quindi le frazioni appartengono a $\mathbb{Z}$

Se cerco il MCD tra le due frazioni, si ottiene che 1 app a S (l'insieme che compare nella dimostrazione dell'esistenza ed unicità del MCD), ed 1 è evidentemente il minimo di tale insieme, ovvero il MCD. □

Dalla slide 4 (dimostrazione inclusa):

Proprietà 9. *(Lemma di Euclide)*

Se $a, b \in \mathbb{Z} - \{0\}$ *sono coprimi,*

$$a|(bc) \implies a|c$$

Dimostrazione. Se $a|(bc)$, allora $\exists h \in \mathbb{Z}$ tale che $bc = ha$.

Poiché $MCD(a,b) = 1$, per l'identità di Bezout $\exists \alpha, \beta \in \mathbb{Z}$ tali che $1 = \alpha a + \beta b$.

Moltiplicando entrambi i membri per c si ottiene

$c = \alpha ac + \beta bc = \alpha ac + \beta ha = (\alpha c + \beta h)a$;

essendo $\alpha c + \beta h \in \mathbb{Z}$, segue $a|c$. □

Dalla slide 5 (dimostrazione inclusa):

Proprietà 10. *Se* $a, b \in \mathbb{Z} - \{0\}$ *sono coprimi,*

$$a|c, b|c \implies (ab)|c$$

Dimostrazione. Poiché $b|c, \exists h \in \mathbb{Z}$ tale che $c = hb$.

Allora $a|c$ diventa $a|(hb)$, che per il Lemma di Euclide implica $a|h$, ovvero $\exists h' \in \mathbb{Z}$ tale che $h = h'a$.

Sostituendo, si ottiene $c = hb = h'ab$, ovvero $(ab)|c$. □

Dalle slide 6 e 7 (dimostrazione inclusa):

Teorema 6. *(Caratterizzazione dei numeri primi)*

Sia $p \in \mathbb{Z}$.

$$p \text{ è primo} \iff (\forall m, n \in \mathbb{Z} \ / \ p|(mn), \text{ allora o } p|m \text{ oppure } p|n)$$

Dimostrazione. $\implies$

Sia p primo. Per ipotesi supponiamo esistano $m, n \in \mathbb{Z}$ tali che $p|(mn)$, con p che non divide n.

Poiché p è primo, significa che n non è multiplo di p, e quindi $MCD(p, n) = 1$.

Per il Lemma di Euclide, da $MCD(p, n) = 1$ e $p|(mn)$ segue $p|m$, ovvero la tesi. □

Dimostrazione. $\impliedby$

Supponiamo ora che $\forall m, n \in \mathbb{Z}$ tali che $p|(mn)$, allora o $p|m$ oppure $p|n$. Immaginiamo di scrivere p come prodotto di due fattori: $p = ab$, con $a, b \in \mathbb{Z}$.

Da $p = ab$ segue $p|(ab)$; per ipotesi, allora, $p|(ab)$ implica o $p|a$ oppure $p|b$. *(ipotesi del teorema).*

Supponiamo *(senza perdita di generalità, si può applicare lo stesso ragionamento nell'altro caso)* che $p|a$. Siccome $p = ab$, sicuramente $a|p$.

Da $p|a$ e $a|p$ segue allora che $a = \pm p$.

Se $a = p$, allora $b = 1$; se $a = -p$, allora $b = -1$.

In entrambi i casi, gli unici divisori di p sono $\pm p$ e ± 1, per cui p è primo. □

Dalla slide 9 (dimostrazione dagli appunti presi in aula ma con supporto dalle videolezioni per gli ultimi passaggi):

Teorema 7. *(Esistenza del Minimo Comune Multiplo)*

Dati $a, b \in \mathbb{Z} - \{0\}, \exists M = mcm(a, b)$*:*

$$M = \frac{|ab|}{MCD(a, b)}.$$

Dimostrazione. Per definizione $mcm(a, b) = mcm(|a|, |b|)$.

Supponiamo $a, b \in \mathbb{Z}^+$.

Consideriamo $M = \frac{|a \cdot b|}{(MCD(a,b))}$

Da dimostrare che $M = mcm(a, b)$

ovvero che

- $a|M$ e $b|M$
- $\forall c \in \mathbb{Z}, a|c$ e $b|c \implies M|c$

Essendo $a, b \in \mathbb{Z}^+$, sappiamo che esiste $MCD(a, b) = d$. Per definizione di MCD, $d|a$ e $d|b$.

- $d|a \implies \exists h \in \mathbb{Z} : a = d \cdot h$
- $d|b \implies \exists k \in \mathbb{Z} : b = d \cdot k$

allora $M = \frac{(a \cdot b)}{d} = \frac{(d \cdot h \cdot d \cdot k)}{d} = d \cdot h \cdot k \in \mathbb{Z}$

che si può scrivere come:

- $M = (dh) \cdot k = a \cdot k => a|M$
- $M = h \cdot (dk) = b \cdot h => b|M$

Resta da dimostrare il secondo punto: $\forall c \in \mathbb{Z}, a|c$ e $b|c \implies M|c$

$h = \frac{a}{MCD(a,b)}$, $k = \frac{b}{MCD(a,b)}$ coprimi

considero $c \in \mathbb{Z} : a|c$ e $b|c$ e voglio provare che $M|c$

- $a|c$ significa che esiste $\alpha \in \mathbb{Z} : c = \alpha \cdot a = d(h \cdot \alpha)$
- $b|c$ significa che esiste $\beta \in \mathbb{Z} : c = \beta \cdot b = d(k \cdot \beta)$

ovvero esiste $c' = h \cdot \alpha$ e $c' = k \cdot \beta : c = d \cdot c'$

- $c' = h \cdot \alpha \implies h|c'$

- $c' = k \cdot \beta \implies k|c'$

Poiché h e k sono coprimi, $hk|c'$, ovvero $\exists \gamma \in \mathbb{Z} : c' = hk \cdot \gamma$

Sostituendo in $c = d \cdot c'$, si ottiene che $c = dhk \cdot \gamma = M \cdot \gamma$ con $\gamma \in \mathbb{Z}$, ovvero che $M|c$ □

Dalla slide 12 (dimostrazione sulle slide):

Teorema 8. *(Esistenza di infiniti numeri primi)*
Esistono infiniti numeri primi.

Dimostrazione. Supponiamo per assurdo che i numeri primi siano finiti, ovvero che esista $N \in \mathbb{N}$ tale che $p_1, p_2, ...p_N$ siano tutti e soli i numeri primi.

Consideriamo ora $\bar{n} = p_1 p_2 ... p_N + 1$

Sicuramente, $\forall i \in \mathbb{N}_N$, non può essere vero $p_i|\bar{n}$, poiché il resto della divisione euclidea tra $\bar{n}$ e p_i vale 1.

D'altra parte, per il teorema fondamentale dell'aritmetica, anche $\bar{n}$ deve poter essere scritto come prodotto di potenze di numeri primi; se $p_1, p_2, ..., p_N$ sono gli unici primi, si ottiene l'assurdo. □

Proprietà 11. $\sqrt{3}$ *è irrazionale.*

Dimostrazione. Supponiamo per assurdo che $\sqrt{3}$ sia razionale, ovvero che $\sqrt{3} = \frac{m}{n}$, con $m, n \in \mathbb{Z}^+$.

Allora $m = \sqrt{3}n$, ed elevando al quadrato si ottiene: $\underbrace{m^2}_{c'} = \underbrace{3n^2}_{c''}$. Poiché, per il teorema fondamentale dell'aritmetica, la scomposizione in fattori primi è unica a meno dell'ordine dei fattori, da $c' = m^2$ segue che gli esponenti di tutti i fattori primi di c' sono pari, mentre da $c'' = 3n^2$ segue che il fattore primo 3 compare in c'' con esponente dispari.

Poiché $c' = c''$, si ha un assurdo. □

Lemma 1. *Se n è dispari, fattorizzare n equivale a scrivere n come differenza di due quadrati.*

Dimostrazione. Poiché $n \in \mathbb{D}$, una sua fattorizzazione $n = ab$ implica che anche $a, b \in \mathbb{D}$, mentre $a + b, a - b \in \mathbb{P}$.

Allora:

$$n = ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2, \text{ con } \frac{a+b}{2}, \frac{a-b}{2} \in \mathbb{Z}$$

Viceversa, è ben noto che:

$$n = x^2 - y^2 = (x - y)(x + y)$$

□

4 Aritmetica modulare

File 5.

Dalla slide 4:

Proprietà 12. *La somma in $\mathbb{Z}_n$, definita come $[a] + [b] = [a + b]$, è ben posta.*

Dimostrazione. Per provare che la somma è ben posta, occorre provare che, $\forall a' \in [a]$ e $\forall b' \in [b]$, si ha $[a' + b'] = [a + b]$.

Per ipotesi *($a' \in [a]$, cioè $a' \equiv_n a$, e lo stesso per b e b')* $\exists h \in \mathbb{Z} \ / \ a' - a = hn$ ed $\exists h' \in \mathbb{Z} \ / \ b' - b = h'n$.

Sommando membro a membro si ottiene $(a' + b') - (a + b) = (h + h')n$; poichè $h + h' \in \mathbb{Z}$, ciò prova la tesi. □

Dalla slide 5:

Proprietà 13. *Il prodotto in $\mathbb{Z}_n$, definito come $[a] \cdot [b] = [a \cdot b]$, è ben posto.*

Dimostrazione. Per provare che il prodotto è ben posto, occorre provare che, $\forall a' \in [a]$ e $\forall b' \in [b]$, si ha $[a' \cdot b'] = [a \cdot b]$.

Per ipotesi *($a' \in [a]$, cioè $a' \equiv_n a$, e lo stesso per b e b')* $\exists h \in \mathbb{Z} \ / \ a' - a = hn$ ed $\exists h' \in \mathbb{Z} \ / \ b' - b = h'n$.

Moltiplicando membro a membro $\forall h \in \mathbb{Z} \ / \ a' = a + hn$ e $\exists h' \in \mathbb{Z} \ / \ b' = b + h'n$ si ottiene $a'b' = ab + ah'n + bhn + hh'n^2$, da cui $a'b' - ab = (ah' + bh + hh'n)n$. Poichè $ah' + bh + hh'n \in \mathbb{Z}$, ciò prova la tesi. □

Teorema 9. *$(\mathbb{Z}_n, +, \cdot)$ è un campo se e solo se n è primo.*

Dimostrazione. È facile verificare che, se n non è primo, l'anello $(\mathbb{Z}_n, +, \cdot)$ ammette divisori dello zero, per cui non è un campo:

$$n = ab \implies [n] = [ab] = [a] \cdot [b] = [0]$$

Per verificare il viceversa, si considera n primo, e si dimostra che ogni elemento non nullo ammette inverso.

Se $[a] \neq [0]$, allora $a \not\equiv_n 0$, ovvero a non è multiplo di n. Poichè per ipotesi n è primo, si ha allora $MCD(a, n) = 1$.

Per l'identità di Bezout, $\exists \alpha, \beta \in \mathbb{Z}$ tali che $1 = \alpha n + \beta a$, ovvero $1 - \beta a = \alpha n$, da cui si ottiene $\beta a \equiv_n 1$. Resta così dimostrato che $[a'] = [\beta]$ è inverso di $[a]$ in $\mathbb{Z}_n$, poichè $[a] \cdot [a'] = [a\beta] = [1]$. □

Dalla slide 9 (dimostrazione sulle slide):

Teorema 10. *Ogni numero intero n è congruo modulo 9 alla somma delle sue cifre.*

Dimostrazione. Esplicitando la natura posizionale del sistema decimale, si ha:

$n = a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + ... + a_k 10^k =$

$= a_0 + a_1(1 + 9) + a_2(1 + 99) + ... + a_k(1 + \underbrace{999...999}_{k}) =$

$= (a_0 + a_1 + a_2 + ... + a_k) + 9a_1 + 99a_2 + ... + \underbrace{999...999}_{k} a_k =$

$= (a_0 + a_1 + a_2 + ... + a_k) + 9(a_1 + 11a_2 + ... + \underbrace{111...111}_{k} a_k) =$

Quindi, n so ottiene dalla somma delle sue cifre, aggiungendo un multiplo di 9; ciò prova la tesi. □

Dalla slide 11 (dimostrazione sulle slide):

Proprietà 14. *(Criterio di divisibilità per 3 e per 9)*
Un numero intero è divisibile per 3 (per 9) se e solo se la somma delle sue cifre è divisibile per 3 (per 9).

Dimostrazione. $n \equiv a_k + a_{k-1} + ... + a_0$ sia modulo 3 che modulo 9. □

Proprietà 15. *(Criterio di divisibilità per 2 e per 5)*
Un numero intero è divisibile per 2 (risp. per 5) se e solo se la cifra delle unità, a_0, è dibisibile per 2 (risp. per 5).

Dimostrazione. Per ogni $k \geq 1, 10^k \equiv 0$ sia modulo 2 che modulo 5. Quindi $n \equiv a_0$ sia modulo 2 che modulo 5. □

Dalla slide 12 (dimostrazione sulle slide):

Proprietà 16. *(Criterio di divisibilità per 4 e per 25)*

Dimostrazione. $100 = 2^2 5^2 \equiv 0$ sia modulo 4 che modulo 25. Allora ogni intero è congruo modulo 4 (risp. modulo 25) all'intero costituito dalla sua cifra delle decine, a_1, e dalla sua cifra delle unità, a_0. □

Proprietà 17. *(Criterio di divisibilità per 2^r) Un intero n è divisibile per 2^r se e solo se 2^r divide il numero costituito dalle ultime r cifre di n.*

Dimostrazione. Basta osservare che $10^k = 2^k 5^k \equiv 0 \pmod{2^r}$ per ogni $k \geq r$. □

Dalla slide 13 (dimostrazione sulle slide):

Proprietà 18. *(Criterio di divisibilità per 11) Un intero n è divisibile per 11 se e solo se è divisibile per 11 la somma a segni alterni delle sue cifre:*

$$a_0 - a_1 + a_2 - ... + (-1)^k a_k \equiv 0 \ mod\ 11.$$

Dimostrazione. Basta osservare che

$$10 \equiv -1 \bmod 11 \implies \begin{cases} 10^{2p} \equiv 1 & \bmod 11 \\ 10^{2p+1} \equiv -1 & \bmod 11 \end{cases}$$

□

Dalla slide 15 (dimostrazione sulle slide):

Teorema 11. *(Esistenza di soluzioni di congruenze lineari)*
La congruenza lineare $ax \equiv b$ (mod n) con $a, b, n \in \mathbb{Z}$ e $n \geq 2$ ammette soluzioni se e solo se $MCD(a, n)|b$.

Dimostrazione. Ad ogni congruenza lineare è possibile associare un'equazione diofantea. Infatti:

$$ax \equiv b \text{ (mod n)} \iff \exists h \in \mathbb{Z} \ / \ b - ax = hn, \text{ ovvero } ax + hn = b.$$

Condizione necessaria e sufficiente per la risolubilità dell'equazione diofantea associata è $MCD(a, n)|b$. □

Dalla slide 16 (dimostrazione dagli appunti):

Teorema 12. *(Risoluzione di congruenze lineari)*
Sia $ax \equiv b \pmod{n}$ una congruenza lineare tale che $d|b$, essendo $d = MCD(a, n)$ e sia x_0 una sua particolare soluzione.
Allora:

- *In $\mathbb{Z}$ le soluzione sono tutti e soli gli interi del tipo*

$$x_0 + h\frac{n}{d}, h \in \mathbb{Z}$$

- *In $\mathbb{Z}_n$ le soluzione sono tutti e soli gli interi del tipo*

$$x_0 + h\frac{n}{d}, h \in \mathbb{Z}_d$$

Inoltre, ogni soluzione in $\mathbb{Z}$ è congrua modulo n ad una delle d soluzioni in $\mathbb{Z}_n$.

Dimostrazione. Suppongo che, oltre ad x_0, anche $\bar{x} \in \mathbb{Z}$ sia soluzione.

- Poiché x_0 è soluzione, $a \cdot x_0 \equiv b \bmod n$
- Poiché $\bar{x}$ è soluzione, $a \cdot \bar{x} \equiv b \bmod n$

Da queste due deriva per sottrazione $a(\bar{x} - x_0) \equiv 0 \bmod n$
Cioè

$$\exists h \in \mathbb{Z} : a \cdot (\bar{x} - x_0) = hn$$

divido ambo i membri per $d = MCD(a, n)$
$\frac{a}{d} \cdot (\bar{x} - x_0) = h \cdot \frac{n}{d} \in \mathbb{Z}$
$\frac{n}{d}$ divide $\frac{a}{d} \cdot (\bar{x} - x_0)$, ed è coprimo con $\frac{a}{d}$
Per il lemma di Euclide: $\frac{n}{d}$ divide $\bar{x} - x_0$
Cioè: $\exists h \in \mathbb{Z} : (\bar{x} - x_0) = h \cdot \frac{n}{d}$
Cioè

$$\bar{x} = x_0 + h \cdot \frac{n}{d} \text{ con } h \in \mathbb{Z}$$

Per dimostrare che in $\mathbb{Z}_n$ le d soluzioni dell'enunciato sono distinte tra loro, suppongo per assurdo che $\exists h, h' \in \mathbb{Z}_d, : x_0 + h \cdot \frac{n}{d} \equiv x_0 + h'\frac{n}{d} \bmod n$
Si semplificano gli x_0, quindi $h \cdot \frac{n}{d} \equiv h' \cdot \frac{n}{d}$ modulo n
quindi h è congruo ad h' modulo $\frac{n}{MCD(\frac{n}{d}, n)}$, ma $MCD(\frac{n}{d}, n) = \frac{n}{d}$, quindi h è congruo ad h' modulo d, ma gli h sono presi in $\mathbb{Z}_d$, quindi se sono congrui tra di loro non possono essere distinti.
Resta da dimostrare che tutte le soluzioni in $\mathbb{Z}$ siano congrue alle d soluzioni in $\mathbb{Z}_d$
considero la generica sol $x_0 + h \cdot \frac{n}{d}$, con $h \in \mathbb{Z}$
considero la divisione euclidea tra h e d, $\exists q \in \mathbb{Z}, \exists r \in \{0, 1, ..., d-1\} : h = q \cdot d + r$
$x_0 + h \cdot \frac{n}{d} = x_0 + (q \cdot d + r)\frac{n}{d} = x_0 + q \cdot n + z \cdot \frac{n}{d}$
$q \cdot n$ è multiplo intero di n
$\implies x_0 + h \cdot \frac{n}{d} \equiv x_0 + r \cdot \frac{n}{d}$ modulo n
ma r appartiene ai possibili resti della divisione per d, ovvero appartiene a $\mathbb{Z}_d$ □

Dalla slide 18 (dimostrazione dagli appunti):

Lemma 2. *Ogni sistema di congruenze lineari del tipo*

$$\begin{cases} a_1 x \equiv b_1 & (mod\ n_1) \\ a_2 x \equiv b_2 & (mod\ n_2) \\ \vdots & \vdots \\ a_r x \equiv b_r & (mod\ n_r) \end{cases}$$

con $MCD(n_i, n_j) = 1\ \forall i \neq j$ *e* $MCD(a_i, n_i) = d_i | b_i\ \forall i \in \mathbb{N}_r$*, è equivalente ad un sistema del tipo:*

$$\begin{cases} x \equiv c_1 & (mod\ n_1') \\ x \equiv c_2 & (mod\ n_2') \\ \vdots & \vdots \\ x \equiv c_r & (mod\ n_r') \end{cases}$$

in cui $MCD(n_i', n_j') = 1\ \forall i \neq j$

Dimostrazione. si dividono entrambi i membri per d_i
allora viene
$\frac{a_i}{d_i} \cdot x \equiv \frac{b_i}{d_i} \bmod \frac{n_i}{MCD(d_i, n_i)}$
ma d_i divide a_i e b_i, quindi le frazioni sono intere
ponendo $a_i' = \frac{a_i}{d_i}, b_i' = \frac{b_i}{d_i}, n_i' = \frac{n_i}{d_i}$, si ottiene

$$a_i' x \equiv b_i' \bmod n_i'$$

questa è una congruenza lineare con $MCD(a_i', n_i') = 1$
che quindi ha una ed una sola soluzione, che chiamiamo c_i
$x \equiv c_i \bmod n_i'$
resterebbe da dimostrare che i nuovi moduli siano coprimi, ma questo è verificato perché abbiamo solo diviso numeri già coprimi tra loro per altri numeri. □

Dalla slide 19 (dimostrazione dagli appunti):

Teorema 13. *(Teorema cinese del resto) Dato un sistema di congruenze lineari del tipo*

$$\begin{cases} x \equiv c_1 & mod\ n_1 \\ x \equiv c_2 & mod\ n_2 \\ \vdots & \vdots \\ x \equiv c_r & mod\ n_r \end{cases}$$

con $MCD(n_i, n_j) = 1\ \forall i \neq j\ (i, j \in \{1, ..., r\})$ *allora esiste sempre una ed una sola soluzione modulo* $N = n_1 \cdot n_2 \cdot ... \cdot n_r$

Dimostrazione. Considero, $\forall i \in \{1, ..., r\}$, l'intero $N_i = \frac{N}{n_i}$ ovvero il prodotto dei moduli escluso n_i.

Considero le r congruenze "fittizie":

$$N_i \cdot x \equiv c_i \bmod n_i\ \forall i = 1, ..., r$$

è evidente che, essendo $MCD(n_i, n_j) = 1 \forall i \neq j$, allora $MCD(N_i, n_i) = 1\ \forall i = 1, ..., r$

quindi, la i-esima congruenza fittizia ha una ed una sola soluzione in $\mathbb{Z}_{n_i}$, chiamata $\bar{x}_i$.

Adesso considero l'intero

$$\bar{x} = N_1 \cdot \bar{x}_1 + N_2 \cdot \bar{x}_2 + ... + N_r \cdot \bar{x}_r$$

e voglio dimostrare che è soluzione del sistema dato.

per provare che modulo N la soluzione sia unica, suppongo per assurdo che $\bar{x}$ e $\bar{y}$ siano due soluzioni del sistema dato per ogni i, guardo se $\bar{x}$ verifica la congruenza i-esima originaria

$$\bar{x} = N_1 \cdot \bar{x}_1 + ... + N_{i-1} \cdot \bar{x}_{i-1} + N_i \cdot \bar{x}_i + N_{i+1} \cdot \bar{x}_{i+1} + ... + N_r \cdot \bar{x}_r$$

ma tutti gli n_j con $j \neq i$ sono multipli di n_i, quindi sono congrui a 0 modulo n_i

Quindi

$$\bar{x} \equiv N_i \cdot \bar{x}_i \text{ modulo } n_i$$

visto che $\bar{x}_i$ è soluzione della congruenza fittizia $N_i \cdot x \equiv c_i \bmod n_i$, allora $\bar{x} \equiv c_i$ modulo n_i, cioè $\bar{x}$ è soluzione della i-esima congruenza del sistema dato.

Dimostrata l'esistenza della soluzione (e il metodo di calcolo), dimostriamo l'unicità modulo N

poiché $\bar{x}$ è soluzione del sistema dato, $\bar{x} \equiv c_i \bmod n_i\ \forall i$ lo stesso vale per $\bar{y}$, per cui $\bar{y} \equiv c_i \bmod n_i$

Quindi $\bar{x} - \bar{y} \equiv 0 \bmod n_i$, ovvero $\bar{x} - \bar{y}$ è multiplo intero di n_i

ma se gli n_i sono coprimi, quindi un numero multiplo di tutti deve essere multiplo del loro prodotto, quindi di N, quindi la differenza tra due soluzioni è multiplo di N, quindi è dimostrata l'unicità modulo N della soluzione. □

Dalla slide 21 (dimostrazione dagli appunti):

Teorema 14. *(Sistemi di due congruenze lineari)*

Un sistema di due congruenze lineari del tipo

$$\begin{cases} x \equiv a & mod\ n \\ x \equiv b & mod\ m \end{cases}$$

ammette soluzioni se e solo se $MCD(n, m) | (a - b)$*; inoltre, se ammette soluzioni, la soluzione è unica modulo* $M = mcm(m, n)$.

Dimostrazione. **Prima parte:** $\bar{x}$ è soluzione $\implies MCD(n,m)|a-b$
Per ipotesi, $\exists h \in \mathbb{Z} : \bar{x} = a + hn$, ed $\exists k \in \mathbb{Z} : \bar{x} = b + km$. Sottraendo queste due equazioni membro a membro, so ottiene:

$$a - b + hn - km = 0 \implies a - b = hn + kn$$

Ma se $MCD(n,m) = d$ divide n (quindi $n = h'd$) ed m (quindi $m = k'd$), allora divide anche $a - b$:

$$a - b = hh'd + kk'd = (hh' + kk')d \text{ con } (hh' + kk') \in \mathbb{Z}$$

cioè $d|a-b$, ovvero la tesi.
Seconda parte: Il sistema ammette sol. mod $mcm(n,m) \impliedby MCD(n,m)|a-b$
Se $MCD(n.m)|a-b$, allora $\exists h \in \mathbb{Z} : a - b = h \cdot d$
Per l'identità di Bezout, $\exists \alpha, \beta \in \mathbb{Z} : d = \alpha n + \beta m$
$a - b = h\alpha n + h\beta n \implies a - h\alpha n = b + h\beta m$
Quindi, se $a - h\alpha n = c$, anche $b + h\beta m = c$
Quindi $c \equiv a \bmod n$ e $c \equiv b \bmod m$, ovvero c'è una soluzione.

□

Dalla slide 23 (dimostrazione sulle slide):
Proprietà 19. *Se r ed s sono coprimi, allora la corrispondenza*

$$f : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$$

definita da

$$[x]_{rs} \mapsto ([x]_r, [x]_s)$$

è una applicazione biunivoca che conserva somma e prodotto (è un "isomorfismo di anelli").

Dimostrazione. Occorre provare che $\forall([a]_r, [b]_s) \in \mathbb{Z}_r \times \mathbb{Z}_s$, $\exists![x]_{rs}$ tale che $f([x]_{rs}) = ([a]_r, [b]_s)$.
La condizione equivale al sistema $\begin{cases} x \equiv a \pmod{r} \\ x \equiv b \pmod{s} \end{cases}$
che, essendo $MCD(r,s) = 1$, ammette una ed una sola soluzione modulo $r \cdot s$. □

Dalla slide 24 (dimostrazioni dagli appunti):
Teorema 15. *(Piccolo teorema di Fermat)*
Sia p un numero primo. Allora, per ogni $a \in \mathbb{Z}$ tale che a non sia multiplo di p, si ha

$$a^{p-1} \equiv 1 \text{ (mod } p\text{)}$$

Dimostrazione. a non è multiplo di p (p primo) $\implies MCD(a,p) = 1$
Consideriamo allora gli interi:

$$a, 2a, 3a, ..., (p-1)a$$

Considerando in $\mathbb{Z}_p$, osserviamo che:

- sono tutti distinti. Infatti, se fosse $r \cdot a \equiv s \cdot a$ con $1 \leq r < s \leq p-1$ si avrebbe $r \cdot a - s \cdot a = h \cdot p$, ovvero $(r-s)a = h \cdot p$. p dovrebbe dividere $(r-s)a$; essendo che a non è un multiplo di p significherebbe $p|s-r$, che è assurdo *(visto che $s - r < p$)*.
- sono tutti non congrui a 0 mod p, infatti suponendo per esempio $r \cdot a \equiv 0 \bmod p$, con $1 \leq r \leq p-1$, ovvero $\exists h \in \mathbb{Z} : r \cdot a = h \cdot p$, ovvero $p|r \cdot a$, ma essendo p ed a coprimi, seguirebbe che $p|r$, che è assurdo.

Allora questi $p-1$ interi sono, in Z_p:

$$1, 2, ..., p-1$$

a meno dell'ordine. Allora:

$$a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \equiv 1 \cdot 2 \cdot ... \cdot (p-1) \text{ mod p}$$

si può scrivere come

$$(1 \cdot 2 \cdot ... \cdot (p-1))a^{p-1} \equiv 1 \cdot 2 \cdot ... \cdot (p-1) \text{ mod p}$$

$$\implies a^{p-1} \equiv 1 \text{ mod} \frac{P}{MCD(p, \underbrace{1 \cdot 2 \cdot ... \cdot p-1}_{\text{nessun fattore multiplo di p primo}}) = 1} = p$$

Resta così dimostrata la tesi ($a^{p-1} \equiv 1 \text{ mod } p$) □

Corollario 1. *Sia p un numero primo. Allora, per ogni $a \in \mathbb{Z}$, si ha*

$$a^p \equiv a \text{ (mod } p).$$

Dimostrazione. Se a non è multiplo di p, il piccolo teorema di Fermat garantisce che $a^{p-1} \equiv 1$ mod p.
Moltiplicando per a si ottiene $a^p \equiv a$ mod p, ovvero la tesi.
Se a è multiplo di p, $a \equiv 0$ mod p, quindi anche $a^p \equiv 0$ mod $p \implies a^p \equiv a$ mod p. □

5 Funzione di Eulero

File 6

Dalla slide 3 (dimostrazione dalle slide):

Proprietà 20. *Il numero di elementi invertibili in $\mathbb{Z}_n$ ($\forall n \geq 2$) è esattamente $\varphi(n)$.*

Dimostrazione. Fissato $n \geq 2$, un elemento $x \in \mathbb{Z}_n$ è invertibile se e solo se $\exists y \in \mathbb{Z}_n$ tale che $xy \equiv 1 \pmod{n}$; questa è una congruenza lineare che ammette soluzione se e solo se $MCD(x, n)|1$, ovvero se e solo se x ed n sono coprimi. Quindi, il numero di elementi invertibili in $\mathbb{Z}_n$ è pari al numero di elementi coprimi ad n in $\mathbb{Z}_n$, ovvero $\varphi(n)$. □

Dalla slide 6 (dimostrazione da appunti presi in aula+videolezione):

Proprietà 21. *(Proprietà della Funzione di Eulero)*

- *Se $p \in \mathbb{Z}^+$ è numero primo, allora $\varphi(p) = p - 1$.*
- *Se $p \in \mathbb{Z}^+$ è numero primo, allora $\varphi(p^h) = p^h - p^{h-1}, h \geq 1$.*
- *Se $p, q \in \mathbb{Z}^+$ sono due numeri primi distinti, allora $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$.*

Dimostrazione. Si dimostrano una ad una le tre proprietà:

- Il primo punto è banale (se p è primo, tutti i numeri tra 1 e $p - 1$ sono coprimi ad esso).
- Per il secondo punto consideriamo gli interi tra 1 e p^h. Tra questi, non sono coprimi a p^h (con p primo) quelli che sono multipli di p, ovvero quelli che si possono scrivere come $q \cdot p$ con $1 \leq q \leq p^{h-1}$ (visto che bisogna arrivare fino a p^h come risultato del prodotto). Quindi ce ne sono p^{h-1} (uno per ogni fattore q possibile).

  Quindi quelli coprimi a p^h sono $\underbrace{p^h}_{\text{interi tra 1 e } p^h} - \underbrace{p^{h-1}}_{\text{interi in quel range non coprimi a } p^h}$
- Per il terzo punto **(non completamente dimostrato, solo un cenno, almeno nella videolezione è considerato così, quindi non dovrebbe chiederlo)** si considera l'isomorfismo di anelli $f : \mathbb{Z}_{p \cdot q} \to \mathbb{Z}_p \times \mathbb{Z}_q$

  $$[x]_{pq} \mapsto ([x]_p, [x]_q)$$

  . Quindi

  $$MCD(x, p \cdot q) = 1 \iff \begin{cases} MCD(x, p) = 1 \\ MCD(x, q) = 1 \end{cases}$$

  Ma ci sono $\varphi(p)$ elementi coprimi con p in Z_p e $\varphi(q)$ elementi coprimi con q in Z_q, quindi ci sono $\varphi(p) \cdot \varphi(q)$ coppie in $\mathbb{Z}_p \times \mathbb{Z}_q$ che rispettano i vincoli.

□

Dalla slide 7 (dimostrazione dagli appunti):

Teorema 16. *(Teorema di Eulero-Fermat)*

$\forall n \in \mathbb{N}$ e $\forall a \in \mathbb{Z}$ tale che $MCD(a, n) = 1$, si ha:

$$a^{\varphi(n)} \equiv 1 \text{ (mod } n)$$

Dimostrazione. La dimostrazione si divide in due parti. La prima si limita al caso in cui n sia potenza di un numero primo, la seconda si estende a qualsiasi n.

Prima parte: $n = p^h$ con p primo

Questa parte si dimostra per induzione su h.

- **passo iniziale** $h = 1 \implies n = p$, ovvero che n è primo.
  in questo caso $\varphi(p) = p - 1$, ovvero $a^{\varphi(p)} = a^{p-1}$, ma $MCD(a, p) = 1$ vuol dire che a non è multiplo di p, e per il piccolo teorema di Fermat
  $$a^{p-1} \equiv 1 \bmod p$$
  .
- **passo induttivo**:
  Ipotesi: $a^{\varphi(p^k)} \equiv 1 \bmod p^k \ \forall a$ coprimo con p^k $(\exists h \in \mathbb{Z} : a^{\varphi(p^k)} = 1 + hp^k)$
  Tesi: $a^{\varphi(p^{k+1})} \equiv 1 \bmod p^{k+1} \ \forall a$ coprimo con p^{k+1}
  Osserviamo che condizione di coprimalità è equivalente rispetto a p^k o a p^{k+1}.
  $\varphi(p^{k+1}) = p^{k+1} - p^k = p(\underbrace{\varphi(p^k)}_{p^k - p^{k-1}})$
  cioè $a^{\varphi(p^{k+1})} = a^{p\varphi(p^k)} = \left[a^{\varphi(p^k)}\right]^p$
  Per ipotesi induttiva, $a^{\varphi(p^k)} = 1 + hp^k$ con $h \in \mathbb{Z}$, quindi $a^{\varphi(p^k+1)} = \left[a^{\varphi(p^k)}\right]^p = \left(1 + hp^k\right)^p$.
  La potenza $(1 + hp^k)^p$ si risolve con il binomio di Newton:
  $$(1 + hp^k)^p = \sum_{r=0}^{p} \binom{p}{r} 1^{p-r} (hp^k)^r = \sum_{r=0}^{p} \binom{p}{r} (hp^k)^r =$$
  $$= 1 + \underbrace{\overbrace{\binom{p}{1}}^{p} \cdot hp^k + \binom{p}{2}(hp^k)^2 + ... + \binom{p}{p}(hp^k)^p}_{\text{tutti multipli di } p^{k+1}} \equiv 1 \bmod p^{k+1}$$
  È verificata la tesi induttiva, e quindi termina la prima parte della dimostrazione.

Seconda parte: n generico, cioè decomponibile in prodotto di potenze di primi

Per le proprietà della funzione di Eulero: $\varphi(n) = \varphi(p_1^{h_1}) \cdot \varphi(p_2^{h_2}) \cdot ... \cdot \varphi(p_r^{h_r})$
$\varphi(p_i^{k_i}) | \varphi(n) \forall i = 1, ..., r$
Per la prima parte della dimostrazione,
$$a^{\varphi(p_i^{h_i})} \equiv 1 \bmod p_i^{h_i} \ \forall i = 1, ..., r$$
Elevo ambo i membri a $\frac{\varphi(n)}{\varphi(p_i^{h_i})} \in \mathbb{Z}$
$\left[a^{\varphi(p_i^{h_i})}\right]^{\frac{\varphi(n)}{\varphi(p_i^{h_i})}} \equiv 1^{\frac{\varphi(n)}{\varphi(p_i^{h_i})}} \bmod p_i^{h_i} \implies a^{\varphi(n)} \equiv 1 \bmod p_i^{h_i} \ \forall i = 1, ..., r$
Quindi $a^{\varphi(n)} - 1$ è multiplo intero di $p_i^{h_i} \forall i = 1, ..., r$
Poiché i primi sono distinti, le loro potenze sono coprime, quindi $a^{\varphi(n)} - 1$ è multiplo di $p_1^{h_1} \cdot p_2^{h_2} \cdot ... \cdot p_r^{h_r}$
Cioè $a^{\varphi(n)} \equiv 1 \bmod n$, ovvero la tesi. □

Teorema 17. *(Teorema di Eulero-Fermat generalizzato)*
$\forall n \in \mathbb{Z}$ *è un intero libero da quadrati, allora:*

$$a^{\varphi(n)+1} \equiv a \text{ (mod } n) \; \forall a \in \mathbb{Z}$$

Inoltre:

$$a^{h\varphi(n)+1} \equiv a \text{ (mod } n) \; \forall a \in \mathbb{Z}, \forall h \in \mathbb{Z}^+$$

Dimostrazione. Per ipotesi $n = p_1 \cdot ... \cdot p_r$ con p_i primi distinti (definizione di intero libero da quadrati).

Consideriamo il sistema di congruenze lineari $\begin{cases} x \equiv a \mod p_1 \\ x \equiv a \mod p_2 \\ \vdots \\ x \equiv a \mod p_r \end{cases}$

Per il teorema cinese del resto (applicabile, essendo i moduli coprimi):

$$\exists! \text{ soluzione modulo } p_1 \cdot p_2 \cdot ... \cdot p_r = n$$

Banalmente, $x = a$ è soluzione.
Se riusciamo a verificare che anche $a^{h\varphi(n)+1}$ è soluzione, vorrebbe dire che $a^{h\varphi(n)+1} \equiv a$ modulo n.
Osserviamo che

$$\varphi(n) = \varphi(p_1 \cdot p_2 \cdot ... \cdot p_r) = \varphi(p_1) \cdot ... \cdot \varphi(p_r) = (p_1 - 1) \cdot ... \cdot (p_r - 1)$$

quindi

$$h \cdot \varphi(n) + 1 = k \cdot (p_i - 1) + 1 \forall i = 1, ..., r \text{ con } k \in \mathbb{Z}$$

Per il piccolo teorema di Fermat

$$a^{h\varphi(n)+1} = a^{k(p_i-1)+1} \equiv a \mod p_i \; \forall a \in \mathbb{Z}$$

Cioè $a^{h\varphi(n)} + 1$ verifica la i-esima congruenza del sistema, quindi verifica tutto il sistema, quindi resta provata la tesi (è soluzione modulo $n = p_1 \cdot p_2 \cdot ... \cdot p_r$). □

6 Calcolo combinatorio

File 7

Dalla slide 9 (dimostrazione dalla videolezione 24):

Proposizione 6. *(numero delle combinazioni con ripetizione)*
Il numero di combinazioni con ripetizione di n oggetti a k a k è:

$$C^R(n;k) = \binom{n+k-1}{k}$$

Dimostrazione. $\mathbb{N}_n = \{1, 2, ..., n\}$
Una combinazione con ripetizione di n oggetti a k a k è una scelta di k elementi

$$1 \leq a_1 \leq a_2 \leq a_3 \leq ... \leq a_{k-1} \leq a_k \leq n \ (*)$$

che si può scrivere come

$$1 \leq \underbrace{a_1}_{b_1} < \underbrace{a_2+1}_{b_2} < \underbrace{a_3+2}_{b_3} < ... < \underbrace{a_k+(k-1)}_{b_k} \leq n+(k-1)$$

Quindi scegliere $a_1, ..., a_k$ che verificano la condizione $(*)$ equivale a scegliere $b_1, ..., b_k$ che verificano

$$1 \leq b_1 < b_2 < b_3 < ... < b_k \leq n+(k-1)$$

ovvero a scegliere k elementi distinti compresi tra 1 e $n+k-1$.
Quindi $C^R(n;k) = C(n+k-1, k) = \binom{n+k-1}{k}$

□

Dalla slide 11 (dimostrazione dalla videolezione 25):

Proposizione 7. *(numero delle ripartizioni)*
Il numero di possibili ripartizioni di un insieme di cardinalità n in r sottoinsiemi di cardinalità rispettivamente $k_1, ..., k_r$ (con $r \geq 1, k_i \geq 1 \forall i \in \{1, ..., r\}$, e tali che $\sum_{i=1}^r k_i = n$), è:

$$\frac{n!}{k_1! \cdot k_2! \cdot ... \cdot k_r!} = P^R(n; k_1, k_2, ..., k_r)$$

Dimostrazione. $A = \{a_1, ..., a_n\}$
Vogliamo ottenere

$$A_1, ..., A_r \subseteq A$$

con $\#A_i = k_i$ e tale che $\bigcup_{i=1}^r A_i = A,\ A_i \cap A_j = \emptyset \ \forall i \neq j$.
Per scegliere gli elementi di A_1 ho $\binom{n}{k_1}$ possibilità.

Dopo aver fissato A_1, per scegliere gli elementi di A_2 ho $\binom{n-k_1}{k_2}$ modi possibili, e il ragionamento procede per i successivi sottoinsiemi A_i.
Quindi, il numero di modi per suddividere A secondo i vincoli dati (per il principio del prodotto) è:

$$\binom{n}{k_1} \cdot \binom{n-k_1}{k_2} \cdot \binom{n-k_1-k_2}{k_3} \cdot ... \cdot \binom{n-(k_1+...+k_{r-2})}{k_{r-1}} \cdot \binom{n-(k_1+...+k_{r-1})}{k_r}$$

Ma $n - (k_1 + ... + k_{r-1}) = k_r$ necessariamente perché devono necessariamente rimanere solo gli ultimi k_r elementi una volta scelti gli elementi che andranno negli altri sottoinsiemi della ripartizione.
Andando ad esplicitare quei coefficienti binomiali,

$$\frac{n!}{k_1!\cancel{(n-k_1)!}} \cdot \frac{\cancel{(n-k_1)!}}{k_2!\cancel{(n-k_1-k_2)!}} \cdot \frac{\cancel{(n-k_1-k_2)!}}{k_3!(n-k_1-k_2-k_3)!} \cdot ... \cdot \frac{(n-k_1-...-k_{r-2})!}{k_{r-1}!\underbrace{(n-k_1-...-k_{r-1})!}_{k_r!}} \cdot \frac{\cancel{k_r!}}{\cancel{k_r!} \cdot 0!}$$

E anche il termine al denominatore del terzo fattore si eliderebbe con il numeratore del quarto (non mostrato), e il numeratore del penultimo con il denominatore del terzultimo, ecc. e si arriva dunque a:

$$\frac{n!}{k_1! \cdot k_2! \cdot ... \cdot k_r!} = P^R(n; k_1, k_2, ..., k_r)$$

cioè la tesi. □

Dalla slide 14 (dimostrazione dagli appunti):

Teorema 18. *(Principio di inclusione/esclusione)*
Siano A e B insiemi finiti, con $\#A = n$e $\#B = m$; allora:

$$\#(A \cup B) = \#A + \#B - \#(A \cap B)$$

Dimostrazione. $\#(A \cup B) = \#(A \underbrace{\cup}_{\text{unione disgiunta}} (B - A))$

Ma $B = (B - A) \underbrace{\cup}_{\text{unione disgiunta}} (A \cap B)$

quindi $\#B = \#(B - A) + \#(A \cap B)$
ovvero $\#(B - A) = \#B - \#(A \cap B)$
allora

$$\#(A \cup B) = \#A + \#(B - A) = \#A + \#B - \#(A \cap B)$$

□

Dalla slide 15 (dimostrazione dagli appunti):

Teorema 19. *(Principio di inclusione/esclusione con tre insiemi)*
Siano A, B e C sono insiemi finiti, allora:

$$\#(A \cup B \cup C) = \#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C)$$

Dimostrazione.

$$\#(A \cup B \cup C) = \#((A \cup B) \cup C) = \#(A \cup B) + \#C - \#((A \cup B) \cap C) =$$

$$= \#A + \#B - \#(A \cap B) + \#C - \#[(A \cap C) \cup (B \cap C)] =$$

$$= \#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C) =$$

□

7 Relazioni ricorsive

File 8

Teorema 20. *(Forma chiusa per relazioni ricorsive lineari del I ordine non omogenee a coefficienti costanti)*

La successione definita da

$$\begin{cases} a_n = b \cdot a_{n-1} + d(n) \quad \forall n > m \\ a_m = c \end{cases}$$

ha come forma chiusa:

$$a_n = b^{n-m} \cdot \left[c + \sum_{i=1}^{n-m} d(m+i) \cdot b^{-i} \right] \quad \forall n \geq m$$

Dimostrazione. Per induzione:

- **Passo iniziale**: $n = m + 1$

  $$a_{m+1} = b^1 \cdot [c + d(m+1) \cdot b^{-1}] = b \cdot c + d(m+1)$$

  è banalmente verificato
- **Passo induttivo**:
  Per ipotesi:

  $$a_{n-1} = b^{n-1-m} \cdot \left[c + \sum_{i=1}^{n-1-m} d(m+i) \cdot b^{-i} \right]$$

  applicando la relazione ricorsiva:

  $$a_n = \underbrace{b \cdot b^{n-1-m}}_{b^{n-m}} \cdot \left[c + \sum_{i=1}^{n-1-m} d(m+i) \cdot b^{-i} \right] + d(n) \cdot \underbrace{b^{n-m} \cdot b^{-(n-m)}}_{=1, \text{ fattore aggiunto}} =$$

  $$= b^{n-m} \left[c + \sum_{i=1}^{n-1-m} d(m+i) \cdot b^{-i} + d(n) \cdot b^{-(n-m)} \right]$$

  includendo l'ultimo termine nella parentesi graffa nella somma si ottiene la tesi.

□

7.1 Relazioni ricorsive lineari omogenee del II ordine a coefficienti costanti

Dalla slide 21 (dimostrazione dagli appunti):

Lemma 3. *(Lemma A)*

Data la relazione ricorsiva $a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2}$, se a'_n e a''_n sono due successioni che la verificano, allora $\forall A, B \in \mathcal{C}$ anche la successione $a_n = A \cdot a'_n + B \cdot a''_n$ verifica la relazione ricorsiva data.

Dimostrazione. **Hp:** a'_n e a''_n rispettano la relazione: $\begin{cases} a'_n = \alpha_1 a'_{n-1} + \alpha_2 a'_{n-2} \\ a''_n = \alpha_1 a''_{n-1} + \alpha_2 a''_{n-2} \end{cases}$

$$a_n = Aa'_n + Ba''_n = A(\alpha_1 a'_{n-1} + \alpha_2 a'_{n-2}) + B(\alpha_1 a''_{n-1} + \alpha_2 a''_{n-2}) =$$

$$= \alpha_1(A \cdot a'_{n-1} + B \cdot a''_{n-1}) + \alpha_2(A \cdot a'_{n-2} + B \cdot a''_{n-2}) = \alpha_1 a_{n-1} + \alpha_2 a_{n-2}$$

ovvero anche a_n ottenuto come combinazione lineare delle due rispetta la relazione ricorsiva. □

Dalla slide 22 (dimostrazione dagli appunti):

Lemma 4. *(Lemma B)*

Data la relazione ricorsiva $a_n = \alpha_1 \cdot a_{n-1} + \alpha_1 \cdot a_{n-2}$, la successione $a_n = r^n, r \neq 0$ è soluzione di tale relazione ricorsiva se e solo se r è radice dell'equazione

$$x^2 - \alpha_1 x - \alpha_2 = 0$$

(detta equazione caratteristica della relazione ricorsiva).

Dimostrazione. **Parte 1:** verso $\implies$

Hp: $a_n = r^n$ verifica $a_n = \alpha_1 a_{n-1} + \alpha_2 \cdot a_{n-1}$

Th: r è soluzione dell'equazione $x^2 - \alpha_1 x - \alpha_2 = 0$

Per ipotesi $r^n = \alpha_1 \cdot r^{n-1} + \alpha_2 \cdot r^{n-2}$

Poiché $r \neq 0$, posso dividere per $r^{n-2} (\neq 0)$ e ottenere $r^2 = \alpha_1 \cdot r + \alpha_2$, cioè che r è radice di $x^2 - \alpha_1 x + \alpha_2$, ovvero la tesi.

Parte 2: verso $\impliedby$

Hp: r è soluzione dell'equazione $x^2 - \alpha_1 x - \alpha_2 = 0$

Th: $a_n = r^n$ verifica $a_n = \alpha_1 a_{n-1} + \alpha_2 \cdot a_{n-1}$

Per ipotesi: $r^2 - \alpha_1 \cdot r - \alpha_2 = 0$

Moltiplico per $r^{n-2} (\neq 0)$ e ottengo $r^n - \alpha_1 \cdot r^{n-1} - \alpha_2 \cdot r^{n-2} = 0$, ovvero

$$r^n = \alpha_1 \cdot r^{n-1} + \alpha_2 \cdot r^{n-2}$$

. □

Dalla slide 23 (dimostrazione dagli appunti):

Lemma 5. *(Lemma C)*

Data

$$\begin{cases} a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2} \quad \forall n > m+1 \\ a_m = c_1 \\ a_{m+1} = c_2 \end{cases}$$

se l'equazione caratteristica della relazione ricorsiva ammette due radici distinte $r_1, r_2 \neq 0$, allora l'unica soluzione della relazione ricorsiva che verifica le condizioni iniziali date è del tipo $a_n = A \cdot r_1^n + B \cdot r_2^n$, con $A, B \in \mathcal{C}$.

Dimostrazione. $a_n = Ar_1^n + br_2^n$

$$\begin{cases} a_m = c_1 & \to \begin{cases} A \cdot r_1^m + B \cdot r_2^m = c_1 \\ A \cdot r_1^{m+1} + B \cdot r_2^{m+1} = c_2 \end{cases} \\ a_{m+1} = c_2 & \to \end{cases}$$

La matrice dei coefficienti è $M = \begin{pmatrix} r_1^m & r_2^m \\ r_1^{m+1} & r_2^{m+1} \end{pmatrix}$

$$detM = \begin{vmatrix} r_1^m & r_2^m \\ r_1^{m+1} & r_2^{m+1} \end{vmatrix} = r_1^m r_2^{m+1} - r_1^{m+1} r_2^m = \underbrace{r_1^m}_{\neq 0} \cdot \underbrace{r_2^m}_{\neq 0} \cdot \underbrace{(r_2 - r_1)}_{\neq 0 \text{ per Hp}} \neq 0$$

Quindi il sistema è di Cramer, ovvero $\exists!$ sol. $(\bar{A}, \bar{B})$, ovvero la tesi. □

Dalla slide 24 (dimostrazione dagli appunti):

Lemma 6. *(Lemma D)*

Data la relazione ricorsiva $a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2}$, se l'equazione caratteristica presenta due radici r coincidenti e non nulle, allora anche la successione $a''_n = n \cdot r^n$ verifica la relazione ricorsiva.

Dimostrazione. L'equazione caratteristica, ovvero $x^2 - \alpha_1 x - \alpha_2 = 0$ si può scrivere, per ipotesi, come $(x - r)^2 = 0$, cioè $x^2 - 2rx + r^2 = 0$

Quindi $a_1 = 2r$ e $a_2 = -r^2$

Considero $a'_n = n \cdot r^n$ e controllo se verifica la relazione ricorsiva $a'_n = \alpha_1 a'_{n-1} + \alpha_2 a'_{n-2}$

$$nr^n \stackrel{?}{=} 2r(n-1)r^{n-1} - r^2(n-2)r^{n-2} = 2nr^n - \cancel{2r^n} - \cancel{nr^n} + \cancel{2r^n} = nr^n$$

è dunque verificata la tesi. □

Dalla slide 25 (dimostrazione dagli appunti):

Lemma 7. *(Lemma E)*

Data

$$\begin{cases} a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2} & \forall n > m+1 \\ a_m = c_1 \\ a_{m+1} = c_2 \end{cases}$$

se l'equazione caratteristica della relazione ricorsiva ammette due radici r coincidenti e non nulle, allora l'unica soluzione della relazione ricorsiva che verifica le condizioni iniziali date è del tipo $a_n = A \cdot r^n + B \cdot n \cdot r^n$, con $A, B \in \mathcal{C}$.

Dimostrazione. Per i lemmi precedenti, $a_n = A \cdot r^n + B \cdot n \cdot r^n$ verifica la relazione ricorsiva data.

Impongo le condizioni iniziali

$$\begin{cases} a_m = c_1 & \to \begin{cases} A \cdot r^m + B \cdot mr^m = c_1 \\ A \cdot r^{m+1} + B \cdot (m+1)r^{m+1} = c_2 \end{cases} \\ a_{m+1} = c_2 & \to \end{cases}$$

La matrice dei coefficienti è $M = \begin{pmatrix} r^m & mr^m \\ r^{m+1} & (m+1)r^{m+1} \end{pmatrix}$

$$detM = \begin{vmatrix} r^m & mr^m \\ r^{m+1} & (m+1)r^{m+1} \end{vmatrix} = r^m(m+1)r^{m+1} - r^{m+1}mr_2^m =$$

$$= \cancel{m \cdot r^{2m+1}} + r^{2m+1} - \cancel{m \cdot r^{2m+1}} = r^{2m+1} \neq 0$$

Quindi il sistema è di Cramer, ovvero $\exists!$ sol. $(\bar{A}, \bar{B})$, ovvero la tesi. □

7.2 Proprietà della successione di Fibonacci

Ho omesso la dimostrazione della forma chiusa della successione di Fibonacci, perché si può considerare un esercizio per l'applicazione dei lemmi precedenti. Ho incluso invece l'identità di Cassini, essendo un risultato teorico che deriva da un procedimento ad hoc (in parole povere, si dimostra in un modo che è diverso da come si risolvono gli esercizi), anche se è parte dello stesso esempio.

Dalla slide 32:

Proprietà 22. *(Identità di Cassini)*

Se F_n denota l'n-esimo numero di Fibonacci, allora:

$$F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n.$$

Dimostrazione. Si procede per induzione. Per $n = 1$ è banalmente vero, perché $1 \cdot 0 - (1)^2 = (-1)^1$. Supponiamo che l'identità valga per $n - 1$ (ovvero: $F_n \cdot F_{n-2} - F_{n-1}^2 = (-1)^{n-1}$.

Sostituendo $F_n = F_{n-1} + F_{n-2}$, da cui $F_{n-2} = F_n - F_{n-1}$, si ha:

$$F_n \cdot (F_n - F_{n-1}) - F_{n-1}^2 = (-1)^{n-1}$$

$$(F_n)^2 - F_n \cdot F_{n-1} - F_{n-1}^2 = (-1)^{n-1}$$

$$(F_n)^2 - F_{n-1} \cdot (F_n + F_{n-1}) = (-1)^{n-1}$$

sostituendo $F_{n+1} = F_n + F_{n-1}$

$$(F_n)^2 - F_{n-1} \cdot F_{n+1} = (-1)^{n-1}$$

e, moltiplicando, ambo i membri per -1, si ottiene l'identità di Cassini per n. □

Il cenno di dimostrazione riguardo il fatto che la soluzione di relazioni ricorsive non omogenee si possa esprimere come una soluzione particolare a cui si sommano tutte le soluzioni dell'omogenea associata (slide 36) non è stato incluso, non essendo una dimostrazione completa. Comunque, essenzialmente, dopo aver scritto due soluzioni particolari, se ne fa la differenza e si nota che è soluzione della omogenea.

8 Funzioni generatrici

File 9. Per questo argomento, a seconda di come lo si guarda soggettivamente, sono tutte dimostrazioni o non lo è nessuna. Visto che c'è tutto sulle slide (o almeno io non ho appunti in più su questo), mi risparmio la fatica di stare a trascrivere praticamente tutte le slide, che avrebbe utilità pari a 0.

9 Teoria dei grafi

File 10

Dalla slide 13 (dimostrazione dagli appunti):

Teorema 21. *Sia g_n il numero di classi di equivalenza rispetto alla relazione di isomorfismo tra grafi con n vertici.*

$$\frac{n^2}{2}\left(1-\frac{1}{n}-\frac{2}{n}log_2 n\right) \leq log_2 g_n \leq \frac{n^2}{2}\left(1-\frac{1}{n}\right)$$

Dimostrazione. **Prima parte**: disuguaglianza $\leq$ a destra.

È ovvio che i grafi tra loro non isomorfi non possono essere più del totale dei grafi con n vertici, quindi $g_n \leq \mathcal{G}_n$.

$$\mathcal{G}_n = \{G = (V, E) \text{ con } V = \{v_1, ..., v_n\} \text{ e } E \subseteq \binom{V}{2}\}$$

$$\implies \#\mathcal{G}_n = \#P\left(\binom{V}{2}\right) = 2^{\#\binom{V}{2}} = 2^{\binom{n}{2}}$$

quindi $g_n \leq 2^{\binom{n}{2}}$

$$\implies log_2 g_n \leq \binom{n}{2} = \frac{\cancel{n!}^{n(n-1)}}{2!\cancel{(n-2)!}} = \frac{n^2}{2}\left(1-\frac{1}{n}\right)$$

Seconda parte: disuguaglianza $\leq$ a sinistra.

$g_n \geq \frac{\#\mathcal{G}_n}{\text{n. max di grafi di } n \text{ vertici tra loro isomorfi}=n!} = \frac{2^{\binom{n}{2}}}{n!}$

Quindi $log_2 g_n \geq \binom{n}{2} - log_2 n!$

ma

$$n! = \underbrace{n \cdot (n-1) \cdot ...}_{\text{n fattori}} \leq n^n \implies log_2(n!) \leq log_2 n^n = n log_2 n$$

quindi, mettendo tutto insieme:

$$log_2 g_n \geq \binom{n}{2} - n log_2 n = \frac{n^2}{2}\left(1-\frac{1}{n}-\frac{2}{n}log_2 n\right)$$

□

Dalle slide 26 (enunciato) e 28 (dimostrazione):

Proprietà 23. *$K_{3,3}$ nonplanare*

Dimostrazione. (pensata solo per ripasso, servono i disegni per capire)

Poniamo $V(K_{3,3}) = \{a, b, c\} \cup \{u, v, w\}$ e supponiamo per assurdo che $K_{3,3}$ si immerga nel piano. Consideriamo ora la curva $\mathcal{C}$ formata dal ciclo su $\{a, u, b, v\}$.

Consideriamo ora, senza perdita di generalità, che $c \in Int\mathcal{C}$.

Sia $\mathcal{C}_1$ la curva formata da $\{a, u, c, v\}$ e $\mathcal{C}_2$ la curva formata da $\{b, u, c, v\}$. Per posizionare w, ci sono 3 possibilità:

- $w \in Int\mathcal{C}_1 \rightarrow$ lo spigolo $\{w, b\}$, per il teorema della curva di Jordan, deve intersecare $\mathcal{C}_1$ e quindi $K_{3,3}$ non può essere planare.
- $w \in Int\mathcal{C}_2 \rightarrow$ lo spigolo $\{w, a\}$, per il teorema della curva di Jordan, deve intersecare $\mathcal{C}_2$ e quindi $K_{3,3}$ non può essere planare.
- $w \in Ext\mathcal{C} \rightarrow$ lo spigolo $\{w, c\}$, per il teorema della curva di Jordan, deve intersecare $\mathcal{C}$ e quindi $K_{3,3}$ non può essere planaere.

In tutti i casi, si giunge ad un assurdo; quindi, $K_{3,3}$ non è planare. □

Dalle slide 30-31-32 (dimostrazione dalle slide).

Proprietà 24. *$K_5 non planare$*

Dimostrazione. (pensata solo per ripasso, servono i disegni per capire)

Poniamo $V(K_5) = \{a, b, c, d, e\}$ e supponiamo per assurdo che K_5 si immerga nel piano. Consideriamo la curva $\mathcal{C}$ formata dal ciclo su $\{a, b, c\}$.

Consideriamo ora, senza perdere di generalità, che $d \in Int\mathcal{C}$.

Sia $\mathcal{C}_1$ la curva formata da $\{a, b, d\}$, $\mathcal{C}_2$ la curva formata da $\{a, c, d\}$ e $\mathcal{C}_3$ la curva formata da $\{b, c, d\}$. Per posizionare il vertice e ci sono quattro possibilità:

- $e \in Int\mathcal{C}_1 \rightarrow$ lo spigolo $\{e, c\}$, per il teorema della curva di Jordan deve intersecare $\mathcal{C}_1$ e quindi K_5 non può essere planare.
- $e \in Int\mathcal{C}_2 \rightarrow$ lo spigolo $\{e, b\}$, per il teorema della curva di Jordan deve intersecare $\mathcal{C}_2$ e quindi K_5 non può essere planare
- $e \in Int\mathcal{C}_3 \rightarrow$ lo spigolo $\{e, a\}$, per il teorema della curva di Jordan deve intersecare $\mathcal{C}_3$ e quindi K_5 non può essere planare.
- $e \in Ext\mathcal{C} \rightarrow$ lo spigolo $\{e, d\}$, per il teorema della curva di Jordan deve intersecare $\mathcal{C}_3$ e quindi K_5 non può essere planare.

In tutti i casi si giunge ad un assurdo; quindi K_5 non è planare. □

Dalla slide 37 (dimostrazione dagli appunti)

Teorema 22. *(Formula di Eulero)*

Se $G = (V, E)$ è un grafo finito, planare e connesso, allora $\#V - \#E + \#F = 2$.

Dimostrazione. per induzione su #F=f.

- **Passo iniziale**: $f = 1$. Poiché $f = 1$, in G non ci sono cicli.

  Essendo G connesso per hp, si ha che G è un albero. Per il teorema di caratterizzazione degli alberi finiti, $\#V - 1 = \#E \implies \#V - \#E = 1$. Quindi $\#V - \#E + \#F = 1 + 1 = 2$

- **Passo induttivo**:

  Hp: $\forall G'$ grafo finito planare connesso con $\#F' = f - 1$ facce ($f - 1 \geq 1$) vale $\#V' - \#E' + \#F' = 2$

  Th: $\forall G'$ grafo finito planare connesso con $\#F = f$ facce vale $\#V' - \#E' + \#F = 2$.

  Poiché $f \geq 2$, in G ci sono cicli, quindi G non è un albero. Negando l'affermazione (c), posso affermare che:

  $$\exists e \in E : G' = (V, E - \{e\}) \text{ continua ad essere connesso}$$

  Quindi G' è finito, planare, connesso ed ha una faccia in meno, visto che lo spigolo e divideva due facce, che ora sono "fuse".

  Quindi $\#F' = \#F - 1$. Quindi per G' vale l'ipotesi induttiva

  $$\underbrace{\#V'}_{\#V} - \underbrace{\#E'}_{\#E-1} + \underbrace{\#F'}_{\#F-1} = 2 \implies \#V - \#E + \cancel{1} + \#F - \cancel{1} = 2$$

□

Dalla slide 38 (dimostrazione dalle slide):

Corollario 2. *Se $G = (V, E)$ è un grafo finito, planare e connesso, allora esiste almeno un vertice v tale che $deg(v) \leq 5$.*

Dimostrazione. Ogni faccia ha almeno 3 lati, ed ogni spigolo appartiene ad al più due facce; quindi $\#E \geq \frac{3\#F}{2}$, ovvero

$$\#F \leq \frac{2\#E}{3}$$

.

Dalla formula di Eulero segue:

$$2 = \#V - \#E + \#F \leq \#V - \#E + \frac{2\#E}{3} = \#V - \frac{\#E}{3}.$$

Di conseguenza:

$$\#E \leq 3\#V - 6$$

Supponiamo per assurdo $deg(v) > 5 \forall v \in V$. Poiché $\sum_{v \in V} deg(v) = 2\#E$, segue $2\#E \geq 6\#V$, cioè $\#E \geq 3\#V$.

Da $3\#V \leq \#E \leq 3\#V - 6$ si arriva all'assurdo.

□

Dalla slide 39 (dimostrazione dalle slide):

Corollario 3. *Se $G = (V, E)$ è un grafo finito, planare e connesso con $\#V < 12$, allora esiste almeno un vertice v tale che $deg(v) \leq 4$.*

Dimostrazione. Supponiamo $deg(v) \geq 5 \forall v \in V$; allora $2\#E \geq 5\#V$, ovvero $\frac{5}{2}\#V \leq E$.

Poiché la planarità di G dà $\#E \leq 3\#V - 6$ (per diretta conseguenza della formula di Eulero, *come dimostrato per il corollario precedente*), segue che

$5\#V \leq 6\#V - 12$, ovvero $\#V \geq 12$

N.B.: La relazione $\#E \leq 3\#V - 6$, valida per tutti i grafi planari, prova immediatamente che K_5 non può essere planare, avendo $\#E = 10$ e $\#V = 5$ □

Dalla slide 41-42 (dimostrazione dalle slide):

Teorema 23. *(Esistenza dello spanning tree) Ogni grafo $G = (V, E)$ finito e connesso ammette albero di copertura.*

Dimostrazione. Si consideri l'insieme

$$\mathcal{C} = \{C / C \text{ sottografo di } G, \text{ connesso e con } V(G) = V(C)\}$$

Siccome $G \in \mathcal{C}$, $\mathcal{C} \neq \emptyset$. Poiché G è finito, $\exists \bar{C} \in \mathcal{C}$ tale che $\#E(\bar{C}) \leq \#E(C), \forall C \in \mathcal{C}$.

Si verifica che $\bar{C}$ è un albero: infatti, se non lo fosse, esisterebbe uno spigolo $e \in E(\bar{C})$ tale che il grafo $(V(\bar{C}), E(\bar{C}) - \{e\})$ sarebbe comunque connesso.

Questo grafo apparterrebbe per definizione ancora a $\mathcal{C}$, ed avrebbe un numero minore di spigoli di $\bar{C}$, che per ipotesi è assurdo.

Resta così provato che $\bar{C}$ è spanning tree. □

Dalla slide 43 (dimostrazione dalle slide):

Teorema 24. *(Caratterizzazione dei grafi bipartiti)*
Condizione necessaria e sufficiente affinché un grafo G sia bipartito è che G sia privo di cicli di lunghezza dispari.

Dimostrazione. Se in G c'è un ciclo di lunghezza dispari, quel ciclo non è bipartito; di conseguenza, G stesso non è bipartito.
Per dimostrare il viceversa, supponiamo, senza perdere di generalità, che G sia connesso e che non ci siano cicli di lunghezza dispari in G. Poiché G è connesso, esiste T albero di copertura. Scelto $r \in V(T)$ *(radice)*, si considerino:

$$V' = \{v \in V / \text{il cammino in } T \text{ da } r \text{ a } v \text{ ha lunghezza pari}\};$$

$$V'' = \{v \in V / \text{il cammino in } T \text{ da } r \text{ a } v \text{ ha lunghezza dispari}\};$$

Rimane da provare che, $\forall e \in E$, i suoi estremi w' e w'' sono tali che $w' \in V'$ e $w'' \in V''$ (o viceversa). Se $e \in E(T)$, è ovvio. Se invece $e \not\in E(T)$, e (insieme agli spigoli di T) chiude un ciclo in G. Ora, se w' e w'' fossero entrambi in V' o entrambi in V'', tale ciclo avrebbe lunghezza dispari, contro l'ipotesi.

□

Dalla slide 48 (dimostrazione dagli appunti):
Teorema 25. *Ogni grafo (finito, connesso) planare è 5-colorabile.*

Dimostrazione. Consideriamo $\#V = n$ e agiamo per induzione su n.
I passi iniziali sono banali (il teorema è ovvio per $n \leq 5$).
Passo induttivo: supponiamo che il teorema valga per i grafi di ordine $n-1$ e lo dimostriamo per grafi di ordine n.
Se $G = (V, E)$ è finito, planare e connesso con $\#V = n$, allora $\exists \bar{v} \in V$ con $deg(\bar{v}) \leq 5$
$G' = (V - \{\bar{v}\}, E - \{(\bar{v}, v_i) / i = 1, ..., s\})$ è grafo finito, planare, con $\#V' = n - 1$. Per ipotesi induttiva, G' è 5-colorabile.
I caso: se i vertici v_1, v_2, v_3, v_4, v_5, che sono i vertici per cui c'è uno spigolo che li collega direttamente a $\bar{v}$ non usno tutti i colori, allora si può colorare G come G', e colorando $\bar{v}$ con un colore diverso da quello dei suoi vicini.
II caso: supp. che, nella colorazione di G', v_1, v_2, v_3, v_4, v_5 (da considerare come ordinati in senso orario o antiorario ai fini del resto della dimostrazione) siano colorati con colori distinti.
Cosnidero il sottografo di G' indotto dai vertici di colori c_1 (colore di v_1) e c_3 (colore di v_3). Ovviamente esso contiene v_1 e v_3.
Chiamiamo $H_{1,3}$ la componente connessa di tale grafo che contiene v_1 e distinguiamo due casi:

- $v_3 \not\in H_{1,3}$, posso scambiare in $H_{1,3}$ le colorazioni con c_1 e c_3. In tal modo, i vertici v_1, v_2, v_3, v_4, v_5 non coinvolgono il colore c_1.
- $v_3 \in H_{1,3}$. Aggiungendo gli spigoli $(\bar{v}, v_1)$ e $(\bar{v}, v_2)$ si otiene un ciclo in G contentente v_1 e v_3. Si forma quindi una curva chiusa $\mathcal{C}$, tale che $v_2 \in Int\mathcal{C}$ e $v_4 \in Ext\mathcal{C}$.

  Per il teorema della curva di Jordan, ogni percorso tra v_2 e v_4 deve intersecare $\mathcal{C}$. Quindi, se indichiamo con $H_{2,4}$ la componente connessa del sottografo indotto dai vertici colorati con i colori c_2 e c_4 che contiene v_2, essa non può contenere v_4, visto che dovrebbe esistere un vertice $\tilde{v} : \tilde{v} \in H_{2,4}$ e $h_{1,3}$, che è assurdo.

  Dunque, visto che $v_4 \in H_{2,4}$, si possono scambiare tutte le colorazioni con c_2 e c_4 in $H_{2,4}$, in modo tale che v_4 sia del colore c_2 e non più c_4, "liberando" quindi c_4 per essere usato per colorare $\bar{v}$.

□

Dalle slide 65 (dimostrazione da slide 66-67 e videolezione 44):

Teorema 26. *(Teorema di Eulero)*

Un grafo $G = (V, E)$ è euleriano se e solo se è connesso con vertici tutti di grado pari.

Dimostrazione. La condizione necessaria è di banale verifica: se il grafo è euleriano vuol dire che, per ogni vertice (che può anche essere ripetuto) c'è uno spigolo entrante ed uno uscente nel ciclo euleriano, ed ogni spigolo nel ciclo deve essere distinto. Essendo il ciclo euleriano, tutti gli spigoli del grafo sono contenuti in esso, e quindi ogni vertice deve avere necessariamente grado pari.

Viceversa, sia G un grafo connesso in cui ogni vertice ha grado pari e sia

$$W = u_0, e_1, u_1, e_2, ..., u_{k-1}, e_k, u_k$$

dove $u_i \in V$ ed $e_i \in E$ una passeggiata in G, in cui nessuno spigolo compare più di una volta (quindi: una passeggiata elementare) di lunghezza massima.

Supponendo per assurdo che $u_k \neq u_0$, per ogni i tale che $u_i = u_k$ (per ogni istanza del vertice u_k in W) si hanno due spigoli (e_i e e_{i+1}) aventi u_k come estremo e contenuti in W, insieme ad e_k, sarebbero un numero dispari di spigoli aventi u_k come estremo.

Dovrebbe esistere, per ipotesi $deg(u_k) \in \mathcal{P}$, un ulteriore spigolo avente u_k come estremo, con cui prolungare W. Questo è impossibile, essendo W la passeggiata elementare di lunghezza massima, segue che $u_0 = u_k$ (quindi l'altro spigolo avente u_k come estremo per raggiungere grado pari è u_0). Ovvero, W è una passeggiata elementare chiusa.

Se dimostriamo che la passeggiata elementare chiusa

$$W = u_0, e_1, u_1, e_2, ..., u_{k-1}, e_k, u_k$$

Contiene tutti gli spigoli, resta provato che è ciclo euleriano in G.

Supponiamo allora, per assurdo, che esista uno spigolo $\bar{e} \in G$, tale che $\bar{e} \notin W$, ma tale da avere (per la connessione di G) uno dei suoi due estremi in W.

Sia $\bar{e} = \{\bar{v}, u_j\}$ un tale spigolo, con $\bar{v} \notin W$ e $u_j \in W$.

È allora possibile costruire la passeggiata

$$W' = \bar{v}, \bar{e}, u_j, e_j, u_{j-1}, e_{j-1}, ..., u_0 = u_k, e_k, u_{k-1}, e_{k-1}, ..., e_{j+1}, u_j$$

che è più lunga di W e in cui nessuno spigolo compare più di una volta. Ciò contraddice la ipotesi iniziale di massimalità di W, e pertanto W deve essere un ciclo euleriano, provando così la tesi. □