Corso di LMM-C. Anno accademico 2005-2006

Note integrative

1. Equivalenze logiche per proposizioni p, q, r (da confrontare con le leggi per l'intersezione, l'unione e il complementare fra insiemi).

   - Leggi di idempotenza: $p \wedge p = p$, $p \vee p = p$
   - Legge della doppia negazione: not (not p)$= p$
   - Leggi commutative: $p \wedge q = q \wedge p$, $p \vee q = q \vee p$
   - Leggi associative: $(p \wedge q) \wedge r = p \wedge (q \wedge r)$, $(p \vee q) \vee r = p \vee (q \vee r)$
   - Leggi distributive: $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$, $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$
   - Leggi di De Morgan: not$(p \wedge q)=$ (not p) $\vee$ (not q), not$(p \vee q)=$(not p)$\wedge$(not q)
   - Leggi di assorbimento: $p \vee (p \wedge q) = p$, $p \wedge (p \vee q) = p$

   Per la dimostrazione si usano le tabelle di verità.

2. Dimostrazione di una relazione fra insiemi.

   Abbiamo visto in classe le leggi per l'intersezione, l'unione e il complementare fra insiemi, e abbiamo osservato che possiamo dimostrare tali leggi a partire dalle equivalenze logiche per proposizioni, ossia usando le tabelle di verità.
   Naturalmente tali leggi si potrebbero dimostrare anche senza scrivere le tabelle di verità. La dimostrazione in sostanza è la stessa, ma può essere esposta in maniera più discorsiva (stiamo quindi facendo un esercizio di linguaggio). Mostriamo con un esempio come si potrebbe procedere:

   Leggi di distributività: dati tre insiemi A, B, C, sottoinsiemi dell'universo Ω, vale che

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

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

   Dimostrazione.
   Scriviamo la dimostrazione della prima delle due leggi, ossia

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

Cominciamo col provare che

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

Per far questo dobbiamo dimostrare che se un elemento x di Ω appartiene a $A \cup (B \cap C)$ allora deve appartenere anche a $(A \cup B) \cap (A \cup C)$. In simboli:

$$x \in A \cup (B \cap C) \Longrightarrow x \in (A \cup B) \cap (A \cup C)$$

.

Infatti se un elemento x appartiene a $A \cup (B \cap C)$ allora vuol dire che $x \in A$ o $x \in B \cap C$. Se $x \in A$ allora $x \in A \cup B$ e $x \in A \cup C$, dunque $x \in (A \cup B) \cap (A \cup C)$ come volevamo dimostrare. Se $x \in B \cap C$ allora, visto che $x \in B$ e $x \in C$ di nuovo vale che $x \in A \cup B$ e $x \in A \cup C$, dunque $x \in (A \cup B) \cap (A \cup C)$.

Resta ora da far vedere che

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

Seguiamo come prima la strategia di mostrare che per un elemento $y \in \Omega$ vale

$$y \in (A \cup B) \cap (A \cup C) \Longrightarrow y \in A \cup (B \cap C)$$

.

Sia dunque $y \in A \cup B$ e $y \in A \cup C$. Perché queste due relazioni siano vere bisogna che $y \in A$ oppure, se ciò non è vero, allora deve essere $y \in B - A$ e $y \in C - A$. Nel primo caso (ossia $y \in A$) segue subito che $y \in A \cup (B \cap C)$ come volevamo dimostrare. Nel secondo caso, $y \in B - A$ e $y \in C - A$ implica che $y \in B$ e $y \in C$ e dunque $y \in B \cap C$, da cui di nuovo segue subito $y \in A \cup (B \cap C)$.

■

Come esercizio, provate a dimostrare in questo modo anche qualche altra legge per l'intersezione, l'unione e il complementare fra insiemi.

3. Il principio di induzione.

Consideriamo la proposizione Q: "per ogni $n \in \mathbb{N}^{>0}$, la somma dei primi n numeri naturali positivi è uguale a $\frac{n(n+1)}{2}$". Per far vedere che è vera, dobbiamo dimostrare che è vera per TUTTI i numeri naturali positivi n, altrimenti è falsa.

Tale proposizione ha al suo interno un numero intero n (in questo caso un numero naturale), ossia la possiamo vedere come la composizione, tramite il connettivo $\wedge$, di tante proposizioni:

$$Q = P(1) \wedge P(2) \wedge P(3) \wedge \cdots\cdots$$

dove $P(3)$ per esempio è: "la somma dei primi 3 numeri naturali è uguale a $\frac{3(3+1)}{2}$". Insomma in generale $P(n)$ è il predicato "la somma dei primi n numeri naturali è uguale a $\frac{n(n+1)}{2}$". Dunque, Q è vera se e solo se sono vere TUTTE le proposizioni $P(1)$, $P(2)$, $P(3)$, $P(4)$.....

In questo paragrafo introduciamo una nuova tecnica di dimostrazione, che si può utilizzare per dimostrare proposizioni tipo la Q, ossia proposizioni che hanno questa struttura: "per ogni intero n maggiore o uguale ad un intero n_0 fissato, vale .....".

Tale tecnica è il principio di induzione. La sua validità è per noi un fatto garantito come assioma, ossia è uno dei principi base su cui si impostano i ragionamenti che faremo nel nostro corso. In effetti il principio di induzione è legato all'esistenza dei numeri naturali, e lo accettiamo perché accettiamo i numeri naturali.

Per semplicità lo enunciamo nel caso che ci servirà per tutti i nostri esercizi e per tutti i nostri esempi, ossia con $n \in \mathbb{N}$ (si potrebbe enunciare con $n \in \mathbb{Z}$).

ASSIOMA. Il principio di induzione.
Supponiamo che $P(n)$ sia un predicato che dipende da un numero naturale $n \in \mathbb{N}$. Se, dato un numero naturale n_0, vale che:

- $P(n_0)$ è vera (*questo si chiama PASSO BASE dell'induzione*);
- per ogni intero $k \geq n_0$, è vera l'implicazione $P(k) \Longrightarrow P(k+1)$ (*questo si chiama PASSO INDUTTIVO e la $P(k)$ si chiama IPOTESI INDUTTIVA*);

allora possiamo concludere che è vera la proposizione Q: "per ogni $n \geq n_0$, $P(n)$ è vera".

Esempio. Applichiamo subito il principio di induzione per dimostrare che Q:"per ogni $n \in \mathbb{N}^{>0}$, la somma dei primi n numeri naturali positivi è uguale a $\frac{n(n+1)}{2}$" è vera.

Il passo base in questo caso consiste nel verificare che $P(1)$ è vera e il passo induttivo consiste nel verificare che per ogni intero $k \geq 1$, è vera l'implicazione $P(k) \Longrightarrow P(k+1)$.

PASSO BASE. Questo non presenta difficoltà perché si verifica subito che P(1): "la somma dei primi 1 numeri naturali è uguale a $\frac{1(1+1)}{2}$" è vera. Infatti "la somma

dei primi 1 numeri naturali" vuol dire che nella nostra somma c'è solo un addendo, il numero 1, e allora dobbiamo solo verificare che $1 = \frac{1(1+1)}{2}$, che è ovviamente vera.

PASSO INDUTTIVO. Sia $k \geq 1$ un intero. Dobbiamo dimostrare che è vera l'implicazione:

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2} \Longrightarrow \sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2}$$

Per far ciò basta dimostrare, che, se assumiamo vera la nostra ipotesi induttiva, ossia $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, allora deve essere vera $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2}$.
Quindi da ora in poi, nella dimostrazione del passo induttivo, siamo in un mondo in cui l'ipotesi induttiva $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ è data per buona: sarà l'arma fondamentale che ci permetterà di dimostrare $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2}$.

Procediamo; scriviamo $\sum_{i=1}^{k+1} i$ spezzando la somma così:

$$\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1)$$

Ma l'ipotesi induttiva ci permette di scrivere, al posto di $\left(\sum_{i=1}^{k} i\right)$, il suo valore $\frac{k(k+1)}{2}$.
Dunque otteniamo

$$\sum_{i=1}^{k+1} i = \frac{k(k+1)}{2} + k + 1$$

che, riorganizzando il secondo membro, è proprio

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

come volevamo.

Riassumendo, abbiamo dimostrato che il passo base e il passo induttivo sono entrambi veri. Il principio di induzione interviene a questo punto e ci permette di concludere che è vera la proposizione Q: "per ogni $n \in \mathbb{N}^{>0}$, la somma dei primi n numeri naturali positivi è uguale a $\frac{n(n+1)}{2}$".

4. Alcuni esercizi sull'induzione.

Problema. Sia $\{u_n\}_{n\in\mathbb{N}}$ la successione così definita:

$$\begin{aligned} u_0 &= 0 \\ u_{k+1} &= 3u_k + 3^k \end{aligned}$$

Dimostrare che $u_k = k3^{k-1}\ \forall\ k \in \mathbb{N}$.

Soluzione. Passo Base: $u_0 = 0 = 0 \cdot 3^{-1}$.

Passo Induttivo: suppongo che, per un $k \geq 0$, sia vero $u_k = k3^{k-1}$ (ipotesi induttiva) e voglio dimostrare $u_{k+1} = (k+1)3^k$. Ma $u_{k+1} = 3u_k + 3^k$ per come è definita la successione. Ora, utilizzando l'ipotesi induttiva posso scrivere che

$$3u_k + 3^k = 3(k3^{k-1}) + 3^k = k3^k + 3^k = (k+1)3^k$$

In conclusione ho trovato $u_{k+1} = (k+1)3^k$ come volevo. Il principio di induzione garantisce allora che $u_k = k3^{k-1}\ \forall\ k \in \mathbb{N}$.

Problema Determinare per quali interi n si ha $n! > 2^n$.

Soluzione.
Verifichiamo subito che la disuguaglianza non è vera per $n = 0, 1, 2$ e 3; mentre è vera per $n = 4$ in quanto $4! = 24 > 16 = 2^4$. Proviamo allora per induzione che il predicato $p(n) : n! > 2^n$ è vero per ogni $n \geq 4$. Il passo base $n = 4$ è stato appena verificato, passiamo quindi a dimostrare il passo induttivo: fissiamo un intero k maggiore o uguale a 4 e proviamo che $p(k) \Rightarrow p(k+1)$.

Infatti $(k+1)! = (k+1)\cdot k! > (k+1)2^k > 2 \cdot 2^k = 2^{k+1}$, dove nella prima disuguaglianza abbiamo usato l'ipotesi induttiva, cioè $p(k)$ è vera, e nella seconda disuguaglianza usiamo $k + 1 > 2$, sicuramente vero per ogni $k \geq 4$ (in realtà basta $k \geq 1$).

Problema Sia $\{(a_n, b_n)\}_{n\geq 0}$ una successione di elementi di $\mathbb{Z} \times \mathbb{Z}$ definita da

$$\begin{cases} (a_0, b_0) = (1, -1), \\ (a_{n+1}, b_{n+1}) = (a_n + b_n, a_n - b_n) \text{ per } n \text{ maggiore o uguale a } 0. \end{cases}$$

Dimostrare che per ogni $n \geq 0$ si ha:

(i) la somma $a_n + b_n$ è un numero pari,

(ii) $(a_{2n}, b_{2n}) = (2^n, -2^n)$,

(iii) $(a_{2n+1}, b_{2n+1}) = (0, 2^{n+1})$.

Soluzione.

(i) Per $n = 0$ abbiamo $a_0 + b_0 = 1 - 1 = 0$ che è un numero pari. Inoltre per ogni intero naturale n abbiamo $a_{n+1} + b_{n+1} = (a_n + b_n) + (a_n - b_n) = 2a_n$; ciò prova che $a_{n+1} + b_{n+1}$ è un numero pari.

(ii) Osserviamo che per $n \geq 1$, usando due volte la definizione induttiva della successione, abbiamo

$$\begin{aligned}(a_{2(n+1)}, b_{2(n+1)}) &= (a_{2n+1} + b_{2n+1}, a_{2n+1} - b_{2n+1}) \\ &= (a_{2n} + b_{2n} + a_{2n} - b_{2n}, a_{2n} + b_{2n} - a_{2n} + b_{2n}) \\ &= (2a_{2n}, 2b_{2n}).\end{aligned}$$

Possiamo ora facilmente dimostrare per induzione che il predicato $p(n) : (a_{2n}, b_{2n}) = (2^n, -2^n)$ è vero per ogni intero naturale $n \geq 0$. Per il passo base abbiamo $(a_0, b_0) = (1, -1) = (2^0, -2^0)$ dalla definizione e quindi $p(0)$ è vera.

Vediamo ora il passo induttivo. Supponiamo quindi vera $p(k)$ e dimostriamo che anche $p(k + 1)$ è vera. Per quanto visto sopra abbiamo $(a_{2(k+1)}, b_{2(k+1)}) = (2a_{2k}, 2b_{2k}) = (2 \cdot 2^k, -2 \cdot 2^k) = (2^{k+1}, -2^{k+1})$. La proposizione $\forall n \geq p(n)$ è quindi provata.

(iii) Usando quanto appena dimostrato nel punto precedente e la definizione induttiva della successione abbiamo: $(a_{2n+1}, b_{2n+1}) = (a_{2n} + b_{2n}, a_{2n} - b_{2n}) = (2^n - 2^n, 2^n + 2^n) = (0, 2^{n+1})$. E quindi quanto richiesto è provato.

5. Forme equivalenti del principio di induzione: il principio del minimo e il principio di induzione forte.

Ci sono altri due modi con cui si può enunciare il principio di induzione: l'assioma del buon ordinamento (detto anche "principio del minimo") e il principio di induzione "forte". Anche se a prima vista non sembrerebbe, si può in realtà dimostrare che il principio di induzione, il principio di induzione forte e l'assioma del buon ordinamento sono EQUIVALENTI: se ne assumiamo per vero uno qualunque, allora grazie a quello possiamo dimostrare gli altri due. Come conseguenza pratica, questo vuol dire che se un esercizio si può risolvere usando uno di questi tre assiomi, allora c'è sicuramente il modo di risolverlo anche usando uno qualunque degli altri due. Con l'esperienza impareremo a scegliere di volta in volta l'assioma più "conveniente", quello che ci aiuta a risolvere l'esercizio nella maniera più elegante o più veloce.

ASSIOMA. Il principio di induzione forte.
Supponiamo che $P(n)$ sia un predicato che dipende da un numero naturale $n \in \mathbb{N}$. Se, dato un numero naturale n_0, vale che:

- $P(n_0)$ è vera (*questo si chiama PASSO BASE dell'induzione*);
- per ogni intero $k \geq n_0$, è vera l'implicazione

$$(P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(k)) \Longrightarrow P(k+1)$$

(*questo si chiama PASSO INDUTTIVO e la* $P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(k)$ *si chiama IPOTESI INDUTTIVA*);

allora possiamo concludere che è vera la proposizione Q: "per ogni $n \geq n_0$, $P(n)$ è vera".

Osserviamo che, in questo caso, il passo base è lo stesso del "normale" principio di induzione, ma il passo induttivo è diverso. Nell'induzione normale, si deve dimostrare che per ogni intero $k \geq n_0$, è vera l'implicazione $P(k) \Longrightarrow P(k+1)$. Questo si traduce nel tentativo di dimostrare $P(k+1)$ assumendo come vera la $P(k)$. Dunque, nel momento in cui dimostriamo la $P(k+1)$, abbiamo un'arma a nostro vantaggio, ossia la $P(k)$.

Nella induzione forte, invece, il passo induttivo chiede di dimostrare che, per ogni intero $k \geq n_0$, è vera l'implicazione

$$(P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(k)) \Longrightarrow P(k+1)$$

Questo si traduce come prima nel tentativo di dimostrare la $P(k+1)$, ma stavolta si possono assumere come vere tutte le proposizioni $P(n_0), P(n_0+1), \ldots, P(k)$; dunque nel momento in cui dimostriamo la $P(k+1)$ siamo più "forti" (ecco perché si chiama induzione "forte"), perché abbiamo a nostro vantaggio molte armi, non solo la $P(k)$, che avevamo anche nell'induzione normale, ma anche le altre proposizioni $P(n_0), P(n_0+1), \ldots, P(k-1)$ (*ricordatevi però che siamo più forti solo apparentemente, perché in realtà l'induzione forte è equivalente all'induzione semplice*).

Esempio. Dimostrare usando l'induzione forte che ogni numero intero ≥ 2 o è primo o si può scrivere come prodotto di numeri primi.

La proposizione che vogliamo provare per induzione forte è Q : "per ogni $n \geq 2$ il numero n o è primo o si può scrivere come prodotto di numeri primi".
Consideriamo dunque il predicato $P(n)$: "il numero n o è primo o si può scrivere come prodotto di numeri primi".

Il passo base, ossia la dimostrazione di $P(2)$, è immediato, perché 2 è appunto un numero primo.
Adesso occupiamoci del passo induttivo. Supponiamo (induzione forte !) che siano vere tutte le proposizioni $P(j)$ con $2 \leq j \leq k$ e cerchiamo di dimostrare che è vera $P(k+1)$, ossia dobbiamo dimostrare che: "il numero $k+1$ o è primo o si può scrivere come prodotto di numeri primi".

Ora si possono verificare due casi: o $k+1$ è primo, e in tal caso la dimostrazione del passo induttivo è già finita, oppure $k+1$ non è primo. In questo secondo caso, allora $k+1$ è composto e si potrà scrivere come prodotto di due numeri a e b, $k+1 = ab$, dove $1 < a < k+1$ e $1 < b < k+1$. Quindi a e b sono tali che le proposizioni $P(a)$ e $P(b)$ risultano vere per ipotesi induttiva, garantendoci che a e b o sono primi o si possono scrivere come prodotto di numeri primi. Di conseguenza $k+1 = ab$ si scrive come prodotto di numeri primi (quelli della decomposizione di a per quelli della decomposizione di $b\ldots$).

Provare a dimostrare questa stessa proposizione usando l'induzione semplice..la dimostrazione è un po' più lunga; in questo caso l'induzione forte è infatti la scelta più adatta.

Nell'introdurre il principio di induzione abbiamo detto che è legato alla esistenza dei numeri naturali. Ecco infatti un altro modo di enunciarlo:

ASSIOMA. Assioma del buon ordinamento (chiamato anche "principio del minimo").
Ogni sottoinsieme NON VUOTO di $\mathbb{N}$ ha un elemento minimo.

Vedremo più avanti in questo corso alcune dimostrazioni in cui conviene applicare l'induzione nella forma data dall'assioma del buon ordinamento. Adesso invece come esercizio (facoltativo, ma raccomandato !) proponiamo:

Esercizio. Dimostrazione che induzione semplice e buon ordinamento sono equivalenti.

Come primo passo dimostriamo l'implicazione:

$$\text{buon ordinamento} \Longrightarrow \text{principio di induzione}$$

Facciamo la dimostrazione per assurdo. Supponiamo dunque che sia vero il principio del buon ordinamento e che sia falso il principio di induzione. Quest'ultimo fatto (per un semplice esercizio di negazione di un enunciato) vuol dire che esiste un predicato $P(n)$ tale che, dato un numero naturale n_0, soddisfa:

- $P(n_0)$ è vera;
- per ogni intero $k \geq n_0$, è vera l'implicazione $P(k) \Longrightarrow P(k+1)$;

ma non è vera la proposizione Q: "per ogni $n \geq n_0$, $P(n)$ è vera".

Allora chiamiamo S il sottoinsieme di $\mathbb{N}$ dato dai numeri $n \geq n_0$ tali che $P(n)$ è falsa. Tale insieme è non vuoto, appunto perché la Q è falsa. Allora S, che è un sottoiniseme di N ed è non vuoto, per il principio del buon ordinamento (che abbiamo preso per VERO), ha un minimo, che noi chiameremo m.

Ora, deve essere $m > n_0$, perché sappiamo che $P(n_0)$ è vera, mentre per costruzione $P(m)$ è falsa. Osserviamo poi che $P(m-1)$ deve essere vera, per la scelta di m, perché altrimenti se $P(m-1)$ fosse falsa m non sarebbe più il minimo intero $\geq n_0$ tale che $P(m)$ è falsa.

Riassumendo, sappiamo che $P(m-1)$ è vera, che $P(m)$ è falsa e che è vera l'implicazione $P(m-1) \implies P(m)$ (questa era una delle proprietà note del predicato $P(n)$). Questo è ASSURDO. La dimostrazione di

$$\text{buon ordinamento} \implies \text{principio di induzione}$$

è dunque terminata. Adesso dimostriamo

$$\text{principio di induzione} \implies \text{buon ordinamento}$$

Procediamo ancora per assurdo. Supponiamo dunque che il principio di induzione sia vero e che il buon ordinamento sia falso. Allora esiste un insieme $G \subseteq \mathbb{N}$, NON VUOTO, che non ha minimo. Costruiamo il predicato $F(n)$: "Nessun numero $\leq n$ appartiene a G". Lo abbiamo costruito apposta in modo tale che, se un numero $m \in G$ allora $F(m)$ è falsa. Quindi se riusciamo a dimostriare che $F(n)$ è invece sempre vera per ogni $n \in \mathbb{N}$, allora G deve essere vuoto, e troviamo un ASSURDO.

Dunque il nostro obiettivo è provare che, dato G non vuoto come sopra, $F(n)$ è sempre vera per ogni $n \in \mathbb{N}$ e, per farlo, possiamo usare il principio di induzione.

PASSO BASE: "F(0) è vera". Questo è vero perché $F(0)$ dice: "0 non appartiene a G", e deve essere vero, altrimenti, se 0 appartenesse a $G \subseteq \mathbb{N}$, G avrebbe un minimo (appunto lo 0) contrariamente a ciò che sappiamo (questa è una mini-dimostrazione per assurdo all'interno della dimostrazione per assurdo che stiamo facendo!).

PASSO INDUTTIVO: "Per ogni $n \geq 0$, vale $F(n) \implies F(n+1)$".
Supponiamo dunque $F(n)$ vera. Se $F(n+1)$ fosse falsa, (anche qui inizia una piccola dimostrazione per assurdo) allora un qualche numero $\leq n+1$ apparterrebbe a G. Ma la verità della $F(n)$ ci garantisce che nessun numero $\leq n$ appartiene a G. Allora dovremmo concludere che $n+1 \in G$ e di conseguenza $n+1$ sarebbe anche il minimo di G. Ma G non ha minimo, dunque abbiamo un assurdo, dunque $F(n+1)$ deve essere vera (fine della piccola dimostrazione per assurdo).

Allora, dato che abbiamo terminato di verificare il passo base e il passo induttivo, il principio di induzione ci garantisce che $F(n)$ è sempre vera per ogni $n \in \mathbb{N}$. ■

Esercizio (facoltativo): provate a dimostrare che

$$\textit{principio di induzione forte} \iff \textit{principio di induzione}$$

6. *Esercizio.* Consideriamo la funzione $g : \mathbb{R} \to \mathbb{R}$ data da

$$g(x) = 9x^2 - 6x + 2$$

Dire se è iniettiva, surgettiva o bigettiva. La stessa domanda per la funzione

$$g' : \mathbb{R}^{\geq 0} \to \{z \in \mathbb{R} \mid z \geq 1\}$$

data dalla stessa legge $g'(x) = 9x^2 - 6x + 2$.

Risposta. Studiamo innanzitutto la surgettività della g, ossia prendiamo un $y \in Imm\ g$ e studiamone le caratteristiche. Deve valere

$$y = 9x^2 - 6x + 2$$

per un qualche $x \in \mathbb{R}$. Si può anche riscrivere

$$y = (3x - 1)^2 + 1$$

da cui si nota subito che deve essere $y \geq 1$ (ossia $Imm\ g \subset \{z \in \mathbb{R} \mid z \geq 1\}$). Dunque la g non è surgettiva, perché ha sempre immagini di valore ≥ 1.

Studiamo la iniettività. Se $y \geq 1$, abbiamo

$$y - 1 = (3x - 1)^2$$

che ha senso perché $y - 1 \geq 0$ e possiamo ricavare

$$3x - 1 = \pm\sqrt{y - 1}$$

$$x = \frac{1 \pm \sqrt{y - 1}}{3}$$

Da questa espressione si ricava che se $y \geq 1$ allora $y \in Imm\ g$ (ossia $Imm\ g = \{z \in \mathbb{R} \mid z \geq 1\}$), perché abbiamo mostrato una formula per ricavare le sue pre-immagini. In particolare si nota che $y = 1$ ha una sola pre-immagine, ossia $\frac{1}{3}$. Se invece $y > 1$ allora ha due preimmagini distinte in $\mathbb{R}$. Dunque la g non è iniettiva.

Consideriamo adesso la g'. Sia y nel codominio di g', dunque $y \geq 1$. Vogliamo controllare se la g' è surgettiva, ossia se troviamo $x \in \mathbb{R}^{\geq 0}$ tale che

$$y = (3x - 1)^2 + 1$$

Provando a risolvere questa equazione si può scrivere, come abbiamo fatto prima,

$$x = \frac{1 \pm \sqrt{y-1}}{3}$$

e, siccome fra le due soluzioni proposte ce ne è sempre una (la $x = \frac{1+\sqrt{y-1}}{3}$) che è ≥ 0 e dunque appartiene al dominio della g', si conclude che la g' è surgettiva.

Quanto alla iniettività, se dimostriamo che, per certi valori di $y > 1$, l'altra soluzione (la $x = \frac{1-\sqrt{y-1}}{3}$, che è distinta dalla prima per $y > 1$) è anch'essa nel dominio, avremo mostrato che la g' non è iniettiva.

Bisogna controllare quando

$$\frac{1 - \sqrt{y-1}}{3} \geq 0$$

e troviamo che questa disuguaglianza è soddisfatta per $y \leq 2$. In conclusione, se scelgo un y tale che $1 < y \leq 2$, tale y ha due pre-immagini secondo la g', che dunque non è iniettiva.

Osservazione. La funzione g ha il grafico dato da una parabola con punto di minimo per $x = \frac{1}{3}$ e valore minimo 1; il grafico permette di "leggere" bene i risultati provati qui sopra.

7. *Teorema.* Sia $f : X \to Y$ una funzione dall'insieme X all'insieme Y. Allora f è invertibile se e solo se è bigettiva. Inoltre, se è invertibile, la sua inversa è unica.

Dimostrazione (fa parte del programma del corso !). Dimostriamo che

$$f \text{ invertibile} \Longrightarrow f \text{ bigettiva}$$

Sia $g = f^{-1}$ l'inversa di f. Dobbiamo dimostrare che f è surgettiva e iniettiva.

Cominciamo col dimostrare che f è surgettiva: se prendiamo un $y \in Y$, dobbiamo trovare un $x \in X$ tale che $f(x) = y$. Proviamo a scegliere $x = g(y)$. Con tale scelta, $f(x) = f(g(y)) = Id_Y(y) = y$ come volevamo.

Ora dimostriamo che la f è iniettiva. Siano $x_1, x_2 \in X$ tali che $f(x_1) = f(x_2)$.

Dobbiamo dimostrare che $x_1 = x_2$. Osserviamo che $f(x_1) = f(x_2)$ implica $g(f(x_1)) = g(f(x_2))$ (abbiamo applicato g ad entrambi i membri), che a sua volta si può riscrivere come $Id_X(x_1) = Id_X(x_2)$ che si può ancora riscrivere come $x_1 = x_2$.

Adesso dimostriamo che

$$f \text{ bigettiva} \Longrightarrow f \text{ invertibile}$$

Dobbiamo costruire l'inversa f^{-1}. Prendiamo allora un $y \in Y$. Chi scegliamo come candidato per $f^{-1}(y)$? Utilizziamo la bigettività della f ricordando che c'è un unico elemento $x_y \in X$ tale che $f(x_y) = y$ e poniamo $f^{-1}(y) = x_y$. In altre parole, per costruzione abbiamo che

$$f(f^{-1}(y)) = f(x_y) = y$$

Questo, vista l' arbitrarietà di $y \in Y$, si può riscrivere dicendo che $f \circ f^{-1} = Id_Y$. Abbiamo dunque ottenuto una delle due relazioni che dobbiamo verificare per sincerarci che f^{-1} così definita è davvero l'inversa di f.

L'altra relazione da verificare è $f^{-1} \circ f = Id_X$. Verifichiamola: sia $x \in X$, allora $f^{-1} \circ f(x) = f^{-1}(f(x)) = x_{f(x)}$ che per costruzione è l'elemento di X tale che $f(x_{f(x)}) = f(x)$. Ma nelle nostre attuali ipotesi f è iniettiva, allora deve essere $x_{f(x)} = x$ cioè $f^{-1}(f(x)) = x$ come volevamo.

Per finire di dimostrare il teorema resta da provare che, quando f è invertibile, f ha un'unica inversa. Supponiamo che g e h siano due funzioni da Y a X, inverse di f. Dobbiamo mostrare che $g = h$, ossia che, $\forall y \in Y$, $h(y) = g(y)$.

Dato $y \in Y$, visto che $f \circ g = Id_Y$ e $f \circ h = Id_Y$, possiamo scrivere

$$f \circ g(y) = y = f \circ h(y)$$

ossia

$$f(g(y)) = y = f(h(y))$$

Ma sappiamo che la f è invertibile, dunque, per la prima parte del teorema, che abbiamo già dimostrato, f è bigettiva, in particolare iniettiva. Allora deve essere $g(y) = h(y)$ come volevamo. ■

8. Esercizio: studio della iniettività e surgettività di una funzione.

Problema

(i) La funzione

$$\begin{array}{rccc} f: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \mapsto & (2x+6y, x+3y) \end{array}$$

è iniettiva, surgettiva, bigettiva?

(ii) Al variare di $a, b \in \mathbb{R}$ la funzione

$$\begin{array}{rccc} f: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \mapsto & (2ax+6by, ax+3by) \end{array}$$

è iniettiva, surgettiva, bigettiva?

Soluzione.

(i) La funzione non è iniettiva, infatti: $f(0,0) = 0$ e $f(3,-1) = (2\cdot 3 + 6\cdot(-1), 3 + 3\cdot(-1)) = (0,0)$. Proviamo ora che l'applicazione non è suriettiva. Osserviamo che abbiamo $f(x,y) = (2(x+3y), x+3y)$, cioè se un elemento $(u,v) \in Immf$ abbiamo $u = 2v$; in conclusione l'applicazione f non è suriettiva perchè ad esempio l'elemento $(1,0)$ non appartiene all'immagine di f. In particolare l'applicazione non è neanche bigettiva.

(ii) Vogliamo ora provare che per ogni $a, b \in \mathbb{R}$ la funzione f non è iniettiva e non è suriettiva. Infatti $f(3b,-a) = (2a\cdot 3b + 6b\cdot(-a), a\cdot 3b + 3b\cdot(-a)) = (0,0) = f(0,0)$, e quindi se la coppia $(a,b) \neq (0,0)$ allora la funzione f non è iniettiva visto che i due elementi distinti $(3b,-a)$ e $(0,0)$ hanno la stessa immagine. Se invece $a = b = 0$ allora abbiamo $f(x,y) = (0,0)$ per ogni $(x,y) \in \mathbb{R}^2$ e quindi f non è certamente iniettiva.

Proviamo ora che f non è suriettiva. Infatti per ogni $(x,y) \in \mathbb{R}^2$ abbiamo $f(x,y) = (2(ax+3by), ax+3by)$; allora per ogni elemento $(u,v) \in Immf$ abbiamo $u = 2v$. Quindi, ad esempio, l'elemento $(1,0)$ non è nell'immagine di f. In particolare l'applicazione f non è bigettiva.

9. Alcuni teoremi su funzioni fra insiemi finiti.

Riportiamo qui alcuni enunciati di cui si è parlato a lezione. Le dimostrazioni sono consigliate come utile esercizio.

Ricordiamo innanzitutto che secondo le nostre definizioni un insieme è finito quando esiste $n \in N$ tale che la cardinalità dell'insieme è uguale a n. Altrimenti l'insieme è infinito.

Cè un solo insieme di cardinalità 0: l'insieme vuoto. Diciamo invece che un insieme X ha cardinalità $n > 1$ se sappiamo che esiste una funzione bigettiva dall'insieme X in questione all'insieme $\mathbb{N}_n$ dei primi n numeri naturali positivi. Abbiamo osservato in classe che questa definizione ha senso, ossia se esibiamo un'altra funzione bigettiva da X a $\mathbb{N}_m$ allora deve essere $m = n$. Questo è una conseguenza del

Lemma dei cassetti Supponiamo di avere una funzione $f : N_n \to \mathbb{N}_m$ con $n > m$. Allora f non è iniettiva.

Tale lemma si dimostra per induzione, come abbiamo visto in classe. Lo possiamo rienunciare in un linguaggio più generale:

Lemma dei cassetti - enunciato "generale" Supponiamo di avere una funzione $f : X \to Y$, dove X è un insieme di cardinalità n e Y è un insieme di cardinalità m, con $n > m$. Allora f non è iniettiva.

Possiamo facilmente ricavare questo corollario (dimostrazione per esercizio !):
Corollario del Lemma dei cassetti Se N oggetti sono sistemati in K scatole, allora c'è almeno una scatola che contiene $\left[\left[\frac{N}{K}\right]\right]$ oggetti (qui $\left[\left[\frac{N}{K}\right]\right]$ è la "parte intera superiore" di $\frac{N}{K}$, ossia il più piccolo numero intero $\geq \frac{N}{K}$).

Ecco qualche altro enunciato che conferma fatti da noi facilmente intuibili. Le dimostrazioni formali sono lasciate come esercizio facoltativo.

Teorema. Supponiamo che X e Y siano insiemi tali che $X \subseteq Y$ e Y sia finito. Allora anche X è finito e $|X| \leq |Y|$.

Teorema. Supponiamo che $f : X \to Y$ sia una funzione fra insiemi finiti e non vuoti tali che $|X| < |Y|$. Allora f non è surgettiva.

Teorema. Supponiamo che X e Y siano insiemi finiti non vuoti della stessa cardinalità. Allora una funzione $f : X \to Y$ è iniettiva se e solo se è surgettiva.
Osservazione. Dunque, in questo caso dove $|X| = |Y|$, per provare che una certa funzione $g : X \to Y$ è bigettiva basta provare una sola fra queste due proprietà: g è iniettiva o g è surgettiva.

Concludiamo con un esercizio, che è una sofisticata applicazione del lemma dei cassetti.

Esercizio. Dimostrare che se mettiamo $n^2 + 1$ numeri reali distinti in una lista ordinata $(a_1, a_2, \ldots, a_{n^2+1})$, da tale lista possiamo estrarre una sottolista di $n + 1$ numeri che risultano o strettamente crescenti o strettamente decrescenti.

Dimostriamolo per assurdo. Supponiamo che l'enunciato non sia vero. Allora, preso un qualunque numero x nella lista, consideriamo tutte le sottoliste crescenti che possiamo

estrarre e che hanno x come primo elemento. Tali sottoliste devono essere composte da al massimo n elementi, altrimenti l'enunciato sarebbe vero. Prendiamo una di queste sottoliste che abbia lunghezza massima possibile e chiamiamo c_x la sua lunghezza, ossia il numero dei suoi elementi. Allo stesso modo, chiamiamo d_x la massima lunghezza di una sottolista strettamente decrescente con primo elemento x. Anche d_x deve essere $\leq n$. Possiamo dunque associare ad ogni elemento x della nostra lista un elemento di $\mathbb{N}_n \times \mathbb{N}_n$, esattamente la coppia (c_x, d_x). Per il lemma dei cassetti, visto che la lista contiene n^2+1 elementi e che la cardinalità di $\mathbb{N}_n \times \mathbb{N}_n$ è n^2, devono esistere due elementi distinti della lista, diciamo a_s e a_t, con $s < t$, a cui viene associata la stessa coppia, ossia tali che $(c_{a_s}, d_{a_s}) = (c_{a_t}, d_{a_t})$. Ora supponiamo che $a_s > a_t$. Allora, poiché a partire da a_t si può estrarre una sottolista di d_{a_t} numeri strettamente decrescenti, questo vuol dire che a partire da a_s si può estrarre una sottolista di almeno $d_{a_t} + 1$ numeri strettamente decrescenti, semplicemente aggiungendo a_s alla sottolista che partiva da a_t. Dunque, per la definizione di d_{a_s}, deve essere $d_{a_s} \geq d_{a_t} + 1$. Questo è ASSURDO visto che a_s e a_t erano tali che tali che $(c_{a_s}, d_{a_s}) = (c_{a_t}, d_{a_t})$, che in particolare implica $d_{a_s} = d_{a_t}$. In modo simile si trova un assurdo se $a_s < a_t$.

10. I coefficienti binomiali.

Dato un insieme X, abbiamo definito a lezione l'insieme delle parti di X, $\mathcal{P}(X)$, come l'insieme i cui elementi sono tutti i sottoinsiemi di X:

$$\mathcal{P}(X) = \{A \mid A \subseteq X\}$$

Nel caso in cui X sia finito di cardinalità n, abbiamo anche calcolato quanti elementi ha $\mathcal{P}(X)$:

Teorema Se X è un insieme finito di cardinalità n, la cardinalità di $\mathcal{P}(X)$ è 2^n.
(Riguardate la dimostrazione per induzione fatta in classe !).

Ma torniamo di nuovo alla situazione generale in cui X è un insieme qualunque, finito o infinito, e costruiamo dei particolari sottoinsiemi di $\mathcal{P}(X)$.

Definizione Dato $r \in \mathbb{N}$, chiamiamo $\mathcal{P}_r(X)$ l'insieme i cui elementi sono tutti i sottoinsiemi di X che hanno cardinalità r:

$$\mathcal{P}_r(X) = \{A \mid A \subseteq X \ \wedge \ |A| = r\}$$

Ora ci poniamo la domanda: se X è finito di cardinalità n, quanti elementi avrà $\mathcal{P}_r(X)$? Certamente $|\mathcal{P}_r(X)|$ sarà un numero naturale $\leq 2^n$, visto che $\mathcal{P}_r(X) \subseteq \mathcal{P}(X)$.

Se vogliamo descriverlo con altre parole, potremmo dire per esempio che $|\mathcal{P}_r(X)|$ è il numero di modi di scegliere r elementi distinti da un insieme che ha n elementi. Questa operazione è cruciale nelle strategie che servono per "contare"; perciò $|\mathcal{P}_r(X)|$ merita un nome e un simbolo:

Definizione Indicheremo $|\mathcal{P}_r(X)|$ con il simbolo $\binom{n}{r}$ (si legge: "coefficiente binomiale n su r").

Possiamo subito osservare alcune proprietà dei coefficienti binomiali:

- $\binom{n}{0} = 1$ per ogni $n \in \mathbb{N}$. Infatti dato un qualunque insieme finito X, questo ha un solo sottoinsieme con 0 elementi, ossia l'insieme vuoto. In particolare vale $\binom{0}{0} = 1$. Similmente si nota che $\binom{n}{n} = 1$ per ogni $n \in \mathbb{N}$.
- se $r > n$ allora $\binom{n}{r} = 0$. Infatti se X ha n elementi, non c'è nessun sottoinsieme di X con $r > n$ elementi.
- $\binom{n}{1} = n$ per ogni $n \in \mathbb{N}$. Infatti se $n = 0$ si ricade nel punto precedente, se invece $n \geq 1$ allora si osserva che, dato X con n elementi, i suoi sottoinsiemi di cardinalità 1 sono solo i "singoletti" del tipo $\{a\}$, al variare di $a \in X$.
- $\binom{n}{n-1} = n$ per ogni $n \in \mathbb{N}^+$. Infatti, per n positivo deve valere $\binom{n}{n-1} = \binom{n}{1}$: dato X con n elementi, i suoi sottoinsiemi di cardinalità 1 sono tanti quanti i sottoinsiemi di cardinalità $n-1$. La corrispondenza biunivoca è data dall'operazione di prendere il complementare.
- Più in generale, dato $0 \leq r \leq n$, vale che $\binom{n}{r} = \binom{n}{n-r}$. Anche questa volta l'operazione di prendere il complementare stabilisce una corrispondenza biunivoca fra i sottoinsiemi di X con r elementi e quelli con $n - r$ elementi.

In classe abbiamo dimostrato alcuni importanti teoremi sui coefficienti binomiali. Il primo è una regola fondamentale che permette di costruirli ricorsivamente.

Teorema. Dati $r, n \in \mathbb{N}^+$ con $1 \leq r \leq n$, vale

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

Dimostrazione. Sia X un insieme con n elementi. Visto che $n \geq 1$, possiamo scegliere un elemento $a \in X$. Per calcolare $\binom{n}{r}$ dobbiamo calcolare la cardinalità di $\mathcal{P}_r(X)$.

Possiamo adesso dividere $\mathcal{P}_r(X)$ in due parti, raggruppando in un sottoinsieme (che chiameremo L_1) tutti i sottoinsiemi di X di cardinalità r che contengono a, e in un altro (che chiameremo L_2) tutti i sottoinsiemi di X di cardinalità r che NON contengono a:

$$\mathcal{P}_r(X) = L_1 \cup L_2$$

Trattandosi di una unione di due insiemi disgiunti, vale che

$$\binom{n}{r} = |\mathcal{P}_r(X)| = |L_1| + |L_2|$$

Ora, un sottoinsieme di cardinalità r che contiene a è univocamente determinato se si dice chi sono gli altri elementi (quelli diversi da a) che contiene; tali elementi costituiscono un sottoinsieme di cardinalità $r-1$ di $X - \{a\}$. Dunque

$$|L_1| = |\mathcal{P}_{r-1}(X - \{a\})| = \binom{n-1}{r-1}$$

Analogamente si osserva che scegliere un sottoinsieme di X di cardinalità r che non contiene a equivale a scegliere un sottoinsieme di $X - \{a\}$ di cardinalità r, dunque

$$|L_2| = |\mathcal{P}_r(X - \{a\})| = \binom{n-1}{r}$$

Allora possiamo concludere che

$$\binom{n}{r} = |\mathcal{P}_r(X)| = |L_1| + |L_2| = \binom{n-1}{r-1} + \binom{n-1}{r}$$

■

Il teorema che abbiamo appena dimostrato è il motivo per cui possiamo disporre i coefficienti binomiali in modo da formare il Triangolo di Pascal-Tartaglia. Dalla terza riga in poi, ogni numero interno al triangolo è infatti la somma dei due numeri che si trovano sopra di lui...

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
\ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots
\end{array}$$

Possiamo anche dare una formula esplicita per $\binom{n}{r}$:

Teorema. Dati $n, r \in \mathbb{N}$, con $0 \leq r \leq n$, vale che

$$\binom{n}{r} = \frac{n\ (n-1)\ (n-2)\ \cdots (n-r+1)}{r!} = \frac{n!}{r!\ (n-r)!}$$

Dimostrazione. Come prima, fissato un insieme X con n elementi, cerchiamo di contare la cardinalità di $\mathcal{P}_r(X)$. Consideriamo $\mathbb{N}_r = \{1, 2, 3, \ldots, r\}$ e una funzione iniettiva

$$f\ :\ \mathbb{N}_r \longrightarrow X$$

Chi è $Imm\ f$? È un sottoinsieme di X di cardinalità r, dunque è un elemento di $\mathcal{P}_r(X)$, proprio uno di quelli che dobbiamo "contare".

Sarà vero che ogni elemento di $\mathcal{P}_r(X)$ lo posso esprimere come immagine di una funzione iniettiva da N_r a X ? Sì, preso infatti un elemento di $\mathcal{P}_r(X)$, cioè un sottoinsieme $\{a_1, a_2, \ldots, a_r\} \subseteq X$, posso facilmente indicare una funzione iniettiva da N_r a X la cui immagine sia proprio $\{a_1, a_2, \ldots, a_r\}$: per esempio posso prendere la $g\ :\ \mathbb{N}_r \longrightarrow X$ definita da $g(1) = a_1, g(2) = a_2, \ldots, g(r) = a_r$.

Insomma, con le funzioni iniettive da $\mathbb{N}_r$ a X "raggiungiamo" tutti gli elementi di $\mathcal{P}_r(X)$. Per trovare $|\mathcal{P}_r(X)|$ potremmo allora cominciare a contare $|Inj\ (\mathbb{N}_r \to X)|$, ossia quante sono le funzioni iniettive da $\mathbb{N}_r$ a X. Ma questo numero lo abbiamo già calcolato in classe in una lezione precedente: è $n\ (n-1)\ (n-2)\ \cdots (n-r+1)$.

È vero allora che $|\mathcal{P}_r(X)| = n\ (n-1)\ (n-2)\ \cdots (n-r+1)$? NO, perché se scriviamo così commettiamo l'errore di contare ogni elemento di $\mathcal{P}_r(X)$ più volte. Precisamente, dato un sottoinsieme $\{a_1, a_2, \ldots, a_r\} \subseteq X$ lo stiamo contando $|Inj\ (\mathbb{N}_r \to \{a_1, a_2, \ldots, a_r\})|$ volte, cioè tante volte quante sono le diverse funzioni iniettive possibili da $\mathbb{N}_r$ a $\{a_1, a_2, \ldots, a_r\}$. Ma sappiamo quanto vale $|Inj\ (\mathbb{N}_r \to \{a_1, a_2, \ldots, a_r\})|$: applicando la formula per il conto delle funzioni iniettive a questo caso particolare in cui dominio e codominio hanno la stessa cardinalità r (dunque stiamo in realtà considerando le funzioni bigettive), troviamo che $|Inj\ (\mathbb{N}_r \to \{a_1, a_2, \ldots, a_r\})| = |Bij\ (\mathbb{N}_r \to \{a_1, a_2, \ldots, a_r\})| = r!$.

Allora, visto che col numero $n\ (n-1)\ (n-2)\ \cdots (n-r+1)$ abbiamo contato $r!$ volte ogni elemento di $\mathcal{P}_r(X)$, per avere$|\mathcal{P}_r(X)|$ basterà dividerlo per $r!$:

$$\binom{n}{r} = |\mathcal{P}_r(X)| = \frac{n\ (n-1)\ (n-2)\ \cdots (n-r+1)}{r!}$$

■

Vediamo adesso perché i numeri $\binom{n}{r}$ si chiamano "coefficienti binomiali". Date due variabili a e b, consideriamo il binomio $(a+b)$ e le sue prime potenze:

$$(a+b)^0 = 1$$

$$(a+b)^1 = a+b$$

$$(a+b)^2 = a^2 + 2ab + b^2$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Come possiamo notare, i coefficienti che compaiono in questi sviluppi sono, riga per riga, gli elementi delle prime righe del Triangolo di Pascal -Tartaglia: 1, 1-1, 1-2-1, 1-3-3-1.

Questa osservazione vale in generale: i coefficienti dello sviluppo del binomio $(a+b)^n$ sono proprio i "coefficienti binomiali" $\binom{n}{r}$, come risulta dal seguente:

Teorema del binomio di Newton. Date due variabili a e b, per ogni $n \in \mathbb{N}$ vale:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

cioè

$$(a+b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1}b^1 + \binom{n}{2} a^{n-2}b^2 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + \binom{n}{n} b^n$$

Schema della dimostrazione. Cominciamo da un esempio, per avere un'idea di come funziona la dimostrazione. Calcoliamo lo sviluppo di $(a+b)^3$. Se non raggruppiamo i termini troviamo:

$$(a+b)^3 = (a+b)(a+b)(a+b) = a(a+b)(a+b) + b(a+b)(a+b) =$$

$$= aa(a+b)+ab(a+b)+ba(a+b)+bb(a+b) = aaa+aab+aba+abb+baa+bab+bba+bbb$$

Abbiamo espresso $(a+b)^3$ come somma di 8 monomi, ognuno dei quali è stato ottenuto, tramite le proprietà distributiva e associativa, scegliendo o a o b da ogni parentesi che compare in $(a+b)(a+b)(a+b)$.

Quindi, raggruppando adesso i termini tramite la propietà commutativa, quale sarà il coefficiente di a^2b? Sarà uguale al numero dei monomi in cui troviamo due a e una b. E questi quanti sono ? Sono $3 = \binom{3}{2}$, ossia sono tanti quanti sono i modi di scegliere due parentesi fra le tre del prodotto $(a+b)(a+b)(a+b)$ (queste saranno le parentesi da cui prendo la a): la prima e la seconda, la prima e la terza, la seconda e la terza. Dunque nello sviluppo avremo $3a^2b$. Ovviamente, saremmo arrivati allo stesso risultato contando i modi di scegliere una parentesi fra le tre del prodotto $(a+b)(a+b)(a+b)$ (quella da cui prendo la b), perché $\binom{3}{1} = \binom{3}{2} = 3$.

Passiamo al caso generale. Nello sviluppo di $(a+b)^n$ produrremo 2^n monomi, ciascuno ottenuto scegliendo o a o b da ognuna delle n parentesi del prodotto

$$(a+b)^n = (a+b)(a+b)(a+b)\cdots(a+b)(a+b)$$

Raggruppando i termini, preso un indice i con $0 \leq i \leq n$, quale sarà allora il coefficiente di $a^{n-i}b^i$? Sarà uguale al numero di modi con cui si possono scegliere i parentesi fra le n del prodotto $(a+b)(a+b)(a+b)\cdots(a+b)(a+b)$ (quelle da cui prendiamo la b); dunque sarà uguale a $\binom{n}{i}$. Oppure sarà uguale al numero di modi con cui si possono scegliere $n-i$ parentesi fra le n del prodotto $(a+b)(a+b)(a+b)\cdots(a+b)(a+b)$ (quelle da cui prendiamo la a): infatti come sappiamo $\binom{n}{i} = \binom{n}{n-i}$. In conclusione, nello sviluppo di $(a+b)^n$ troveremo il termine $\binom{n}{i}a^{n-i}b^i$. Siccome questo è vero per ogni i, con $0 \leq i \leq n$, abbiamo dimostrato il teorema.

■

Esercizio. Dimostrare che per ogni $n \in \mathbb{N}$ vale $\sum_{i=0}^{n}\binom{n}{i} = 2^n$ (in base a quanto abbiamo visto nel corso, ci sono varie dimostrazioni possibili..).

Esercizio. Dimostrare che per ogni $n \in \mathbb{N}$ vale $\sum_{i=0}^{n}(-1)^i\binom{n}{i} = 0$.

11. *Esercizio.* Supposto che le regole del poker a 52 carte (poker USA versione standard) siano note, determinare il numero di mani servite per

    (a) una qualunque configurazione (il numero delle mani servite possibili).

    (b) Scala reale massima.

    (c) Scala reale.

    (d) Colore.

    (e) Scala.

    (f) Nessun punto.

    (g) Poker.

    (h) Full.

    (i) Tris.

    (j) Doppia coppia.

    (k) Una coppia.

    Soluzione.

    (a) Devo scegliere 5 carte su 52, senza ripetizioni, nessuna restrizione. Il numero che cerco è quindi il numero di sottoinsiemi di 5 elementi di un insieme di 52 elementi, quindi $\binom{52}{5}$.

(b) Per una scala reale massima le carte devono essere dello stesso seme, in scala e finire con un asso. Cè quindi una scala reale massima per ogni seme, quindi ce ne sono in totale 4.

(c) Per una scala reale, le carte devono essere tutte e 5 dello stesso seme, e la più grande può essere $5, 6, \ldots, A$, quindi ce ne sono 10 per seme. Per 4 semi, 40. Si ricorda che la scala reale minima ($A, 2, 3, 4, 5$ dello stesso seme) batte la massima.

(d) Per avere un colore, le 5 carte devono essere tutte dello stesso seme. Ne dobbiamo scegliere quindi 5 su 13, cioè $\binom{13}{5}$. Dato che ci sono 4 semi il numero di colori è $\binom{13}{5} * 4$. Il numero dei colori che non sono una scala reale è $\binom{13}{5} * 4 - 40$.

(e) Ci sono 10 sequenze di valori possibili per una scala. Dato che non abbiamo restrizioni sul seme da scegliere, il totale delle scale è $10 * \binom{4}{1}^5$. Il numero delle scale non reali è $10 * \binom{4}{1}^5 - 40$.

(f) Per non avere nessun punto, devo non avere nessun valore uguale e devo poi sottrarre al numero ottenuto il numero delle scale reali, delle scale e dei colori. Il numero di mani senza un valore ripetuto è $\binom{13}{5} * \binom{4}{1}^5$. Infatti devo scegliere 5 valori su 13 e per ciascuno un seme su quattro.

(g) Poker: scelgo un valore su tredici $\binom{13}{1}$, quattro carte su quattro per quel valore $\binom{4}{4}$ e mi rimane una carta da scegliere su quarantotto $\binom{48}{1}$. Il numero totale è quindi $\binom{13}{1} * \binom{4}{4} * \binom{48}{1}$.

(h) Full: scelgo il primo valore, quello per il tris, in $\binom{13}{1}$ modi; posso scegliere le tre carte del tris in $\binom{4}{3}$ modi diversi. Scelgo il valore per la coppia, (uno sui dodici rimanenti) $\binom{12}{1}$. Posso scegliere le due carte della coppia in $\binom{4}{2}$ modi diversi. Il numero totale è quindi $\binom{13}{1} * \binom{4}{3} * \binom{12}{1} * \binom{4}{2}$.

(i) Tris: scelgo un valore su tredici $\binom{13}{1}$; posso scegliere queste tre carte su quattro in $\binom{4}{3}$ modi diversi. Per le restanti due carte, devo avere: nessuna coppia, su le 48 carte rimanenti (48 e non 49 perchè voglio evitare di contre anche i poker che potrebbero essere generati da un tris). Devo quindi scegliere due valori su dodici $\binom{12}{2}$ senza restrizioni sul seme $\binom{4}{1}^2$. Il totale è $\binom{13}{1} * \binom{4}{3} * \binom{12}{2} * \binom{4}{1}^2$.

(j) Doppia coppia: scelgo il valore delle coppie $\binom{13}{2}$; posso scegliere le due carte in $\binom{4}{2}$ modi diversi per la prima coppia e similarmente per la seconda. Scelgo il valore della carta rimanente $\binom{11}{1}$; posso scegliere questa carta in $\binom{4}{1}$ modi diversi. Il totale è quindi $\binom{13}{2} * \binom{4}{2}^2 * \binom{11}{1} * \binom{4}{1}$.

(k) Coppia: Scelgo il valore della coppia $\binom{13}{1}$; posso scegliere le due carte in $\binom{4}{2}$ modi diversi. Per le restanti tre carte, scelgo tre valori distinti $\binom{12}{3}$. Non ho restrizioni sul seme di queste tre carte, quindi il fattore è $\binom{4}{1}^3$. Il totale è quindi $\binom{13}{1} * \binom{4}{2} * \binom{12}{3} * \binom{4}{1}^3$.

Osservazioni. 1) Un altro modo di calcolare il numero di mani che mi dà un tris è: in un tris ci devono essere tre valori distinti, che posso quindi scegliere in $\binom{13}{3}$ modi

diversi. Posso scegliere le carte del tris in $\binom{4}{3}$ modi diversi, e le due carte rimanenti in $\binom{4}{1}$ modi ciascuna. Devo ancora considerare che devo scegliere quale dei tre valori scelti sia quello del tris, e questo posso farlo in 3 modi diversi. Il numero totale sarebbe quindi $\binom{13}{3} * \binom{4}{3} * \binom{4}{1}^2 * 3$.
2) Notiamo che le mani con un full sono 3744 mentre quelle con un colore sono 5108, in concordanza col fatto che nel poker americano il full batte il colore.

12. Un esercizio sui gelati.

Esercizio. Un gelataio ha 20 gusti di gelato, 12 alla frutta e 8 non di frutta.
a) In quanti modi si può fare un cono con 4 gusti ?
b) In quanti modi si può fare un cono con 4 gusti, di cui almeno due di frutta ?
c) In quanti modi si può fare un cono con 4 gusti, di cui almeno due di frutta, ma in cui non si trovano insieme il limone e il fiordilatte ?

Risposta.

a) In $\binom{20}{4}$ modi, si tratta infatti di scegliere 4 elementi in un insieme di 20.

b) Qui bisogna stare attenti, conviene contare il complementare: infatti se dai $\binom{20}{4}$ coni possibili togliamo gli $\binom{8}{4}$ coni senza frutta e i $12\binom{8}{3}$ coni in cui c'è esattamente un solo gusto di frutta, quelli che restano sono i coni con almeno due gusti di frutta, ossia proprio quelli che ci interessano. Dunque la risposta è $\binom{20}{4} - \binom{8}{4} - 12\binom{8}{3}$.

c) Anche qui conviene contare il complementare: se dai $\binom{20}{4} - \binom{8}{4} - 12\binom{8}{3}$ coni con almeno due gusti di frutta si levano quelli che hanno fiordilatte e limone insieme, i coni che restano sono proprio quelli che ci interessano. Quanti sono i coni con almeno due gusti di frutta che hanno fiordilatte e limone insieme? Visto che fiordilatte e limone ci sono, restano da decidere due palline. Se sono entrambe di frutta, si possono scegliere in $\binom{11}{2}$ modi. Se sono una di frutta (11 possibilità) e una non di frutta (7 possibilità), si possono scegliere in $11 \cdot 7$ modi. Ricordiamo che non contempliamo il caso in cui sono entrambe non di frutta perché vogliamo che nel nostro cono ci siano almeno due gusti di frutta. Dunque la risposta è $\binom{20}{4} - \binom{8}{4} - 12\binom{8}{3} - \binom{11}{2} - 11 \cdot 7$.

13. Un esercizio sulle estrazioni.

Problema. In una scatola vi sono 30 palline numerate da 1 a 30. Le palline da 1 a 10 sono colorate di rosso, le palline da 11 a 20 sono colorate di verde e le palline da 21 a 30 sono colorate di giallo. In quanti modi diversi si possono estrarre:

(i) 3 palline di diverso colore,

(ii) 3 palline dello stesso colore,

(iii) 3 palline di al più 2 colori.

N.B.: consideriamo come diversi due gruppi di palline con stessi colori ma diversi numeri.

Soluzione.

(i) Estrarre 3 palline di diverso colore significa estrarre una pallina rossa, una pallina verde ed una pallina gialla. Visto che le scelte sono indipendenti e che vi sono 10 palline per ogni colore, abbiamo

$$10^3$$

scelte possibili.

(ii) Abbiamo 3 modi di scegliere il colore e, una volta fissato il colore, basta estrarre 3 pallina da un gruppo di 10 palline del colore fissato. Quindi il numero totale di scelte totale possibili è

$$3\begin{pmatrix} 10 \\ 3 \end{pmatrix}.$$

(iii) Scegliere 3 palline di al più 2 colori è equivalente ad escludere le scelte con 3 palline di colore diverso. Allora visto che tutte le possibili estrazioni sono $\begin{pmatrix} 30 \\ 3 \end{pmatrix}$ abbiamo che le scelte cercate sono

$$\begin{pmatrix} 30 \\ 3 \end{pmatrix} - 3\begin{pmatrix} 10 \\ 3 \end{pmatrix}$$

per quanto visto sopra.

14. Il principio di Inclusione-Esclusione.
L'enunciato fa parte del programma del corso, la dimostrazione è facoltativa e, ovviamente, consigliata !

Teorema. Consideriamo un intero $n \geq 1$ e siano $A_1, A_2, \ldots, A_n$ insiemi finiti. Dato un sottoinsieme $I = \{i_1, i_2, \ldots, i_r\}$ di $\mathbb{N}_n$ poniamo

$$A_I = \bigcap_{i \in I} A_i = A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}$$

Allora

$$|\bigcup_{i=1}^{n} A_i| = \sum_{\emptyset \neq I \subseteq \mathbb{N}_n} (-1)^{|I|-1} |A_I|$$

(si noti che l'indice I nella formula varia fra tutti i sottoinsiemi di $\mathbb{N}_n$ escluso l'insieme vuoto)

Dimostrazione. La nostra strategia sarà quella di dimostrare che il membro di sinistra e quello di destra forniscono lo stesso numero, ossia la cardinalità di $\bigcup_{i=1}^{n} A_i$.

Mostreremo cioè che ogni elemento $x \in \bigcup_{i=1}^{n} A_i$ è contato esattamente una volta nel membro di sinistra e in quello di destra della formula. Visto che questo è ovvio per il membro di sinistra, studiamo il membro di destra.

Preso dunque un $x \in \bigcup_{i=1}^{n} A_i$, questo apparterrà ad alcuni degli A_i, diciamo che appartenga esattamente a r di essi: $A_{i_1}, A_{i_2}, \cdots, A_{i_r}$.

Allora x nel membro di destra viene contato esattamente con questo coefficiente:

$$r - \binom{r}{2} + \binom{r}{3} - \binom{r}{4} + \cdots + (-1)^{r-1} \binom{r}{r}$$

Infatti nel membro di destra vengono conteggiati col segno più gli elementi di tutti gli r insiemi $A_{i_1}, A_{i_2}, \cdots, A_{i_r}$, col segno meno gli elementi di tutte le loro $\binom{r}{2}$ intersezioni a due a due, col segno più gli elementi di tutte le loro $\binom{r}{3}$ intersezioni a 3 a 3 e così via... (*Ovviamente se si vuole si può formalizzare questo "e così via" con una induzione..*).

Ma noi sappiamo che

$$0 = (1-1)^n = \binom{r}{0} - \binom{r}{1} + \binom{r}{2} - \binom{r}{3} + \cdots + (-1)^r \binom{r}{r}$$

da cui, visto che $\binom{r}{0} = 1$ e $\binom{r}{1} = r$,

$$1 = r - \binom{r}{2} + \binom{r}{3} - \binom{r}{4} + \cdots + (-1)^{r-1} \binom{r}{r}$$

Questo permette di concludere che (indipendentemente da quale sia r) il coefficiente con cui viene contato x nel membro di destra è 1, come volevamo.

■

Esercizio (*facoltativo*). Trovare una formula per contare quante sono le permutazioni di un insieme di n elementi che non lasciano fisso neppure un elemento.

15. Qualche appunto sugli insiemi di cardinalità infinita.

Ripercorriamo e integriamo la lezione fatta in classe. Per prima cosa abbiamo discusso la seguente:
Definizione. Diciamo che due insiemi X e Y hanno la stessa cardinalità ($|X| = |Y|$), o che sono equipotenti, se esiste una funzione bigettiva $f : X \to Y$. Se esiste una funzione iniettiva da X a Y si dice che X ha cardinalità minore o uguale a quella di Y e si scrive $|X| \leq |Y|$. Scriviamo $|X| < |Y|$ (e diciamo che X ha cardinalità strettamente minore di quella Y) quando vale $|X| \leq |Y|$ e X e Y non sono equipotenti.

I primi insiemi infiniti che abbiamo preso in considerazione sono gli insiemi "infiniti numerabili", ossia gli insiemi equipotenti all'insieme dei numeri naturali $\mathbb{N}$. Abbiamo dimostrato che:

Teorema. Se X è un insieme infinito numerabile e Y è un insieme finito o infinito numerabile, allora $X \cup Y$ è un insieme infinito numerabile.

Il "primo procedimento diagonale di Cantor" ci ha permesso di dimostrare che:

Teorema. Il prodotto cartesiano di due insiemi infiniti numerabili è infinito numerabile.

Abbiamo cercato poi esempi di insiemi numerabili; abbiamo osservato che $|\mathbb{N}| = |\mathbb{Z}|$ e che:

Teorema. I numeri razionali sono equipotenti ai numeri naturali: $|\mathbb{N}| = |\mathbb{Q}|$.
La dimostrazione, svolta in classe, utilizza il teorema precedente sul prodotto cartesiano di due insiemi infiniti numerabili e il fatto che se A è un sottoinsieme infinito di un insieme infinito numerabile allora A è infinito numerabile.

I numeri reali invece non sono numerabili:

Teorema. I numeri reali hanno cardinalità strettamente maggiore di quella dei numeri naturali: $|\mathbb{N}| < |\mathbb{R}|$.
La dimostrazione che abbiamo mostrato in classe utilizza la scrittura decimale dei numeri reali e il "secondo procedimento diagonale" di Cantor.

Per mostrare che esistono anche cardinalità maggiori di quella del continuo, ossia di quella di $\mathbb{R}$, abbiamo enunciato a lezione il seguente teorema di cui in queste note diamo la dimostrazione (facoltativa, consigliata !).

Teorema. Per ogni insieme, finito o infinito, X, vale che

$$|X| < |\mathcal{P}(X)|$$

Nota: ricordiamo che $\mathcal{P}(X)$ indica l'insieme delle parti di X. In particolare per $\mathbb{R}$ vale $|\mathbb{R}| < |\mathcal{P}(\mathbb{R})|$.

Dimostrazione Il caso dell'insieme vuoto è banale: $|\emptyset| = 0 < |\mathcal{P}(\emptyset)| = |\{\emptyset\}| = 1$.

Sia dunque X non vuoto. Bisogna innanzitutto costruire una funzione iniettiva da X a $\mathcal{P}(X)$, in modo da poter dire che $|X| \leq |\mathcal{P}(X)|$. Poi concluderemo dimostrando che non può esistere una funzione surgettiva - dunque in particolare bigettiva - da X a $\mathcal{P}(X)$.

Una funzione iniettiva da X a $\mathcal{P}(X)$ è per esempio quella che manda ogni $x \in X$ in $\{x\} \in \mathcal{P}(X)$ ossia ogni elemento x nel suo "singoletto".

Supponiamo ora di avere una funzione $f : X \to \mathcal{P}(X)$. Qualunque sia f, esibiremo un elemento di $\mathcal{P}(X)$, ossia un sottoinsieme di X, che non è nell'immagine di f. Dunque f non è surgettiva e, vista la arbitrarietà di f, questo vuol dire che non possono esistere funzioni surgettive da X a $\mathcal{P}(X)$, in particolare neppure funzioni bigettive.

Ecco il sottoinsieme "cattivo":

$$A = \{x \in X \mid x \notin f(x)\}$$

Leggiamo bene chi è A; A è il sottoinsieme di X i cui elementi sono tutti quegli $x \in X$ che hanno la seguente proprietà: $x \notin f(x)$ (ricordiamo che $f(x)$ è un elemento di $\mathcal{P}(X)$ e dunque è a sua volta un sottoinsieme di X, per cui ha senso chiedersi se $x \in f(x)$ o $x \notin f(x)$).

Come dicevamo prima, dobbiamo mostrare che questo A non appartiene a $Imm\ f$ e dunque f non è surgettiva. Supponiamo (dimostrazione per assurdo) che $A \in Imm\ f$, ossia che esista $a \in X$ tale che $f(a) = A$. Mostriamo che questo conduce ad un assurdo. Basta considerare a (ricordiamo che appartiene a X) e A (ricordiamo che è un sottoinsieme di X), e chiedersi se $a \in A$ o $a \notin A$ e scoprire che nessuno dei due casi può accadere.

Infatti se $a \in A$ allora, vista la definizione di A, a è uno di quegli elementi x tali che $x \notin f(x)$. Ossia per a accade che $a \notin f(a)$. Ma $f(a) = A$ e dunque accade che $a \notin A$. Assurdo !

Se invece $a \notin A$ allora, vista la definizione di A, a non è uno di quegli elementi x tali che $x \notin f(x)$. Ossia per a accade che $a \in f(a)$ cioè $a \in A$. Assurdo!

■

Dunque possiamo costruire una lista di insiemi infiniti con cardinalità strettamente crescenti:

$$|\mathbb{N}| < |\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < \cdots$$

A questo punto nascono alcune domande: esistono infiniti "più piccoli" del numerabile, insoma tali da poter essere messi prima di $\mathbb{N}$ in questa lista ? Cosa si può dire di $|\mathcal{P}(\mathbb{N})|$: lo possiamo aggiungere come un nuovo elemento della lista ? Questi nella lista sono tutti gli infiniti possibili ? Cerchiamo intanto di rispondere alle prime due. Cominciamo con un esercizio.

Esercizio. Dimostrare che, dato un insieme infinito X, si può sempre trovare un suo sottoinsieme infinito numerabile.
(idea iniziale: cominciamo con lo scegliere un elemento $x_1 \in X$. Allora $X - \{x_1\}$ è ancora infinito. Scegliamo dunque un elemento x_2 in $X - \{x_1\}$..... Dunque per induzione sappiamo che, per ogni numero $n \in \mathbb{N}$ possiamo costruire un sottoinsieme di X di cardinalità n. Se ammettiamo di saper scegliere un elemento da ciascuno di questi sottoinsiemi possiamo costruire il nostro insieme infinito numerabile.. (ATTENZIONE! Saper fare questa scelta sembra molto naturale, e infatti noi la ammettiamo, ma in realtà si tratta di un fatto collegato all'"assioma della scelta", di cui in questo corso non parleremo).

Questo esercizio ci permette dunque di concludere che se X è un insieme infinito allora $|\mathbb{N}| \leq |X|$. Abbiamo risposto alla prima domanda: non esistono infiniti "più piccoli" del numerabile !

Esercizio. Dimostrare che se un insieme infinito X è in corrispondenza biunivoca con un insieme Y, e se Z è un insieme finito o numerabile, allora anche $X \cup Z$ è in corrispondenza biunivoca con Y.
(idea: supponiamo per esempio che Z sia infinito numerabile e sia $f : X \to Y$ la corrispondenza biunivoca fra X e Y. Estraiamo da X un insieme infinito numerabile N (esercizio precedente..): allora $f(N)$ è un sottoinsieme infinito numerabile di Y e $X - N$ è equipotente a $Y - f(N)$. Per dimostrare dunque che $X \cup Z$ è equipotente a Y resta da verificare che $N \cup Z$ è equipotente a $f(N)$. Ma $N \cup Z$ è unione di infiniti numerabili, dunque è infinito numerabile, e $f(N)$ è infinito numerabile..)

In altre parole possiamo dire che la cardinalità di un insieme infinito non cambia se lo uniamo a un insieme finito o numerabile. Questo implica subito (facile esercizio!) che la cardinalità di un insieme infinito non cambia se gli sottraiamo un insieme finito (attenzione invece quando si sottrae un insieme numerabile da un insieme numerabile: se per esempio a $\mathbb{N}$ sottraggo $\mathbb{N}$ stesso, o $\mathbb{N} - \{1\}$....). Possiamo ora rispondere alla seconda domanda:

Teorema. L' insieme delle parti di $\mathbb{N}$ ha la cardinalità del continuo:

$$|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$$

Dimostrazione (facoltativa, consigliata !). Per prima cosa si osserva che $|\mathbb{R}| = |(0,1)|$: una funzione bigettiva fra questi due insiemi è, per esempio, $g : (0,1) \to \mathbb{R}$, con $g(x) = \tan[\pi(x - \frac{1}{2})]$, la cui inversa $g^{-1} : \mathbb{R} \to (0,1)$ è data da $g^{-1}(x) = (\frac{1}{\pi} \arctan x) + \frac{1}{2}$.

Dobbiamo dunque dimostrare che $|\mathcal{P}(\mathbb{N})| = |(0,1)|$. Per l'esercizio precedente sappiamo che $|\mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{N}) - \{\mathbb{N}\}|$ (la cardinalità non cambia se togliamo un elemento), dunque possiamo ridurci a dimostrare che $|\mathcal{P}(\mathbb{N}) - \{\mathbb{N}\}| = |(0,1)|$.
Scriviamo i numeri reali in $(0,1)$ in base binaria. Avremo dunque delle espressioni di questo tipo:

$$0,00110101110011100000 10\ldots$$

Per essere sicuri di rappresentare in modo unico ogni elemento di $(0,1)$ ci mettiamo d'accordo di non accettare code infinite di 1.

Ora costruiamo una mappa $h : \mathcal{P}(\mathbb{N}) - \{\mathbb{N}\} \longrightarrow (0,1)$ che risulterà essere bigettiva. L'idea di base sarebbe questa: dato un sottoinsieme $A \subsetneq \mathbb{N}$, vorremmo porre

$$h(A) = 0, a_0 a_1 a_2 \cdots$$

dove $a_i = 0$ se $i \notin A$ e $a_i = 1$ se $i \in A$. Siamo vicini ad una buona definizione, ma bisogna aggiustare qualcosa. Infatti se A contenesse tutti i numeri da un certo numero fissato M in poi, ossia se $\mathbb{N} - A$ fosse finito, allora $h(A)$ risulterebbe un numero scritto con una coda infinita di 1. Dovremmo riscriverlo nella forma da noi accettata, ossia trasformando tutti gli 1 della coda in 0 e facendo diventare 1 l'ultimo 0 che appariva nella vecchia scrittura di $h(A)$. Esisterebbe allora un insieme finito $B \subseteq \mathbb{N}$ tale che $h(A) = h(B)$, insomma h non sarebbe iniettiva. Come si può rimediare ? Bisogna trattare separatamente gli insiemi $A \subsetneq \mathbb{N}$ che sono finiti, quelli che sono infiniti ma hanno complementare finito e quelli che sono infiniti e hanno complementare infinito. Scriviamo allora

$$\mathcal{P}(\mathbb{N}) - \{\mathbb{N}\} = F \cup I_1 \cup I_2$$

dove

$$F = \{A \subsetneq \mathbb{N} \mid A \text{ è finito}\}$$

$$I_1 = \{A \subsetneq \mathbb{N} \mid A \text{ è infinito } e\, \mathbb{N} - A \text{ è finito non vuoto }\}$$

$$I_2 = \{A \subsetneq \mathbb{N} \mid A \text{ è infinito } e\, \mathbb{N} - A \text{ è infinito}\}$$

e dunque l'unione è disgiunta.
Ora definiamo la h "giusta". Se $A \in F$ poniamo

$$h(A) = h(A) = 0, 1 a_0 a_1 a_2 \ldots$$

dove la prima cifra dopo la virgola è 1 e poi, per ogni i, $a_i = 0$ se $i \notin A$ e $a_i = 1$ se $i \in A$. Osserviamo in particolare che, se $A = \emptyset$, allora $h(A) = 0, 1$.

Se invece $C \in I_1$ innanzitutto chiamiamo M l'elemento più grande di $\mathbb{N}$ che non appartiene ad C (tale M esiste perché $\mathbb{N} - C$ è finito e non vuoto!). Poi poniamo

$$h(C) = 0, 0c_0c_1c_2\ldots$$

dove osserviamo che la prima cifra dopo la virgola è 0, e poi $c_M = 1$ e $c_i = 0$ per $i > M$. Inoltre, se $M > 0$, per $0 \leq i \leq M - 1$ poniamo $c_i = 0$ se $i \notin C$ e $c_i = 1$ se $i \in C$.

Se invece prendiamo un $B \in I_2$ poniamo

$$h(B) = 0, b_0b_1b_2\ldots$$

dove, per ogni i, $b_i = 0$ se $i \notin B$ e $b_i = 1$ se $i \in B$. Questo non produce una scrittura con una coda di 1 giacchè il complementare di B è infinito.

Resta a voi la facile verifica del fatto che la $h : \mathcal{P}(\mathbb{N}) - \{\mathbb{N}\} \longrightarrow (0, 1)$ così definita è bigettiva. ■

Osserviamo che, siccome i due teoremi precedenti ci garantiscono che $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$ e che $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$, avremmo anche potuto seguire questa strada "più generale" per dimostrare che la cardinalità del continuo è strettamente maggiore del numerabile.
Torniamo ora alla nostra lista di insiemi infiniti, che sono tutti costruiti a partire da $\mathbb{N}$ ripetendo l'operazione di prendere l'insieme delle parti:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| = |\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < \cdots$$

Resta la nostra terza domanda: questi sono tutti i possibili insiemi infiniti ? Formuliamo anche una domanda che si pone un obiettivo più modesto: ci sono insiemi infiniti di cardinalità strettamente compresa fra $|\mathbb{N}|$ e $|\mathbb{R}|$?

Queste due domande sono in realtà molto famose e sono note come:

Congettura (ipotesi del continuo). Ogni X sottoinsieme di $\mathbb{R}$ che sia infinito non numerabile ha la stessa cardinalità di $\mathbb{R}$.

Congettura (ipotesi generalizzata del continuo). Se X è un insieme infinito, la sua cardinalità è una di quelle che appaiono nella lista.

Nel 1963 Cohen dimostrò che non è possibile né dimostrare che tali congetture sono vere né dimostrare che tali congetture sono false, se si parte dagli assiomi generalmente accettati della teoria degli insiemi. In altre parole si possono costruire due "teorie degli insiemi" alternative, una in cui valgono le ipotesi del continuo e una in cui non valgono.

Terminiamo queste note soffermandoci ancora sull'esempio dei numeri reali. Sappiamo che

$$\mathbb{N} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

e che

$$|\mathbb{N}| = |\mathbb{Q}| < |\mathbb{R}|$$

Introduciamo ora un nuovo sottoinsieme di $\mathbb{R}$ che contiene $\mathbb{Q}$.

Definizione. Un numero reale si dice algebrico se è radice di un polinomio

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

dove i coefficienti a_i sono numeri razionali. Se un numero reale non è algebrico allora si dice trascendente.

In altre parole, preso un numero reale a, se si trova un polinomio a coefficienti razionali di cui a è radice, allora a è algebrico. Se un tale polinomio non esiste allora a è trascendente. Notiamo che il fatto che il polinomio della definizione sia monico, ossia inizi con x^n, non è importante. Quello che è importante è che sia a coefficienti razionali (perché non é cosí importante che sia monico ?).

Vale che tutti i numeri razionali sono algebrici, ossia $\mathbb{Q} \subseteq \mathcal{A}$ dove $\mathcal{A}$ è l'insieme dei numeri algebrici. Se infatti ho un numero razionale $\frac{m}{n}$ $(n \neq 0)$, tale numero è radice del polinomio a coefficienti razionali $x - \frac{m}{n}$ (o di $nx - m$. . . .a riguardo della domanda fatta poche righe fa. . .).

Ma è algebrico anche il numero $\sqrt{2}$ che noi sappiamo non essere razionale. Infatti $\sqrt{2}$ soddisfa il polinomio a coefficienti razionali (addirittura interi) $x^2 - 2$. Dunque $\mathbb{Q} \subsetneq \mathcal{A}$.

Ma non sarà mica che $\mathcal{A} = \mathbb{R}$, ossia che tutti i numeri reali sono algebrici? La risposta è no. Nel XIX secolo furono trovati da vari matematici (Liouville, Hermite, Lindemann. . .) dei numeri che non sono algebrici: tali numeri si chiamano "trascendenti".

Per esempio Hermite dimostrò nel 1873 che e, la base dei logaritmi naturali, è trascendente, e Lindemann nel 1882 dimostrò che π è trascendente.

Il problema di trovare numeri trascendenti è molto complicato: credo (vedi anche Eccles, pag. 180) che non sia ancora noto, per esempio, se $\pi + e$ è trascendente.

Questa complicazione ci può sorprendere: possiamo infatti dimostrare che i numeri trascendenti sono "di più" dei numeri algebrici (e dunque dei numeri razionali). Come fare ?

Tutto comincia col seguente esercizio (facoltativo - provate a lanciarvi).

Esercizio. Dimostrare che $\mathcal{A}$ è infinito numerabile. (idea: i polinomi a coefficienti razionali si possono individuare in base al loro grado, che è un numero naturale, e in

base ai loro coefficienti, che sono numeri razionali (insomma appartengono ad un insieme numerabile). Dunque i polinomi a coefficienti razionali sono numerabili. D'altra parte, le radici di un polinomio sono finite..)

Ora scriviamo $\mathbb{R} = \mathcal{A} \cup \mathcal{T}$, dove $\mathcal{T}$ è l'insieme dei numeri trascendenti: a questo punto, anche se non conoscessimo nemmeno un numero trascendente, potremmo comunque affermare che $\mathcal{T}$ non è vuoto, visto che altrimenti avremmo $\mathbb{R} = \mathcal{A}$ e $\mathbb{R}$ sarebbe numerabile. Inoltre $\mathcal{T}$ non può essere né finito né infinito numerabile (altrimenti $\mathbb{R}$ sarebbe unione di due insiemi dei quali uno è infinito numerabile e l'altro è o finito o infinito numerabile e noi sappiamo che questo implicherebbe che $\mathbb{R}$ è numerabile !).

Dunque $\mathcal{T}$ è infinito e non numerabile; insomma $|\mathbb{N}| < |\mathcal{T}|$, che si può scrivere anche $|\mathcal{A}| < |\mathcal{T}|$. In questo senso i numeri trascendenti sono "di più" dei numeri algebrici !

16. La divisione euclidea.

Come posso distribuire 150 penne fra 70 studenti? Darò ad ognuno $\frac{150}{70} = 2,142857$ penne? Oppure il problema lo devo affrontare dicendo che posso dare 2 penne ad ogni studente e poi mi avanza un resto di 10 penne ? Questo secondo modo è il più adatto: visto che le penne non si possono "spezzare", il problema era relativo ai numeri interi e deve avere risposta in termini di numeri interi. La divisione che abbiamo fatto, con un quoziente intero (70) e un resto intero (10), è un esempio di "divisione euclidea".

Teorema della divisione euclidea. Siano $a, b \in \mathbb{Z}$, con $b > 0$. Allora esistono UNICI due interi q e r tali che

$$a = bq + r \quad \text{e} \quad 0 \leq r < b$$

Osservazione. Questa si chiama "divisione euclidea di a per b", a è il "dividendo", b è il "divisore", q è il "quoziente" e r è il "resto" della divisione.

Dimostrazione. Dati a e b come sopra, bisogna dimostrare due cose:

(a) che ESISTONO questi q e r tali che $a = bq + r \quad \text{e} \quad 0 \leq r < b$;

(b) che tali q e r sono UNICI.

Dimostriamo il punto a). Consideriamo il seguente sottoinsieme di $\mathbb{N}$:

$$R = \{x \in \mathbb{N} \mid x = a - bk \quad \text{con} \quad k \in \mathbb{Z}\}$$

Lo abbiamo chiamato R per ricordare che questo insieme è composto da tutti i possibili "resti" non negativi che si ottengono quando si sottrae o si somma ad a un multiplo di b. Scopriremo che fra tutti questi resti uno ed uno solo soddisfa le richieste della divisione euclidea. Intanto osserviamo che R è non vuoto (infiniti numeri della forma

$a - bk$ appartengono a $\mathbb{N}$, pensiamo per esempio a quando k è negativo..) e che per definizione $\mathbb{R} \subseteq \mathbb{N}$.

Possiamo allora appellarci al Principio del Buon Ordinamento (ATTENZIONE! Questa è la prima dimostrazione in cui utilizziamo il principio di induzione in questa forma!) per concludere che R ha un elemento minimo, che chiameremo r. Siccome $r \in \mathbb{R}$, vuol dire che esiste un certo $q \in \mathbb{Z}$ tale che posso scrivere $r = a - bq$. Ecco, questo r e questo q che abbiamo trovato saranno proprio il quoziente e il resto della divisione euclidea di a per b. Come mai ?

Innanzitutto, per come abbiamo scelto q e r, vale

$$a = bq + r$$

Resta da vedere che è soddisfatta l'altra condizione chiesta dalla divisione euclidea, ossia $0 \leq r < b$. Certamente $r \geq 0$, visto che $r \in R \subseteq \mathbb{N}$. Ora supponiamo per assurdo che $r \geq b$. Allora avremmo $0 \leq r - b$ e, dato che $b > 0$,

$$0 \leq r - b < r$$

Ma $r - b$ è un intero non negativo e può essere scritto come

$$r - b = (a - bq) - b = a - (q + 1)b$$

dunque $r - b \in R$. Questo è ASSURDO perché contraddice il fatto che r è il minimo di R.

Dimostriamo ora il punto b). Supponiamo di avere due coppie di interi q_1, r_1 e q_2, r_2 che soddisfano ENTRAMBE le condizioni per essere quoziente e resto della divisione euclidea di a per b. Mostreremo che deve essere $q_1 = q_2$ (e di conseguenza $r_1 = r_2$). Infatti vale

$$a = bq_1 + r_1 \quad \text{e} \quad 0 \leq r_1 < b$$
$$a = bq_2 + r_2 \quad \text{e} \quad 0 \leq r_2 < b$$

Possiamo supporre, a meno di cambiare gli indici, che $q_1 \geq q_2$.

Allora $r_1 \leq r_2$, visto che $r_1 = a - bq_1$ e $r_2 = a - bq_2$.

Possiamo dunque scrivere

$$0 \leq r_2 - r_1 < b$$

da cui con semplici passaggi:

$$0 \leq (a - bq_2) - (a - bq_1) < b$$
$$0 \leq b(q_1 - q_2) < b$$
$$0 \leq (q_1 - q_2) < 1$$

Ma q_1 e q_2 sono interi, dunque l'unica possibilità è che $q_1 - q_2 = 0$ ossia $q_1 = q_2$ da cui si ricava subito anche $r_1 = r_2$. ■

Esempio. Se $a = -25$ e $b = 8$ quale fra queste due è la divisione euclidea di a per b ?

$$-25 = (-4)8 + 7$$

$$-25 = (-3)8 + (-1)$$

Risposta: la prima, perché ha il resto 7 che soddisfa la condizione richiesta $0 \leq r < 8$.

17. Il MCD e una dimostrazione dell'identità di Bezout.

Notazione. Ricordiamo che, dati due numeri interi c e d, diciamo che c divide d se esiste un numero intero k tale che $ck = d$. In tal caso scriviamo $c|d$.

Definizione Siano $a, b \in \mathbb{Z}$, con almeno uno dei due diverso da 0 (notare che questo si può scrivere così: $(a, b) \in \mathbb{Z} \times \mathbb{Z} - \{(0, 0)\}$). Allora il "massimo comun divisore" di a e b è l'unico intero positivo d tale che:

- $d|a$ e $d|b$;
- d è più grande di ogni altro divisore comune di a e b: se $c|a$ e $c|b$, allora deve essere $c \leq d$.

Notazione. Indicheremo il massimo comun divisore di a e b come $MCD\ (a, b)$.

Osservazione. Innanzitutto osserviamo che la definizione è ben posta. Almeno un divisore comune positivo di a e b esiste sempre (il numero 1) e dunque l'insieme di tutti i divisori comuni positivi è un sottoinsieme di $\mathbb{N}$ non vuoto e finito (si noti a questo proposito che i suoi elementi sono tutti minori o uguali al minimo fra a e b). Allora esiste unico il massimo di tale insieme, che è appunto il $MCD\ (a, b)$.

Quella che esporremo qui di seguito è una dimostrazione "esistenziale" (che fa parte del programma) della identità di Bezout; abbiamo visto in classe anche una dimostrazione "costruttiva" che utilizza l'algoritmo di Euclide.

Teorema (Identità di Bezout). Dati due numeri interi a e b con $(a, b) \neq (0, 0)$, esistono due numeri interi m e n tali che

$$MCD(a, b) = am + bn$$

Si dice che $MCD(a, b)$ può essere espresso come combinazione lineare a coefficienti interi di a e di b.

Osservazione. Il teorema dice che esistono m ed n tali che $MCD(a,b) = am + bn$, ma non dice che sono unici. Infatti, come risulterà dalla teoria delle equazioni diofantee lineari, ci sono infinite scelte possibili di una coppia (m,n) tale che $MCD(a,b) = am+bn$.

Dimostrazione. Consideriamo l'insieme $CL(a,b)$ di tutte le possibili combinazioni lineari POSITIVE a coefficienti interi di a e b, ossia

$$CL(a,b) = \{ar + bs \mid r \in \mathbb{Z},\ s \in \mathbb{Z},\ ar + bs > 0\}$$

Tale insieme è non vuoto. Infatti supponiamo che $a \neq 0$ (altrimenti si fa lo stesso ragionamento con b). Allora si trovano degli elementi dell'insieme $CL(a,b)$ per esempio scegliendo $s = 0$ e r tale che $ra > 0$. Già così abbiamo esibito infiniti elementi nell'insieme $CL(a,b)$.

Inoltre $CL(a,b) \subseteq \mathbb{N}$. Dunque, per il principio del buon ordinamento, $CL(a,b)$ ammette minimo.

Sia d tale minimo: in particolare, dato che $d \in CL(a,b)$, esistono un $m \in \mathbb{Z}$ ed un $n \in \mathbb{Z}$ tali che

$$d = am + bn$$

Vogliamo dimostrare che $d = MCD(a,b)$. Se ci riusciamo abbiamo anche dimostrato il teorema perché (pur senza sapere come COSTRUIRLA !) abbiamo visto che deve esistere una coppia di numeri interi (m,n) tale che

$$MCD(a,b) = am + bn$$

Per dimostrare che $d = MCD(a,b)$ basta dimostrare che soddisfa le proprietà del massimo comune divisore, ossia:

- $d|a$ e $d|b$
- se $c|a$ e $c|b$ allora $c \leq d$

Per il primo punto, facciamo la divisione euclidea fra a e d. Sarà $a = qd + r$ con $0 \leq r < d$.

Allora

$$a = q(am + bn) + r$$

da cui

$$r = (-qm + 1)a + (-qn)b$$

Ma allora r si esprime come combinazione lineare a coefficienti interi di a e di b. Se fosse $r > 0$ avremmo che $r \in CL(a,b)$ per definizione di $CL(a,b)$. Questo non può succedere perché $0 \leq r < d$ e d era stato scelto come MINIMO elemento di $CL(a,b)$.

Dunque deve essere $r = 0$. Questo vuol dire che $a = qd + 0$, ossia che $d|a$. Allo stesso modo si dimostra che $d|b$.

Il secondo punto è immediato. Infatti se $c|a$ e $c|b$ allora $c|am+bn$ cioè $c|d$, in particolare $c \leq d$.

■

Se riguardiamo la dimostrazione del teorema, scopriamo che ci ha regalato di più di quello che volevamo, ossia abbiamo dimostrato una cosa di cui nell'enunciato non si faceva cenno. Anche se è una dimostrazione solo "esistenziale", perché non ci ha fornito nessuna strategia concreta per trovare m e n tali che $MCD(a,b) = am + bn$, le dobbiamo dunque essere molto grati..

Ecco il regalo della dimostrazione appena vista:

Teorema. Dati due numeri interi a e b con $(a,b) \neq (0,0)$, vale che $MCD(a,b)$ è il più piccolo numero intero positivo ottenibile come combinazione lineare intera di a e di b.

Abbiamo anche verificato il seguente IMPORTANTE corollario della identità di Bezout:

Corollario. Dati due numeri interi a e b con $(a,b) \neq (0,0)$, se $c|a$ e $c|b$, allora non solo $c \leq MCD(a,b)$ ma più precisamente vale che $c|MCD(a,b)$.

18. Perché funziona l'algoritmo di Euclide.

Supponiamo di voler trovare il MCD di due numeri $a, b \in \mathbb{Z}$ non entrambi nulli.

Se uno dei due numeri (per esempio a) è 0, allora sappiamo subito dire che $MCD\ (0,b)$ è $|b|$.

Se invece entrambi i numeri sono diversi da zero possiamo usare (e può essere molto conveniente!) l'algoritmo di Euclide. Se vale per esempio che $|a| \geq |b| > 0$ applichiamo l'algoritmo direttamente al calcolo di $MCD\ (|a|,|b|)$; questo non cambia il risultato perché

$$MCD\ (a,b) = MCD\ (b,a) = MCD\ (|a|,|b|) = MCD\ (|b|,|a|)$$

per come è definito il MCD. Cominciamo:

$$|a| = |b|q + r \quad \text{con} \quad 0 \leq r < |b|$$

Se $r = 0$ abbiamo finito, perché possiamo concludere subito che $|b| = MCD\ (|a|,|b|) = MCD\ (a,b)$. Altrimenti proseguiamo finché non si trova un resto uguale a 0:

$$|a| = |b|q + r \quad \text{con} \quad 0 < r < |b|$$

$$|b| = r \cdot q_1 + r_1 \quad \text{con} \quad 0 < r_1 < r$$

$$r = r_1 q_2 + r_2 \quad \text{con} \quad 0 < r_2 < r_1$$

$$\cdots\cdots\cdots$$

$$r_{n-2} = r_{n-1} q_n + r_n \quad \text{con} \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1} + 0$$

A questo punto concludiamo che $r_n = MCD\ (|a|, |b|) = MCD\ (a, b)$.

Perché l'algoritmo si è fermato ? Perché ad ogni passo otteniamo un resto r_j che è un numero naturale ed è strettamente minore del resto precedente. Se potessimo continuare all'infinito l'insieme dei resti contraddirrebbe il principio del buon ordinamento (sarebbe un sottoinsieme di $\mathbb{N}$ senza minimo..).

Perché r_n è proprio il MCD che cercavamo ? Ripetiamo in forma più compatta l'osservazione fatta in classe. Il punto cruciale è il seguente:

Lemma. Se per certi $a, b, q, r \in \mathbb{Z}$, con $(a, b) \neq (0, 0)$ e $(b, r) \neq (0, 0)$ vale

$$a = bq + r$$

allora $MCD\ (a, b) = MCD\ (b, r)$.

Dimostrazione. Sia $d = MCD\ (a, b)$ e $d' = MCD\ (b, r)$. Per la definizione di MCD vale che $d|a$ e $d|b$, e allora $d|\ a - bq$ cioè $d|r$. Dunque d è un divisore comune di b e di r,e, come tale, deve soddisfare $d \leq d'$.

D'altra parte d', visto che è MCD, divide b e r. Dunque divide anche $bq + r$, ossia a. Allora d' è un divisore comune di b e di a e come tale deve soddisfare $d' \leq d$. Siccome poco fa abbiamo mostrato che $d \leq d'$ possiamo concludere che

$$d = d'$$

■

Applicando questo lemma ai vari passaggi del nostro algoritmo di Euclide otteniamo:

$$MCD\ (|a|, |b|) = MCD\ (|b|, r) = MCD\ (r, r_1) = MCD\ (r_1, r_2) = \ldots$$

e così via (questo "così via" nasconde una facile induzione!) fino a

$$\ldots = MCD\ (r_{n-2}, r_{n-1}) = MCD\ (r_{n-1}, r_n)$$

Ma $MCD\ (r_{n-1}, r_n)$ è proprio r_n, visto che $r_n | r_{n-1}$. Ripercorrendo tutta la catena di uguaglianze scopriamo di aver dimostrato che

$$MCD\ (|a|, |b|) = r_n$$

e dunque ora sappiamo perché l'algoritmo di Euclide funziona!

Esercizio "sfida": trovare una qualche buona stima, in funzione di a e b, del numero dei passi necessari per portare a termine l'algoritmo di Euclide.

19. Esempio di risoluzione di una equazione diofantea.

Troviamo tutte le soluzioni dell'equazione diofantea

$$435x + 102y = 15$$

Ricordiamo che una soluzione è una coppia $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$ che soddisfa l'equazione data:

$$435\overline{x} + 102\overline{y} = 15$$

- Per prima cosa verifichiamo se l'equazione proposta ammette soluzioni: sappiamo che questo accade se e solo se $MCD\ (435, 102)\ |15$. Usiamo dunque l'algoritmo di Euclide per calcolare $MCD\ (435, 102)$.

$$435 = 102 \cdot 4 + 27$$

$$102 = 27 \cdot 3 + 21$$

$$27 = 21 \cdot 1 + 6$$

$$21 = 6 \cdot 3 + 3$$

$$6 = 3 \cdot 2 + 0$$

  Dunque $MCD\ (435, 102) = 3\ |15$ e la nostra equazione ammette soluzioni.

- Adesso troviamo una soluzione particolare dell'equazione. Come primo passo usiamo Euclide (alla rovescia..) per trovare una combinazione lineare di Bezout, ossia un $m \in \mathbb{Z}$ e un $n \in \mathbb{Z}$ tali che

$$3 = MCD\ (435, 102) = 435m + 102n$$

  Scriviamo i resti dell'algoritmo di Euclide appena svolto:

$$27 = 435 - 102 \cdot 4$$

$$21 = 102 - 27 \cdot 3$$

$$6 = 27 - 21 \cdot 1$$

$$3 = 21 - 6 \cdot 3$$

e sostituiamoli uno dopo l'altro nelle combinazioni lineari qui sotto:

$$3 = 21 - 6 \cdot 3 = 21 - (27 - 21)3 = 21 \cdot 4 - 27 \cdot 3 =$$

$$= (102 - 27 \cdot 3)4 - 27 \cdot 3 = 102 \cdot 4 - 27 \cdot 15 = 102 \cdot 4 - (435 - 102 \cdot 4) \cdot 15 =$$

$$= 102 \cdot 64 - 435 \cdot 15$$

In conclusione abbiamo trovato

$$3 = 102 \cdot 64 - 435 \cdot 15$$

(insomma $m = -15$ e $n = 64$).

Se moltiplichiamo questa uguaglianza per $\dfrac{15}{MCD\ (435, 102)} = 5$ otteniamo

$$15 = 102 \cdot 320 - 435 \cdot 75$$

Abbiamo dunque che $(-75, 320)$ è una soluzione particolare di

$$435x + 102y = 15$$

- Troviamo adesso tutte le infinite soluzioni della equazione diofantea data. Consideriamo la omogenea associata

$$435x + 102y = 0$$

e calcoliamone tutte le soluzioni. Dividendo entrambi i membri per $3 = MCD\ (435, 102)$ (IMPORTANTE: ricordarsi sempre di dividere per il MCD a questo punto dello svolgimento!) ci riduciamo a

$$145x + 34y = 0$$

ossia

$$145x = -34y$$

Adesso 145 e 34 sono coprimi (controllate bene di aver capito perché.. -abbiamo diviso per il MCD...) e dunque se (x, y) è una soluzione deve valere $y = 145q$, con $q \in \mathbb{Z}$. Sostituendo

$$145x = -34 \cdot 145q$$

da cui ricaviamo $x = -34q$. Dunque una soluzione di

$$145x + 34y = 0$$

deve essere della forma $(-34q, 145q)$ con $q \in \mathbb{Z}$. Le osservazioni fatte in classe ci permettono a questo punto di concludere l'esercizio: le soluzioni di

$$145x + 34y = 0$$

sono tutte e sole le coppie $(-34q, 145q)$ al variare di $q \in \mathbb{Z}$ e l'insieme di tutte le soluzioni di

$$435x + 102y = 15$$

è

$$\{(-75 - 34q, 320 + 145q) \mid q \in \mathbb{Z}\}$$

20. Regole per lavorare con le congruenze.

Dati $m \in \mathbb{Z}^+$, $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ e $a \in \mathbb{Z} - \{0\}$ vale:

- $$a_1 \equiv b_1 \quad (m) \quad <=> \quad a_1 - b_1 \equiv 0 \quad (m)$$
- $$a \equiv b \quad (m) \quad <=> \quad -a \equiv -b \quad (m)$$
- Se
$$a_1 \equiv b_1 \quad (m)$$
e
$$a_2 \equiv b_2 \quad (m)$$
allora
$$a_1 + a_2 \equiv b_1 + b_2 \quad (m)$$
- Se
$$a_1 \equiv b_1 \quad (m)$$
e
$$a_2 \equiv b_2 \quad (m)$$
allora
$$a_1 - a_2 \equiv b_1 - b_2 \quad (m)$$
- Se
$$a_1 \equiv b_1 \quad (m)$$
e
$$a_2 \equiv b_2 \quad (m)$$
allora
$$a_1 a_2 \equiv b_1 b_2 \quad (m)$$

- $$a\ b_1 \equiv a\ b_2 \quad (m) \quad <=> \quad b_1 \equiv b_2 \quad \left(\frac{m}{MCD(a,m)}\right)$$

La dimostrazione di queste regolette è immediata. Svolgiamo qui esplicitamente la dimostrazione dell'ultima regola (dimostrazione che è un po' più lunga delle altre).

Dimostrazione. Ricordiamo che stiamo considerando $a \in \mathbb{Z} - \{0\}$. Supponiamo che

$$a\ b_1 \equiv a\ b_2 \quad (m)$$

Allora per definizione di congruenza vale che

$$m \mid ab_1 - ab_2$$

ossia esiste un $q \in \mathbb{Z}$ tale che

$$ab_1 - ab_2 = mq$$

Possiamo dividere per $MCD(a,m)$ e otteniamo

$$\frac{a}{MCD(a,m)}(b_1 - b_2) = \frac{m}{MCD(a,m)}q$$

Da questo, visto che $\frac{a}{MCD(a,m)}$ e $\frac{m}{MCD(a,m)}$ sono coprimi (come mai ? -controllate di saper rispondere), segue che

$$\frac{m}{MCD(a,m)} \mid b_1 - b_2$$

ovvero che

$$b_1 \equiv b_2 \quad \left(\frac{m}{MCD(a,m)}\right)$$

Supponiamo ora, viceversa, che sia vero

$$b_1 \equiv b_2 \quad \left(\frac{m}{MCD(a,m)}\right)$$

Allora $\frac{m}{MCD(a,m)} \mid (b_1 - b_2)$, ossia esiste un $t \in \mathbb{Z}$ tale che

$$t\frac{m}{MCD(a,m)} = b_1 - b_2$$

da cui, moltiplicando per $MCD(a,m)$ otteniamo

$$tm = (b_1 - b_2)MCD(a,m)$$

Osserviamo dunque che

$$m \mid (b_1 - b_2)MCD(a, m)$$

da cui a maggior ragione ricaviamo

$$m \mid (b_1 - b_2)a$$

(abbiamo usato il fatto che $MCD(a, m)|a$) che si riscrive come

$$a\ b_1 \equiv a\ b_2 \quad (m)$$

21. Il teorema fondamentale per la risoluzione delle congruenze lineari.

Teorema. Dato $m \in \mathbb{Z}^+$, l'equazione

$$ax \equiv b \quad (m)$$

ha soluzione se e solo se $MCD(a, m)|b$. In questo caso l'equazione ha $MCD(a, m)$ soluzioni modulo m.

Nota: quando diciamo "l'equazione ha $MCD(a, m)$ soluzioni modulo m" intendiamo dire che se prendiamo l'insieme di tutte le soluzioni dell'equazione e controlliamo che resto hanno queste soluzioni quando facciamo la divisione euclidea per m allora troviamo esattamente $MCD(a, m)$ diversi resti. Possiamo esprimerci anche così: l'insieme delle soluzioni dell'equazione è composto da esattamente $MCD(a, m)$ soluzioni x che soddisfano $0 \leq x < m$ e tutte le altre soluzioni differiscono da queste per un multiplo di m.

Dimostrazione. Prima dimostriamo che, se l'equazione ha soluzione allora $MCD(a, m)|b$.

Scegliamo di dimostrare la contronominale, ossia che, se $MCD(a, m)$ non divide b allora non esiste soluzione dell'equazione.

Supponiamo dunque che $MCD(a, m)$ non divida b; ora supponiamo che, per assurdo, esista una soluzione x_0 di $ax \equiv b \quad (m)$.

Questo vuol dire che $m|ax_0 - b$, ossia che esiste un $q \in \mathbb{Z}$ tale che $qm = ax_0 - b$. Si può dunque scrivere $b = ax_0 - mq$. Ma a questo punto $MCD(a, m)$ divide il membro di destra, dunque deve dividere b, assurdo visto che siamo fin dall'inizio nel caso in cui $MCD(a, m)$ non divide b.

Dimostriamo adesso l'altra implicazione, cioè che, se $MCD(a, m)|b$ allora l'equazione ha soluzione.

Supponiamo dunque che $MCD(a,m)|b$. Allora, viste le proprietà delle congruenze (vedi "regole per lavorare con le congruenze" in questi stessi appunti) possiamo scrivere che

$$ax \equiv b \quad (m)$$

equivale a

$$\frac{a}{MCD(a,m)}x \equiv \frac{b}{MCD(a,m)} \quad \left(\frac{m}{MCD(a,m)}\right)$$

Ora notiamo che, per definizione di congruenza, un numero x è soluzione di questa equazione se e solo se

$$\frac{m}{MCD(a,m)} \mid \left(\frac{a}{MCD(a,m)}x - \frac{b}{MCD(a,m)}\right)$$

ossia se e solo se esiste un $y \in \mathbb{Z}$ tale che

$$\frac{m}{MCD(a,m)}y = \frac{a}{MCD(a,m)}x - \frac{b}{MCD(a,m)}$$

Se dunque troviamo una soluzione (x,y) della equazione diofantea

$$\frac{a}{MCD(a,m)}x - \frac{m}{MCD(a,m)}y = \frac{b}{MCD(a,m)}$$

allora il numero x sarà anche soluzione della congruenza

$$\frac{a}{MCD(a,m)}x \equiv \frac{b}{MCD(a,m)} \quad \left(\frac{m}{MCD(a,m)}\right)$$

Ma la equazione diofantea che stiamo considerando ha soluzione ? Certo, perché $\frac{a}{MCD(a,m)}$ e $\frac{m}{MCD(a,m)}$ sono coprimi (come mai ? -controllate di saper rispondere) e dunque il loro massimo comun divisore, 1, divide $\frac{b}{MCD(a,m)}$ come richiede il criterio di risolubilità per le equazioni diofantee.

In conclusione abbiamo dimostrato che la congruenza

$$\frac{a}{MCD(a,m)}x \equiv \frac{b}{MCD(a,m)} \quad \left(\frac{m}{MCD(a,m)}\right)$$

ha soluzione.

Quante sono le soluzioni modulo $\frac{m}{MCD(a,m)}$? Una sola: consideriamo infatti due numeri interi x_1 e x_2 che sono soluzione e che dunque soddisfano

$$\frac{a}{MCD(a,m)}x_1 \equiv \frac{b}{MCD(a,m)} \quad \left(\frac{m}{MCD(a,m)}\right)$$

$$\frac{a}{MCD(a,m)}x_2 \equiv \frac{b}{MCD(a,m)} \quad \left(\frac{m}{MCD(a,m)}\right)$$

Allora vale che

$$\frac{a}{MCD(a,m)}x_1 \equiv \frac{a}{MCD(a,m)}x_2 \quad \left(\frac{m}{MCD(a,m)}\right)$$

Siccome $\frac{a}{MCD(a,m)}$ e $\frac{m}{MCD(a,m)}$ sono coprimi, possiamo dividere per $\frac{a}{MCD(a,m)}$ e otteniamo

$$x_1 \equiv x_2 \quad \left(\frac{m}{MCD(a,m)}\right)$$

Abbiamo cioè mostrato che due numeri che sono soluzione sono sempre congrui fra loro modulo $\frac{m}{MCD(a,m)}$. Questo significa che l' equazione ha infinite soluzioni ma che ce ne è una sola, X, con $0 \leq X < \frac{m}{MCD(a,m)}$.

Siamo ora in grado di contare quante soluzioni ci sono, modulo m, della equazione nel testo del teorema, ossia di

$$ax \equiv b \quad (m)$$

Innanzitutto, visto che le soluzioni di questa equazione sono esattamente tutte e sole le soluzioni della

$$\frac{a}{MCD(a,m)}x \equiv \frac{b}{MCD(a,m)} \quad \left(\frac{m}{MCD(a,m)}\right)$$

sappiamo in particolare che X è soluzione. Poi sappiamo anche che tutte e sole le soluzioni sono i numeri del tipo $X + \frac{m}{MCD(a,m)}q$ con $q \in \mathbb{Z}$. E' facile verificare che, fra tali numeri, solo $MCD(a,m)$ sono ≥ 0 e $< m$:

$$X,\ X + \frac{m}{MCD(a,m)},\ X + 2\frac{m}{MCD(a,m)},\ \cdots, X + (MCD(a,m)-1)\frac{m}{MCD(a,m)}$$

Tutte le altre soluzioni differiscono da una di queste per un multiplo di m.

■

22. Esempio: risoluzione di una congruenza lineare.

Esercizio: data la congruenza

$$195x \equiv 6 \quad (42)$$

trovare
a) tutte le sue soluzioni,
b) le sue soluzioni modulo 42, ossia quelle comprese fra 0 e 41.

Osserviamo che $MCD\ (195, 42) = 3 \mid 6$ dunque la congruenza ha soluzione. Il teorema dimostrato nel paragrafo precedente ci dice anche che avremo 3 soluzioni modulo 42. Per prima cosa possiamo sostituire 195 con il suo resto modulo 42, ossia 27.

$$27x \equiv 6 \quad (42)$$

Poi possiamo dividere per $MCD\ (195, 42) = 3$: la regola per la divisione dimostrata nel paragrafo "regole per lavorare con le congruenze" ci garantisce che otteniamo una equazione equivalente.

$$9x \equiv 2 \quad (\frac{42}{MCD\ (3, 42)} = 14)$$

Un modo possibile di procedere adesso è il seguente: si nota "a occhio" che $3 \cdot 9 = 27$ è congruo a -1 modulo 14. Dunque ci conviene moltiplicare il membro di sinistra e quello di destra per 3. Visto che 3 è primo con 14, la solita regola per la divisione ci dice che l'equazione che otteniamo è equivalente (si vede subito infatti che si potrebbe "tornare indietro" dividendo per 3...).

$$27x \equiv 6 \quad (14)$$

che si può riscrivere

$$-x \equiv 6 \quad (14)$$

$$x \equiv -6 \quad (14)$$

Abbiamo dunque trovato tutte le soluzioni dell'equazione

$$195x \equiv 6 \quad (42)$$

L'insieme delle soluzioni si può scrivere anche

$$\{x = -6 + 14q \mid q \in \mathbb{Z}\}$$

Per rispondere alla domanda b), dobbiamo indicare le tre soluzioni x con $0 \leq x \leq 41$. Si tratta di $-6 + 14, -6 + 2 \cdot 14, -6 + 3 \cdot 14$, cioè 8, 22 e 36.

23. Esempio di risoluzione di una equazione diofantea (usando le congruenze lineari).

In questo esempio mostriamo un'altra possibile tecnica per risolvere le equazioni diofantee, che prevede la risoluzione di una congruenza lineare. Consideriamo l'equazione

$$224x + 108y = 700$$

Commento: Se esiste una soluzione (X, Y)*, il numero intero* X *deve anche soddisfare*

$$224X \equiv 700 \quad (108)$$

(infatti $108Y = 224X - 700$ *dunque* $108 \mid 224X - 700$*). Viceversa, se un certo numero intero* X *soddisfa la congruenza, allora, siccome* $108 \mid 224X - 700$*, deve esistere un* Y *tale che*

$$224X + 108Y = 700$$

cioè la coppia (X, Y) *risolve la diofantea.*

Dunque abbiamo osservato che l'insieme delle soluzioni della congruenza

$$224x \equiv 700 \quad (108)$$

coincide con l'insieme dato dalle prime componenti delle coppie che risolvono la diofantea.

Risolviamo la congruenza

$$224x \equiv 700 \quad (108)$$

Per prima cosa osserviamo che $MCD\ (224, 108) = 4 \mid 700$ dunque la congruenza ha soluzione (questa del resto è la stessa condizione che ci dice che la diofantea ha soluzione). Ora possiamo dividere per 4, per semplificare (ATTENZIONE: QUANDO SI DIVIDE BISOGNA SEMPRE RISPETTARE LA REGOLA DIMOSTRATA NELLA SEZIONE "regole per lavorare con le congruenze"):

$$56x \equiv 175 \quad (\frac{108}{MCD(108, 4)} = 27)$$

Notiamo anche che 7|56 e che 7|175, dunque possiamo semplificare ulteriormente dividendo per 7:

$$8x \equiv 25 \quad (\frac{27}{MCD(27, 7)} = 27)$$

Questa si può risolvere "a occhio": infatti notiamo che $8 \cdot 10 = 80$ è congruo a -1 modulo 27 (infatti $3 \cdot 27 = 81$). Ora, 10 è primo con 27 dunque posso moltiplicare per 10 il membro di destra e quello di sinistra senza cambiare l'insieme delle soluzioni. Ottengo allora la equazione equivalente:

$$80x \equiv 250 \quad (27)$$

che si riscrive come

$$-x \equiv 7 \quad (27)$$

$$x \equiv -7 \quad (27)$$

Dunque l'insieme delle soluzioni di

$$224x \equiv 700 \quad (108)$$

è

$$\{x = -7 + 27q \mid q \in \mathbb{Z}\}$$

Possiamo sostituire queste soluzioni al posto della x nella equazione diofantea

$$224x + 108y = 700$$

(che comunque per semplificare possiamo dividere per 4, ottenendo $56x + 27y = 175$):

$$56(-7 + 27q) + 27y = 175$$

Svolgiamo i conti:

$$27y = 392 + 175 - 27q$$

$$27y = 567 - 27q$$

$$y = 21 - q$$

Abbiamo dunque trovato che l'insieme delle soluzioni di

$$224x + 108y = 700$$

è:

$$\{(-7 + 27q \ , \ 21 - q) \mid q \in \mathbb{Z}\}$$

Osserviamo che abbiamo trovato in un colpo solo tutte le soluzioni della diofantea, senza dividere il problema nella ricerca di una soluzione particolare e poi di tutte le soluzioni della omogenea associata. Di volta in volta potrete scegliere il metodo di risoluzione che vi sembra più conveniente.

24. Esempio: risoluzione di una congruenza lineare (usando le equazioni diofantee).

Nell'esempio precedente abbiamo mostrato come le congruenze lineari possono aiutarci a risolvere le equazioni diofantee. Vale anche il viceversa, ossia talvolta nel risolvere una congruenza lineare può convenire introdurre e risolvere una equazione diofantea. Consideriamo l'equazione

$$341x \equiv 15 \quad (912)$$

Calcoliamo $MCD(341, 912)$:

$$912 = 341 \cdot 2 + 230$$

$$341 = 230 + 111$$

$$230 = 111 \cdot 2 + 8$$

$$111 = 8 \cdot 13 + 7$$

$$8 = 7 + 1$$

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

Dunque $MCD(341, 912) = 1$ |15 e la congruenza ha soluzione.

Se troviamo una coppia (X, Y) che risolve l'equazione diofantea

$$341X - 912Y = 15$$

allora la X sarà una soluzione particolare della nostra congruenza. Per il teorema sulla soluzione delle congruenze lineari sappiamo che tutte le soluzioni della congruenza si ottengono sommando a X i multipli di 912.

Cerchiamo dunque una soluzione particolare della diofantea. Scriviamo i resti dell'algortmo di Euclide:

$$230 = 912 - 341 \cdot 2$$

$$111 = 341 - 230$$

$$8 = 230 - 111 \cdot 2$$

$$7 = 111 - 8 \cdot 13$$

$$1 = 8 - 7$$

Ora, sostituendo i resti uno dopo l'altro, possiamo trovare una combinazione di Bezout:

$$1 = 341m + 912n$$

poi $15m = X$ sarà la soluzione particolare che stiamo cercando. Dunque in realtà di questa combinazione di Bezout a noi interessa solo la m che dovrà poi (moltiplicata per 15) comparire in una congruenza modulo 912. Per questo possiamo semplificare i conti riducendo i nostri passaggi modulo 912, ottenendo alla fine

$$1 \equiv 341m \quad (912)$$

Ecco qui:

$$1 = 8 - 7 = 8 - (111 - 8 \cdot 13) = -111 + 14 \cdot 8 = -111 + (230 - 111 \cdot 2)14 =$$

$$= -29 \cdot 111 + 14 \cdot 230 = -29(341 - 230) + 14 \cdot 230 = 43 \cdot 230 - 29 \cdot 341 =$$

$$= 43(912 - 341 \cdot 2) - 29 \cdot 341 \equiv$$

(da questo punto in poi semplifichiamo passando alle congruenze modulo 912)

$$\equiv -86 \cdot 341 - 29 \cdot 341 \equiv -115 \cdot 341 \quad (912)$$

Dunque

$$1 \equiv -115 \cdot 341 \quad (912)$$

da cui, moltiplicando per 15 otteniamo

$$15 \equiv -115 \cdot 15 \cdot 341 \quad (912)$$

e deduciamo che $-115 \cdot 15$ è una soluzione particolare di

$$341x \equiv 15 \quad (912)$$

L'insieme di tutte le soluzioni è allora dato da

$$x \equiv -115 \cdot 15 \equiv -1725 \equiv 99 \quad (912)$$

che si può scrivere anche come

$$\{99 + 912q \mid q \in \mathbb{Z}\}$$

25. Il piccolo teorema di Fermat.

Daremo in questa sezione due dimostrazioni (facoltative, molto raccomandate!), entrambe belle e istruttive, del piccolo teorema di Fermat (l'enunciato fa parte del programma del corso), accompagnate da qualche commento. La prima è la dimostrazione svolta in classe.

Teorema ("il piccolo teorema di Fermat"). Se p è un numero primo e a è un numero intero che non è un multiplo di p, allora vale

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

Dimostrazione. Consideriamo l'anello $\mathbb{Z}_p$ delle classi di resto modulo p:

$$\mathbb{Z}_p = \{[0], [1], \ldots, [p-1]\}$$

Vista la scelta di a, sappiamo che $[a] \neq [0]$. Moltiplichiamo ora tutti gli elementi di $\mathbb{Z}_p$ per $[a]$:

$$[a][0], [a][1], \ldots, [a][p-1]$$

ossia, per la definizione di prodotto in $\mathbb{Z}_p$,

$$[a \cdot 0], [a \cdot 1], \ldots, [a \cdot (p-1)]$$

Questi p elementi sono tutti diversi fra loro ? Se la risposta è sì, allora sappiamo che sono esattamente tutti gli elementi di $\mathbb{Z}_p$, che ha proprio cardinalità p.

Verifichiamo dunque che sono tutti diversi fra loro: supponiamo, per assurdo, che esistano i e j, con $0 \leq i < j \leq p-1$, tali che $[a \cdot i] = [a \cdot j]$.

Osservazione. In classe abbiamo visto che $\mathbb{Z}_p$ è un campo, dato che p è primo. Ricordiamo il perché: se prendiamo una classe $[a] \neq [0]$ in $\mathbb{Z}_p$, essendo $MCD\ (a,p) = 1$ allora la congruenza $ax \equiv 1 \quad (p)$ ha soluzione, dunque esiste $b \in \mathbb{Z}$ tale che $ab \equiv 1 \quad (p)$. Come conseguenza in $\mathbb{Z}_p$ vale $[a][b] = [ab] = [1]$. Abbiamo allora dimostrato che $[a]$ è invertibile in $\mathbb{Z}_p$ e che $[b]$ è il suo inverso.

Sia dunque $[b]$ l'inverso di $[a]$. Moltiplicando per $[b]$ otteniamo:

$$[b][a \cdot i] = [b][a \cdot j]$$

che si riscrive

$$[b][a][i] = [b][a][j]$$

Siccome $[b][a] = [1]$ (stiamo utilizzando anche la proprietà associativa) allora abbiamo

$$[i] = [j]$$

Poiché però i e j sono numeri naturali strettamente minori di p deve valere $i = j$. ASSURDO, dato che avevamo supposto $i \neq j$.

Dunque la lista

$$[a \cdot 0], [a \cdot 1], \ldots, [a \cdot (p-1)]$$

comprende esattamente tutti gli elementi di $\mathbb{Z}_p$. Allora se facciamo il prodotto degli elementi della lista, eccetto $[a \cdot 0] = [0]$, deve valere:

$$[a \cdot 1] \cdots [a \cdot (p-1)] = [1][2][3] \cdot [p-1]$$

visto che nel membro di sinistra e in quello di destra abbiamo gli stessi elementi (che compaiono magari in ordine diverso). Scritto in termini di congruenze questo significa:

$$(a \cdot 1) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdot (p-1) \qquad (p)$$

che si riscrive

$$a^{p-1}(p-1)! \equiv (p-1)! \qquad (p)$$

Visto che $(p-1)!$ è primo con p possiamo dividere (vedi "regole per lavorare con le congruenze") e troviamo

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

che è l'enunciato del piccolo teorema di Fermat. ■

Diamo adesso una diversa dimostrazione del piccolo teorema di Fermat dovuta ad Eulero.

Dimostrazione (Eulero). Per prima cosa dimostriamo che p divide $\left(\begin{array}{c} p \\ i \end{array} \right)$ quando $0 < i < p$. Infatti sappiamo che

$$\left(\begin{array}{c} p \\ i \end{array} \right) i!\ (p-i)! = p!$$

e, per il teorema di decomposizione unica in prodotto di fattori primi, p, che divide il membro di destra, deve dividere il membro di sinistra. Poiché p non può dividere $i!\ (p-i)!$ (che sono prodotti di numeri positivi strettamente minori di p) possiamo dedurre, per la proprietà caratterizzante dei numeri primi (ossia quella che dice che se p è primo e divide un prodotto ab allora p deve dividere a o p deve dividere b), che p deve dividere $\left(\begin{array}{c} p \\ i \end{array} \right)$.

A questo punto possiamo osservare che, dati due numeri interi a e b, lo sviluppo del binomio $(a+b)^p$ ha, modulo p, una scrittura molto semplificata. Infatti vale

$$(a+b)^p = \sum_{i=0}^{p} \left(\begin{array}{c} p \\ i \end{array} \right) a^i b^{p-i} \equiv a^p + b^p \qquad (p)$$

dato che, appunto, p divide tutti i coefficienti $\left(\begin{array}{c} p \\ i \end{array} \right)$ $(1 < i < p)$.

In particolare, nel caso $b = 1$, abbiamo

$$(a+1)^p \equiv a^p + 1 \qquad (p)$$

Ora proviamo che, per ogni $a \in \mathbb{Z}$ vale

$$a^p \equiv a \quad (p)$$

Questa relazione, nel caso in cui a non è multiplo di p, ci dà (dividendo per a) l'enunciato del teorema.

Ci basta dimostrare che, per ogni $a \in \mathbb{N}$,

$$a^p \equiv a \quad (p)$$

(il caso dei numeri negativi si ricava poi immediatamente).

Lo dimostriamo per induzione su a.

Il caso base, per $a = 0$,

$$0^p \equiv 0 \quad (p)$$

è banale.

Supponiamo ora che questa relazione sia vera fino ad $a = n$ e proviamo a dimostrare che

$$(n+1)^p \equiv n+1 \quad (p)$$

(se ci riusciamo la nostra dimostrazione è terminata).

Ora, per quanto visto sopra possiamo scrivere che

$$(n+1)^p \equiv n^p + 1 \quad (p)$$

Ma, per ipotesi induttiva, $n^p \equiv n \quad (p)$ per cui

$$(n+1)^p \equiv n+1 \quad (p)$$

■

Esempio di applicazione del piccolo teorema di Fermat. Se vogliamo calcolare

$$15^{1443} \equiv ? \quad (17)$$

possiamo utilizzare il piccolo teorema di Fermat che ci dice che

$$15^{16} \equiv 1 \quad (17)$$

Ora $1443 = 16 \cdot 90 + 3$ dunque

$$15^{1443} \equiv (15^{16})^{90}\, 15^3 \equiv 1^{90}\, 15^3 \quad (17)$$

Ma $15 \equiv -2 \quad (17)$ dunque

$$15^{1453} \equiv (-2)^3 \equiv -8 \equiv 9 \quad (17)$$

Esempio nel caso in cui il modulo non è primo. Se p non è primo, l'enunciato del piccolo teorema di Fermat non vale più: non è vero, per esempio, che $2^5 \equiv 1 \quad (6)$. Infatti

$$2^5 = 32 \equiv 2 \quad (6)$$

Osserviamo che, nel corso della seconda dimostrazione del teorema abbiamo dimostrato un enunciato leggermente modificato, ossia una formula che vale anche per la classe $[0]$. Visto che la ritroviamo frequentemente nelle applicazioni, riproponiamo di nuovo qui questa formula sotto forma di corollario, e la ridimostriamo, a vantaggio di coloro che non hanno letto la seconda dimostrazione.

Corollario. Se p è un numero primo, per ogni numero intero a vale

$$a^p \equiv a \quad (p)$$

Dimostrazione. Infatti, se a non è multiplo di p per Fermat vale:

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

Moltiplicando entrambi i membri per a otteniamo l'enunciato. Se invece a è un multiplo di p allora $a \equiv 0 \quad (p)$ e dunque

$$a^p \equiv 0 \equiv a \quad (p)$$

■

Questo ci dà un criterio per decidere se un numero non è primo:

Corollario. Se $n > 1$ è un numero intero tale che per qualche numero intero a vale

$$a^n \neq a \quad (n)$$

allora n non è primo.

Dimostrazione. È vero perché si tratta della contronominale del corollario precedente!
■

È interessante capire se con questi ragionamenti si può trovare un criterio per dire con certezza se un numero è primo (non solo per dire se un numero NON è primo).
Saremmo infatti tentati di pensare che se prendiamo un numero intero $n > 1$ e scopriamo che per tutti i numeri interi a vale

$$a^n \equiv a \quad (n)$$

allora n è primo. Questo non è vero: ci sono infiniti numeri che soddisfano questa proprietà ma NON SONO PRIMI. Si chiamano "numeri di Carmichael" o "falsi primi". In classe, per esempio, abbiamo dato la traccia per dimostrare che 561 è un numero di Carmichael (un altro è 1729: esercizio...).