Appunti provvisori del corso di LMM

Alessandro Berarducci

Questi appunti sono in corso d'opera e ancora molto imperfetti. Puo' tuttavia essere utile consultarli per i primi due capitoli e per il capitolo sull'aritmetica. Per gli argomenti mancanti si vedano gli appunti di Gaiffi.

12 dicembre

Indice

CAPITOLO 1

Proposizioni e connettivi

"La matematica non si capisce, alla matematica ci si abitua." von Neumann.

Una **proposizione** è un enunciato di cui nel dato contesto ha senso chiedersi (o affermare, o ipotizzare) se esso sia vero o falso. Ad esempio "$3 > 2$" è una proposizione vera, mentre "$2 > 3$" è una proposizione falsa [1]. Assumiamo la concezione classica secondo cui una proposizione è o vera o falsa (principio del terzo escluso), ma non può essere sia vera che falsa (principio di non contraddizione).

Esercizio 0.1. Quali delle seguenti è una proposizione?

(1) L'assassino è l'autista.
(2) Posso avere un'altra brioche?
(3) Non ti permetto di parlarmi in questo modo.
(4) $x > y$.

Soluzione: la (1) è una proposizione. La (2) e la (3) non lo sono. La (4) è più problematica. Chiaramente non possiamo stabilire se l'enunciato $x > y$ sia vero o falso non sapendo chi siano x ed y. Tuttavia esistono contesti in cui ha senso *ipotizzare* che $x > y$ sia vero (assumendo implicitamente che x, y siano numeri reali). Ad esempio può capitare nel corso di una dimostrazione di ipotizzare che $x > y$ sia vero per concluderne che $y > x$ è falso, o che $3x > 3y$ è anch'esso vero. Secondo le nostre definizioni in tale contesto la (4) va quindi considerata una proposizione.

1. Tavole di verità

I **connettivi booleani** sono usati per costruire proposizioni complesse a partire da proposizioni semplici. Nella formalizzazione del linguaggio matematico i connettivi di cui faremo maggiore uso sono indicati con i simboli $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$. La loro traduzione approssimativa in italiano è la seguente:

"$\neg A$" significa "non A" (negazione),
"$A \wedge B$" significa "A e B" (congiunzione),
"$A \vee B$" significa "A o B" (disgiunzione),
"$A \rightarrow B$" significa "se A, allora B" (implicazione),
"$A \leftrightarrow B$" significa "A se e solo se B" (doppia implicazione).

Le lettere A, B sopra usate indicano generiche proposizioni. Ad una proposizione associamo il **valore di verità 1** o **0** a seconda che essa sia vera o falsa.

I connettivi booleani sono *vero-funzionali* nel senso che il valore di verità di una proposizione composta dipende solo dal valore di verità delle proposizioni semplici che la costituiscono. Questo avviene secondo le seguenti **tavole di verità** che precisano il significato dei connettivi.

[1] Alcuni sostengono che una proposizione è espressa da un enunciato ma non può essere identificata con l'enunciato che la esprime. Ad esempio "oggi piove" e "today it rains" esprimono la stessa proposizione in lingue diverse. Per semplicità trascuriamo di fare queste distinzioni.

A	$\neg A$
0	**1**
1	**0**

La tavola dice che la proposizione $\neg A$ è vera se A è falsa, ed è invece falsa se A è vera. La negazione inverte il valore di verità. Diamo ora le tavole degli altri connettivi.

A	B	$A \wedge B$	$A \vee B$	$A \to B$	$A \leftrightarrow B$
0	**0**	**0**	**0**	**1**	**1**
0	**1**	**0**	**1**	**1**	**0**
1	**0**	**0**	**1**	**0**	**0**
1	**1**	**1**	**1**	**1**	**1**

Le prime due colonne indicano i quattro possibili valori di verità di A e B. Le altre colonne indicano i corrispondenti valori degli enunciati composti $A \wedge B$, $A \vee B$, $A \to B$, $A \leftrightarrow B$.

La tavola di verità del connettivo $\wedge$ dice che $A \wedge B$ è vera se e solo se sia A che B sono vere.

La tavola di verità del connettivo $\vee$ dice che $A \vee B$ è vera se almeno uno di A e B è vero, senza escludere la possibilità che entrambi siano veri. Questa modalità di disgiunzione corrisponde al "vel" della lingua latina e viene chiamata *disgiunzione inclusiva*.

La tavola del $\leftrightarrow$ dice che $A \leftrightarrow B$ è vera se A e B si **equivalgono**, ovvero sono entrambe vere o entrambe false. Scriveremo anche

$$A \iff B$$

per affermare che A e B sono tra loro equivalenti.

Dalla tavola dell'implicazione $\to$ risulta che $A \to B$ è falsa solo nel caso in cui la premessa A è vera e il conseguente B è falso. In particolare se la premessa A è falsa, l'enunciato $A \to B$ è sempre vero a prescindere da quale sia l'enunciato B: da una premessa falsa segue ogni proposizione. L'implicazione così definita viene detta **implicazione materiale**. Scriveremo anche

$$A \Longrightarrow B$$

per affermare che A implica B, ovvero che l'implicazione $A \to B$ è vera.[2].

Oltre alla disgiunzione inclusiva $A \vee B$ esiste anche una *disgiunzione escusiva*, corrispondente all' "aut" latino, che indichiamo con il simbolo $\oplus$ ed è definita dalla seguente tavola di verità:

[2]C'è una piccola sfumatura di significato tra $A \to B$ e $A \Longrightarrow B$. Con $A \Longrightarrow B$ stiamo *affermando* $A \to B$, ovvero stiamo dicendo che $A \to B$ è vera. Similmente con $A \iff B$ stiamo dicendo che $A \leftrightarrow B$ è vera. In molti casi non c'è differenza tra scrivere una cosa e affermare che è vera, quindi spesso useremo indifferentemente $\to$ o $\Longrightarrow$ (e similmente per $\leftrightarrow$ e $\iff$). Un caso in cui è però importante fare una distinzione è quando diciamo ad esempio che $A \leftrightarrow B$ equivale a $(A \to B) \wedge (B \to A)$. Conviene scrivere tale affermazione nella forma

$$(A \leftrightarrow B) \iff ((A \to B) \wedge (B \to A))$$

per far capire che stiamo parlando di due formule (quelle a sinistra e a destra del $\iff$), e sarebbe invece fonte di confusione scrivere la singola formula $(A \leftrightarrow B) \leftrightarrow ((A \to B) \wedge (B \to A))$. Non è importante che si seguano esattamente queste convenzioni, ma è importante fare le distinzioni necessarie. Ad esempio molti autori non usano mai $\to, \leftrightarrow$ e usano $\Longrightarrow$, $\iff$ al loro posto, ma in tal caso se si vuole dire in simboli che due formule sono equivalenti occorre introdurre un'altra notazione.

A	B	$A \oplus B$
0	**0**	**0**
0	**1**	**1**
1	**0**	**1**
1	**1**	**0**

La disgiunzione esclusiva può essere espressa usando i connettivi precedentemente incontrati:

ESEMPIO 1.1. $A \oplus B$ equivale a $(A \vee B) \wedge \neg(A \wedge B)$.

2. Esempi

Il sequente esempio illustra le tavole delle congiunzione e della disgiunzione.

ESEMPIO 2.1. Siano x, y numeri reali.

(1) La proposizione "$xy = 0$" equivale a "$(x = 0) \vee (y = 0)$".
(2) La proposizione "$|x| = 3$" equivale a "$|x| = 3 \vee |x| = -3$".
(3) La proposizione "$|x| < 3$" equivale a "$-3 < x \wedge x < 3$".

I seguenti due esempi illustrano la tavola di verità dell'implicazione.

ESEMPIO 2.2. Supponiamo che il signor Rossi dica: "se vinco alla lotteria vado a fare il giro del mondo." Questo corrisponde alla proposizione $A \to B$ dove $A =$ vinco alla lotteria, $B =$ vado a fare il giro del mondo. Cè un unico caso in cui possiamo affermare che il signor Rossi dice una cosa falsa: quando per l'appunto A è vera e B è falsa, ovvero lui vince alla lotteria, ma ciò nonostante non va a fare il giro del mondo. In tutti gli altri casi, compreso il caso in cui va a fare il giro del mondo pur non avendo vinto, non possiamo dire che abbia mentito. Ciò è in accordo con la tavola dell'implicazione.

ESEMPIO 2.3. Dato un numero reale x, consideriamo l'enunciato:

$$x > 2 \to x^2 > 4$$

L'uso comune in matematica è di considerare tale enunciato sempre vero, cioè vero qualsiasi sia il valore di x. Questo però significa che dobbiamo considerarlo vero non solo per i valori di x maggiori di 2, ma anche ad esempio per $x = 1$, ovvero anche in quei casi in cui la premessa $x > 2$ è falsa. Questo è in accordo con la tavola del connettivo $\to$.

Il seguente esempio mostra che non sempre le tavole si accordano perfettamente con l'uso che si fa in italiano dei connettivi.

ESEMPIO 2.4. Date due proposizioni A, B, in base alle tavole $A \wedge B$ equivale a $B \wedge A$. Tuttavia questo non sempre concorda con l'uso della congiunzione "e" in italiano. Ad esempio si confronti "ho preso la medicina e mi sono sentito male" con "mi sono sentito male e ho preso la medicina". È presumibile che chi pronuncia queste frasi intenda "e" nel senso di "e poi". In un simile contesto una delle due proposizioni può essere vera e l'altra falsa.

La seguente definizione fornisce un altro modo di leggere l'implicazione:

DEFINIZIONE 2.5. Se $A \implies B$, diciamo che A è una **condizione sufficiente** per B, e che B è una **condizione necessaria** per A. Ovvero per poter asserire B è sufficiente che A sia vera, e affinché A sia vera è necessario che lo sia anche B.

ESEMPIO 2.6. Siano a, b, c tre numeri reali e supponiamo di sapere che $a > b$. La condizione aggiuntiva $b \geq c$ è sufficiente per poter concludere $a > c$? È anche necessaria?

Soluzione: $b \geq c$ è sufficiente, ma non necessaria: infatti, fermo restando che $a > b$, la tesi $a > c$ potrebbe essere vera anche se b non fosse maggiore o uguale a c (ad esempio $a = 10, c = 5, b = 4$). Possiamo quindi asserire che vale l'implicazione $(a > b \wedge b \geq c) \rightarrow a > c$, ma non l'implicazione inversa.

ESEMPIO 2.7. $xy = 0$ equivale a $(x = 0) \vee (y = 0)$, ma in generale non equivale a $(x = 0) \oplus (y = 0)$. Infatti se $x = y = 0$ abbiamo che $xy = 0$ è vera mentre $(x = 0) \oplus (y = 0)$ è falsa.

ESEMPIO 2.8. Dati due numeri reali x, y le seguenti proposizioni sono equivalenti:

(1) $x \leq 3$;
(2) $(x < 3) \vee (x = 3)$;
(3) $(x < 3) \oplus (x = 3)$.

Infatti se $x \leq 3$, allora o $x < 3$ o $x = 3$, e chiaramente non valgono entrambe le alternative. Quindi la (1) equivale alla (3). D'altra parte equivale anche alla (2) in quanto l'unico caso in cui $A \vee B$ non equivale a $A \oplus B$ è quando A, B sono entrambe vere, ma questo non può verificarsi nel nostro esempio. Infatti comunque si scelga x, non può capitare che $x < 3$ e $x = 3$ siano entrambe vere (stiamo naturalmente dando per note queste proprietà del $<$).

3. Equivalenze notevoli

Diamo alcune equivalenze che si possono verificare applicando le tavole di verità.

ESEMPIO 3.1. $A \leftrightarrow B$ equivale a $(A \rightarrow B) \wedge (B \rightarrow A)$.

ESEMPIO 3.2. Date due proposizioni A e B le sequenti proposizioni si equivalgono:

(1) $A \rightarrow B$;
(2) $\neg A \vee B$;
(3) $\neg B \rightarrow \neg A$".

Ad esempio: "Se non è zuppa è pan bagnato" equivale a: "O è zuppa o è pan bagnato", ed anche a "Se non è pan bagnato è zuppa".

ESEMPIO 3.3. (1) $\neg(A \rightarrow B)$ equivale a $(A \wedge \neg B)$.
(2) $\neg(a \rightarrow \neg B)$ equivale a $(A \wedge B)$.

Come esempio della (2) sia $A =$ dormo, $B =$ piglio pesci. La proposizione "non è vero che se dormo non piglio pesci" equivale a "dormo e piglio pesci".

ESERCIZIO 3.4. Date tre proposizioni p, q, r valgono le seguenti equivalenze:

- Leggi di idempotenza:
  $p \wedge p \iff p$;
  $p \vee p \iff p$;
- Legge della doppia negazione: $\neg(\neg p) \iff p$;
- Leggi commutative:
  $p \wedge q \iff q \wedge p$;
  $p \vee q \iff q \vee p$;
- Leggi associative:
  $(p \wedge q) \wedge r \iff p \wedge (q \wedge r)$;
  $(p \vee q) \vee r \iff p \vee (q \vee r)$;

- Leggi distributive:
  $p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$;
  $p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$;
- Leggi di De Morgan: $\neg(p \wedge q) \iff (\neg p \vee \neg q)$;
  $\neg(p \vee q) \iff (\neg p \wedge \neg q)$;
- Leggi di assorbimento:
  $p \vee (p \wedge q) \iff p$,
  $p \wedge (p \vee q) \iff p$.

Esercizio 3.5. Sia t una proposizione vera, e sia f una proposizione falsa. Valgono le seguenti equivalenze:

- $t \wedge p \iff p$;
- $t \vee p \iff t$;
- $f \wedge p \iff p$;
- $f \vee p \iff p$.

Esercizio 3.6. Usando le leggi di De Morgan esprimere le negazioni di $x \in (a, b)$ e di $|x| = a$.

Soluzione: ($x \in (a, b)$ significa $a < x \wedge x < b$. La sua negazione $\neg(x \in (a, b))$ equivale a $\neg(a < x) \vee \neg(x < b)$, cioè $x \leq a \vee b \leq x$.

$|x| = 3$ significa $x = 3 \vee x = -3$. La sua negazione $\neg(|x| = 3)$ equivale a $x \neq 3 \wedge x \neq -3$. (Dove $x \neq y$ sta per $\neg(x = y)$.)

4. Esercizi

Esercizio 4.1. $a < b$ implica $4ab < (a + b)^2$.
Suggerimento: Conviene ragionare "all'indietro", cioè partiamo dalla conclusione e vediamo da cosa è implicata.

Esercizio 4.2. Quali implicazioni valgono tra:

$$(a \geq c) \wedge (b \geq d)$$
$$a + b \geq c + d$$

Soluzione: la prima implica la seconda. La seconda non implica sempre la prima. Ad esempio se $a = 10, b = 3, c = 4, d = 5$ la seconda è vera ma la prima è falsa.

Esempio 4.3. Ricordiamo che $|x| = x$ se $x \geq 0$, $|x| = -x$ se $x \leq 0$. Sono equivalenti:
$|x| = a$
$x = a \vee x = -a$
$|x| = |a|$
$x^2 = a^2$.

Esercizio 4.4. Esprimere la relazione $x^2 \geq y^2$ senza usare i quadrati.

Soluzione: Equivale a $|x| \geq |y|$, che a sua volta equivale a $x \geq |y| \vee x \leq -|y|$, che a sua volta equivale a $(y \geq 0 \wedge x \geq y) \vee (y \leq 0 \wedge x \geq -y) \vee (y \geq 0 \wedge x \leq -y) \vee (y \leq 0 \wedge x \leq y)$. Disegnare le regioni corrispondenti sul piano degli assi coordinati x, y.

Esercizio 4.5. Trovare le formule equivalenti:

$$\tfrac{1}{3}x^3 \geq 3x^2$$
$$x \geq 9$$
$$x \geq 9 \vee x = 0$$
$$x \geq 9 \wedge x \neq 0$$
$$x \neq 0 \to x \geq 9$$

Stabilire inoltre quali implicazioni valgono tra le formule precedenti.

Soluzione: $x \geq 9$ implica $\frac{1}{3}x^3 \geq 3x^2$ ma non viceversa.

La formula $\frac{1}{3}x^3 \geq 3x^2$ equivale a $x \geq 9 \vee x = 0$. Infatti se prendiamo $x = 0$ sono entrambe vere. Anche nel caso $x \geq 9$ sono entrambe vere. Nel rimanente caso, ovvero per x minore di 9 ma diverso da zero, sono entrambe false.

Analogamente si stabilisce che la prima, la terza e la quinta sono equivalenti, e sono tutte e tre implicate dalla seconda. La quarta implica tutte le altre. E ovviamente ogni formula implica anche se stessa.

Esercizio 4.6. Esprimere i seguenti enunciati usando la relazione d'ordine $\geq$ e i connettivi ma senza usare max e min: $x \geq \max\{a, b\}$, $x \geq \min\{a, b\}$, $\max\{a, b\} \geq \max\{a, b\}$, $\max\{a, b\} \geq \min\{a, b\}$, $\min\{a, b\} \geq \max\{a, b\}$, $\min\{a, b\} \geq \min\{a, b\}$.

5. Formule e tautologie

Una espressione come $\neg(A \vee B)$ può essere considerata in due modi: (1) Se si pensano A, B come proposizioni che si suppongono fissate (seppure non specificate), allora $\neg(A \vee B)$ è essa stessa una proposizione; (2) Se invece si pensano A, B come a variabili al posto delle quali possiamo sostituire proposizioni arbitrarie, allora $\neg(A \vee B)$ non è una proposizione ma è un esempio di "formula proposizionale", ovvero è uno schema astratto da cui possiamo ottenere infinite proposizioni per sostituzione.

Definizione 5.1. Una **formula proposizionale** è una espressione costruito a partire da certe "variabili proposizionali" $A, B, C, \ldots$ i connettivi $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$, e le parentesi, da cui possiamo ottenere infinite proposizioni sostituendo le variabili proposizionali con proposizioni vere e proprie. In particolare ciascuna variabile proposizionale $A, B, C, \ldots$ è essa stessa una formula proposizionale, e se ϕ e ψ sono formula proposizionali lo sono anche $\neg\phi$, $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \rightarrow \psi)$, $(\phi \leftrightarrow \psi)$. Niente altro è una formula proposizionale se non ciò che si ottiene con una applicazione ripetuta di queste regole.

Definizione 5.2. Una formula proposizionale ϕ si dice una **tautologia** se è vera per ogni valore delle sue variabili, cioè otteniamo una proposizione vera comunque sostituiamo delle proposizioni al posto delle sue variabili. Una formula proposizionale ϕ è **contraddittoria** se è falsa per ogni valore delle sue variabili, ovvero se la sua negazione ϕ è una tautologia.

Ad esempio $A \vee \neg A$ è una tautologia, in quanto risulta vera sia nel caso in cui A è una proposizione vera, sia nel caso in cui A è una proposizione falsa. Analogamente $(A \rightarrow B) \wedge \neg B \rightarrow \neg A$ è una tautologia, in quanto usando le tavole si vede che essa risulta vera nei quattro possibili casi per i valori di A e B (A vera e B vera, A vera e B falsa, A falsa e B vera, A falsa e B falsa). Un metodo per riconoscere se una formula con n variabili proposizionali è una tautologia è quello di considerare i 2^n possibili casi per i valori di verità delle sue variabili e verificare usando le tavole che in ognuno dei casi la proposizione composta che ne risulta è vera.

Osservazione 5.3. Esistono altri metodi per controllare se una formula è una tautologia, ma tutti i metodi noti richiedono una quantità di passaggi esponenziale al crescere del numero delle variabili. Il problema di stabilire se esistano metodi più efficienti (che permettano di riconoscere le tautologie in tempo polinomiale anziché esponenziale) è tuttora irrisolto.

DEFINIZIONE 5.4. Una proposizione ottenuta per sostituzione da una tautologia sarà anch'essa detta tautologia, e una proposizione ottenuta per sostituzione da una formula proposizionale contradditoria sarà essa stessa detta contraddittoria.

Ad esempio la proposizione "piove $\vee$ $\neg$piove" è una tautologia essendo ottenuta per sostituzione dalla tautologia $A \vee \neg A$. Come si vede da questo esempio una tautologia ha contenuto informativo nullo. Affermare "piove o non piove" non ci dà alcuna informazione sul fatto se piova o meno. In generale un enunciato che esprime una tautologia è vero a prescindere dalla verità o falsità degli enunciati elementari che lo costituiscono, e quindi non comunica nulla riguardo alla verità o falsità di questi ultimi. Una tautologia è vera in virtù esclusivamente della sua forma sintattica, e non del suo contenuto. Visto che non comunicano informazione, è lecito domandarsi a cosa servano le tautologie. Una possibile risposta è che esse giocano un ruolo importante nelle argomentazioni logiche. Consideriamo il seguente esempio:

ESEMPIO 5.5. L'assassino è il professore o l'assessore. Ma non è l'assessore. Quindi è il professore.

Per condurre questo ragionamento, cioè per mostrare che la tesi è implicata logicamente delle premesse, abbiamo implicitamente utilizzato la tautologia $((A \vee B) \wedge \neg B) \rightarrow A$, applicandola al caso in cui A sta per "l'assassino è il professore", e B sta per "l'assassino è l'assessore".

DEFINIZIONE 5.6. Due formule proposizionali ϕ e ψ si dicono **logicamente equivalenti**, e scriviamo in tal caso $\phi \iff \psi$ (oppure $A \equiv B$), se la formula $\phi \leftrightarrow \psi$ è una tautologia. Questo avviene se e solo se ϕ e ψ hanno la stessa tavola di verità, cioè se forniscono lo stesso valore di verità per qualsiasi valore $\mathbf{1}, \mathbf{0}$ che sia assegnato alle loro variabili. Ad esempio $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$ (legge distributiva della congiunzione sulla disgiunzione), come si può verificare assegnando ad A, B, C i valori $\mathbf{1}, \mathbf{0}$ negli otto modi possibili e verificando che in ciascun caso il valore di $A \wedge (B \vee C)$ è uguale a quello di $(A \wedge B) \vee (A \wedge C)$. Analogamente si ritrovano le altre equivalenze notevoli (legge di De Morgan etc.) già precedentemente viste.

DEFINIZIONE 5.7. Una formula proposizionale ϕ **implica formalmente** (o **logicamente**) un'altra formula proposizionale ψ se la formula $\phi \rightarrow \psi$ è una tautologia. Scriviamo in tal caso $A \Longrightarrow B$. Questo equivale a dire che per tutti i valori delle variabili per cui ϕ assume il valore $\mathbf{1}$, anche ψ assume il valore $\mathbf{1}$ (ma ψ potrebbe assumere il valore $\mathbf{1}$ in un numero maggiore di casi). Ad esempio $A \wedge B$ implica logicamente $A \vee B$, in quanto nei casi in cui $A \wedge B$ risulta vera (ovvero nell'unico caso $A + B =$ vero), anche $A \vee B$ risulta vera. Osserviamo che due formule sono equivalenti se l'una implica logicamente l'altra e viceversa.

OSSERVAZIONE 5.8. Mentre a livello di proposizioni abbiamo usato indifferentemente $\rightarrow$ o $\Longrightarrow$, quando si parla di formule proposizionali il discorso si fa per l'appunto formale e dobbiamo quindi essere precisi riguardo alla distinzione tra $\rightarrow$ e $\Longrightarrow$ (e similmente tra $\leftrightarrow$ e $\equiv$). I simboli $\rightarrow$ e $\leftrightarrow$ vengono usati all'interno delle formule, mentre $\leftrightarrow$ e $\equiv$ (o $\iff$) vengono usati per fare delle affermazioni riguardo alle formule. Ad esempio se ϕ, ψ sono formule proposizionali, allora $\phi \rightarrow \psi$ è una formula proposizionale, e in quanto tale non ha senso chiedersi se sia vera o falsa, ovvero potrebbe risultare vera per certi valori delle sue variabili proposizionali e falsa per altri. Quando invece scriviamo $\phi \Longrightarrow \psi$ stiamo affermando che $\phi \rightarrow \psi$ è una tautologia, e questa è una affermazione di cui, una volta date ϕ e ψ, possiamo stabilire se sia vera o falsa. Ad esempio $(A \vee B) \Longrightarrow (A \wedge B)$ è falsa (cioè è falso che $(A \vee B) \rightarrow (A \wedge B)$ sia una tautologia). Non avrebbe invece

senso affermare che la formula $(A \vee B) \rightarrow (A \wedge B)$ in quanto tale è falsa: l'unica cosa che possiamo dire in questo caso è che essa risulta vera per certi valori delle variabili (ad esempio $A = B =$ vero) e falsa per altri (ad esempio $A =$ vero, $B =$ falso).

CAPITOLO 2

Predicati e quantificatori

1. Predicati, variabili e parametri

Un **predicato** P associa a ciascun elemento x di di un fissato dominio di oggetti una proposizione $P(x)$, che può essere vera o falsa. Ad esempio se P è il predicato "essere un numero primo" ed x è un numero, allora $P(x)$ è la proposizione "x è un numero primo". Useremo anche il termine "**relazione**" come sinonimo di "predicato". Il termine relazione suggerisce una pluralità di soggetti che per l'appunto stanno in relazione, e quindi verrà impiegato preferibilmente per i predicati a più argomenti. Ad esempio il predicato "è minore di" tra numeri reali associa a ciascuna coppia ordinata (x, y) di numeri reali la proposizione "$x < y$", che sarà ovviamente vera o falsa a seconda di come si scelgono x ed y. In generale se P è una relazione ad n posti dovrà essere applicata ad n argomenti per ottenere una proposizione. Così ad esempio se P è un predicato a tre posti, ed x, y, z sono nel dominio specificato, allora $P(x, y, z)$ sarà una proposizione che afferma che la terna (x, y, z) verifica la relazione.

Quando scriviamo una formula come $x < y$, i termini x ed y possono essere pensati come sia come **parametri**, ovvero numeri reali che si suppongono fissati (seppure non esplicitati), sia come **variabili**. Nel primo caso $x < y$ rappresenta una proposizione, vera o falsa a seconda di chi siano x, y. Nel secondo caso si può essere tentati di pensare che $x < y$ rappresenti semplicemente la relazione "essere minore di" che associa ad ogni coppia di numeri reali (a, b) la proposizione $a < b$. Ad esempio uno potrebbe dire che la relazione $x < y$ è verificata dalla coppia $(1, 2)$. Questo però è impreciso perché si sta dando per scontato che 1 va al posto di x e 2 al posto di y. Sarebbe più corretto dire che $x < y$ rappresenta la relazione "x è minore di y", verificata da $x = 1, y = 2$. In generale per poter associare una relazione ad una espressione complicata come $xe^n + x^m > x \cdot e$ bisogna specificare: 1) quali sono le variabili, 2) dove variano, 3) in che ordine vadano considerate. Ad esempio se si decide che le variabili sono e, x in quest'ordine (e che n, m sono parametri) allora l'espressione rappresenta la relazione che ad ogni coppia di numeri reali (a, b) associa la proposizione $ba^n + b^m > b \cdot a$ ottenuta sostituendo il numero a al posto della variabile e e il numero b al posto della variabile x.

I seguenti esempi presuppongono qualche conoscenza dell'algebra e dell'analisi matematica.

Esempio 1.1. Trovare la derivata delle funzioni a^x ed x^a. Soluzione: la prima è $\log(a)a^x$, la seconda è ax^{a-1}. Chi è la variabile e chi è il parametro?

Esempio 1.2. Risolvere l'equazione $ax = 1/a + x$. Soluzione: $x = \frac{1}{a(a-1)}$. Chi è la variabile e chi è il parametro?

Esempio 1.3. Trovare il limite della derivata di $a\pi x + \pi x$ per a tendente a zero. Soluzione: la derivata è $a\pi + \pi$ e il suo limite è π. Chi è la costante, chi è il parametro, chi è la variabile? La questione è sottile: il termine a si tiene fisso quando si fa la derivata $\frac{\partial a\pi x + \pi x}{\partial x} = a\pi + \pi$ e quindi in questa espressione a gioca il ruolo di parametro. Quando

però si calcola il limite $\lim_{a\to 0} a\pi+\pi = \pi$ il termine a gioca il ruolo di variabile (si dice che a è una variabile libera nell'espressione $a\pi+\pi$ ed è una variabile legata in $\lim_{a\to 0} a\pi+\pi$).

2. Quantificatori

Introduciamo ora i quantificatori $\forall$ (per ogni) e $\exists$ (esiste). Se P è un predicato unario, la proposizione $\exists x P(x)$ esprime il fatto che esiste almeno un oggetto a nel dominio considerato che verifica il predicato, ovvero tale che valga $P(a)$. La proposizione $\forall x P(x)$ dice che per tutti gli oggetto a nel dominio considerato vale $P(a)$. Per predicati binari possiamo avere diverse combinazioni di $\forall$ e $\exists$. $\forall x \exists y P(x,y)$ significa che dato un x posso sempre trovare un y, che in genere dipenderà da x, tale che $P(x,y)$, mentre invece $\exists y \forall x P(x,y)$ significa che è possibile trovare un y che va bene per tutti gli x, ovvero un y tale che per ogni x vale $P(x,y)$. Ad esempio se il dominio delle variabili è un insieme di persone, e $P(x,y)$ è la relazione "y è la mamma di x", $\forall x \exists y P(x,y)$ dice che ogni persona ha una mamma, mentre $\exists y \forall x P(x,y)$ esprime la proposizione (falsa) che asserisce l'esistenza di una persona y che è la mamma di tutti (inclusa se stessa).

3. Esempi

Esercizio 3.1. Formalizzare usando i quantificatori e le operazioni aritmetiche
x è primo.
x divide y.
x è il massimo comun divisore tra x ed y.

Esempio 3.2. (Uno o due quantificatori) Determinare quali formule sono vere in $\mathbb{N}$ (cioè assumendo che il dominio delle variabili sia $\mathbb{N}$), quali in $\mathbb{Z}$, quali in $\mathbb{R}$.

$$\forall x(x \geq 0)$$
$$\exists x(x^2 > 3x)$$
$$\forall x(x^2 > 3x)$$
$$\forall x, y((x+y)^2 = x^2 + 2xy + y^2)$$
$$\exists x, y((x+y)^2 = x^2 + 2x + 1)$$
$$\forall x \forall y(x > y)$$
$$\exists x \exists y(x > y)$$
$$\forall x \exists y(x > y)$$
$$\exists y \forall x(x > y)$$
$$\forall x \exists y(x + y = 0)$$
$$\exists x \forall y(x + y = 0)$$
$$\forall x \exists y(xy = 1)$$
$$\exists x \forall y(xy = 1)$$
$$\exists x \forall y(xy = y)$$

Esempio 3.3. (Tre quantificatori) Determinare quali formule sono vere in $\mathbb{Z}$.

$$1.\forall x \exists y \forall z(x + y = z)$$
$$2.\exists x \forall y \exists z(x + y = z)$$
$$3.\forall x \exists y \forall z(z(x + y) = z)$$

Prima di risolverlo facciamo una digressione:

Interpretazione dei quantificatori in termini di giochi: Immaginiamo un gioco tra due giocatori chiamati $\forall$ ed $\exists$ che assegnano a turno i valori alle variabili nel modo seguente. Leggendo la formula da sinistra a destra quando si incontra un $\forall t$ (dove t può essere una qualsiasi variabile $x, y, z, \ldots$ tra quelle presenti) allora il giocatore $\forall$ assegna

un valore a t, mentre quando si incontra un $\exists t$ allora è il turno del giocatore $\exists$ a scegliere un valore per la t. Lo scopo di $\exists$ è cercare di fare in modo che, una volta sostituite tutte le variabili con i valori scelti a turno dai due giocatori, si ottenga un enunciato vero. Lo scopo di $\forall$ è invece quello di cercare di ottenere un enunciato falso. Se $\exists$ ha una strategia per vincere l'enunciato di partenza è vero, mentre se la strategia per vincere la ha $\forall$ l'enunciato è falso. Vediamo come funziona la cosa nel nostro esempio.

La 1. è falsa. Infatti il primo turno di gioco spetta a $\forall$ che sceglie un valore per la x, ad esempio $x = 0$. Poi tocca a $\exists$ che dà un valore alla y, poniamo $y = a$ (dove a è un numero ben preciso, ad esempio potrebbe essere 7). L'ultima parola spetta però a $\forall$ che, qualunque fosse il numero a precedentemente scelto, è sicuramente in grado di scegliere un valore per la z che renda falso $0 + a = z$, ad esempio potrebbe prendere $z = a + 1$.

La 2. è vera. Infatti il primo turno spetta a $\exists$, che può scegliere $x = 0$. Poi tocca a $\forall$ che sceglie un valore per la y, poniamo $y = a$. Ora tocca a $\exists$ che può scegliere $z = a$ ottenendo l'enunciato vero $0 + a = a$.

La 3. è vera. Infatti inizia $\forall$, che sceglie un valore per la x, poniamo $x = a$. Poi tocca a $\exists$ che decide di dare alla y il valore $1 - a$. Questa è in effetti una buona strategia per $\exists$ in quanto, nonostante l'ultimo turno di gioco spetti a $\forall$, questi non può in alcun modo scegliere un valore per z che falsifichi $z(x + y) = z$ dove $x = a$ e $y = (1 - a)$. In effetti sostituendo i valori scelti per x, y si ottiene $x + y = 1$ e non c'è modo di falsificare $z \cdot 1 = z$.

4. Equivalenze notevoli

FATTO 4.1. *Valgono le sequenti equivalenze:*

$$\begin{array}{ccc}
\forall x P(x) & \iff & \forall y P(y) \\
\exists x P(x) & \iff & \exists y P(y) \\
\neg \forall x P(x) & \iff & \exists x \neg P(x) \\
\neg \exists x P(x) & \iff & \forall x \neg P(x) \\
\exists x (P(x) \vee Q(x)) & \iff & \exists x P(x) \vee \exists x Q(x) \\
\forall x (P(x) \wedge Q(x)) & \iff & \forall x P(x) \wedge \forall x Q(x) \\
\exists x P(x) \wedge \exists x Q(x) & \iff & \exists x \exists y (P(x) \wedge Q(y)) \\
\forall x P(x) \vee \forall x Q(x) & \iff & \forall x \forall y (P(x) \vee Q(y)) \\
\exists x (P(x) \wedge R) & \iff & (\exists x P(x)) \wedge R \\
\forall x (P(x) \vee R) & \iff & (\forall x P(x)) \vee R \\
\exists x (P(x) \vee R) & \iff & (\exists x P(x)) \vee R \\
\forall x (P(x) \wedge R) & \iff & (\forall x P(x)) \wedge R
\end{array}$$

dove "$P(x)$" sta per "x verifica il predicato P", "$Q(x)$" sta per "x verifica il predicato Q", ed R non dipende da x (potrebbe essere una proposizione o un predicato dipendente da altre variabili $z, w, \ldots$).

OSSERVAZIONE 4.2. Per trovare le regole riguardanti $\rightarrow, \forall, \exists$ si scriva $A \rightarrow B$ come $\neg A \vee B$ e si applichino le regole precedenti.

ESERCIZIO 4.3. Sia $P(x)$ un predicato unario e Q una proposizione (non dipendente da x). Stabilire per ciascuna delle delle seguenti formule se essa è equivalente a qualcuna delle altre.

(1) $(\exists x P(x)) \rightarrow Q$;
(2) $\forall x (P(x) \rightarrow Q)$;
(3) $\exists x (P(x) \rightarrow Q)$;

(4) $(\exists x \neg P(x)) \vee Q$.

SOLUZIONE: La 1 equivale alla 2. La 3 equivale alla 4. Non vi sono altre equivalenze che valgano per ogni scelta di $P(x)$ e Q.

GIUSTIFICAZIONE: Le 1 equivale a $(\neg \exists x P(x)) \vee Q$, che equivale a $(\forall x \neg P(x)) \vee Q$. Ora visto che Q non dipende da x otteniamo una formula equivalente risistemando le parentesi nella forma $\forall x((\neg P(x)) \vee Q)$. Questa a sua volta equivale a $\forall x(P(x) \rightarrow Q)$, cioè alla 2.

La 3 equivale a $\exists x(\neg P(x) \vee Q)$, che equivale (in quanto Q non dipende da x) a $(\exists x \neg P(x)) \vee Q$, cioè alla 4.

Non vi sono altre equivalenze valide. Ad esempio se come $P(x)$ prendiamo il predicato "x è pari, come Q prendiamo una proposizione falsa, e facciamo variare x tra gli interi, allora la 2 risulta falsa e la 4 vera (cercate di capire perché). Quindi la 2 non equivale alla 4.

Osservazione 4.4. In particolare abbiamo scoperto l'equivalenza valida:

$$(\exists x P(x)) \rightarrow Q \iff \forall x(P(x) \rightarrow Q)$$

5. Formule predicative

Una **formula predicativa** è una espressione costruita per mezzo dei connettivi e dei quantificatori a partire da certi simboli che rappresentano dei predicati o delle proposizioni. Ad esempio $\forall x P(x) \vee Q$ è una formula predicativa, dove $P(x)$ rappresenta un predicato (ad esempio potrebbe essere il predicato "x è un numero primo") e Q rappresenta una proposizione (ad esempio potrebbe essere la proposizione "$2 > 3$"). Un altro esempio di formula predicativa è $\forall x \exists y R(x, y)$, dove $R(x, y)$ rappresenta un predicato con due variabili (ad esempio il predicato $x > y$).

Una formula predicativa è *logicamente valida* se è sempre vera indipendentemente da come vengono interpretati i simboli per predicati e proposizioni che vi compaiono, e anche indipendentemente dalla scelta del dominio delle variabili (che assumiamo sempre non vuoto), dai valori che si assegnino alle eventuali variabili libere. Ad esempio $\exists x \neg P(x) \rightarrow \neg \forall x P(x)$ è logicamente valida in quanto è vera qualunque sia il significato di $P(x)$. La formula dice che se esiste un x per cui non vale $P(x)$ allora non può essere che per tutti gli x valga $P(x)$. Si osservi che ogni tautologia è logicamente valida. La formula $\forall x P(x) \vee Q$ precedentemente considerata non è logicamente valida in quanto è falsa per certe interpretazioni di Q e di $P(x)$.

Date due formule predicative ϕ e ψ, diciamo che ϕ **implica logicamente** ψ, se la formula $\phi \rightarrow \psi$ è logicamente valida. Scriviamo in tal caso $\phi \Longrightarrow \psi$.

Due formule predicative ϕ e ψ sono **logicamente equivalenti**, se l'una implica logicamente l'altra e viceversa. Scriviamo in tal caso $\phi \iff \psi$, o $\phi \equiv \psi$.

Tutte le implicazioni e le equivalenze logiche che abbiamo visto nella sezione sui connettivi booleani continuano ad essere valide. In più nel caso dei quantificatori abbiamo ulteriori implicazioni ed equivalenze logiche, come ad esempio quelle viste nella sezione precedente, e le seguenti:

Esempio 5.1. (1) $\forall x P(x) \wedge \forall x Q(x) \iff \forall x(P(x) \wedge Q(x))$,
(2) $\exists x P(x) \vee \forall x Q(x) \iff existsx(P(x) \vee Q(x))$,
(3) $\forall x P(x) \vee \forall x Q(x) \Longrightarrow \forall x(P(x) \vee Q(x))$,
(4) $\exists x(P(x) \wedge Q(x)) \Longrightarrow \exists x P(x) \wedge \exists x Q(x)$,
(5) $\forall x(P(x) \rightarrow Q(x)) \Longrightarrow \forall x P(x) \rightarrow \forall x Q(x)$,
(6) $\forall x P(x) \rightarrow Q \iff \exists x(P(x) \rightarrow Q)$,

(7) $\exists x P(x) \to Q \iff \forall x(P(x) \to Q)$.

Una formula predicativa ψ è **conseguenza logica** di altre formula predicative $\phi_1, \ldots, \phi_n$, se la congiunzione $(\phi_1 \wedge \ldots \wedge \phi_n)$ implica logicamente ϕ.

In prima approssimazione possiamo dire che una dimostrazione matematica, almeno nei casi semplici, consiste sostanzialmente di una serie di passaggi che deducono la verità di una data formula dalla verità di altre formule per mezzo di una serie di passaggi di cui ognuno è conseguenza logica dei passaggi precedenti. Omettiamo per il momento una discussione più approfondita.

Da una formula predicativa si possono ottenere delle proposizioni per sostituzione. Ad esempio $\forall x((x > 0) \vee \neg(x > 0))$ è una proposizione ottenuta da $\forall x(P(x) \vee \neg P(x))$ attribuendo a $P(x)$ il significato "$x > 0$". Se la formula è logicamente valida le proposizioni da essa ottenuta saranno tutte vere.

6. Forma normale prenessa

Definizione 6.1. Una *forma normale prenessa* è una formula predicativa in cui tutti i quantificatori sono all'inizio della formula. Ad esempio $\forall x \exists y(x > y \to \neg y > x)$ è una forma normale prenessa, mentre $\exists x(x > 0) \vee \forall y(y \leq 0)$ non lo è. Più precisamente una forma normale prenessa è una formula predicativa della forma $Q_1 x_1 \ldots Q_n x_n \theta$ dove ogni Q_i è o un quantificatore esistenziale $\exists$ o un quantificatore universale $\forall$ e dove θ è una formula senza quantificatori detta *matrice* della forma prenessa.

Teorema 6.2. *(Forma normale prenessa) Le equivalenze studiate nella sezione "equivalenze notevoli" sono sufficienti a portare tutti i quantificatori che compaiono in una formula predicativa all'esterno (cioè all'inizio) della formula. Prima si eliminano i* $\to$ *e i* $\leftrightarrow$*. Poi si spingono le negazioni all'interno usando le opportune regole, e infine si portano* $\forall$ *ed* $\exists$ *all'esterno di* $\wedge$ *e* $\vee$ *con le rimanenti regole (se la formula è complessa si parte dalle sottoformule più interne).*

Esercizio 6.3.

$$\exists x P(x) \to \exists y Q(y) \iff \forall x \exists y(P(x) \to Q(y))$$

Definizione 6.4. L'algoritmo per trasformare una formula predicativa in una forma normale prenessa e lei logicamente equivalente è il seguente. Si applicano da sinistra verso destra le equivalenze

(1) $\neg \forall x P(x) \equiv \exists x \neg P(x)$.
(2) $\neg \exists x P(x) \equiv \forall x \neg P(x)$.

per spingere le negazioni verso l'interno delle formula e i quantificatori verso l'esterno. Se è possibile si applicano da sinistra verso destra le equivalenze

(1) $P \wedge \forall x Q(x) \equiv \forall x(P \wedge Q(x))$;
(2) $P \vee \exists x Q(x) \equiv \exists x(P \vee Q(x))$;
(3) $P \vee \forall x Q(x) \equiv \forall x(P \vee Q(x))$;
(4) $P \wedge \exists x Q(x) \equiv \exists x(P \wedge Q(x))$.

per spingere le congiunzioni e le disgiunzioni verso l'interno delle formula e i quantificatori verso l'esterno, a condizione che P non dipenda da x. Si intende ovviamente che le regole valgano anche se al posto della x c'è una qualsiasi altra variabile. In altre parole, se una delle due formule nella congiunzione o disgiunzione inizia con un quantificatore su una certa variabile, e l'altra formula non ha occorrenze libere di quella variabile, allora possiamo spostare il quantificatore all'esterno. (Questa regola però non si applica

se c'è una implicazione: se si vuole seguire questo metodo occorre prima eliminare le implicazioni trasformando $A \to B$ in $\neg A \vee B$.)

Valgono anche tutte le varianti delle quattro equivalenze precedenti che si ottengono usando la commutatività di $\vee$ e di $\wedge$, ad esempio dal punto 1. si ottiene anche per commutatività: $\forall x Q(x) \wedge P \equiv \forall x(Q(x) \wedge P)$.

Se al posto della formula P abbiamo una formula $P'(x)$ che dipende da x, allora le regole precedenti non sono applicabili. In quel caso conviene ridenominare le variabili quantificate usando le seguenti regole:

(1) $\forall x Q(x) \equiv \forall y Q(y)$.
(2) $\exists x Q(x) \equiv \exists y Q(y)$.

dove la y è una variabile nuova che non entra in conflitto con le altre variabili in circolazione. Lo scopo di ridenominare le variabili quantificate è di ricondursi ad una situazione in cui le precedenti regole diventino di nuovo applicabili. Ad esempio nella formula $P(x) \wedge \forall x Q(x)$ possiamo ridenominare le variabili quantificate ottenendo la formula equivalente $P(x) \wedge \forall y Q(y)$, e poi possiamo spostare il quantificatore $\forall y$ all'esterno usando le precedenti regole ottenendo $\forall y(P(x) \wedge Q(y))$.

E' facile vedere che se una formula non è in forma normale prenessa, almeno una delle regole sopra date risulta applicabile. Applicando ripetutamente le regole, i quantificatori vengono progressivamente spostati verso l'esterno, e si giunge in un numero finito di passi ad una forma normale prenessa equivalente alla formula data.

Possiamo inoltre eliminare i quantificatori ridondanti usando la regola $\forall x P \equiv P$ se P non contiene la x libera, e similmente per $\exists$.

Esempio 6.5. Consideriamo la formula

$$\forall x(P(x) \to Q(x)) \to (\forall x P(x) \to \forall x Q(x))$$

Per trovare una forma normale prenessa ad essa equivalente come primo passo ridenominiamo le variabili:

$$\equiv \forall x(P(x) \to Q(x)) \to (\forall y P(y) \to \forall z Q(z))$$

Usiamo l'equivalenza $A \to B \equiv \neg A \vee B$ ottenendo:

$$\equiv \neg\forall x(\neg P(x) \vee Q(x)) \vee (\neg\forall y P(y) \vee \forall z Q(z))$$

Usando le regole relative a $\neg\exists$ e $\neg\forall$ spingiamo le negazioni all'interno (ed eliminiamo anche le parentesi superflue):

$$\equiv \exists x\neg(\neg P(x) \vee Q(x)) \vee \exists y\neg P(y) \vee \forall z Q(z)$$

Portiamo fuori i quantificatori usando ripetutamente le regole date:

$$\equiv \exists x\exists y\forall z(\neg(\neg P(x) \vee Q(x)) \vee \neg P(y) \vee Q(z)$$

L'ultima formula ottenuta è una forma normale prenessa della formula da cui siamo partiti. Possiamo ulteriormente semplificarla usando le usuali regole sui connettivi booleani:

$$\equiv \exists x\exists y\forall z[(P(x) \wedge \neg Q(x)) \vee \neg P(y) \vee Q(z)]$$

7. Esercizi

Esercizio 7.1. (Esempio di dimostrazione di un enunciato della forma $\exists a\forall x P(x, a)$). Si dimostri che: $\exists a\forall x \geq a(x^3 \geq 3x^2 + 2x + 5)$.

Soluzione: detto altri termini si tratta di trovare un intero a tale che per ogni $x \geq a$ si abbia:
$x^3 \geq 3x^2 + 2x + 5$.

Soluzione. Scriviamo $x^3 = \frac{1}{3}x^3 + \frac{1}{3}x^3 + \frac{1}{3}x^3$ e confrontiamolo con $3x^2 + 2x + 5$ termine a termine. Ragionando all'indietro, si trova:
$\frac{1}{3}x^3 \geq 3x^2 \leftarrow \frac{1}{3}x > 3 \leftarrow x \geq 9$,
$\frac{1}{3}x^3 \geq 2x \leftarrow \frac{1}{3}x^2 \geq 2 \leftarrow x \geq 3$,
$\frac{1}{3}x^3 \geq 5 \leftarrow x^3 \geq 15 \leftarrow x \geq 3$.
Quindi possiamo prendere $a = 9$.

Commento: in modo analogo si può dimostrare un polinomio maggiora definitivamente ogni polinomio di grado inferiore. (Non serve l'induzione, infatti vale tra i reali.)

Commento: Scrivendo $x^3 = \frac{1}{2}x^3 + \frac{1}{4}x^3 + \frac{1}{4}x^3$ si trova una soluzione migliore.
$\frac{1}{2}x^3 \geq 3x^2 \leftarrow \frac{1}{2}x > 3 \leftarrow x \geq 6$,
$\frac{1}{4}x^3 \geq 2x \leftarrow \frac{1}{4}x^2 \geq 2 \leftarrow x \geq 3$,
$\frac{1}{4}x^3 \geq 5 \leftarrow x^3 \geq 20 \leftarrow x \geq 3$.
Quindi possiamo prendere $a = 6$. È ottimale? (no, basta $a = 4$).

Esempio 7.2. (Per chi conosce i rudimenti dell'analisi matematica) Data $f\colon \mathbb{R} \to \mathbb{R}$, formalizzare usando i quantificatori: f è iniettiva. f è crescente. f è surgettiva. f è limitata. f è continua in 0, f è continua in tutti i punti. Formalizzare poi la negazione di ognuna spingendo le negazioni all'interno.

CAPITOLO 3

Insiemi

Questa sezione è ancora da completare.
NOTAZIONI PER GLI INSIEMI. $\{a, b, c\}$, $\{x \mid P(x)\}$, $\{f(x) \mid P(x)\}$.

1. Esempi

ESEMPIO 1.1. Quanti insiemi compaiono nella seguente lista?

$$\{1, 5, 4, 5\}$$
$$\{5, 4, 1\}$$
$$\{5, 5\}$$
$$\{5\}$$
$$\{1, 3, 4, 5\}$$
$$\{5, 4, 3, 1\}$$
$$\{1, 3, 6\}$$

Soluzione. Vi compaiono quattro insiemi.
Altra domanda: quali inclusioni valgono?

OSSERVAZIONE 1.2. I seguenti enunciati sono equivalenti:

$$\{x \mid P(x)\} \subset \{x \mid Q(x)\} \tag{1.1}$$
$$\forall x(P(x) \to Q(x)) \tag{1.2}$$

Ad esempio dire che $\forall x(x \geq 9 \to x \geq 5)$ equivale a dire che la semiretta $\{x \mid x \geq 9\}$ è inclusa nella semiretta $\{x \mid x \geq 5\}$.

CORRISPONDENZA TRA IDENTITA' INSIEMISTICHE E TAUTOLOGIE
Leggi distributive. L'inclusione si rovescia passando al complemento.

ESERCIZIO 1.3. $A \subset U \ \wedge \ (A \cap (U \setminus B) = \emptyset) \Longrightarrow A \subset B$.

ESEMPIO 1.4. (Inclusione esclusione) Dimostrare le formule di inclusione-esclusione per due, tre e quattro insiemi.

Per due insiemi: $|A \cap B| = |A| + |B| - |A \cap B|$. Suggerimento: scrivere $A \cap B$ come unione di tre insiemi disgiunti e usare il fatto che la cardinalità dell'unione disgiunta è la somma delle cardinalità.

Per tre: $|A \cap B \cap C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

Per quattro: $|A \cap B \cap C \cap D| = |A| + |B| + |C| + |D| - |A \cap B| - |A \cap C| - |B \cap C| - |A \cap D| - |B \cap D| - |C \cap D| + |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| - |A \cap B \cap C \cap D|$.

Fino a tre conviene fare i diagrammi di Venn. Per quattro insiemi A, B, C, D i diagrammi possono essere ingannevoli e conviene ricondursi al caso precedente spezzanso $A \cup B \cup C \cup D$ in $(A \cup B \cup C) \cup D$ e usando le leggi distributive.

Esempio 1.5. (Inclusione-esclusione) Quanti sono gli interi tra 1 e 1000 divisibili per 7 o per 11?

Soluzione: ce ne sono $\lfloor 1000/7 \rfloor = 142$ divisibili per 7, $\lfloor 1000/11 \rfloor = 90$ divisibili per 11, e $\lfloor 1000/7 \cdot 11 \rfloor = 12$ divisibili sia per 7 che per 11. Quindi in totale: $142 + 90 - 12 = 220$.

Esempio 1.6. (Inclusione-esclusione) Quante sono le stringhe binarie di lunghezza 8 che iniziano per 0 o finiscono per 11?

Soluzione: $2^7 + 2^6 - 2^5 = 128 + 64 - 32 = 160$.

CAPITOLO 4

Il principio di induzione

Vedere appunti di Gaiffi.

1. Altri esercizi

ESERCIZIO 1.1. Trovare b tale per ogni $n \geq a$ valga $n^2 \leq 2^n$.
Soluzione: $b = 4$.
Commento: per $b = 0$ funziona la base ma non il passo induttivo. Per $b = 3$ funziona il passo induttivo ma non la base.

ESERCIZIO 1.2. $\sum_{i=1}^{n} i = n(n+1)/2$.

ESERCIZIO 1.3. Serie aritmetica. Somma dei primi n quadrati $= n^2$. Due dimostrazioni. La prima diretta per induzione. La seconda distribuendo le sommatorie e riconducendosi al caso dei primi n interi positivi.

ESERCIZIO 1.4. Serie geometrica. $\sum_{i=0}^{n} x_n = \frac{x^{n+1}-1}{x-1}$ per $x \neq 1$. Commentare il caso $x = 1/2$ (Achille e la tartaruga) e il caso $x = 2$ (notazione binaria).

ESERCIZIO 1.5. Per ogni $n \geq 4$ $n! > 2^n$.

ESERCIZIO 1.6. Determinare per quali n si ha $2^n > n^2 + 3n + 1$.

ESERCIZIO 1.7. $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

ESERCIZIO 1.8. $\sum_{i=1}^{n} i^3 = \left[\frac{n(n+1)}{2}\right]^2$.

ESERCIZIO 1.9. $\sum_{i=1}^{n} \frac{1}{\sqrt{k}} \geq \sqrt{n}$.

ESERCIZIO 1.10. Sia $H_k = \sum_{1=1}^{k} \frac{1}{i}$. Si dimostri che $H_{2^n} \geq 1 + \frac{n}{2}$.

I seguenti esercizi richiedono l'induzione in forma forte.

ESEMPIO 1.11. Fibonacci: $F_1 = 1, F_2 = 1, F_{n+2} = F_{n+1} + F_n$. $F_n = (\alpha^n - \beta^n)/\sqrt{5}$ dove $\alpha = (1 + \sqrt{5})/2$ e $\beta = (1 - \sqrt{5})/2$ sono le due radici di $x^2 = x + 1$.

ESEMPIO 1.12. $F_n \geq n^2$ per $n \geq 3$.

ESEMPIO 1.13. Ogni intero positivo ha un divisore primo.

ESERCIZIO 1.14. Per ogni intero positivo n, $2^{2^n} - 1$ ha almeno n divisori primi diversi fra loro.
Suggerimento: $2^{2^{n+1}} - 1 = (2^{2^n} - 1)(2^{2^n} + 1)$.

CAPITOLO 5

Prodotto cartesiano, relazioni e funzioni

Ancora da completare.

Definizione di funzione da un insieme X ad un insieme Y.

Grafico di una funzione.

Due funzioni sono uguali se hanno lo stesso dominio, codominio e grafico.

Dominio della funzione $1/x$.

Funzioni definite per casi: $f(x) = 0$ se $x = 0$, $1/x$ altrimenti.

Sia $f\colon X \to Y$. Se $f(x) = a$ diciamo che a è l'immagine di x (ce ne è una sola) e x è una controimmagine di a. Diciamo che f è iniettiva se ogni b nel suo codominio ha al più una controimmagine (zero o una), ed è surgettiva se ne ha almeno una (una o più). L'immagine di f è l'insieme $\{f(x) \mid x \in X\}$.

1. Esercizi

ESERCIZIO 1.1. Sia $f\colon \mathbb{Q} \to \mathbb{Q}$ data da $g(x) = x^2$. Trovare le controimmagini di $0, 2, 4$.

ESERCIZIO 1.2. Sia $f\colon \mathbb{R} \to \mathbb{R}$ la funzione $f(x) = 3x-2$. Determinare se f è iniettiva, surgettiva. Stessa domanda con $\mathbb{N}$ al posto di $\mathbb{R}$ come dominio e codominio.

ESERCIZIO 1.3. Sia $f\colon \mathbb{R} \to \mathbb{R}$ data da $f(x) = x^2$. Determinare se f è iniettiva, surgettiva. Siano $a < b$ in $\mathbb{R}$. Per quali valori di a, b la restrizione di f ad $[a, b]$ è iniettiva?

ESERCIZIO 1.4. Sia $f\colon \mathbb{R} \to \mathbb{R}$ data da $f(x) = (x - 3)^2 + 5$. Determinare se f è iniettiva, surgettiva. Per quali scelte di a e b, f ristretta ad $[a, b]$ è iniettiva?

ESERCIZIO 1.5. Sia $g\colon \mathbb{R} \to \mathbb{R}$ data da $g(x) = ax^2+bx+c$. Trovate le controimmagini di zero. Suggerimento: $4ag(x) = (2ax + b)^2 + (4ac - b^2)$. Determinare se g è surgettiva. Determinare per quali a, b la restrizione di g ad $[a, b]$ è iniettiva.

ESERCIZIO 1.6. Sia $f\colon \mathbb{R} \to \mathbb{R}$ data da $f(x) = x + 2^x$. Determinare se f è iniettiva.

ESERCIZIO 1.7. Sia $f\colon \mathbb{Z}^2 \to \mathbb{Z}$ data da $f(x, y) = x + y$. Determinare se f è iniettiva, surgettiva.

ESERCIZIO 1.8. Sia $f(x) = x^3$. Dimostrare che f è biunivoca.

Dim: basta mostrare che f è crescente. Sia $x < y$. Vogliamo mostrare $x^3 < y^3$. Il caso difficile è quando x, y sono entrambi negativi. Ricordiamo che la moltiplicazione per un numero negativo rovescia le disuguaglianze. Da $x < y$ ottengo allora moltiplicando per x, $x^2 > xy$. Moltiplicando $x < y$ per y ottengo $xy > y^2$. Mettendo insieme le due disuguaglianze ottengo $x^2 > y^2$. Ora moltiplico questa per x e ottengo $x^3 < xy^2$. D'altra parte moltiplicando $x < y$ per il numero positivo y^2 ottengo $xy^2 < y^3$. Combinando le disuguaglianze ottenute ottengo $x^3 < y^3$.

Composizione di funzioni.

Esercizio 1.9. Sia $f(x) = 3x + 5$ e $g(x) = 7x - 11$. Calcolare $f \circ g$ e $g \circ f$.

Esercizio 1.10. Siano $f(x) = x^2$ e $g(x) = \sqrt{x}$, prendendo come dominio e codominio di entrambe l'insieme dei reali positivi. Allora $f(g(x)) = x$ e $g(f(x)) = x$. Diciamo che f, g sono l'una l'inversa dell'altra.

Osservazione 1.11. Per x reale, $\sqrt{x^2} = |x|$.

Teorema 1.12. *Sia $f(g(u)) = u$. Allora f è surgettiva e g è iniettiva.*

Dimostrazione. Se $g(u) = g(v)$ applicando f trovo $u = v$. Quindi g è iniettiva. Per risolvere $f(x) = b$, prendo $x = g(b)$. Quindi g è surgettiva. □

Corollario 1.13. *Se f, g sono l'una l'ionversa dell'altra (ovvero $f(g(y)) = y$ e $g(f(x)) = x$), allora f, g sono biunivoche e $g(y)$ è la controimmagine di y tramite f (quindi l'inversa di una funzione biunivoca è unica).*

Teorema 1.14. *Se f è biunivoca, e $g(y)$ è la controimmagine di y tramite f, allora $f(g(y)) = y$ (ovvio) e $g(f(x)) = x$ (in quanto la controimmagine di $f(x)$ tramite f è x). Quindi f è biunivoca se e solo se f è invertibile.*

CAPITOLO 6

Calcolo combinatorio

Da scrivere.

1. Esercizi

ESERCIZIO 1.1. Quante sono le funzioni $f\colon \{1,2,3,4,5\} \to \{1,2,3,4,5\}$ tali che per ogni x nel dominio di f si ha $f(x) \geq x$? Dimostrare per induzione un risultato generale.

ESEMPIO 1.2. Sia $f\colon A \to B$ con A, B insiemi finiti, e supponiamo che ogni $b \in B$ abbia n controimmagini in A. Quale è il rapporto tra $|A|$ e $|B|$?

ESEMPIO 1.3. Ci sono 2^n stringhe binarie di lunghezza n.

ESEMPIO 1.4. Quante sono le funzioni surgettive da $\{1,2,3,4\}$ a $\{1,2\}$?

INSIEME DELLE PARTI

ESERCIZIO 1.5. Un insieme con n elementi ha 2^n sottoinsiemi. Due dimostrazioni. Una riconducendosi alle stringhe, l'altra diretta per induzione.

ESEMPIO 1.6. Quante sono le permutazioni di un insieme di n elementi?

ESEMPIO 1.7. Quante sono le stringhe di k elementi distinti presi da un insieme di n elementi?

ESEMPIO 1.8. Quanti sottoinsiemi di k elementi possiede un insieme X di n elementi?
Suggerimento: Sia A l'insieme delle stringhe di k elementi distinti presi da X. Sia B l'insieme dei sottoinsiemi di X di k elementi. Sia $f\colon A \to B$ la funzione che associa ad una stringa l'insieme dei suoi elementi. Quante controimmagini ha un generico $b \in B$?

ESERCIZIO 1.9. Dato un intero n, quante sono le triple (x, y, z) di interi non negativi che verificano $x + y + z = n$?
Soluzione: tante quante le stringhe binarie di lunghezza $n + 2$ con esattamente due zeri. Quindi $\binom{n}{2}$.

ESEMPIO 1.10. Triangolo di Tartaglia. Formule di Stiefel. Dimostrazione combinatoria e algebrica.

ESEMPIO 1.11. Binomio di Newton. Dimostrazione combinatoria e induttiva.

CAPITOLO 7

Aritmetica

1. 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 1.1. *(Teorema della divisione euclidea). Dati a, b interi con $b > 0$ esistono (e sono unici) due interi q (quoziente) ed r (resto) con*

$$a = bq + r \tag{1}$$

$$0 \leq r < b \tag{2}$$

OSSERVAZIONE 1.2. Rimarchiamo subito che uno dei punti qualificanti della definizione della divisione euclidea è la richiesta sul resto, ossia che valga $0 \leq r < b$. Per esempio, volendo distribuire 22 penne fra sette studenti, potrei darne 2 per uno e lasciarne avanzare 8:

$$22 = 7 \cdot 2 + 8$$

Oppure potrei darne tre per uno e avere una sola penna come resto:

$$22 = 7 \cdot 3 + 1$$

Solo quest'ultima è la divisione euclidea di 22 per 7. Infatti 1 soddisfa la condizione $0 \leq 1 < 7$ mentre 8 non soddisfa $0 \leq 8 < 7$. Il teorema che abbiamo enunciato, e che stiamo per dimostrare, dice appunto, a riguardo di questo esempio, che fra le scritture

$$22 = 7a + c$$

con a e c numeri interi, ne esiste una e una sola che è la divisione euclidea di 22 per 7.

DIMOSTRAZIONE DEL TEOREMA. Notiamo che incrementando il numero q anche bq aumenta (essendo b positivo). Esisterà quindi un valore di q (ed uno solo) tale che $bq \leq a < b(q+1)$ (basta prendere il minimo q tale che $a < b(q+1)$). Dividendo per b otteniamo: $q \leq a/b < q + 1$. Quindi:

$$q = \lfloor a/b \rfloor.$$

Una volta trovato q il resto $r = \text{Resto}(a, b)$ è dato da:

$$r = a - bq.$$

□

ESEMPIO 1.3. $a = 1781293$, $b = 1481$, $a/b \approx 1202.7637$, $q = 1202 = \lfloor a/b \rfloor$, $r = 1781293 - 1481 \times 1202 = 1131$.

Esempio 1.4. $a = -7856123$, $b = 9812$, $a/b \approx -800.66840$, $q = -801 = \lfloor a/b \rfloor$, $r = -7856123 - 9812 \cdot (-901) = 3289$.

Esempio 1.5. Oggi è lunedi. Che giorno della settimana sarà tra 30 giorni? Soluzione: $30 = 7 \cdot 4 + 2$. Quindi: mercoledi.

Esempio 1.6. E in che giorno eravamo 30 giorni fa? Soluzione: $-30 = 7 \cdot (-4) + (-2)$. Quindi: sabato.

Esempio 1.7. Che ore saranno tra 101 ore? Soluzione: $101 = 24 \cdot 4 + 5$. Quindi devo spostare la lancetta delle ore in avanti di 5 ore.

Esempio 1.8. Che ore erano 101 ore fa? Soluzione:

$$\begin{aligned} -101 &= 24 \cdot (-4) + (-5) \\ &= 24 \cdot (-4) - 24 + 24 - 5 \\ &= 24 \cdot (-5) + 19 \end{aligned}$$

Quindi devo spostare la lancetta delle ore in indietro di 5 ore, o equivalentemente in avanti di 19 ore.

2. Congruenze

Definizione 2.1. Dato un intero b e due interi x, y, scriviamo

$$x \equiv y \bmod c$$

(si legge: x è congruo ad y modulo b), se $x - y$ è un multiplo di b, ovvero se esiste un intero k tale che $bk = x - y$.

Osservazione 2.2. Dati due interi a, b, le soluzioni x della congruenza $a \equiv x \bmod (b)$ sono tutti e soli i numeri x della forma $a + bk$ con k intero. Ricordiamo che la divisione euclidea permette di scrivere a nella forma $a = bq + r$ con $0 \leq r < b$. Il resto $r = esto(a, b)$ verifica la congruenza $a \equiv r \bmod (b)$ ed inoltre è l'unico numero che la verifica che cade nell'intervallo $0 \leq r < b$.

Osservazione 2.3. La relazione di congruenza modulo c è una relazione di equivalenza, nel senso che verifica le proprietà:

Riflessiva:: $x \equiv x \bmod (c)$;
Simmetrica:: Se $x \equiv y \bmod (c)$ allora $y \equiv x \bmod (c)$;
Transitiva:: Se $x \equiv y \bmod (c)$ e $y \bmod z \bmod (c)$, allora $x \bmod z \bmod (c)$.

Teorema 2.4. *Le congruenze "rispettano" somme e prodotti, nel senso che se* $a \equiv a' \bmod c$ *e* $b \equiv b' \bmod c$, *allora* $a + b \equiv a' + b' \bmod (c)$ *e* $aa' \equiv bb' \bmod c$.

Dimostrazione. Supponiamo che $a' = a + kc$ e $b' = b + k'c$.
Allora $a' + b' = a + b + (k + k')c$, e quindi $a + b \equiv a' + b' \bmod c$.
Inoltre $a'b' = (a + kc)(b + k'c) = ab + kcb + k'ca + kk'c^2$, e siccome $kcb + k'ca + kk'c^2$ è un multiplo di c possiamo concludere $a'b' \equiv ab \bmod c$. □

Esempio 2.5. Trovare il resto della divisione euclidea di $1253423 \cdot 134432$ per 5. Soluzione: $1253423 \cdot 134432 \equiv (3 \cdot 2 \bmod 5) \equiv 6 \equiv 1 \bmod (5)$. Quindi il resto è 1.

Esempio 2.6. Trovare il resto della divisione euclidea di 2^{99} per 7. Soluzione: $2^{99} \equiv 2^{3 \cdot 33} \equiv 8^{33} \equiv 1^{33} \equiv 1 \bmod 7$. Quindi il resto è 1.

Esempio 2.7. Trovare il resto della divisione di 3^{11} per 5. Soluzione: Modulo 5 abbiamo le seguenti congruenze: $3^{11} \equiv 3^2 3^2 3^2 3^2 3^2 3 \equiv 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 3 \equiv (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot 3 \equiv -3 \equiv 2 \bmod (5)$. Quindi il resto è 2.

3. Basi numeriche

Ricordiamo che quando scriviamo un numero, ad esempio 1234567, implicitamente sottointendiamo che esso è scritto in base 10, ovvero:

$$1234567 = 1 \cdot 10^6 + 2 \cdot 10^5 + 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10 + 7$$

Esempio 3.1. Trovare il resto della divisione di 1234567 per 3. Soluzione: Siccome $10 \equiv 1 \bmod 3$, nel fare le congruenze modulo 3 possiamo sostituire 10 con 1 nell'espanzione decimale ottenendo: $1234567 \equiv 1+2+3+4+5+6+7 \equiv 1 \bmod (3)$. Quindi il resto è 1.

Esempio 3.2. Trovare il resto della divisione di 1234567 per 11. Soluzione: Siccome $10 \equiv -1 \bmod (11)$, nel fare le congruenze modulo 11 possiamo sostituire 10 con -1 nell'espanzione decimale ottenendo: $1234567 \equiv 1 - 2 + 3 - 4 + 5 - 6 + 7 \equiv 4$. Quindi il resto è 4.

Esempio 3.3. Trovare il resto della divisione di 1234567 per 4. Soluzione: osserviamo che $100 = 25 \cdot 4 \equiv 0 \bmod (4)$. Quindi $1234567 = 12345 \cdot 100 + 67 \equiv 67 \equiv 3 \bmod (4)$.

Esempio 3.4. Si dimostri che $\sqrt{1234567}$ non è un intero. Soluzione: per assurdo supponiamo che vi sia un intero x tale che $x^2 = 1234567$. Per l'esercizio precedente $x^2 \equiv 1234567 \equiv 3 \bmod (4)$. Quindi basta mostrare che x^2 non può essere congruente a 3 modulo 4. Siccome x è congruo a $0, 1, 2$ o 3 modulo 4, ci sono solo quattro verifiche da fare:

$$\begin{aligned} 0^2 &\equiv 0 \bmod (4) \\ 1^2 &\equiv 1 \bmod (4) \\ 2^2 &\equiv 0 \bmod (4) \\ 3^2 &\equiv 1 \bmod (4) \end{aligned}$$

Esempio 3.5. Cambiamento di base: $(12345)_{10} = (30071)_8$. Infatti

$$\begin{aligned} 12345 &= 8 \cdot 8 \cdot 1543 + 1 \\ 1543 &= 8 \cdot 192 + 7 \\ 192 &= 8 \cdot 24 + 0 \\ 24 &= 8 \cdot 3 + 0 \\ 3 &= 8 \cdot 0 + 3 \end{aligned}$$

4. Classi resto

Definizione 4.1. La classe resto di x modulo c è l'insieme $[x]_c = \{y \mid y \equiv x \bmod (c)\}$.

Osservazione 4.2. Osserviamo che

$$x \equiv y \bmod c \iff [x]_c = [y]_c$$

e che date due classi $[x]_c$ ed $[y]_c$ esse sono uguali oppure disgiunte (ovvero non si intersecano). Per verificarlo si usa il fatto che le congruenze sono relazioni di equivalenza.

Definizione 4.3. (Somma e prodotto di classi resto.) Siccome le congruenze rispettano le somme e i prodotti, possiamo definire la somma e il prodotto di classi resto nel modo seguente:

$$[x]_c + [y]_c = [x + y]_c$$
$$[x]_c \cdot [y]_c = [xy]_c$$

Esempio 4.4. $2^5 \not\equiv 2^2 \bmod 3$, nonostante $5 \equiv 2 \bmod 3$. Quindi non è possibile definire l'esponenziazione di classi resto.

5. Massimo comun divisore e teorema di Bezout

DEFINIZIONE 5.1. (Massimo comun divisore) Siano a, b due interi di cui almeno uno diverso da zero. Definiamo $(a, b) = \max\{d \mid d|a \wedge d|b\}$.

OSSERVAZIONE 5.2. Osserviamo che $(a, b) = (b, a) = (|a|, |b|)$ e $(a, a) = (a, 0) = |a|$.

TEOREMA 5.3. *Se* $a \equiv a' \bmod b$, *allora* $(a, b) = (a', b)$. *In particolare* $(a, b) = (\text{Resto}(a, b), b)$.

DIMOSTRAZIONE. Supponiamo che $d|b$. Allora $d|a$ sse $d|a'$. Quindi i divisori comuni di b ed a coincidono con i divisori comuni di b ed a'. Anche i massimi devono allora coincidere. □

ESEMPIO 5.4. Calcolare $(252, 198)$. Soluzione: Notiamo che:

$$\begin{array}{rcrcl} \text{Resto}(252, 198) & = & 252 - 198 & = & 54 \\ \text{Resto}(198, 54) & = & 198 - 54 \cdot 3 & = & 36 \\ \text{Resto}(54, 36) & = & 54 - 36 & = & 18 \end{array}$$

Applicando ripetutamente la regola $(a, b) = (\text{Resto}(a, b), b) = (b, \text{Resto}(a, b))$ otteniamo:

$$\begin{array}{rcl} (252, 198) & = & (198, 54) \\ & = & (54, 36) \\ & = & (36, 18) \\ & = & (18, 0) \\ & = & 18 \end{array}$$

Riprova: $252 = 18 \cdot 14$, $198 = 18 \cdot 11$.

ESEMPIO 5.5. Trovare x, y interi tali che $18 = 252x + 198y$.

Soluzione: L'idea è la seguente. Dati a, b interi e supponendo di saper trovare soluzioni intere alle equazione $a = 252x + 198y$ e $b = 252x' + 198y'$ possiamo anche risolvere $\text{Resto}(a, b) = 252x'' + 198y''$. Infatti $\text{Resto}(a, b)$ è della forma $a - kb$, e quindi basta prendere $x'' = x - kx'$ e $y'' = y - ky'$. Applicando ripetutamente questo procedimento otteniamo:

$$\begin{array}{rcrcrcrcl} & & 252 & = & 252 \cdot \boxed{1} & + & 198 \cdot \boxed{0} \\ & & 198 & = & 252 \cdot \boxed{0} & + & 198 \cdot \boxed{1} \\ 252 - 198 & = & 54 & = & 252 \cdot \boxed{1} & + & 198 \cdot \boxed{(-1)} \\ 198 - 54 \cdot 3 & = & 36 & = & 252 \cdot \boxed{(-3)} & + & 198 \cdot \boxed{4} \\ 54 - 36 & = & 18 & = & 252 \cdot \boxed{4} & + & 198 \cdot \boxed{(-5)} \end{array}$$

Quindi la soluzione è $x = 4, y = -5$.

TEOREMA 5.6. *(Teorema di Bezout) Dati* a, b *interi di cui almeno uno diverso da zero, esistono* x, y *interi tali che* $ax + by = (a, b)$.[1]

DIMOSTRAZIONE. Consideriamo l'insieme A dei numeri n per i quali è possibile risolvere l'equazione $n = ax + by$, con x, y interi. Il nostro scopo è dimostrare che $(a, b) \in A$. Innanzitutto notiamo che $a \in A$ (prendo $x = 1, y = 0$) e $b \in A$ (prendo $x = 0, y = 1$). Similmente $|a|$ e $|b|$ appartengono ad A.

Inoltre vale la seguente proposizione:

> (*): Dati due interi n, m con $m \neq 0$, se n ed m appartengono ad A anche $\text{Resto}(n, m)$ appartiene ad A.

[1] Ricordiamo che $(0, 0)$ non è definito.

Infatti supponiamo che

$$n = ax + by \tag{1}$$

e

$$m = ax' + by' \tag{2}$$

per certi interi x, y, x', y'. Vogliamo trovare x'', y'' interi tali che

$$\text{Resto}(n, m) = ax'' + by'' \tag{3}$$

Visto che $\text{Resto}(n, m)$ è della forma $n - km$ (con $k = \lfloor n/m \rfloor$), moltiplicando la (2) per k e sottraendola dalla (1) vediamo che si può prendere $x'' = x - kx', y'' = y - ky'$.

La (*) è quindi dimostrata. Ora consideriamo il minimo intero d strettamente positivo che appartiene ad A (osserviamo che A contiene almeno un numero strettamente positivo, quindi d esiste). Visto che d appartiene ad A esistono x, y interi che risolvono l'equazione

$$d = ax + by$$

Se mostriamo che $d = (a, b)$ possiamo concluderne che l'equazione

$$(a, b) = ax + by$$

è risolubile.

Mostriamo dunque che $d = (a, b)$.

Cominciamo con l'osservare che d deve dividere tutti gli altri interi n appartenenti ad A. Infatti nel caso contrario il resto $r = \text{Resto}(n, d)$ verificherebbe $0 < r < d$ e $r \in A$ (per la (*)). Questo contraddice però il fatto che d era il minimo elemento positivo di A.

In particolare d divide sia a che b visto che a e b appartendono ad A, e quindi $d \leq (a, b)$.

Resta da dimostrare che $(a, b) \leq d$.

A tal fine osserviamo che poichè (a, b) divide sia a che b, dividerà anche qualsiasi combinazione lineare $ax + by$ con x, y interi, e in particolare (a, b) divide d. Essendo entrambi positivi ne segue che $(a, b) \leq d$.

D'altra parte avevamo già dimostrato la disuguaglianza opposta e quindi $d = (a, b)$. □

LEMMA 5.7. *Il massimo comun divisore (a, b) di a e b è un multiplo di qualsiasi altro divisore comune di a e b.*

DIMOSTRAZIONE. Per l'identità di Bezout esistono x, y interi tali che $(a, b) = ax + by$. Se c divide sia a che b esso deve dividere anche $ax + by$, e quindi c divide (a, b). □

TEOREMA 5.8. *Dati a, b, n interi, l'equazione $n = ax + by$ ammette soluzioni intere x, y se e solo se $(a, b)|n$.*

DIMOSTRAZIONE. Supponiamo che $(a, b)k = n$. Allora una soluzione in numeri interi di $n = ax + by$ si può ottenere nel modo seguente. Prima si trovano x', y' interi tali che $(a, b) = ax' + by'$. Poi si pone $x = kx'$ ed $y = ky'$.

Se invece (a, b) non divide n, per far vedere che l'equazione non ha soluzioni basta osservare che (a, b) divide qualsiasi combinazione lineare del tipo $ax + by$ con x, y interi, e siccome per ipotesi non divide n, non può essere che $ax + by = n$. □

ESEMPIO 5.9. Dimostrare che $15x + 12y = 20$ non ha soluzioni intere x, y.

Soluzione: Poiché $3 = (15, 12)$ divide sia 15 che 12, esso divide anche qualsiasi combinazione lineare $15x + 12y$ con x, y interi. Siccome 3 non divide 20, non possiamo avere $15x + 12y = 20$.

Esempio 5.10. Trovare x, y interi tali che $54 = 252x + 198y$.

Soluzione: Abbiamo $(252, 198) = 18$ e per il teorema di Bezout possiamo risolvere l'equazione $18 = 252x' + 198y'$. Abbiamo infatti visto che

$$18 = 252 \cdot 4 + 198 \cdot (-5)$$

Siccome $54 = 3 \cdot 18$, moltiplicando per 3 otteniamo:

$$54 = 252 \cdot (4 \cdot 3) + 198 \cdot (-5 \cdot 3)$$

Una soluzione di $54 = 252x + 198y$ è quindi $x = 12, y = -15$.

Osservazione 5.11. Se esistono x, y interi tali che $ax + by = 1$, allora $(a, b) = 1$.

Dimostrazione. Siccome (a, b) divide sia a che b divide anche $ax + by$, cioè 1. Ma allora necessariamente $(a, b) = 1$. □

Teorema 5.12. *Il massimo comun divisore è un multiplo di ciascun divisore comune. Più formalmente, se $n|a$ e $n|b$, allora $n|(a, b)$.*

Dimostrazione. Se n divide sia a che b, allora deve dividere qualsiasi combinazione $ax + by$ con x, y interi. D'altra parte grazie al teorema di Bezout posso scegliere x, y in modo che $(a, b) = ax + by$ con x, y interi. Quindi n deve dividere (a, b). □

Teorema 5.13. *Se $a|bc$ e $(a, b) = 1$, allora $a|c$.*

Dimostrazione. Posso scrivere $ax + by = 1$ con x, y interi. Moltiplico per c ottenendo $acx + bcy = c$. Ora a divide sia acx che bcy. Quindi divide la loro somma c. □

Teorema 5.14. *Se $(a, b) = 1$, $a|n$ e $b|n$, allora $ab|n$.*

Dimostrazione. Moltiplico per n l'uguaglianza di Bezout $ax + by = 1$ ottenendo $anx + bny = n$. Ora basta osservare che ab divide il termine a sinistra. □

Teorema 5.15. *Siano a, b interi non entrambi nulli e siano $a' = \frac{a}{(a,b)}$ e $b' = \frac{b}{(a,b)}$. Allora $(a', b') = 1$.*

Dimostrazione. Sia k un divisore positivo di a' e b'. Esiste dunque un intero h con $kh = a'$ e un intero s con $ks = b'$. Ricordando la definizione di a', b', abbiamo $kh(a, b) = a$ e $ks(a, b) = b$. Quindi $k(a, b)$ divide sia a che b. Ma (a, b) è il massimo divisore comune di a e b. Quindi $k = 1$. □

Definizione 5.16. Un inverso di a modulo n è un intero x tale che $ax \equiv 1 \bmod (n)$.

Esempio 5.17. 2 è un inverso di 3 modulo 5 in quanto $2 \cdot 3 = 6 \equiv 1 \bmod (5)$.

Esempio 5.18. Non ci sono inversi di 2 modulo 4.

Dimostrazione. Dato un intero qualunque x, esso è congruo modulo 4 ad uno dei numeri $0, 1, 2$ o 3. Visto che nessuno di questi è un inverso di 2 modulo 4 (verificatelo!), neanche x lo è. □

Teorema 5.19. *Un numero a ha un inverso modulo m se e solo se $(a, m) = 1$.*

Dimostrazione. Se $(a, m) = 1$ per il teorema di Bezout possiamo trovare u, v interi tali che $au + mv = 1$ con u, v interi. Abbiamo $au + bv \equiv au + 0 \equiv au \bmod (m)$. Quindi u è un inverso di a modulo m.

Viceversa supponendo che a abbia un inverso u modulo m, ovvero $au \equiv 1 \bmod (m)$, allora per definizione di congruenza esiste k tale che $au + mk = 1$. Questo implica $(a, m) = 1$. □

OSSERVAZIONE 5.20. Non sempre possiamo dividere in una congruenza. Ad esempio $2 \cdot 7 \equiv 2 \cdot 4 \bmod 6$, ma $7 \not\equiv 4 \bmod 6$.

TEOREMA 5.21. *Se* $ac \equiv bc \bmod m$ *e* $(c, m) = 1$, *allora* $a \equiv b \bmod m$.
Casi particolari: m *primo,* $0 < c < m$.

DIMOSTRAZIONE. Dall'ipotesi $(c, m) = 1$ segue che esiste un inverso u di c modulo m. Moltiplicando entrambi i termini della congruenza $ac \equiv bc \bmod m$ per u (cosa sempre lecita) otteniamo $acu \equiv bcu \bmod (m)$. Siccome $cu \equiv 1 \bmod (m)$, possiamo cancellare cu dai due termini della congruenza ottenendo $a \equiv b \bmod (m)$. □

ESEMPIO 5.22. Trovare tutte le soluzioni intere x, y di

$$54 = 252x + 198y.$$

Soluzione: dividendo tutto per $18 = (252, 198)$ otteniamo il sistema equivalente (cioè con le stesse soluzioni):

$$3 = 14x + 11y$$

Il problema si riduce a trovare tutte le soluzioni intere di quest'ultima equazione. Abbiamo $(14, 11) = 1$. Quindi per il teorema di Bezout esistono u, v con $14u + 11v = 1$. In effetti applicando il metodo per trovare u, v si trova $1 = 14 \cdot 4 + 11 \cdot (-5)$. Moltiplicando per tre otteniamo $3 = 14 \cdot 12 + 11 \cdot (-15)$. Quindi una soluzione è

$$x_0 = 12, y_0 = -15.$$

Altre soluzioni sono

$$x = 12 + 11k,\ y = -15 - 14k$$

come si vede osservando che $14(x_0 + 11k) + 11(y_0 - 14k) = 14x_0 + 11y_0 = 3$. Al variare di k queste sono tutte le soluzioni. Per dimostrarlo osserviamo che dall'equazione $1 \equiv 14 \cdot 4 \bmod (11)$, si deduce che 4 è l'inverso di 14 modulo 11. Moltiplicando per 4 l'equazione $3 = 14x + 11y$ otteniamo l'equazione equivalente $3 \cdot 4 = 14 \cdot 4x + 11 \cdot 4y$. Riducendola modulo 11 e semplificando otteniamo $12 \equiv x \bmod (11)$, quindi x è dellla forma $x = 12 + 11k$ che è appunto uno dei valori trovati in precedenza. Visto che $14x + 11y$ deve essere 3, nota la $x = 12 + 11k$ la y è deteminata, e facendo i conti si ritrova $y = -15 - 14k$.

6. Metodi per risolvere le congruenze lineari in una incognita

PROBLEMA 6.1. Dati $a, b, c \in \mathbb{Z}$ con $c > 0$ vogliamo trovare $x \in Z$ che risolve la congruenza

$$ax \equiv b \bmod (c) \tag{1}$$

Possiamo innanzitutto fare le seguenti osservazioni:

OSSERVAZIONE 6.2. Se esiste un intero d che divide a e c ma non divide b, allora la congruenza (1) non ha soluzioni. In particolare se il massimo comun divisore (a, c) di a e c non divide b la congruenza non ha soluzioni.[2]

DIMOSTRAZIONE. Se (1) ha soluzioni esiste un intero x_0 e un intero k tali che $ax_0 = b + kc$, ma supponendo che d divide a e c si vede subito che deve dividere anche b. □

ESEMPIO 6.3. $6x \equiv 3 \bmod 4$ non ha soluzioni perché 2 divide 6 e 4 ma non divide 3.

OSSERVAZIONE 6.4. Se esiste un intero e che è un inverso di a modulo c allora la congruenza (1) ha soluzioni e inoltre, conoscendo e, è facile trovarle tutte.

[2]Vedremo in seguito che se invece (a, c) divide b allora la congruenza ha soluzioni.

DIMOSTRAZIONE. Se e è un inverso di a modulo c allora per definizione abbiamo $ae \equiv 1 \bmod (c)$. Moltiplicando entrambi in membri della (1) per e, otteniamo la congruenza equivalente: $aex \equiv be \bmod (c)$ e visto che $ae \equiv 1 \bmod (c)$ possiamo semplificare ottenendo la congruenza equivalente

$$x \equiv be \bmod (c) \tag{2}$$

che ha come soluzioni tutti e soli gli interi x della forma $be + kc$ al variare di k in $\mathbb{Z}$. □

ESEMPIO 6.5. Ad esempio, visto che 2 è un inverso di 3 modulo 5, la congruenza $3x \equiv 4 \bmod 5$ si semplifica in $x \equiv 2 \cdot 4 \bmod 5$ e ha come soluzioni tutti e soli i valori di x della forma $8 + 5k$ al variare di k in $\mathbb{Z}$.

Potrebbe accadere che nessune delle due precedenti osservazioni sia applicabile. Ad esempio consideriamo la congruenza $4x \equiv 8 \bmod 10$. Tuttavia dopo opportune semplificazioni ci possiamo sempre ricondurre ad uno dei due casi visti sopra.

OSSERVAZIONE 6.6. Nel risolvere la (1) possiamo ricondurci al caso in cui $0 \leq a < c$ e $0 \leq b < c$ sostituendo a e b con il loro resti modulo c.

OSSERVAZIONE 6.7. Se esiste un intero $d > 1$ che divide tutti e tre i numeri a, b, c allora possiamo rimpiazzare a, b, c con $a' = a/d, b' = b/d, c' = c/d$ ottenendo la congruenza equivalente (dimostratelo)

$$a'x \equiv b' \bmod (c') \tag{$*$}$$

che coinvolge numeri più piccoli.

Ora supponendo di aver diviso per il valore di d più grande possibile, ci riconduciamo al caso in cui nella (*) non vi siano altre semplificazioni possibili, ovvero non vi siamo altri fattori positivi che dividono tutti e tre i numeri a', b', c'.

Possiamo ora dimostrare il seguente teorema, la cui dimostrazione fornisce anche un algoritmo per trovare tutte le soluzioni quando esistono.

TEOREMA 6.8. *La congruenza (1) ha soluzione se e solo se il massimo comun divisore tra a e b divide c.*

DIMOSTRAZIONE. Se (a, c) non divide b sappiamo già che la (1) non ha soluzioni. Quindi consideriamo il caso in cui (a, c) divide b. Dividendo a, b, c per il massimo fattore positivo comune a tutti e tre i numeri otteniamo la congruenza equivalente (*). Per ipotesi nella (*) non vi sono fattori > 1 che dividono tutti e tre i numeri a', b', c' (altrimenti avremmo potuto ulteriormente semplificare). A questo punto calcoliamo il massimo comun divisore (a', c'). Esso deve necessariamente dividere b' visto che (a, c) divideva b (dimostratelo!). Ma allora (a', c') deve essere necessariamente uguale a 1 (altrimenti a', b', c' avrebbero avuto un fattore in comune maggiore di 1). Quindi a' e c' sono coprimi e sappiamo che in questo caso a' ha un inverso e' modulo c' (si può applicare l'algoritmo di Bezout per ottenere due interi x', y' che risolvono l'equazione $1 = a'x' + c'y'$ e poi si prende $e' = x'$). Una volta trovato e' sappiamo che le soluzioni della (*), e quindi anche della congruenza equivalente (1), sono tutti e soli gli interi della forma $e'b' + kc'$ al variare di k in $\mathbb{Z}$. □

ESERCIZIO 6.9. 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.

SOLUZIONE: 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 membro di destra, membro di sinistra e modulo per $MCD\ (195, 42) = 3$, ottenendo l'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. □