Università degli Studi di Palermo
Corso di Laurea in Informatica

Corso di metodi matematici per l'informatica

Docente del corso:
Prof.ssa Sabrina Mantaci

Anno Accademico 2013-2014

Indice

Capitolo 1

Elementi di Logica Matematica

1.1 Proposizioni e predicati

Definizione 1 *Si definisce* proposizione logica (o brevemente *proposizione) una frase di senso compiuto in cui sia contenuta un'affermazione che può assumere valore* `vero` *o* `falso`.

Il nome della proposizione può essere una qualunque successione di caratteri alfabetici e numerici, per esempio P, $Prop$, P_1 etc..

Esempio 2 Diamo alcuni esempi:

- $P =$ "$10 > 6$"
  è un esempio di proposizione vera: P è il *nome della proposizione*, fra virgolette si trova il *testo o enunciato della proposizione*.
- $Q =$ "Palermo è una città della Liguria"
  è una proposizione (falsa);
- $R =$ "Ciao"
  non è una proposizione (è un saluto ma non contiene un'affermazione).

- $T =$ "esiste vita intelligente al di fuori della terra"
  è una proposizione (anche se non sappiamo attualmente se sia vera o falsa).

Il valore di verità o falsità di una proposizione può anche non essere conosciuto.

Inoltre le proposizioni possono essere combinate tra loro per costruire delle proposizioni più complesse utilizzando dei connettivi, quali "e", "o", "non", "se... allora...", ecc. Chiameremo *atomiche* quelle proposizioni che non sono ottenute da proposizioni più semplici mediante l'uso di connettivi. Ad esempio:

- "4 è un numero pari" è una proposizione atomica,
- "Se c'è il sole allora vado al mare" è una proposizione composta (le cui componenti sono "C'è il sole" e "Vado al mare").

1.1.1 Linguaggi formali

Per formalizzare questi concetti abbiamo bisogno di costruire un linguaggio formale che permetta di esprimere e comporre tutte le proposizioni. I linguaggi formali si rendono necessari tutte le volte che il linguaggio naturale (l'italiano, l'inglese, il francese...) non è sufficiente a descrivere dei concetti matematici e informatici in maniera semplice, schematica e non ambigua. La logica matematica in particolare, ha bisogno di un linguaggio molto più semplice di quelli naturali, che chiameremo *linguaggio formale*.

Per costruire un linguaggio formale bisogna fissare un *alfabeto*, cioè un insieme di simboli che ci serviranno a costruire delle "frasi" (che, in questo contesto, chiameremo *formule*). Le "frasi" non sono altro che delle sequenze finite (stringhe) di simboli che appartengono all'alfabeto che abbiamo fissato.

Si dà inoltre un insieme di regole per stabilire quali sequenze di simboli sono accettabili nel nostro linguaggio e quali no. Queste regole danno la

sintassi, ossia il modo di stabilire se una formula è corretta secondo le regole fissate
Attenzione: la sintassi si occupa solo della forma delle frasi e non del loro contenuto, che riguarda invece la *semantica*.

Esempio 3 Un primo esempio di linguaggio formale, ben noto a tutti, è quello delle espressioni aritmetiche. L'alfabeto è fatto dall'insieme dei numeri reali (ma anche interi, razionali, complessi...), degli operatori aritmetici binari che servono a formare nuove espressioni, e degli operatori di confronto che devono confrontare due espressioni.

- $8 \cdot (3 - 2) = 8$, è una formula sintatticamente corretta;
- $= 8 + +(6(+ ==)$, è una formula sintatticamente non corretta
- $2 + 1 = 6$, è una formula sintatticamente corretta

Com'è ben noto, il risultato dell'ultima espressione non è corretto dal punto di vista del significato (semantico) pur essendo una formula formalmente corretta.

Esempio 4 Un altro classico esempio di linguaggi formali sono, nell'informatica, i linguaggi di programmazione. In tali linguaggi viene infatti stabilito un numero finito di parole chiave e regole che permettono di esprimere in maniera schematica le istruzioni di un algoritmo. Un programma sarà corretto sintatticamente se le istruzioni rispettano le regole del linguaggio. I compilatori, che sono programmi che si occupano di creare la versione eseguibile di un programma, non fa altro, prima di creare l'eseguibile, che verificare la correttezza del programma dal punto di vista sintattico, rispetto alle regole del linguaggio di programmazione considerato. Il fatto che il programma sia sintatticamente corretto non garantisce comunque che il programma svolga il compito che abbiamo in mente, se la semantica (in questo caso l'algoritmo) non è corretta. Detto in altre parole, non basta che il programma compili affinchè il programma sia corretto per il nostro scopo.

Le formule sintatticamente corrette saranno chiamate *Formule Ben Formate (FBF)*. Riassumendo: il compito della *sintassi* è quello di fornire un

insieme di regole per costruire le FBF. Solo quando una formula è sintatticamente corretta si può poi parlare del suo significato. Questo è il compito della *semantica*: assegnare un significato a tutte le frasi sintatticamente corrette (cioè a tutte le FBF).

1.1.2 Predicati

Introduciamo in questa sezione un concetto più generale di quello di proposizione.

Definizione 5 *Si definisce* predicato logico *(o brevemente* predicato*) una frase di senso compiuto che contiene un'affermazione relativa ad alcune variabili (spesso indicate con lettere come $x, y, z, \ldots$) e che diventa una proposizione (vera o falsa) quando si fanno assumere valori concreti alle variabili.*

Esempio 6

$$P(x, y) = \text{“}x + y > 40\text{”}$$

è un predicato nelle 2 variabili x, y. P è il *nome del predicato*, seguito dall'elenco (x, y), facoltativo, delle *variabili*; fra virgolette è contenuto il *testo* o *enunciato* del predicato. Se facciamo per esempio assumere alle variabili rispettivamente i valori $x = 19$, $y = 28$, otteniamo la proposizione (vera) $P(9, 8) = \text{“}19 + 28 > 40\text{”}$ mentre se facciamo per esempio assumere alle variabili rispettivamente i valori $x = 4$, $y = 5$, otteniamo la proposizione (falsa) $P(4, 5) = \text{“}4 + 5 > 40\text{”}$

La scelta arbitraria dei valori delle variabili potrebbe però portare a frasi senza senso logico (che quindi non sono delle proposizioni): se nel predicato $Q(x) = \text{“}x > 10\text{”}$ facessimo assumere alla variabile x il valore *“Palermo”* la frase ottenuta “*Palermo* > 10” sarebbe priva di senso. Per ovviare a questo inconveniente, talvolta si stabilisce in un predicato l'insieme dei valori possibili che possono assumere le variabili, indicando il *campo di variabilità* o *universo* (ossia indicando i valori permessi per le variabili).

Esempio 7 : Scrivendo il predicato

$$P(x) = \text{“}x < 20\text{”}$$

e precisando *universo = numeri interi positivi* si intende che nel predicato P gli unici valori leciti che si possono attribuire alla variabile x sono appunto gli interi positivi.

Osservazione 8 Si noti che una proposizione si può in pratica considerare un predicato senza variabili: in tal senso tutto ciò che diremo in seguito sui predicati si potrà applicare come caso particolare alle proposizioni.

1.2 Operatori logici

Al fine di definire le Formule ben formate in logica matematica, e quindi definirne il linguaggio formale, introduciamo alcuni operatori (logici) fra i predicati: essi permettono, dati uno o più predicati (detti *operandi*), di costruire un nuovo predicato (detto *risultato*) i cui valori di verità o falsità dipendono da quelli dei predicati operandi.

1.2.1 Congiunzione Logica

Definizione 9 *Dati due predicati P, Q, si chiama* congiunzione logica di P, Q *il predicato che:*

- *ha come nome $P \wedge Q$ (si legge "P and Q" oppure "P e Q");*
- *ha come testo i testi di P e Q separati dalla congiunzione "e" (di conseguenza ha come variabili le variabili di P e quelle di Q)*
- *è vero solo per i valori delle variabili che rendono veri sia P che Q, ed è falso per tutti gli altri valori delle variabili (quindi è falso per i valori delle variabili che rendono falso uno dei 2 predicati P, Q o che rendono falsi entrambi i predicati P, Q)*

Esempio 10 Dati i due predicati (con *universo = numeri interi positivi*)

$$P(x, y) = \text{“}x > y\text{”}$$

$$Q(y,z) = \text{“}y < z^2\text{”}$$

la loro congiunzione logica è il predicato

$$[P \wedge Q](x,y,z) = \text{“}x > y \text{ e } y < z^2\text{”}$$

nelle 3 variabili x, y, z. Tale nuovo predicato è vero solo per i valori di x, y che rendono vero P e i valori di y, z che rendono vero Q. Per esempio

$$[P \wedge Q](5,3,2) = \text{“}5 > 3 \text{ e } 3 < 2^2\text{”}$$

è una proposizione vera in quanto

$$P(5,3) = \text{“}5 > 3\text{”}$$

$$Q(3,2) = \text{“}3 < 2^2\text{”}$$

sono entrambe proposizioni vere. Invece

$$[P \wedge Q](6,4,1) = \text{“}6 > 4 \text{ e } 4 < 1^2\text{”}$$

è una proposizione falsa in quanto

$$P(6,4) = \text{“}6 > 4\text{”}$$

è una proposizione vera, ma

$$Q(4,1) = \text{“}4 < 1^2\text{”}$$

è una proposizione falsa. Analogamente

$$[P \wedge Q](1,2,4)$$

$$[P \wedge Q](2,4,2)$$

sono proposizioni false, la prima perché $P(1,2)$ è falsa (pur essendo $Q(2,4)$ vera), e la seconda perché entrambe $P(2,4), Q(4,2)$ sono false.

Se conveniamo che il simbolo 1 rappresenti “vero”e il simbolo 0 rappresenti “falso”, i possibili valori di verità della congiunzione $P \wedge Q$, in funzione di quelli di P e Q, sono schematicamente rappresentati dalle seguenti eguaglianze:

$$1 \wedge 1 = 1 \quad 1 \wedge 0 = 0 \quad 0 \wedge 1 = 0 \quad 0 \wedge 0 = 0$$

e si possono raccogliere in modo sintetico in una tavola della verità come nella Tabella 1.2.1. In alternativa si può considerare oppure come la Tabella1.2.1, con la convenzione che alle righe si fanno corrispondere i valori di P, alle colonne i valori di Q e nelle caselle all'incrocio fra righe e colonne i valori di $P \wedge Q$.

P	Q	$P \wedge Q$
1	1	1
1	0	0
0	1	0
0	0	0

Tabella 1.1: Tavola di verità dell'operatore $\wedge$

$\wedge$	1	0
1	1	0
0	0	0

Tabella 1.2: Altra rappresentazione della Tavola di verità dell'operatore $\wedge$

1.2.2 Disgiunzione Logica

Definizione 11 *Dati due predicati P, Q, si chiama* disgiunzione logica *di P, Q il predicato che:*

- *ha come nome $P \vee Q$ (si legge "P or Q" oppure "P o Q");*
- *ha come testo i testi di P e Q separati dalla congiunzione "o" (di conseguenza ha come variabili le variabili di P e quelle di Q)*
- *è falso solo per i valori delle variabili che rendono falsi sia P che Q, ed è vero per tutti gli altri valori delle variabili (quindi è vero per i valori delle variabili che rendono vero uno dei 2 predicati P, Q o quelli che rendono veri entrambi i predicati P, Q)*

Esempio 12 *Dati i 2 predicati (con universo = numeri interi positivi):*

$$P(x) = \text{“}x > 10\text{”}$$

$$Q(y) = \text{“}y \text{ è pari”}$$

la loro congiunzione logica è il predicato

$$[P \vee Q](x, y) = \text{“}x > 10 \text{ o } y \text{ è pari”}$$

Tale nuovo predicato è falso solo per i valori di x che rendono falso P e i valori di y che rendono falso Q. Per esempio

$$[P \vee Q](11, 3) = \text{“}11 > 10 \text{ } o \text{ } 3 \text{ } è \text{ } pari\text{”}$$

è una proposizione vera in quanto $P(11) =$ “$11 > 10$” è una proposizione vera, pur essendo $Q(3) =$ “3 è pari” una proposizione falsa. Invece

$$[P \vee Q](9, 5) = \text{“}9 > 10 \text{ } o \text{ } 5 \text{ } è \text{ } pari\text{”}$$

è una proposizione falsa in quanto entrambe le proposizioni $P(9), Q(5)$ sono false.

I possibili valori di verità della disgiunzione $P \vee Q$, in funzione di quelli di P e Q, sono schematizzati come segue:

$$1 \vee 1 = 1 \quad 1 \vee 0 = 1 \quad 0 \vee 1 = 1 \quad 0 \vee 0 = 0$$

Nella tabelle 1.2.2 e 1.2.2 sono indicate due possibili modi di rappresentare le tavole di verità della disgiunzione logica $P \vee Q$. Nella tabella 1.2.2 si conviene che alle righe si fanno corrispondere i valori di P, alle colonne i valori di Q, e nelle caselle all'incrocio fra righe e colonne i valori di $P \vee Q$.

P	Q	$P \vee Q$
1	1	1
1	0	1
0	1	1
0	0	0

Tabella 1.3: Tavola di verità dell'operatore $\vee$

$\vee$	1	0
1	1	1
0	1	0

Tabella 1.4: Altra rappresentazione della tavola di verità dell'operatore $\vee$

Osservazione 13 Si noti come la disgiunzione logica ora definita sia "non esclusiva" ossia è vera anche quando i 2 predicati sono entrambi veri e non solo quando uno solo dei 2 predicati è vero. Nel linguaggio comune il significato della congiunzione "o" può essere invece "esclusivo" e quindi diverso da quello da noi definito: per esempio se affermiamo che è vero che "$x > 5$ o $y < 7$", nel linguaggio comune ciò potrebbe significare che $x > 5$ oppure $y < 7$ ma non simultaneamente $x > 5$ e $y < 7$. In questo caso parleremo di "or" esclusivo o "xor".

1.2.3 Negazione Logica

Definizione 14 *Dati un predicato P si chiama* negazione logica di P *il predicato che:*

- *ha come nome $\neg P$ (si legge not "P" oppure "non P");*
- *ha un testo che è opposto di quello di P da un punto di vista logico (di conseguenza ha le stesse variabili di P);*
- *è vero per tutti i valori delle variabili per cui è falso P, ed è falso per tutti i valori delle variabili per cui è vero P.*

Per esempio dato il predicato:

$$P(x) = \text{“}x > 6\text{”}$$

(con campo di variabilità x numero intero positivo) la sua negazione logica può essere

$$\neg P(x) = \text{“non è vero che } x > 6\text{”}$$

oppure, più elegantemente:

$$P(x) = \text{“}x \leq 6\text{”}.$$

I possibili valori di verità della negazione logica P, in funzione di quelli di P, sono i seguenti: $\neg 1 = 0 \quad \neg 0 = 1$ La tavola di verità della negazione logica $\neg$ è rappresentata nella Tabella 1.2.3

P	$\neg P$
1	0
0	1

Tabella 1.5: Tavola di verità dell'operatore $\neg$

Esercizi 15 *Per quali valori in corrispondenza dei predicati indicati nei diversi esercizi, i predicati:* $P \wedge Q$, $P \vee Q$, $\neg P$, $\neg Q$ *sono veri?*

1. $P =$ "$x^2 > 5$"; $Q =$ "$2 \cdot x^2 - 3 \cdot x + 1 < 0$"

1.3 Implicazioni ed Equivalenze

1.3.1 Implicazioni Logiche

Definizione 16 *Dati due predicati* P,Q, *definiti sullo stesso insieme di variabili, diremo che* P implica Q *(oppure:* da P segue Q, *o ancora:* se P allora Q, *o* P è condizione sufficiente per Q, *o* Q è condizione necessaria per P*) quando tutti i valori delle variabili che rendono vero* P *rendono vero anche* Q. *In questo caso scriveremo il simbolo* $P \Rightarrow Q$

Anche per l'implicazione logica si può costruire la tavola di verità

P	Q	$P \Rightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

Le ultime due righe significano che nel momento in cui sappiamo che l'ipotesi è falsa, niente può essere detto sul valore assunto dalla tesi (entrambe le possibilità di implicazione sono vere).

Per esempio se la nostra proposizione è "se piove allora ci sono le nuvole in cielo", la falsità dell'ipotesi (piove) fa si che entrambe le possibilità per Q (ci sono o non ci sono le nuvole in cielo) danno luogo ad una implicazione vera.

Esempio 17 *Se sono dati i seguenti predicati (con universo = numeri interi positivi):*

$$P(x) = \text{“}x < 4\text{”}'' \text{ e } Q(x) = \text{“}x + 3 < 9\text{”}$$

allora è vero che P implica Q perché i valori della x che rendono vero P sono esattamente $x = 1, 2, 3$ e si verifica facilmente che essi rendono vero anche Q.

Dimostrare questa implicazione è molto facile perchè i valori che verificano P e Q sono in numero finito. Spesso però i valori delle variabili che rendono vero P sono in numero infinito, e in tal caso non è possibile, come nell'esempio precedente, verificare singolarmente che ciascuno di essi rende vero anche Q.

1.3.2 Equivalenza logica

Definizione 18 *Dati due predicati P, Q, nelle stesse variabili, e se $P \Rightarrow Q$ ed anche $Q \Rightarrow P$, diremo che P, Q sono* equivalenti *(diremo anche: P* se e solo se *Q, o ancora: P è* condizione necessaria e sufficiente per *Q): in tal caso scriveremo $P \Leftrightarrow Q$.*

In questo caso i valori delle variabili che rendono vero P rendono vero anche Q e viceversa, quindi i valori delle variabili che rendono vero P sono esattamente gli stessi che rendono vero Q: possiamo dire che P, Q in pratica rappresentano la stessa affermazione da un punto di vista logico. La tavola di verità dell'equivalenza logica è quindi la seguente:

P	Q	$P \Rightarrow Q$
1	1	1
1	0	0
0	1	0
0	0	1

Esempio 19 Nell'universo dei numeri interi positivi, i predicati

$$P(x) = \text{“}x < 4\text{”}$$
$$Q(x) = \text{“}x^2 < 12\text{”}$$

sono equivalenti. Infatti i valori della variabile x che rendono vero P sono $x = 1, 2, 3$ e sono esattamente gli stessi valori della variabile x che rendono vero Q: si conclude che $P \Leftrightarrow Q$. Quindi (nell'universo dei numeri interi positivi) “$x < 4$” ed “$x^2 < 12$” sono la stessa affermazione dal punto di vista logico.

Notiamo che, se modifichiamo l'universo della variabile (pur lasciando invariati i predicati) essi possono anche non essere più equivalenti: per esempio (con P, Q definiti come sopra) se l'universo è quello dei numeri razionali positivi, allora non è più vero che $P \Leftrightarrow Q$ (basta notare che P non implica Q perché per esempio il valore della variabile $x = \frac{7}{2}$ rende vero P ma falso Q).

1.3.3 Applicazioni

Si considerino i seguenti predicati logici:

$P =$ “x è multiplo di 5”
$Q =$ “x è multiplo di 2”
$P \vee Q =$ “x è multiplo di 5 o x è multiplo di 2”
$P \wedge Q =$ “x è multiplo di 5 e x è multiplo di 2”
$\neg P =$ “x non è multiplo di 5”
$\neg Q =$ “x non è multiplo di 2”

$\neg P \vee \neg Q =$ "x non è multiplo di 5 o x non è multiplo di 2"
$\neg P \wedge Q =$ "x non è multiplo di 5 e non è multiplo di 2"
$\neg(P \vee Q) =$ "non è vero che x è multiplo di 2 o di 5= "x non è multiplo né di 2 né di 5"
$\neg(P \wedge Q) =$ "non è vero che x è multiplo di 2 e di 5= "x non è multiplo di 2 o x non è multiplo di 5"
$\neg(\neg P) =$" non è vero che x non è multiplo di 5= "x è multiplo di 5"

Si può osservare che $\neg P \vee \neg Q$ e $\neg(P \wedge Q)$ hanno lo stesso significato logico ossia ad ogni scelta del valore della x assumono lo stesso valore. Analogamente $\neg P \wedge \neg Q$ e $\neg(P \vee Q)$, e P e $\neg(\neg P)$. Questa cosa è sempre vera e si può dedurre dalle seguenti tabelle di verità:

P	Q	$P \vee Q$	$P \wedge Q$	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$	$\neg P \vee \neg Q$	$\neg(P \wedge Q)$	$\neg(P \vee Q)$	$\neg(\neg P)$
1	1	1	1	0	0	0	0	0	0	1
1	0	1	0	0	1	1	0	0	1	1
0	1	1	0	1	0	1	0	0	0	0
0	0	0	0	1	1	1	1	1	1	0

Da cui si possono dedurre le equivalenza fra diverse espressioni logiche. In particolare:

$$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$$
$$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$$

Queste due equivalenze logiche sono note come le *leggi di De Morgan* Inoltre l'equivalenza

$$\neg(\neg P) \Leftrightarrow P$$

è nota come proprietà della *doppia negazione*.

L'utilizzo delle tavole di verità dà un metodo per stabilire alcune equivalenze logiche. Se due espressioni logiche hanno la stessa tavola di verità allora sono equivalenti

Esercizi

Dimostrare le seguenti equivalenze logiche:

1. $P \vee \neg P \Leftrightarrow 1$;
2. $(P \wedge \neg P) \Leftrightarrow 0$;
3. $P \wedge 1 \Leftrightarrow P$;
   $P \vee 0 \Leftrightarrow P$ (*cancellazione*);
4. $P \vee 1 \Leftrightarrow 1$
   $P \wedge 0 \Leftrightarrow 0$ (*dominanza*);
5. $P \vee P \Leftrightarrow P$
   $P \wedge P \Leftrightarrow P$ (*idempotenza*);
6. $P \vee Q \Leftrightarrow Q \vee P$
   $P \wedge Q \Leftrightarrow Q \vee P$ (*commutatività*);
7. $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$
   $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \vee R)$ (*associatività*);
8. $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$
   $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$ (*distributività*);
9. $[P \vee (P \wedge Q)] \Leftrightarrow P$
   $[P \wedge (P \vee Q)] \Leftrightarrow P$ (*assorbimento*).

1.3.4 Formule Ben Formate

Siamo a questo punto pronti per definire una Formula Ben Formata (FBF) nella logica proposizionale.

Definizione 20 *Una* formula ben formata *(o* formula *più brevemente) nella* logica proposizionale *e nella* logica dei predicati o logica del I ordine *è definita ricorsivamente come segue:*

- *un predicato atomico è una formula;*
- *se P è una formula allora (P), $\neg(P)$ sono formule;*

- *se P e Q sono formule allora $P \wedge Q$, $P \vee Q$, $P \Rightarrow Q$, $P \Leftrightarrow Q$ sono formule.*

Tutte le formule ben formate sono generate applicando le regole precedenti

1.4 Metodi di dimostrazione

In questa sezione indichiamo alcuni metodi per la dimostrazione dei teoremi. La validità dei metodi è dettata da opportune equivalenze logiche.

1.4.1 Dimostrazione diretta

Spesso i valori delle variabili che rendono vero P sono in numero infinito, e in tal caso non è possibile, come nell'esempio 17, verificare singolarmente che ciascuno di essi rende vero anche Q. In tal caso per dimostrare le implicazioni (e quindi le equivalenze) logiche si ricorre a una **dimostrazione logico-deduttiva o diretta**: si suppone di avere un valore generico (ma non precisato) delle variabili che rende vero P (*ipotesi*), e attraverso delle deduzioni logiche (*passaggi della dimostrazione*) giustificate da conoscenze acquisite in precedenza, si cerca di dimostrare che tale valore delle variabili rende vero anche Q (*tesi*).

Esempio 21 Se sono dati i seguenti predicati (con universo: numeri interi positivi):

$$P(x) = \text{“}x > 7\text{”} \text{ e } Q(x) = \text{“}x + 5 > 8\text{”}$$

per dimostrare che $P \Rightarrow Q$ si potrebbe procedere operando i seguenti passaggi:
1) supponiamo che x sia un valore che renda vero P (ipotesi) quindi che x sia un intero positivo tale che $x > 7$

2) sommando 5 ad ambo i membri della diseguaglianza $x > 7$ si ha $x+5 > 12$ (applicando la proprietà delle diseguaglianze che permette di sommare ad ambo i membri lo stesso numero ottenendo una diseguaglianza ancora valida)
3) da $x + 5 > 12$ e $12 > 8$ si ottiene $x + 5 > 8$ (applicando la cosiddetta proprietà transitiva dell'ordinamento dei numeri interi positivi) quindi x rende vero anche Q (tesi)

Esempio 22 Date le seguenti definizioni: un intero n è *pari* se esiste un intero k tale che $n = 2 \cdot k$. Un intero n è *dispari* se esiste un intero k tale che $n = 2 \cdot k + 1$.

Dimostrare che "e n è un intero dispari allora n^2 è dispari".

$$P(n) = \text{“}n \text{ è un intero dispari”}$$
$$Q(n) = \text{“}n^2 \text{ è un intero dispari”}$$

l'enunciato del teorema equivale a dire che $P(n) \Rightarrow Q(n)$.

Dimostrazione (diretta): Se n è un intero dispari, allora esiste un k tale che $n = 2 \cdot k + 1$. Allora $n^2 = (2 \cdot k + 1)^2 = 4 \cdot k^2 + 4 \cdot k + 1 = 2 \cdot (2 \cdot k^2 + 2k) + 1$, cioè esiste $h = (2 \cdot k^2 + 2 \cdot k)$ tale che $n \cdot 2 = 2 \cdot h + 1$. Quindi n^2 è dispari. □

Tutti i **teoremi matematici** sono in pratica espressi sotto forma di implicazione fra 2 predicati. Per esempio il famoso Teorema geometrico:

"la somma delle ampiezze degli angoli interni di un triangolo è 180"

non è altro che l'implicazione $P \Rightarrow Q$ dove i predicati P, Q sono i seguenti: $P(x)$ ="x è un triangolo", $Q(x)$ ="la somma delle ampiezze degli angoli interni di x è 180°" (con universo = poligoni nel piano).

ESERCIZI: Dimostrare in maniera diretta le seguenti affermazioni:

1. Dato un numero dispari a, esistono due interi b e c tali che $a^2 + b^2 = c^2$.

2. Dimostrare che se n è multiplo di 12 allora n è multiplo di 4.

1.4.2 Dimostrazione per assurdo

Abbiamo già illustrato una tecnica per dimostrare vera un'implicazione $P \Rightarrow Q$ fra 2 predicati: si suppone di avere fissato un valore generico (ma non precisato) delle variabili che rende vero P (*ipotesi*), e attraverso dei passaggi intermedi (giustificati da conoscenze acquisite in precedenza) si cerca di dimostrare che tale valore rende vero anche Q (*tesi*).

La tecnica dimostrativa illustrata sopra è detta anche diretta. Vi è però anche una diversa tecnica dimostrativa, detta *per assurdo*. Per dimostrare vera l'implicazione $P \Rightarrow Q$:
1. Si suppone (per assurdo) che sia dato un valore delle variabili che renda vero P ma falso Q (quindi si suppone per assurdo vera l'ipotesi e falsa la tesi ossia si considera $\neg Q \wedge P$);
2. Attraverso dei passaggi intermedi (sempre opportunamente giustificati) si cerca di pervenire ad una *contraddizione logica*, ossia un'affermazione che è contemporaneamente vera e falsa;
3. se tale contraddizione viene raggiunta, si può concludere che in effetti non esiste un valore delle variabili che renda vero P e falso Q, e che dunque in effetti $P \Rightarrow Q$).

Detto in termini formali, una dimostrazione per assurdo corrisponde all'equivalenza logica

$$(P \Rightarrow Q) \Leftrightarrow (\neg Q \wedge P \Rightarrow 0).$$

Esempio 23 Per esempio se sono dati i seguenti predicati (con universo=numeri interi positivi):

$$P(x) = \text{“}x \text{ è pari”}$$
$$Q(x) = \text{“}x + 1 \text{ è dispari”}.$$

Per dimostrare che $P \Rightarrow Q$ con la tecnica della dimostrazione per assurdo si potrebbe procedere operando i seguenti passaggi:

1) supponiamo (per assurdo) che esista un valore della variabile x che renda vero P ma falso Q (cioè $\neg Q$ vero), quindi x sia pari, ma $x+1$ non sia dispari, cioè $x+1$ sia pari
2) applicando la definizione di numero pari, si ha $x = 2 \cdot z$, $x+1 = 2 \cdot t$, dove z, t sono opportuni numeri interi positivi
3) sottraendo la prima eguaglianza dalla seconda eguaglianza, si ha $1 = 2 \cdot t - 2 \cdot z$
4) applicando la proprietà distributiva della differenza rispetto al prodotto si ha $1 = 2(t - z)$ e si ottiene che 1 è multiplo di 2 (contraddizione logica).

Avendo ottenuto una contraddizione logica, si può concludere che in effetti è vero che $P \Rightarrow Q$.

ESERCIZI: Provare per contraddizione i seguenti fatti:

1. 200 non è un quadrato perfetto;
2. Per tutti i numeri naturali $n^2 + 7n + 12$ è un numero pari.
3. dimostrare che se a^2 è pari, allora a è pari.
4. dimostrare che $\sqrt{2}$ è irrazionale.
5. dimostrare che 29 è un numero primo.

1.4.3 Dimostrazione per contrapposizione

Un particolare tipo di dimostrazione è quella per contrapposizione.

Si considerino due predicati P e Q e le loro negazioni $\neg P$ e $\neg Q$ Consideriamo la tabella di verità:

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg Q \Rightarrow \neg P$	$\neg Q \wedge P$	$\neg Q \wedge P \Rightarrow 0$
1	1	1	0	0	1	0	1
1	0	0	0	1	0	1	0
0	1	1	1	0	1	0	1
0	0	1	1	1	1	0	1

Si noti che nella tabella sopra la terza, la sesta e l'ottava colonna hanno gli stessi valori, quindi rappresentano delle equivalenze logiche. La terza colonna descrive la dimostrazione diretta, la sesta la dimostrazione per contrapposizione e l'ottava quella per assurdo. Quindi $P \Rightarrow Q$ è equivalente a $\neg Q \Rightarrow \neg P$. Significa che la negazione della tesi implica la negazione dell'ipotesi (contraddizione).

Quindi una dimostrazione per contrapposizione si effettua nel modo seguente:
1, $\neg Q$ è l'ipotesi.
2. Dimostrare che vale $\neg P$.

Esempio 24 Se n è un intero e $3n + 2$ è dispari allora n è dispari.

Ipotesi: $P(n)$: " n è un intero" $\wedge$ "$3n + 2$ è dispari"
Tesi: $Q(n)$: "n è dispari"

Dimostrazione[Per contrapposizione] Assumiamo $Q(n)$ falso, cioè n pari. Per definizione di numero pari $n = 2 \cdot k$, con k intero. Sostituiamo n con $2 \cdot k$:

$$3n + 2 = 3 \cdot (2k) + 2 = 6k + 2 = 2(3k + 1)$$

pertanto, $3n + 2$ è multiplo di 2 cioè $3n + 2$ è pari (negazione dell'ipotesi)
□

La stessa affermazione può essere dimostrata per assurdo nel modo seguente:
Dimostrazione[per assurdo] Supponiamo che sia vero $\neg Q \wedge P$. Quindi supponiamo n pari e $3n + 2$ dispari. Ma se n è pari, lo è anche $3n$. Poichè se

sottraiamo a un numero dispari un numero pari otteniamo un numero dispari, quindi $(3n+2)-(3n)=2$ è un numero dispari. Siamo arrivati a una conclusione assurda (2 è contemporaneamente pari e dispari).

□

1.4.4 I Controesempi

Se non è vero che un predicato P implica un predicato Q, diremo che P *non implica* Q. E' ovvio che se si vuole verificare che un predicato P non implica un predicato Q, allora non si deve procedere con una dimostrazione, ma cercare almeno un valore delle variabili che renda vero P ma renda falso Q, detto *controesempio.*

In uno degli esempi precedenti:
$P(x)=$ "$x>7$"
$Q(x)=$ "$x+5>8$"
abbiamo già dimostrato che si ha $P \Rightarrow Q$. Tuttavia non è vero che $Q \Rightarrow P$, in quanto è possibile esibire valori di x che rendono vero Q ma falso P (per es. $x=5$).

ESERCIZI: Far vedere che le seguenti affermazioni sono false:

1. Per tutti i numeri naturali n, $7n+2$ è un quadrato perfetto.
2. se n è multiplo di 3 allora n è multiplo di 7.
3. Ogni numero positivo può essere scritto come la somma di quadrati di tre interi

1.4.5 Parallelismi tra metodi di dimostrazione in Matematica e programmazione nell'Informatica

Una buona dimostrazione deve essere: corretta, completa, chiara, breve, elegante, ben organizzata, in ordine. Tutte queste caratteristiche sono condivise con i programmi. Scrivere dimostrazioni è come scrivere programmi, eccetto che ogni passo della dimostrazione deve essere giustificato! Un buon codice è "well-commented" ed è scritto in modo chiaro, che possa cioè essere capito facilmente anche da altri. In maniera simile buone dimostrazioni devono essere facili da capire. Una buona dimostrazione fa uso di frasi esplicative. Un buon programma fa uso di commenti.

La dimostrazione (come un programma) deve essere di semplice lettura, quindi non fare ricorso a troppe variabili, non essere prolissa, non deve fare riferimento a fatti mai dimostrati da nessuno (come richiamare in un programma una funzione non dichiarata), e in ogni caso la dimostrazione (come il programma) deve ricoprire tutti i casi (non farlo è un tipico errore in cui si incorre nelle dimostrazioni per induzione, di cui parleremo in seguito).

Tipico errore dei (giovani) programmatori è quello di giustificare la correttezza dei loro programmi mediante l'apporto di un numero finito di esempi. Poiché i programmi generalmente devono funzionare su un universo infinito (cioè devono valere per ogni input), dare un numero finito di esempi non dà una dimostrazione della correttezza del programma, che generalmente può essere provata mediante una dimostrazione matematica. Tutti gli algoritmi non sono altro che teoremi matematici costruttivi (ossia che costruiscono una soluzione) e come tali devono essere dimostrati. In definitiva non esiste la dimostrazione della correttezza di un algoritmo mediante esempi. Viceversa, un controesempio può essere solo un modo per dimostrare che il programma non funziona.

1.4.6 Quantificatori esistenziali e universali

Per concludere questa breve trattazione sulla logica elementare, introduciamo quelli che sono detti quantificatori (universale e esistenziale) L'affermazione "Tutti gli uomini sono mortali" è un'affermazione universale (vera), ossia che è sempre valida per ogni elemento dell'universo preso in considerazione. Ma anche l'affermazione "ogni numero che è multiplo di 6, è multiplo anche di 3" è un'affermazione universale (vera). Anche l'affermazione "ogni multiplo di 3 è anche multiplo di 6" è un'affermazione universale, ma questa volta è falsa (per esempio, 3 è multiplo di 3 ma non di 6). Da ciò si deduce che affinchè un'affermazione universale sia falsa, occorre trovare un controesempio, ossia un valore delle variabili che rende falsa l'affermazione.

Per rappresentare le affermazioni (o predicati) universali, utilizziamo il simbolo $\forall$, che è un'abbreviazione dell'espressione "per tutti". Questo simbolo si chiama *quantificatore universale*. Si può trovare in predicati del tipo "$\forall x \in \mathbb{N}, x^2$ è pari " ("per ogni numero naturale, il suo quadrato è pari". Ovviamente un predicato sempre falso).

Un'affermazione esistenziale è un'affermazione del tipo "Esiste un uomo che corre i 100 piani in meno di 10 secondi" (vero), oppure "esiste un intero n tale che $n^2 = 144$" (vero) oppure "Esistono due numeri interi n ed m tali che $n^2 = 2m^2$" (falso).

Il simbolo $\exists$ è un'abbreviazione per "esiste". Si chiama *quantificatore esistenziale*. Si può trovare in predicato del tipo "$\exists x \in N, x^2$ è pari" ("esiste un numero naturale tale che il suo quadrato è pari". Ovviamente questo predicato è vero, in quanto il quadrato di ogni numero pari è pari)

I quantificatori esistenziali e universali sono legati dalle seguenti relazioni

$$\neg(\exists x : P(x)) \Leftrightarrow \forall x : \neg P(x)$$
$$\neg(\forall x : P(x)) \Leftrightarrow \exists x : \neg P(x)$$

Cioè negare che esiste un x che verifica $P(x)$ significa dire che per ogni x, $P(x)$ è falsa. Analogamente negare che per ogni x, $P(x)$ è vera, significa dire che esiste un x che falsifica $P(x)$.

Si noti che spesso i teoremi si esprimono in forma esistenziale o universale. Per esempio, il teorema di Pitagora, nella sua forma discreta si può esprimere nel modo seguente: esistono delle triple di numeri interi (a, b, c) tali che $a^2 + b^2 = c^2$ (dette terne pitagoriche).

La prova di un teorema "esistenziale" può essere o di natura costruttiva (genera l'elemento che soddisfa l'affermazione) e nel qual caso abbiamo un algoritmo, oppure di natura esistenziale, in cui l'esistenza dell'oggetto è dimostrata senza bisogno di fornire l'oggetto. Una dimostrazione per assurdo, per esempio, darebbe una dimostrazione non costruttiva di un teorema esistenziale.

Osservazione 25 Una generalizzazione del teorema di Pitagora è il famoso Teorema di Fermat. Esso afferma che per ogni numero naturale $n > 2$, non è possibile trovare una tripla di interi (a, b, c) per cui $a^n + b^n = c^n$. Fermat nel 1637 affermò, scrivendolo a margine di un libro, di avere trovato una dimostrazione per questa affermazione, e che tuttavia quel margine era troppo piccolo per trascrivere l'intera dimostrazione. Non fu mai trovata fra le sue carte la dimostrazione di questo teorema. Da allora molta della ricerca matematica si è mossa per dare la dimostrazione di questo teorema, e solo nel 1996 Wiley dimostrò il teorema, utilizzando metodi sofisticati di algebra moderna, il che ha fatto pensare che Fermat non avesse veramente trovato una dimostrazione corretta del problema.

Capitolo 2

La Teoria degli Insiemi

Studieremo la teoria "ingenua" degli insiemi (in contrapposizione alla cosiddetta teoria "assiomatica"), in cui il concetto di insieme si considera primitivo, ossia non si definisce, intendendo immediatamente evidente il concetto di insieme come sinonimo di raccolta, collezione di elementi. Gli elementi di un insieme possono avere natura arbitraria, ed anche natura diversa fra loro: potremmo per esempio costruire un insieme che ha come elementi il numero 5, la città di Milano e il concetto astratto di bontà.

2.1 Gli insiemi

Se A è un insieme ed x un suo elemento, diremo che x *appartiene ad* A e scriveremo $x \in A$. Se invece x non è elemento dell'insieme A, diremo che x *non appartiene ad* A e scriveremo $x \notin A$.

Un insieme può essere descritto in modo *esplicito*, elencando tutti i suoi elementi. Per esempio possiamo costruire il seguente insieme di nome A:

$$A = \{3, 5, 7, 9\}$$

contenente i 4 numeri interi elencati fra parentesi.

Un insieme si distinguerà solo per gli elementi che contiene, che si consideravano sempre distinti senza ripetizioni, e non per l'ordine in cui sono elencati. Quindi lo stesso insieme A dell'esempio precedente può essere descritto in modo esplicito anche da

$$A = \{5, 9, 7, 3\}.$$

Ovviamente tale modo esplicito di descrivere un insieme è esauriente solo nel caso di insiemi che contengano un numero finito di elementi.

Oltre che in modo esplicito, un insieme può essere descritto anche in modo *implicito*, indicando le proprietà che caratterizzano i suoi elementi mediante un predicato. Se $P(x)$ è un predicato nella variabile x, possiamo costruire l'insieme di nome B:

$$B = \{x \mid P(x)\}$$

(si legge: "B è l'insieme di tutti gli x tali che $P(x)$"; il simbolo $\mid$ essere sostituito dal simbolo : o /); con tale simbologia si intende che gli elementi dell'insieme B sono esattamente tutti i valori della variabile x che rendono vero il predicato $P(x)$.

Per esempio possiamo costruire il seguente insieme di nome B:

$$B = \{x \mid x \text{ è un intero positivo pari}\}$$

(si legge: "B è l'insieme di tutti gli x tali che x è un intero positivo pari"). In tale esempio il predicato che definisce l'insieme B è appunto $P(x) =$ "x è un intero positivo pari" e gli elementi di B sono i valori di x che lo rendono vero (quindi tutti gli interi positivi pari).

Dato un insieme A, ed un elemento x, per verificare se $x \in A$:

- se A è definito in modo esplicito, basta verificare che x appaia nell'elenco degli elementi di A;
- se A è definito in modo implicito mediante un predicato $P(x)$, basta verificare che x renda vero $P(x)$.

2.1.1 Antinomia di Russell

Nella teoria "ingenua" degli insiemi, il fatto che la natura degli elementi sia completamente arbitraria può portare a dei problemi logici, che furono messi in evidenza da Russell.

Partiamo da alcuni esempi: costruiamo l'insieme A i cui elementi sono tutti gli insiemi che contengono più di 3 elementi

$$A = \{x \mid x \text{ è un insieme che contiene più di 3 elementi}\}$$

Alcuni esempi di elementi di A sono gli insiemi $\{1, 2, 3, 4\}$, $\{a, b, c, d, e\}$, $\{a, 1, 7, 8, b, d\}$, $\{1, 3, 5, 7\}$. Poiché A stesso contiene più di 3 elementi si ha che A è elemento di sé stesso: $A \in A$.

Invece se costruiamo l'insieme B i cui elementi sono tutti gli insiemi che contengono meno di 3 elementi:

$$B = \{x \mid x \text{ è un insieme che contiene meno di 3 elementi}\}$$

Esempi di elementi di B sono $\{1, 2\}$, $\{a\}$, $\{2, 5\}$, $\{a, b\}$ etc.. Poiché B contiene più di 3 elementi si ha che B non è elemento di sé stesso: $B \notin B$.

Abbiamo visto dunque che esistono insiemi che hanno sé stessi come elementi, ed insiemi che non hanno sé stessi come elementi. Costruiamo allora l'insieme C i cui elementi sono tutti gli insiemi che non hanno sé stessi come elementi

$$C = \{x \mid x \text{ è un insieme ed } x \notin x\}$$

(un elemento di C è per esempio l'insieme B costruito sopra).

Domanda: $C \in C$ oppure $C \notin C$? Ma se $C \in C$ allora dalla proprietà che caratterizza gli elementi di C segue che $C \notin C$; viceversa se $C \notin C$ allora dalla proprietà che caratterizza gli elementi di C segue che $C \in C$: siamo in presenza di una contraddizione logica (antinomia di Russell), perché un'affermazione è vera e falsa nello stesso tempo.

Per risolvere questi problemi logici legati alla teoria "ingenua" degli insiemi si può ricorrere alla teoria "assiomatica" (più precisa dal punto di vista

formale ma più complicata) oppure evitare costruzioni del tipo "l'insieme di tutti gli insiemi tali che ...": nel nostro corso sceglieremo questa seconda modalità.

2.1.2 Insieme vuoto

Può accadere che un insieme sia descritto in modo implicito mediante un predicato che è falso per ogni valore della variabile. Per esempio:

$$A = \{x \mid x \text{ è un intero positivo minore di } 1/2\}$$

In tal caso l'insieme ottenuto è un insieme privo di elementi, detto *insieme vuoto*, e indicato con il simbolo $\emptyset$.

2.1.3 Sottoinsiemi di un insieme

Dati gli insiemi A, B, diremo che A è *sottoinsieme di* B (oppure che A *è contenuto in* B, o anche che A *è incluso in* B) e scriveremo $A \subseteq B$, se ogni elemento di A è anche elemento di B. Se A non è sottoinsieme di B, esisterà almeno un elemento di A che non appartiene a B.

Se gli insiemi sono descritti in modo esplicito, per verificare se $A \subseteq B$ basta verificare che ogni elemento nell'elenco di A è presente anche nell'elenco di B. Per esempio se $B = \{1, 3, 4, 5, 6, 8\}$, $A = \{6, 5, 3\}$, $C = \{8, 4, 2\}$ si ha $A \subseteq B$ (ogni elemento 6, 5, 3 dell'elenco di A è presente nell'elenco di B), ma si ha anche che C non è sottoinsieme di B (l'elemento 2 dell'elenco di C non è presente nell'elenco di B).

Se gli insiemi sono invece descritti in modo implicito, mediante predicati:

$$A = \{x \mid P(x)\}$$

$$B = \{x \mid Q(x)\}$$

allora verificare che $A \subseteq B$ equivale ad affermare che ogni x che soddisfa P deve soddisfare anche Q, quindi equivale a dimostrare che vale l'implicazione $P \Rightarrow Q$.

Due insiemi A, B sono *uguali* se contengono gli stessi elementi: questo equivale ad affermare che ogni elemento di A è anche elemento di B e che viceversa ogni elemento di B è anche elemento di A. Quindi l'eguaglianza di insiemi $A = B$ equivale alla "doppia inclusione" $A \subseteq B$ e $B \subseteq A$.

Se gli insiemi sono descritti in modo esplicito, per verificare se $A = B$ basta verificare che gli elenchi degli elementi di A e B siano uguali (anche se gli elementi sono elencati in ordine diverso). Per esempio se $A = \{1, 3, 4, 5, 6, 8\}$, $B = \{4, 8, 6, 5, 3, 1\}$, allora si ha $A = B$.

Se gli insiemi sono descritti in modo implicito, mediante predicati:

$$A = \{x \mid P(x)\}$$

$$B = \{x \mid Q(x)\}$$

allora verificare che $A = B$ equivale a dimostrare vera sia l'implicazione $P \Rightarrow Q$ che l'implicazione inversa $Q \Rightarrow P$, quindi l'eguaglianza di insiemi $A = B$ corrisponde all'equivalenza dei predicati $P \Leftrightarrow Q$.

Osservazione 26 Uno dei più importanti problemi aperti dell'informatica è proprio un problema di inclusione fra insiemi. In teoria della Complessità e della Calcolabilità, la Macchina di Turing è un modello di calcolo per la formalizzazione del concetto di funzione calcolabile: per tutti i problemi che sono intuitivamente calcolabili, esiste una macchina di Turing che lo calcola.

Si indica con $\mathcal{P}$ l'insieme dei problemi che si possono risolvere in tempo polinomiale mediante una macchina di Turing Deterministica (cioè su un input, trovandosi in un certo stato, la macchina può assumere un'unica configurazione successiva), e si indica con $\mathcal{NP}$ l'insieme dei problemi che si possono calcolare in tempo polinomiale mediante una macchina di Turing non deterministica (ad ogni input, e per ogni stato della macchina, più configurazioni successive sono possibili). Si dimostra che tutto quello che si può calcolare con macchine di Turing non deterministiche si può calcolare con macchine di Turing deterministiche e viceversa. Tuttavia le macchine di Turing non deterministiche di solito danno una risposta al problema con un numero di computazioni minori rispetto a una macchina di Turing deterministica (quindi in un tempo inferiore, inteso come numero di istruzioni eseguite per arrivare alla soluzione). Ci si chiede quindi se tutto quello che

una macchina di Turing non deterministica risolve in tempo polinomiale, può essere risolto in tempo polinomiale (e non esponenziale) da una macchina di Turing deterministica. Ci si chiede dunque se $\mathcal{NP} \subseteq \mathcal{P}$. Poiché ovviamente $\mathcal{P} \subseteq \mathcal{NP}$ (ogni macchina deterministica è una particolare macchina non deterministica), questo implicherebbe l'uguaglianza dei due insiemi, ossia $\mathcal{P} = \mathcal{NP}$.

Gli scienziati sono per lo più propensi a credere che l'inclusione di $\mathcal{P}$ in $\mathcal{NP}$ sia stretta, ossia che i due insiemi non coincidano. Tuttavia non è mai stato trovato un contresempio di un problema che sta in $\mathcal{NP}$ e non in $\mathcal{P}$. Se si volesse invece provare l'uguaglianza, occorrerebbe fornire un teorema che dimostra che ogni problema in $\mathcal{NP}$ sta anche in $\mathcal{P}$.

Per ogni insieme A, è ovvio che A è sottoinsieme di sé stesso:

$$A \subseteq A$$

Se $B \subseteq A$ e se $B \not\subseteq A$, si dice anche che B è contenuto *propriamente* in A e si scrive $B \subset A$. Per convenzione l'insieme vuoto $\emptyset$ si considera sottoinsieme di qualunque insieme A. Poiché, dato un insieme A qualunque, si ha sempre $\emptyset \in A$ e $A \subseteq A$, i due sottoinsiemi $\emptyset$, A sono detti *sottoinsiemi banali* o *impropri* dell'insieme A.

Fissato un arbitrario insieme A, possiamo costruire l'*insieme delle parti di* A (indicato con il simbolo $\mathfrak{P}(A)$), i cui elementi sono tutti i possibili sottoinsiemi di A. Per esempio se $A = \{a, b, c\}$, l'insieme delle parti di A è l'insieme:

$$\mathfrak{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}$$

Si può notare che A contiene 3 elementi e $\mathfrak{P}(A)$ contiene $8 = 2^3$ elementi: dimostreremo in seguito che ciò non è casuale (cioè dimostreremo che se l'insieme A contiene un numero n di elementi, allora il numero dei suoi sottoinsiemi è 2^n).

Se A è un insieme fissato, possiamo descrivere in forma implicita un sottoinsieme B di A nel modo seguente:

$$B = \{x \in A \mid P(x)\}$$

dove $P(x)$ è un predicato, intendendo che gli elementi del sottoinsieme B sono tutti e soli gli elementi di A che rendono vero $P(x)$. Per esempio, se $A = \{x \mid x \text{ è intero positivo pari}\}$, e se descriviamo in modo implicito il seguente sottoinsieme di A:

$$B = \{x \in A \mid x < 10\}$$

la rappresentazione esplicita di B è data da $B = \{2, 4, 6, 8\}$.

2.2 Operazioni fra insiemi

Anche fra gli insiemi è possibile definire delle operazioni, che permettono di costruire un nuovo insieme (*risultato*) a partire da alcuni insiemi dati (*operandi*) i cui elementi dipendono dagli elementi degli insiemi operandi.

2.2.1 Intersezione di insiemi

Definizione 27 *Dati gli insiemi A, B, si chiama insieme* intersezione di A e B *(indicato con $A \cap B$) l'insieme degli elementi che appartengono ad ambedue gli insiemi A, B.*

Se A, B non hanno elementi in comune si ha $A \cap B = \emptyset$ e si dice che A e B sono *disgiunti*.

Se A, B sono descritti in modo esplicito, $A \cap B$ è descritto in modo esplicito da un elenco di tutti gli elementi che sono presenti sia nell'elenco di A che nell'elenco di B.

Per esempio se $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{8, 5, 6, 9\}$ allora $A \cap B = \{5, 6\}$.

Se A, B sono descritti in modo implicito:

$$A = \{x \mid P(x)\}$$

$$B = \{x \mid Q(x)\}$$

allora $A \cap B$ è descritto in modo implicito dal predicato congiunzione logica $P \wedge Q$:

$$A \cap B = \{x \mid [P \wedge Q](x)\}$$

infatti i valori che rendono vero $P \wedge Q$ sono esattamente quelli che rendono vero sia P che Q (quindi sono gli elementi che appartengono sia ad A che a B). Per esempio se

$$A = \{x \mid \ x \text{ è intero positivo dispari}\}$$

$$B = \{x \mid \ x \text{ è intero} > 12\}$$

allora:

$$A \cap B = \{x \mid x \text{ è intero positivo dispari e } x \text{ è intero } > 12\}$$

(quindi $A \cap B$ contiene tutti gli interi dispari da 13 in poi).

Proprietà evidenti dell'intersezione sono le seguenti:

1. dato un insieme A si ha $A \cap A = A$ (*idempotenza*)
2. dati due insiemi A, B si ha $A \cap B = B \cap A$ (*proprietà commutativa*)
3. dati tre insiemi A, B, C, si ha $(A \cap B) \cap C = A \cap (B \cap C)$ (*proprietà associativa*)

Le proprietà 1 e 2 seguono immediatamente dalla definizione di intersezione. Per la 3 basta notare che sia $(A \cap B) \cap C$ che $A \cap (B \cap C)$ coincidono con l'insieme degli elementi che appartengono a tutti e tre gli insiemi A, B, C.

2.2.2 Unione di insiemi

Definizione 28 *Dati gli insiemi A, B, si chiama* insieme unione di A e B *(indicato con $A \cup B$) l'insieme degli elementi che appartengono ad almeno uno degli insiemi A, B.*

Se A, B sono descritti in modo esplicito, $A \cup B$ è descritto in modo esplicito da un elenco di tutti gli elementi che sono presenti nell'elenco di A o nell'elenco di B o in ambedue (questi ultimi elencati 1 sola volta per evitare ripetizioni dello stesso elemento). Per esempio se

$$A = \{1, 2, 3, 4, 5, 6\}$$

$$B = \{8, 5, 6, 9\}$$

allora

$$A \cup B = \{1, 2, 3, 4, 5, 6, 8, 9\}.$$

Se A, B sono descritti in modo implicito:

$$A = \{x \mid P(x)\}$$

$$B = \{x \mid Q(x)\}$$

allora $A \cup B$ è descritto in modo implicito dal predicato disgiunzione logica $P \vee Q$:

$$A \cup B = \{x \mid [P \vee Q](x)\}$$

infatti gli elementi di $A \cup B$ (valori che rendono vera la disgiunzione $P \vee Q$) saranno gli elementi che appartengono ad A (valori che rendono vero P) oppure gli elementi che appartengono a B (valori che rendono vero Q).

Proprietà evidenti dell'unione sono le seguenti:

1. dato un insieme A si ha $A \cup A = A$ (*idempotenza*)
2. dati 2 insiemi A, B si ha $A \cup B = B \cup A$ (*proprietà commutativa*)
3. dati 3 insiemi A, B, C si ha $(A \cup B) \cup C = A \cup (B \cup C)$ (*proprietà associativa*).

Le proprietà 1 e 2 seguono immediatamente dalla definizione di unione. Per la 3 basta notare che sia $(A \cup B) \cup C$ che $A \cup (B \cup C)$ coincidono con l'insieme degli elementi che appartengono ad almeno uno fra i tre insiemi A, B, C.

2.2.3 Differenza di insiemi

Definizione 29 *Dati gli insiemi A, B, si chiama* insieme differenza di A e B *(indicato con $A - B$) l'insieme degli elementi che appartengono ad A ma non appartengono a B.*

Se A, B sono descritti in modo esplicito, $A - B$ è descritto in modo esplicito da un elenco di tutti gli elementi che sono presenti nell'elenco di A ma non nell'elenco di B. Per esempio se

$$A = \{1, 2, 3, 4, 5, 6\}$$

$$B = \{8, 5, 6, 9\}$$

allora

$$A - B = \{1, 2, 3, 4\}$$

mentre

$$B - A = \{8, 9\}$$

Se invece A, B sono descritti in modo implicito:

$$A = \{x \mid P(x)\}$$

$$B = \{x \mid Q(x)\}$$

allora $A-B$ è descritto in modo implicito dal predicato $P \wedge \neg Q$, congiunzione logica di P e della negazione di Q.

$$A - B = \{x \mid [P \wedge \neg Q](x)\}$$

Per esempio se

$$A = \{x \mid x \text{ è intero positivo dispari}\}$$

$$B = \{x \mid x \text{ è intero } > 12\}$$

allora:

$A-B = \{x \mid x$ è intero positivo dispari ed x è intero $\leq 12\} = \{1, 3, 5, 7, 9, 11\}$

mentre:

$B-A = \{x \mid x$ è intero > 12 ed x è intero positivo pari$\} = \{14, 16, 18, 20, \ldots\}$

(quindi $B - A$ contiene tutti gli interi pari da 14 in poi). Dall'esempio precedente si deduce che in generale $A - B \neq B - A$ (dunque l'operazione differenza non soddisfa la proprietà commutativa).

2.2.4 Complementare di un sottoinsieme in un insieme

Dati gli insiemi A, B e nel caso particolare in cui l'insieme B sia sottoinsieme dell'insieme A, la differenza $A - B$ è detta *complementare di B rispetto ad A* e indicata con B^c: dunque il complementare di B in A ha come elementi tutti gli elementi di A che non appartengono a B.

Le proprietà principali del complementare sono espresse dalle *leggi di De Morgan*: se B, C sono sottoinsiemi dell'insieme A (notare che anche $B \cap C$, $B \cup C$ sono sottoinsiemi di A e si possono considerare i quattro complementari B^c, C^c, $(B \cap C)^c$, $(B \cup C)^c$) si ha:

$$(B \cup C)^c = B^c \cap C^c$$

$$(B \cap C)^c = B^c \cup C^c$$

Le dimostrazione di ognuna di queste due proprietà comporta la dimostrazione di una doppia inclusione. Per esempio per dimostrare la prima proprietà, si devono dimostrare le due inclusioni:

$$(B \cup C)^c \subseteq B^c \cap C^c$$

$$B^c \cap C^c \subseteq (B \cup C)^c$$

Dimostriamo la prima delle due inclusioni (la dimostrazione della seconda é analoga): se x è un elemento generico di $(B \cup C)^c$, allora, per definizione di complementare, si ha $x \in A$ ma $x \notin B \cup C$, e per definizione di unione si ha $x \notin B$ e $x \notin C$, dunque $x \in A$ e $x \notin B$ e simultaneamente $x \in A$ e $x \notin C$, ossia $x \in B^c$ e simultaneamente $x \in C^c$, e si può concludere che $x \in B^c \cap C^c$.

Per concludere la trattazione delle operazioni fra insiemi, notiamo che valgono le seguenti proprietà distributive di unione e intersezione: dati gli insiemi A, B, C si ha

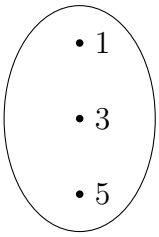
$$A \cap (B \cup C) = (A \cup B) \cap (A \cup C)$$

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

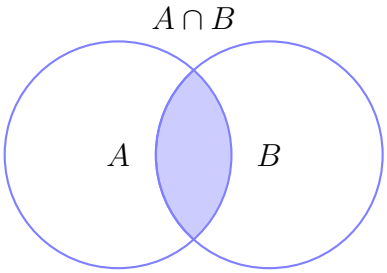
Esse si dimostrano facilmente con le doppie inclusioni.

2.3 Diagrammi di Eulero-Venn

I diagrammi di Eulero-Venn sono rappresentazioni grafiche di un insieme, in cui gli elementi si rappresentano come punti del piano all'interno di una curva chiusa (spesso una circonferenza). Esempio di diagramma di Eulero-Venn che rappresenta l'insieme $A = \{1, 3, 5\}$:

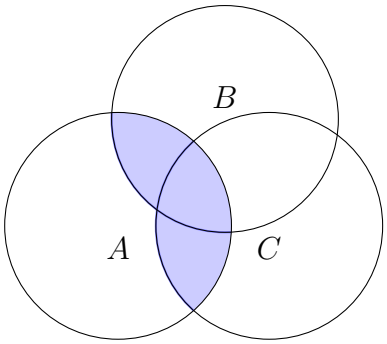


Si possono rappresentare con tali diagrammi anche i risultati delle operazioni fra insiemi: unione, intersezione e differenza. Per esempio l'intersezione $A \cap B$ è rappresentata dalla parte colorata della seguente figura:



Le proprietà già enunciate per le operazione fra insiemi si possono facilmente verificare graficamente sui diagrammi di Eulero-Venn: per esempio per verificare la proprietà distributiva

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



basta rappresentare con i diagrammi di Venn gli elementi di A, B, C poi quelli di $(A \cup B), (A \cup C)$, infine rappresentare gli elementi di $A \cap (B \cup C)$ e di $(A \cap B) \cup (A \cap C)$ e verificare che siano esattamente gli stessi punti del piano.

2.4 Gli insiemi numerici e le relazioni fra insiemi

2.4.1 Gli insiemi numerici

I simboli che useremo per indicare gli insiemi numerici più comuni saranno i seguenti:

- $\mathbb{N}$ indicherà l'insieme dei numeri *interi positivi* (detti anche numeri naturali);
- $\mathbb{Z}$ indicherà l'insieme dei numeri *interi relativi* (ossia dei numeri interi positivi, negativi e lo zero);
- $\mathbb{Q}$ indicherà l'insieme dei numeri *razionali* (ossia delle frazioni in cui numeratore e denominatore sono numeri interi relativi, e il denominatore è diverso da 0);

- $\mathbb{R}$ indicherà l'insieme dei numeri *reali* (per una loro definizione formale si rinvia al corso di Analisi; per i nostri scopi basta conoscere la loro rappresentazione con una parte "intera" ed una parte "decimale" dopo la virgola).

Si hanno le seguenti inclusioni proprie di insiemi:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Un asterisco $*$ sul simbolo indicherà che dall'insieme è tolto lo 0: per esempio $\mathbb{Z}^*$ indicherà l'insieme dei numeri interi relativi diversi da 0; un $+$ sul simbolo indicherà che dell'insieme si considerano solo i numeri positivi: per esempio $\mathbb{R}^+$ indicherà l'insieme dei numeri reali positivi (ovviamente $\mathbb{Z}^+ = \mathbb{N}$).

2.4.2 Prodotto cartesiano di insiemi

Se a, b sono due elementi (di natura arbitraria, nello stesso insieme o in insiemi diversi ed anche possibilmente coincidenti fra loro) la *coppia ordinata* (a, b) con primo elemento a e con secondo elemento b è per definizione una struttura insiemistica in cui si tiene conto sia degli elementi a, b che dell'ordine in cui sono elencati. Dunque il concetto di coppia ordinata (a, b) è diverso da quello di insieme $\{a, b\}$ perché si ha $(a, b) \neq (b, a)$, almeno quando $a \neq b$ (mentre invece come insiemi si ha $\{a, b\} = \{b, a\}$).

Definizione 30 *Dati due insiemi A, B si chiama* prodotto cartesiano $A \times B$ *l'insieme che contiene tutte le possibili coppie ordinate (a, b) dove il primo elemento $a \in A$, ed il secondo elemento $b \in B$.*

Esempio 31 Se $A = \{3, a, 5\}$, $\{a, 5, 2\}$ allora

$$A \times B = \{(3, a), (3, 5), (3, 2), (a, a), (a, 5), (a, 2), (5, a), (5, 5), (5, 2)\}$$

Notiamo anche che se l'insieme A contiene un numero finito n di elementi e se l'insieme B contiene un numero finito m di elementi, allora il prodotto cartesiano $A \times B$ contiene esattamente un numero nm di coppie. Infatti dobbiamo accoppiare il primo elemento di A con tutti gli m elementi di B

(ottenendo m coppie), poi il secondo elemento di A con tutti gli m elementi di B (ottenendo altre m coppie), e così via accoppiando ogni elemento di A con tutti gli m elementi di B (ottenendo ad ogni passaggio sempre m coppie): il numero totale di coppie che otteniamo è dunque una somma:

$$m + m + \cdots + m$$

con n addendi (tanti addendi quanti sono gli elementi di A) ossia è effettivamente nm.

2.4.3 Relazioni fra insiemi

Definizione 32 *Dati gli insieme A, B, si chiama* relazione dall'insieme A all'insieme B *un qualunque sottoinsieme $\mathcal{R}$ del prodotto cartesiano $A \times B$*

Quindi $\mathcal{R}$ è un insieme di coppie (a, b) con il primo elemento in A e il secondo in B.

Se una coppia (a, b) (con $a \in A$, $b \in B$) appartiene ad $\mathcal{R}$, diremo che l'elemento $a \in A$ è associato nella relazione $\mathcal{R}$ all'elemento $b \in B$ e scriveremo il simbolo $a\mathcal{R}b$; se invece la coppia (a, b) non appartiene ad $\mathcal{R}$ diremo che l'elemento $a \in A$ non è associato nella relazione $\mathcal{R}$ all'elemento $b \in B$.

Esempio 33 Se $A = \{1, 2, 3, 6\}$, $B = \{2, 3, 5\}$ e se la relazione da A a B è il seguente sottoinsieme di $A \times B$:

$$\mathcal{R} = \{(1, 2), (1, 3), (2, 3), (6, 2)\}$$

Allora $1\mathcal{R}2$ perché la coppia $(1, 2)$ appartiene ad $\mathcal{R}$ (quindi l'elemento $1 \in A$ è associato all'elemento $2 \in B$), ma l'elemento $1 \in A$ non è associato all'elemento $5 \in B$ perché la coppia $(1, 5)$ non appartiene ad $\mathcal{R}$.

Come si vede dall'esempio, in una relazione $\mathcal{R}$ da A a B un elemento di A può essere associato a più di un elemento di B, oppure non essere associato a nessun elemento di B.

Dati due insiemi A, B, una relazione $\mathcal{R}$ dall'insieme A all'insieme B può essere descritta in vari modi:

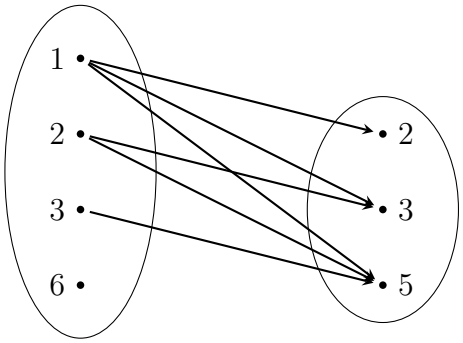
1. In modo *esplicito*: si elencano tutte le coppie che formano il sottoinsieme $\mathcal{R}$ del prodotto cartesiano $A \times B$ (questo modo è stato usato nell'esempio precedente). E' ovvio che tale modo esplicito è esauriente solo quando $\mathcal{R}$ è formato da un numero finito di coppie.

2. In modo *implicito*: si fissa un predicato $P(x, y)$ in due variabili (in cui A è l'universo della variabile x, B è l'universo della variabile y) e si conviene che, dati un elemento $a \in A$ e un elemento $b \in B$, si ha $a\mathcal{R}b$ (quindi l'elemento $a \in A$ è associato nella relazione $\mathcal{R}$ all'elemento $b \in B$) solo quando la proposizione logica $P(a, b)$ è vera (dove ricordiamo che $P(a, b)$ è la proposizione ottenuta dal predicato $P(x, y)$ sostituendo x con a, y con b). In pratica il predicato $P(x, y)$ fornisce la "regola" con cui stabilire quali elementi di A e quali elementi di B sono associati fra di loro nella relazione $\mathcal{R}$.

   Esempio 34 Se $A = \{1, 2, 3, 6\}$, $B = \{2, 3, 5\}$ e se la relazione $\mathcal{R}$ da A a B è descritta in modo implicito dal predicato $P(x, y) =$ "$x < y$" allora un elemento $a \in A$ è associato nella relazione $\mathcal{R}$ ad un elemento $b \in B$ proprio quando $a < b$. In tale esempio la rappresentazione esplicita della relazione $\mathcal{R}$ è il seguente sottoinsieme del prodotto cartesiano $A \times B$:
   $$R = \{(1, 2), (1, 3), (1, 5), (2, 3), (2, 5), (3, 5)\}$$

3. *Rappresentazione grafica*: si rappresentano A, B con i diagrammi di Eulero-Venn, e si conviene di unire con una freccia un elemento $a \in A$ con un elemento $b \in B$ solo quando $a\mathcal{R}b$, cioè solo quando l'elemento $a \in A$ è associato nella relazione $\mathcal{R}$ all'elemento B.

   Esempio 35 La rappresentazione grafica della relazione $\mathcal{R}$ nell'esempio precedente è la seguente:



Osservazione 36 Il concetto di relazione assume una grandissima importanza in vari settori dell'Informatica, primo fra tutti nelle Basi di Dati, dove il concetto di relazione è alla base del cosiddetto Modello Logico Relazionale. Al concetto matematico di Relazione, che è strettamente "posizionale", ossia per conoscere il ruolo di un valore in una n-upla occorre conoscere la sua posizione, si sostituisce quello che associa degli attributi alle colonne, ossia dei "nomi" identificativi che distinguono le colonne, togliendo quindi i vincoli della notazione posizionale. Inoltre si osserva che ogni relazione binaria fra elementi di un insieme si può sempre rappresentare con un grafo, e viceversa un grafo è sempre una rappresentazione di una relazione binaria (individuata dalle coppie di nodi legate da un arco).

2.4.4 Relazioni di equivalenza

Una relazione $\mathcal{R}$ su un insieme A si dice di *equivalenza* se soddisfa le seguenti proprietà:

1. *Riflessiva*: per ogni $a \in A$ si ha $a\mathcal{R}a$;
2. *Simmetrica*: per ogni $a, b \in A$ si ha $a\mathcal{R}b \Rightarrow b\mathcal{R}a$;
3. *Transitiva*: per ogni $a, b, c \in A$, $a\mathcal{R}b$ e $b\mathcal{R}c \Rightarrow a\mathcal{R}c$.

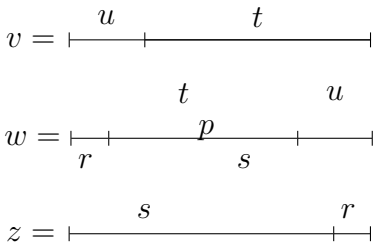
Esempio 37 Diamo alcuni esempi di relazione di equivalenza:

1. L'uguaglianza fra i numeri reali è una relazione di equivalenza. Infatti valgono banalmente le proprietà riflessiva, simmetrica e transitiva.

2. La similitudine fra figure geometriche del piano è definita come segue: "Due figure geometriche con lo stesso numero di lati sono simili se hanno gli angoli ordinatamente uguali e i lati incidenti su angoli uguali in proporzione." Anche la similitudine è banalmente una relazione di equivalenza.

3. Fra gli studenti iscritti all'università, sono in relazione quelli che sono iscritti allo stesso corso di Laurea.

4. Date due sequenze di lettere sullo stesso alfabeto (parole) di uguale lunghezza, $v = a_1 a_2 \cdots a_n$ e $w = b_1 b_2 \cdots b_n$, diciamo che v e w sono coniugate se esistono due sottoparole u, t tali che $v = ut$ e $w = tu$. Sull'insieme di tutte le parole su uno stesso alfabeto, la relazione di congruenza è una relazione di equivalenza. Infatti ogni parola v è coniugata di se stessa. Se v è coniugata di w, allora per definizione w è coniugata di v. Se v è coniugata di w e w è coniugata di z, significa che esistono due parole u, t tali che $v = ut$ e $w = tu$, ma anche esistono s ed r tali che $w = rs$ e $z = sr$.



Come si evince dalla figura, si ha che $t = rp$ e che $s = pu$. Sostituendo queste uguaglianze nelle espressioni di v, w, z, si ha $v = ut = urp$, e $z = sr = pur$, ossia $v = (ur)p$ e $z = p(ur)$. Dunque v e z sono coniugate.

2.4.5 Classi di equivalenza

Sia definita nell'insieme A una relazione di equivalenza $\mathcal{R}$. Fissato un $a \in A$, possiamo costruire il sottoinsieme di A formato dagli elementi x che sono

associati ad a nella relazione $\mathcal{R}$:

$$\{x \in A \mid a\mathcal{R}x\}$$

(notiamo che è equivalente scrivere $a\mathcal{R}x$ oppure $x\mathcal{R}a$ per la proprietà simmetrica)

Tale sottoinsieme contiene almeno l'elemento a stesso (infatti per la proprietà riflessiva si ha aRa) dunque non è vuoto: esso è chiamato *classe di equivalenza rappresentata dall'elemento a* ed è indicato con il simbolo $[a]$:

$$[a] = \{x \in A \mid a\mathcal{R}x\}$$

L'elemento a è detto rappresentante della classe $[a]$.

Esempio 38 Definiamo la relazione $\mathcal{R}$ nell'insieme dei numeri naturali $\mathbb{N}$ mediante il predicato "$x + y$ è pari", e verifichiamo se è una relazione di equivalenza.
Proprietà riflessiva: per ogni $a \in A$ si ha $a\mathcal{R}a$, perché $a + a = 2a$ è pari.
Proprietà simmetrica: per ogni $a, b \in A$, se $a\mathcal{R}b$ allora $b\mathcal{R}a$, perché se $a + b$ è pari anche $b + a = a + b$ lo è (per la proprietà commutativa della somma).
Proprietà transitiva: per ogni $a, b, c \in A$, se $a\mathcal{R}b$ e $b\mathcal{R}c$ allora $a\mathcal{R}c$, perché se $a + b$, $b + c$ sono pari, allora è pari la loro somma $a + c + 2b$, dunque, sottraendo il pari $2b$, anche $a + c$ è pari.
Si conclude che $\mathcal{R}$ è un esempio di relazione di equivalenza definita nell'insieme $\mathbb{N}$ dei numeri naturali.

Costruiamo alcune classi di equivalenza fissando vari rappresentanti:

$$[3] = \{x \in \mathbb{N} \mid 3\mathcal{R}x\} = \{x \in \mathbb{N} \mid 3 + x \text{ è pari}\} = \{1, 3, 5, 7, \ldots\} =$$
$$= \{\text{numeri naturali dispari}\}$$
$$[8] = \{x \in \mathbb{N} \mid 8\mathcal{R}x\} = \{x \in \mathbb{N} \mid 8 + x \text{ è pari}\} = \{2, 4, 6, 8, \ldots\} =$$
$$= \{\text{numeri naturali pari}\}$$
$$[5] = \{x \in \mathbb{N} \mid 5\mathcal{R}x\} = \{x \in \mathbb{N} \mid 5 + x \text{ è pari}\} = \{1, 3, 5, 7, \ldots\} =$$
$$= \{\text{numeri naturali dispari}\}$$

In generale, ricordando che la somma di due numeri naturali è pari solo quando sono entrambi pari o dispari, si ottiene che per un generico rappresentante

$a \in \mathbb{N}$ la classe $[a]$ da esso rappresentata coincide con l'insieme dei numeri naturali dispari (se a è dispari) o con l'insieme dei numeri naturali pari (se a è pari): dunque in questo esempio le diverse classi di equivalenza sono in tutto due sottoinsiemi di $\mathbb{N}$: {numeri naturali dispari}, {numeri naturali pari}.

Come visto nell'ultimo esempio, elementi diversi dell'insieme possono essere rappresentanti di classi di equivalenza uguali: il numero 3 e il numero 5 sono rappresentanti della stessa classe di equivalenza $[3] = [5] =$ {numeri naturali dispari}. Il criterio per stabilire quando due elementi sono rappresentanti della stessa classe di equivalenza è il seguente:

Teorema 39 *Sia definita nell'insieme A una relazione di equivalenza $\mathcal{R}$. Allora dati $a, b \in A$ si ha:*

$$[a] = [b] \Leftrightarrow a\mathcal{R}b$$

Dimostrazione ($\Rightarrow$): per ipotesi $[a] = [b]$; l'elemento $a \in [a]$ (per la proprietà riflessiva), e dunque $a \in [b]$ (essendo per ipotesi $[a] = [b]$), ossia $a\mathcal{R}b$ (tesi).
($\Leftarrow$): per ipotesi $a\mathcal{R}b$; la tesi $[a] = [b]$ richiede la dimostrazione di una doppia inclusione insiemistica $[a] \subseteq [b]$ e $[a] \subseteq [b]$. Dimostriamo che $[a] \subseteq [b]$: preso un generico elemento $x \in [a]$ si ha $x\mathcal{R}a$; da $x\mathcal{R}a$ e dall'ipotesi $a\mathcal{R}b$ si ha $b\mathcal{R}x$ (per la proprietà transitiva), dunque $x \in [b]$, e si può concludere che $[a] \subseteq [b]$. Viceversa dimostriamo che $[b] \subseteq [a]$: preso un generico elemento $x \in [b]$ si ha $x\mathcal{R}b$; dall'ipotesi $a\mathcal{R}b$ segue $b\mathcal{R}a$ (per la proprietà simmetrica); da $x\mathcal{R}b$ e da $b\mathcal{R}a$ si ha $x\mathcal{R}a$ (per la proprietà transitiva), dunque $x \in [a]$, e si può concludere che $[b] \subseteq [a]$. □

Osservazione 40 Come si può notare nella dimostrazione precedente, tutte e tre le proprietà simmetrica, riflessiva e transitiva sono utilizzate.

Le classi di equivalenza hanno una importante proprietà:

Definizione 41 *Dato un insieme A, si definisce partizione dell'insieme A una famiglia $\mathcal{P}$ di sottoinsiemi di A tali che:*

1. *tutti i sottoinsiemi in $\mathcal{P}$ sono non vuoti;*

2. *I sottoinsiemi contenuti in $\mathcal{P}$ sono a due a due disgiunti (ossia hanno intersezione vuota);*

3. *L'unione di tutti i sottoinsiemi di $\mathcal{P}$ è uguale a tutto l'insieme A.*

Teorema 42 *Sia definita nell'insieme A una relazione di equivalenza $\mathcal{R}$. Le diverse classi di equivalenza formano una partizione dell'insieme A.*

Dimostrazione Dimostriamo le proprietà che caratterizzano una partizione di A

- Le classi di equivalenza sono sottoinsiemi non vuoti di A: questo è già stato notato prima, sfruttando la proprietà riflessiva (la classe rappresentata da a contiene almeno l'elemento a)
- Date due generiche classi diverse $[a] \neq [b]$, esse sono disgiunte, ossia hanno intersezione vuota: per assurdo supponiamo che abbiano un elemento in comune x; dunque $x\mathcal{R}a$ (perché $x \in [a]$) e anche $x\mathcal{R}b$ (perché $x \in [b]$). Ma allora da $a\mathcal{R}x$ segue $x\mathcal{R}a$ (per la simmetrica) e da $a\mathcal{R}x$ e $x\mathcal{R}b$ segue $a\mathcal{R}b$ (per la transitiva). Infine da $a\mathcal{R}b$ segue, per il teorema precedente, l'eguaglianza $[a] = [b]$, contraddizione.
- L'unione di tutte le classi di equivalenza è uguale all'insieme A: ciò è ovvio, perché preso un generico elemento $a \in A$, tale elemento appartiene ad almeno una classe di equivalenza (per esempio alla classe $[a]$, sempre per la proprietà riflessiva).

□

Esempio 43 Nell'esempio 38 si sono ottenute due diverse classi di equivalenza {numeri naturali pari} e {numeri naturali dispari}, e in effetti esse costituiscono una partizione di $\mathbb{N}$, come affermato dal Teorema.

2.4.6 Relazione d'ordine

Diciamo che una relazione $\mathcal{R}$ definita su un insieme A è una relazione d'ordine se valgono le seguenti proprietà

1. *Riflessiva*: per ogni $a \in A$ si ha $a\mathcal{R}a$.
2. *Antisimmetrica*: per ogni $a, b \in A$, $a\mathcal{R}b$ e $b\mathcal{R}a \Rightarrow a = b$.
3. *Transitiva*: per ogni $a, b, c \in A$, se $a\mathcal{R}b$ e $b\mathcal{R} \Rightarrow a\mathcal{R}c$.

Una relazione d'ordine si dice un *ordine totale su* A se per ogni coppia di elementi $a, b \in A$, o $a\mathcal{R}b$ o $b\mathcal{R}a$. Un insieme su cui è definita una relazione d'ordine totale si dice *totalmente ordinato*.

Esempio 44 Diamo alcuni esempi di relazione d'ordine:

1. La relazione $\leq$ sui numeri reali (e su tutti i sottoinsiemi dei reali) è una relazione d'ordine totale. Infatti $a \leq a$; se $a \leq b$ e $b \leq a$ allora $a = b$; se $a \leq b$ e $b \leq c$ allora $a \leq c$. Inoltre comunque presi due numeri reali, è sempre possibile stabilire chi dei due è più grande e chi più piccolo, ossia sono sempre confrontabili.
2. La relazione d'ordine alfabetico sull'alfabeto è una relazione d'ordine totale
3. Dato un alfabeto A, su cui è stabilito un certo ordine alfabetico, considerato l'insieme delle parole sull'alfabeto A, denotato con A^*, si definisce l'*ordine lessicografico* nel modo seguente: se $u = a_1a_2 \cdots a_n$ e $w = b_1b_2 \cdots b_m$, allora $u <_{lex} w$ se
   - o u è prefisso di w;
   - oppure esiste un $1 \leq j \leq \min\{n, m\}$ tale che $a_1 = b_1, a_2 = b_2, \ldots, a_{j-1} = b_{j-1}, a_j < b_j$. Significa che u e w sono uguali per un certo prefisso e appena c'è un simbolo che li rende diversi il simbolo di u è alfabeticamente più piccolo del simbolo di w.

   L'ordine lessicografico è una relazione d'ordine totale (dimostrarlo). Di fatto si tratta dell'ordine adottato nei vocabolari o negli elenchi telefonici.
4. La relazione d'inclusione fra insiemi è una relazione d'ordine (dimostrarlo). Tuttavia non è una relazione d'ordine totale. Infatti se due insiemi non sono inclusi uno nell'altro, non è possibile metterli in relazione.

Le relazioni d'ordine entrano in gioco nei cosiddetti Algoritmi di sorting o di ordinamento. Sono degli algoritmi che tendono a disporre una lista di elementi ordinatamente dal più piccolo al più grande secondo una certa relazione d'ordine.

2.5 Funzioni

Data una relazione $\mathcal{R}$ dall'insieme A all'insieme B, può avvenire che qualche elemento di A non sia associato nella relazione $\mathcal{R}$ a nessun elemento di B oppure che qualche elemento di A sia associato nella relazione $\mathcal{R}$ a più di un elemento di B. Questa osservazione conduce al concetto di funzione.

Definizione 45 *Dati gli insiemi A, B, una* funzione da A a B *è una relazione da A a B tale che ogni elemento di A è associato ad uno e un solo elemento di B.*

L'insieme A è detto *dominio* della funzione, l'insieme B *codominio*.

Esempio 46 Se $A = \{1, 2, -2, 3\}$, $B = \{1, 3, 4, 9\}$, e se la relazione da A a B è descritta dal predicato

$$P(x, y) = \text{“}x^2 = y\text{”}$$

(quindi in pratica un elemento di A è associato ad un elemento di B se il quadrato del primo è uguale al secondo) allora si ottiene una funzione da A a B in quanto il sottoinsieme $\mathcal{R}$ del prodotto cartesiano $A \times B$ che descrive in modo esplicito la relazione è

$$\mathcal{R} = \{(1, 1), (2, 4), (-2, 4), (3, 9)\}$$

e si osserva che ogni elemento di A è associato ad uno e un solo elemento di B.

Spesso una funzione da A a B è indicata col simbolo

$$f\colon A \to B$$

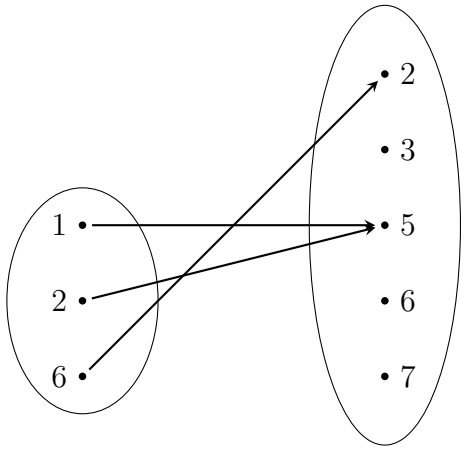
Dato un elemento a del dominio A, l'unico elemento b del codominio B che è associato all'elemento a è detto *corrispondente* o *immagine di* a, ed è indicato con il simbolo $f(a)$. L'insieme $\{f(x) \mid x \in X\}$ si chiama *insieme immagine di* X *tramite la* f.

Nel caso di funzioni matematiche fra insiemi numerici, talvolta una funzione $f\colon A \to B$ è definita scrivendo un'espressione del tipo $f(x) = \ldots$ dove i puntini contengono una formula algebrica nella variabile x, intendendo con ciò che, dato un elemento $a \in A$, l'immagine $b = f(a) \in B$ si ottiene sostituendo nella formula la variabile x con il valore a, e calcolando il risultato. Naturalmente non tutte le formule producono funzioni da A a B, come mostra il seguente esempio.

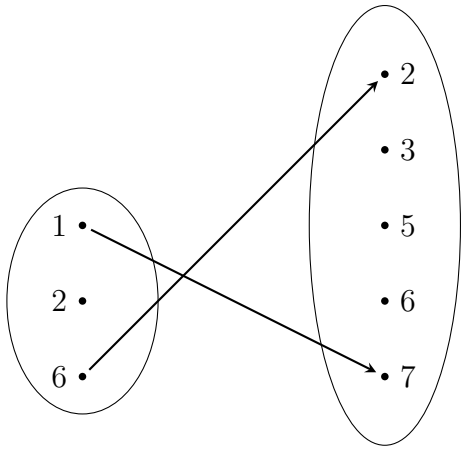
Esempio 47 $\mathbb{Z}$ è l'insieme dei numeri interi relativi ed $\mathbb{N}$ quello dei numeri naturali (interi positivi), la formula $f(x) = x^2 + 1$ definisce una funzione da $\mathbb{Z}$ a $\mathbb{N}$ (perché ad ogni intero relativo a, positivo, negativo o nullo, è associato un unico intero positivo $f(a) = a^2 + 1$). Invece se $\mathbb{Q}$ è l'insieme dei numeri razionali relativi, $f(x) = 1/(x - 2)$ non definisce una funzione da $\mathbb{Z}$ a $\mathbb{Q}$ (perché l'intero relativo 2 non ha immagine $f(2)$ in $\mathbb{Q}$).

Se la relazione è rappresentata graficamente (con le frecce e i diagrammi di Eulero-Venn), essa è una funzione quando da ogni elemento del dominio A ha origine una e una sola freccia verso il codominio B.

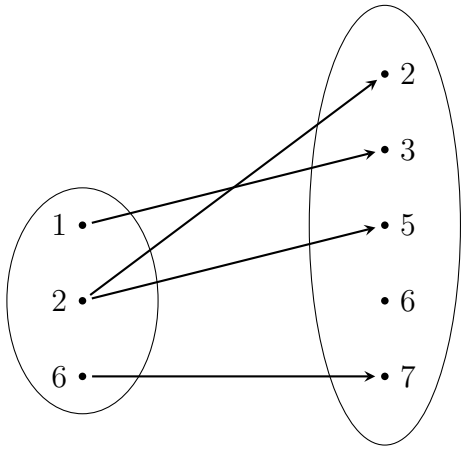
Esempio 48 *Di seguito diamo una rappresentazione grafica di una relazione che è una funzione tra* A *e* B*:*



Esempio di rappresentazione grafica di una relazione che non è una funzione da A a B (l'elemento $2 \in A$ non ha immagine in B).



Esempio di rappresentazione grafica di una relazione che non è una funzione da A a B (l'elemento $2 \in A$ ha più di un'immagine in B).



Una matrice è intuitivamente definita come una tabella con n righe e m colonne. In particolare le matrici possono essere utilizzate per rappresentare relazioni e funzioni su insiemi finiti. Infatti le righe della matrice possono rappresentare gli elementi del dominio e le colonne quelli del codominio. Dunque metteremo un 1 all'incrocio della riga i e della colonna j se l'elemento i-esimo di A e l'elemento j-esimo di B sono in relazione, e 0 altrimenti.

Se la relazione è rappresentata con una matrice, essa è una funzione quando ogni riga contiene un solo valore = 1 (e tutti gli altri = 0), ossia se ogni elemento di A è associato a un solo elemento di B. Negli esempi che seguono (di relazioni da un insieme A con 4 elementi ad un insieme B con 3 elementi) la prima matrice rappresenta una relazione che è una funzione, la seconda e la terza no (nella seconda matrice la seconda riga non contiene valori = 1, nella terza matrice la seconda riga contiene più di un valore = 1):

0	1	0
0	1	0
0	0	1
1	0	0

Tabella 2.1: Rappresentazione matriciale di una funzione

1	0	0
0	0	0
0	0	1
0	1	0

Tabella 2.2: Rappresentazione matriciale di una relazione che non è una funzione (2 non ha nessuna immagine)

0	0	1
0	1	1
0	0	1
0	1	0

Tabella 2.3: Rappresentazione matriciale di una relazione che non è una funzione (l'elemento 2 ha due immagini distinte)

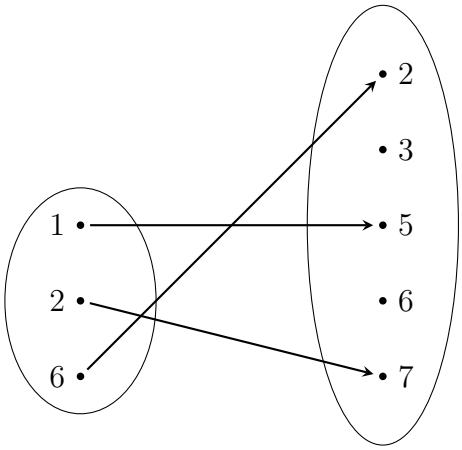
2.5.1 Funzioni iniettive

Definizione 49 *Dati gli insiemi A, B una funzione $f: A \to B$ è detta iniettiva quando elementi diversi del dominio A hanno sempre immagini diverse nel codominio B.*

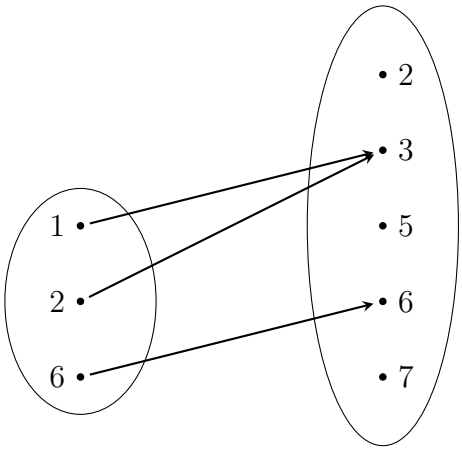
Quindi f sarà non iniettiva quando esistono almeno due elementi diversi del dominio A che hanno la stessa immagine nel codominio B.

Se la funzione f è rappresentata graficamente, la f è iniettiva quando le frecce che hanno origine dagli elementi del dominio A arrivano su elementi tutti diversi nel codominio B (cioè non devono esistere due frecce che hanno la "punta" sullo stesso elemento di B).

Esempio 50 *Esempio di rappresentazione grafica di una funzione iniettiva:*



Esempio di rappresentazione grafica di una funzione non iniettiva (gli elementi diversi 1 e 2 del dominio A hanno la stessa immagine)



Se f è rappresentata con una matrice, la f è iniettiva quando ogni colonna non contiene più di un valore $= 1$ (quindi in ogni colonna non vi sono valori $= 1$ oppure vi è esattamente un solo valore $= 1$).

In modo formale, per verificare se una funzione è iniettiva si deve dimostrare la seguente implicazione:

$$\forall a, b \in A, a \neq b \Rightarrow f(a) \neq f(b)$$

1	0	0	0
0	0	0	1
0	1	0	0

Tabella 2.4: Rappresentazione matriciale di una funzione iniettiva

La dimostrazione si effettua in genere per assurdo: si suppone vera l'ipotesi e falsa la tesi (quindi si suppone per assurdo che $a, b \in A, a \neq b$ ma $f(a) = f(b)$) e si cerca di pervenire alla contraddizione logica $a = b$).

Esempio 51 Se $f: \mathbb{N} \to \mathbb{Z}$ è la funzione definita da $f(x) = 3x - 4$ (si verifica facilmente che è effettivamente una funzione da $\mathbb{N}$ a $\mathbb{Z}$), allora f è iniettiva. Infatti se per assurdo supponiamo $a, b \in A, a \neq b, f(a) = f(b)$, si ha: $3a-4 = 3b - 4$ da cui, sommando 4 ad ambo i membri e dividendo ambo i membri per 3, si ottiene $a = b$ (contraddizione).

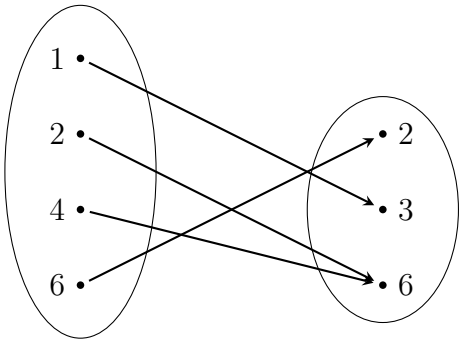
2.5.2 Funzioni surgettive

Definizione 52 *Dati gli insiemi A, B una funzione $f: A \to B$ è detta surgettiva quando ogni elemento b del codominio B é l'associato di almeno un elemento a del dominio A.*

Quindi f sarà non surgettiva quando esiste qualche elemento del codominio B che non è l'associato di nessun elemento del dominio A.

Se f è rappresentata graficamente, la f è surgettiva quando ogni elemento di B è coperto da almeno una punta delle frecce che partono dagli elementi del dominio A. Le funzioni rappresentate nell'Esempio 50 sono entrambe non surgettive (non tutti gli elementi sono immagini di qualcosa

Esempio 53 *Esempio di rappresentazione grafica di una funzione surgettiva (ogni elemento del codominio è immagine di almeno un elemento del dominio)*



Se f è rappresentata con una matrice, la f è surgettiva quando ogni colonna contiene almeno un valore = 1 (quindi non vi sono colonne con tutte le caselle contenenti valori = 0).

0	0	1
0	1	0
1	0	0
0	1	0

Tabella 2.5: Rappresentazione matriciale di una funzione surgettiva

Per verificare formalmente se una funzione $f: A \to B$ é surgettiva, fissato un generico elemento $b \in B$, si cerca almeno un elemento $a \in A$ tale che si abbia $f(a) = b$: se un tale elemento $a \in A$ esiste sempre (comunque sia preso $b \in B$) allora f é surgettiva; se invece per alcuni valori di $b \in B$ un tale elemento $a \in A$ non esiste, allora la f non è surgettiva. Si tratta in pratica di risolvere un'equazione in cui b è termine noto, ed a è l'incognita di cui si cercano soluzioni nel dominio A: se almeno una soluzione per a esiste nel dominio A (per ogni valore di b in B) allora la funzione è surgettiva.

Esempio 54 Se A é l'insieme dei numeri interi > 8, la funzione $f: A \to \mathbb{N}$ definita da $f(x) = x - 8$ é surgettiva. Infatti, fissato un generico elemento $b \in \mathbb{N}$ (quindi b è un intero positivo), la ricerca di un valore $a \in A$ tale che si abbia $f(a) = b$ porta all'equazione $a - 8 = b$, che ha (nell'incognita a) la soluzione $a = b + 8$ (soluzione il cui valore appartiene al dominio A, perché, essendo b un intero positivo, certamente $a = b + 8$ è un intero > 8). Invece la funzione $f: A \to \mathbb{N}$ definita da $f(x) = x - 5$ non é surgettiva. Infatti,

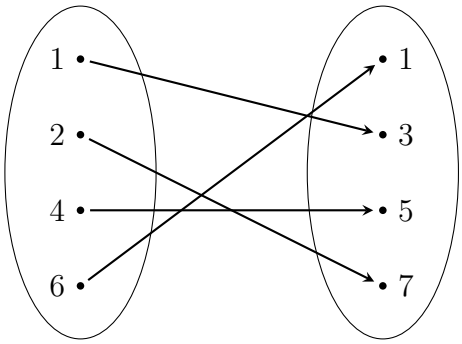
fissato un generico elemento $b \in \mathbb{N}$ (quindi b è un intero positivo), la ricerca di un valore $a \in A$ tale che si abbia $f(a) = b$ porta all'equazione $a - 5 = b$, che ha nell'incognita a la soluzione $a = b + 5$ (soluzione che però, per alcuni valori di b, può non appartenere al dominio A: per esempio per $b = 2$ si ha $a = 7 \notin A$).

2.5.3 Funzioni biunivoche

Definizione 55 *Dati gli insiemi A, B una funzione $f: A \to B$ è detta* biunivoca *(o* bigettiva *o* biiettiva*) quando f è sia iniettiva che surgettiva.*

Ciò significa che elementi diversi del dominio A hanno sempre associati elementi diversi nel codominio B, e ogni elemento del codominio B é associato di almeno un elemento del dominio A.

La seguente figura rappresenta una funzione bigettiva.



2.6 Cardinalità di un insieme e funzioni

Diremo che un insieme A è un *insieme finito* se A contiene un numero finito di elementi; in caso contrario diremo che A è un insieme infinito. Se A è un insieme finito, si definisce *cardinalità di A* (e si indica con il simbolo $|A|$) il

numero degli elementi distinti di A. Per esempio se $A = \{1, a, 2, 3, b\}$ si ha $|A| = 5$. Ovviamente $|\emptyset| = 0$.

Per il momento, se A è un *insieme infinito*, ci limiteremo a dire che la sua cardinalità è infinita (in seguito approfondiremo l'argomento distinguendo vari tipi di infinito).

Teorema 56 *Se A, B sono insiemi finiti, se $|A| = n$, $|B| = m$, e se esiste una funzione iniettiva $f\colon A \to B$ allora $n \leq m$.*

Dimostrazione Elenchiamo esplicitamente gli n elementi distinti di A:

$$A = \{a_1, a_2, a_3, \ldots, a_n\}$$

(dove a_1 indica l'elemento al primo posto nell'elenco, a_2 quello al secondo posto,..., a_n quello al posto n, ultimo nell'elenco). Poiché per ipotesi f è iniettiva, le loro immagini: $f(a_1), f(a_2), f(a_3), \ldots, f(a_n)$ sono elementi tutti diversi nel codominio B, quindi tali immagini sono esattamente in numero di n. Poiché per ipotesi B contiene esattamente m elementi, si conclude che $n \leq m$ (tesi). □

Una conseguenza immediata del teorema precedente è la seguente: se A, B sono insiemi finiti e se la cardinalità n di A è maggiore della cardinalità m di B, allora non è possibile costruire nessuna funzione iniettiva $f\colon A \to B$.

Teorema 57 *Se A, B sono insiemi finiti, se $|A| = n$, $|B| = m$, e se esiste una funzione surgettiva $f\colon A \to B$, allora $n \geq m$.*

Dimostrazione Elenchiamo esplicitamente gli m elementi distinti di B:

$$B = \{b_1, b_2, b_3, \ldots, b_m\}$$

Poiché per ipotesi f è surgettiva, troviamo almeno un elemento $a_1 \in A$ tale che $f(a_1) = b_1$ (se ne esiste più di uno, ne scegliamo a piacere uno fra i tanti che hanno come immagine b_1); per lo stesso motivo troviamo almeno un elemento $a_2 \in A$ tale che $f(a_2) = b_2$ e così procediamo fino a trovare almeno un elemento $a_m \in A$ tale che $f(a_m) = b_m$. Gli elementi trovati $a_1, a_2, \ldots, a_m$ sono tutti diversi fra loro (se due fra essi coincidessero, la f non

sarebbe più una funzione perché esisterebbe qualche elemento di A con due immagini distinte in B): si deduce che il numero degli elementi $a_1, a_2, \ldots, a_m$ è esattamente m. Poiché per ipotesi l'insieme A contiene esattamente n elementi, si conclude che $n \geq m$ (tesi). □

Una conseguenza immediata del teorema precedente è la seguente: se A, B sono insiemi finiti e se la cardinalità n di A è minore della cardinalità m di B, allora non è possibile costruire nessuna funzione surgettiva $f\colon A \to B$.

Teorema 58 *Se A, B sono insiemi finiti, se $|A| = n$, $|B| = m$ e se esiste una funzione biunivoca $f\colon A \to B$, allora $n = m$.*

Dimostrazione Essendo f iniettiva, per il Teorema 56 si ha $n \leq m$; essendo f surgettiva, per il Teorema 57 si ha $n \geq m$. Si conclude allora che $n = m$. □

Una conseguenza del teorema precedente è la seguente: se A, B sono insiemi finiti e se la cardinalità n di A è diversa dalla cardinalità m di B, allora non è possibile costruire nessuna funzione biunivoca $f\colon A \to B$.

Il prossimo risultato dimostra che, nel caso di dominio e codominio finiti e con la stessa cardinalità, i concetti di funzione iniettiva e surgettiva in pratica coincidono.

Teorema 59 *Siano A, B insiemi di cardinalità finita, e supponiamo anche che essi abbiano uguale cardinalità $|A| = n = |B|$. Allora, data una funzione $f\colon A \to B$, si ha:*

$$f \text{ è iniettiva } \Leftrightarrow f \text{ è surgettiva}$$

Dimostrazione Dimostriamo la prima implicazione $\Rightarrow$, in cui l'ipotesi è che f sia iniettiva e la tesi è che f sia surgettiva. Elenchiamo esplicitamente gli n elementi distinti di A:

$$A = \{a_1, a_2, a_3, \ldots, a_n\}$$

Poiché per ipotesi f è iniettiva, le immagini:

$$f(a_1), f(a_2), f(a_3), \ldots, f(a_n)$$

sono elementi tutti diversi nel codominio B, quindi tali immagini sono esattamente in numero di n. Ma l'insieme B contiene esattamente n elementi, e dunque tali immagini esauriscono tutti gli n elementi di B. Questo vuol dire che ogni elemento di B è immagine di qualche elemento di A, cioè f è surgettiva (tesi).

Dimostriamo la seconda implicazione $\Leftarrow$, in cui l'ipotesi è che f sia surgettiva e la tesi è che f sia iniettiva. Ragioniamo per assurdo: supponiamo vera l'ipotesi e falsa la tesi, cioè supponiamo f surgettiva ma f non iniettiva. Elenchiamo esplicitamente gli n elementi distinti di A:

$$A = \{a_1, a_2, a_3, \ldots, a_n\}$$

Poiché per assurdo f non è iniettiva, le immagini:

$$f(a_1), f(a_2), f(a_3), \ldots, f(a_n)$$

non sono tutti distinti, quindi sono in numero minore di n. Ma l'insieme B contiene esattamente n elementi, dunque tali immagini non esauriscono tutti gli n elementi di B. Questo vuol dire che esiste qualche elemento di B che non è immagine di nessun elemento di A, cioè f non é surgettiva (contraddizione). □

2.6.1 Funzione identica

Dato un insieme A, si definisce la cosiddetta *funzione identica di* A: essa è la funzione che ha dominio e codominio coincidenti entrambi con A, ed associa ogni elemento di A con sé stesso. Tale funzione si indica con il simbolo:

$$i_A \colon A \to A$$

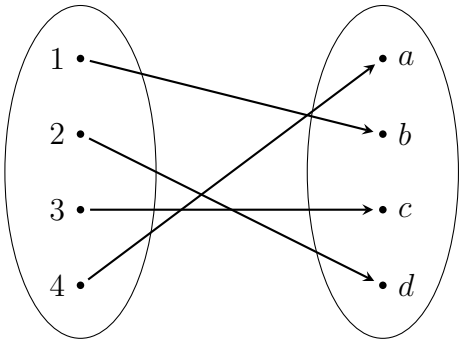
ed è quindi definita ponendo $i_A(x) = x$ per ogni $x \in A$. E' facile verificare che la funzione identica è biunivoca.

2.6.2 Funzione inversa di una funzione biunivoca

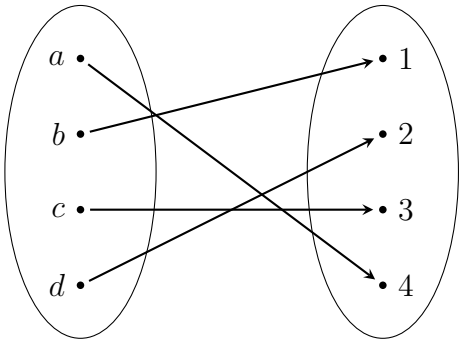
Sia data una funzione biunivoca $f \colon A \to B$. Comunque preso un elemento $b \in B$, essendo f surgettiva esiste almeno un elemento $a \in A$ tale che si

abbia $f(a) = b$. Ma questo elemento $a \in A$ tale che si abbia $f(a) = b$ è anche unico, perché f è iniettiva. Se allora associamo all'elemento $b \in B$ quest'unico elemento $a \in A$ che soddisfa la proprietà $f(a) = b$, otteniamo una nuova funzione da B ad A, detta *funzione inversa di* f. Tale funzione inversa è indicata con il simbolo $f^{-1}: B \to A$. Se la funzione f è rappresentata graficamente come nella prima figura dell'Esempio60, la f^{-1} è rappresentata graficamente semplicemente invertendo il verso delle frecce, come rappresentato nella seconda figura.

Esempio 60 *La seguente funzione è una funzione biunivoca:*



Quella descritta di seguito è la sua funzione inversa:



Formalmente, per costruire la funzione inversa di una funzione biunivoca, si deve seguire il procedimento usato per dimostrarne la surgettività; in tale

procedimento, dato un elemento generico del codominio, si cerca un elemento del dominio la cui immagine è l'elemento dato: tale elemento del dominio è per costruzione proprio l'immagine dell'elemento di partenza mediante la funzione inversa.

Esempio 61 Se $\mathbb{Z}$ è l'insieme dei numeri interi relativi e se $f : \mathbb{Z} \to \mathbb{Z}$ è la funzione definita da $f(x) = x - 5$, è facile verificare che f è iniettiva. Dimostriamo che f è surgettiva: preso un generico elemento $b \in Z$ (quindi b è un numero intero relativo), cerchiamo l'esistenza di un elemento $a \in Z$ tale che $f(a) = a - 5 = b$. Si ottiene la soluzione $a = b + 5 \in Z$. Ciò dimostra che f è surgettiva (quindi biunivoca), ma permette anche di costruire la funzione inversa $f^{-1}: \mathbb{Z} \to \mathbb{Z}$, definita appunto da $f^{-1}(x) = x + 5$.

Osservazione 62 *E' ovvio che se A è un insieme, la funzione inversa della funzione identica $i_A: A \to A$ è la stessa funzione i_A, quindi $i_A^{-1} = i_A$.*

2.6.3 Composizione di funzioni

Siano $A, B, C,$ tre insiemi e siano $f : A \to B$, $g : B \to C$ delle funzioni (notare che siamo in una situazione particolare: il codominio B di f coincide con il dominio B di g). Se prendiamo un elemento generico $a \in A$, la f associa a tale elemento a un unico elemento $b = f(a) \in B$; a sua volta la g associa a tale elemento b un unico elemento $c = g(b) \in C$. In tal modo, associando ad ogni $a \in A$ l'unico elemento $c \in C$ costruito sopra si ottiene una nuova funzione con dominio A e codominio C, detta composizione di f e g (o anche prodotto operatorio di f e g), e indicata con il simbolo

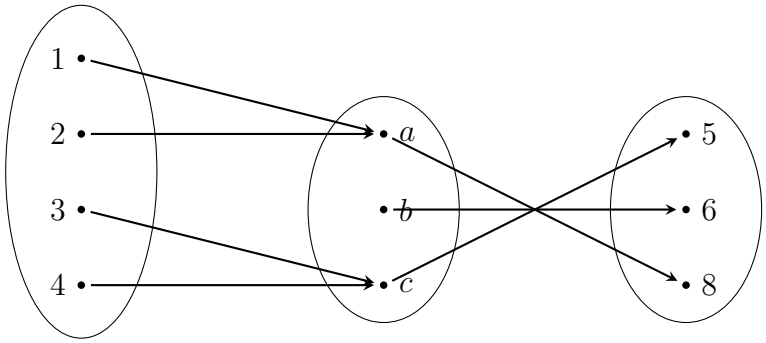
$$g \circ f: A \to C$$

In pratica l'azione di $g \circ f$ è ottenuta applicando f e poi g:

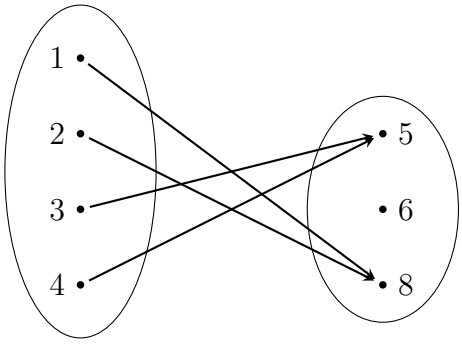
$$(g \circ f)(x) = g(f(x))$$

(notare che la funzione f, che agisce per prima, è scritta per seconda nel simbolo $g \circ f$).

Esempio 63 *Siano $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$, $C = \{5, 6, 8\}$ e siano $f: A \to B$, $g: B \to C$ le funzioni descritte graficamente da:*



Allora la composizione $g \circ f: A \to C$ è descritta graficamente da:



Esempio 64 *Se $\mathbb{N}$ è l'insieme dei numeri naturali, $\mathbb{Q}$ l'insieme dei numeri razionali, $\mathbb{R}$ l'insieme dei numeri reali, date le due funzioni $f: A \to B$, $g: B \to C$ definite dalle formule:*

$$f(x) = x/3, g(x) = \sqrt{x^2 - 1}$$

la composizione $g \circ f: A \to C$ è definita da:

$$(g \circ f)(x) = g(f(x)) = g(x/3) = \sqrt{(x/3)^2 - 1} = \sqrt{x^2 - 9/9}$$

Teorema 65 *La composizione di due funzioni iniettive è una funzione iniettiva. La composizione di due funzioni surgettive è una funzione surgettiva. La composizione di due funzioni biunivoche è una funzione biunivoca.*

Dimostrazione Siano $f : A \to B$, $g : B \to C$ due funzioni. Supponiamo dapprima che f, g siano iniettive e dimostriamo che $g \circ f$ è iniettiva: se $a, b \in$

A, $a \neq b$, si ha $f(a) \neq f(b)$ (per l'iniettività di f), e allora $g(f(a)) \neq g(f(b))$ ((per l'iniettività di g) dunque si conclude che $(g \circ f)(a) \neq (g \circ f)(b)$, ossia $g \circ f$ è iniettiva.

Supponiamo ora che f, g siano surgettive e dimostriamo che $g \circ f$ è surgettiva: dato $c \in C$, cerchiamo una elemento $a \in A$ tale che $(g \circ f)(a) = c$; ma, per la surgettività di g, esiste $b \in B$ tale che $g(b) = c$; inoltre, per la surgettività di f, esiste $a \in A$ tale che $f(a) = b$, da cui in totale $(g \circ f)(a) = c$. La terza affermazione segue ovviamente dalle prime due. □

Calcoliamo la composizione di funzioni in alcuni casi particolari.

- Siano A, B insiemi, sia $f : A \to B$ una funzione e consideriamo la funzione identica di B:
$$i_B : B \to B$$
Possiamo allora considerare la composizione $i_B \circ f : A \to B$. Per ogni elemento $x \in A$ si ha $(i_B \circ f)(x) = i_B(f(x)) = f(x)$, e si conclude che le funzioni $i_B \circ f$ ed f sono uguali (perché agiscono allo stesso modo su un generico elemento x):
$$i_B \circ f = f$$

- Analogamente siano A, B insiemi, sia $f : A \to B$ una funzione e consideriamo la funzione identica di A:
$$i_A : A \to A$$
Possiamo allora considerare la composizione $f \circ i_A : A \to B$. Per ogni elemento $x \in A$ si ha $(f \circ i_A)(x) = f(i_A(x)) = f(x)$, e di nuovo si conclude che le funzioni $f \circ i_A$ ed f sono uguali:
$$f \circ i_A = f$$

- Se poi $f : A \to B$ è una funzione biunivoca e se $f^{-1} : A \to B$ è la funzione inversa di f, possiamo considerare la composizione $f^{-1} \circ f : A \to A$. Per definizione di funzione inversa si ha ovviamente, per ogni elemento $x \in A$:
$$(f^{-1} \circ f)(x) = x$$

dunque la composizione $f^{-1} \circ f$ coincide con la funzione identica di A:

$$f^{-1} \circ f = f^{-1}(f(x)) = i_A$$

- Con ragionamento analogo si ottiene che la composizione $f \circ f^{-1} : B \to B$ coincide con la funzione identica di B:

Capitolo 3

Aritmetica dei numeri naturali

Dell'insieme dei numeri naturali $\mathbb{N}$ supporremo note le seguenti nozioni e proprietà (che fisseremo come assiomi alla base della teoria):

1. La definizione delle operazioni di *somma* $a + b$ e *prodotto* $a \cdot b$ fra due generici numeri naturali a, b (entrambe con risultato uguale ad un numero naturale), con le relative proprietà:

   (a) Proprietà associativa: comunque presi $a, b, c \in \mathbb{N}$ si ha

   $$(a + b) + c = a + (b + c), \quad (ab)c = a(bc)$$

   (b) Proprietà commutativa: comunque presi $a, b \in \mathbb{N}$ si ha

   $$a + b = b + a, \quad ab = ba$$

   (c) Proprietà distributiva della somma rispetto al prodotto: comunque presi $a, b, c \in \mathbb{N}$ si ha

   $$a(b + c) = ab + ac$$

2. La definizione di *ordinamento dei numeri naturali* cioè il significato del simbolo $a < b$ per due generici numeri naturali a, b, con le relative proprietà:

(a) comunque presi $a, b, c \in \mathbb{N}$ se $a < b$ si ha $(ac) < (bc)$ e $(a + c) < (b + c)$;

(b) comunque presi $a, b, c, d \in \mathbb{N}$ se $a < b$ e se $c < d$ si ha $(a + c) < (b + d)$ e $(ac) < (bc)$;

Scriveremo $a \leq b$ per indicare che $a < b$ oppure $a = b$: anche per le diseguaglianze della forma $a \leq b$ sono valide proprietà analoghe alle 2a, 2b citate sopra.

3. A queste proprietà aggiungeremo il cosiddetto *Assioma del minimo* (o *Assioma del buon ordinamento dei naturali*): In ogni sottoinsieme non vuoto S di $\mathbb{N}$ esiste sempre un elemento minimo, cioè esiste un $s \in S$ tale che sia abbia $s > x$ per ogni $x \in S$.

Tale assioma ha un intuitivo significato geometrico: rappresentando i numeri naturali come punti di una retta (a distanza unitaria ognuno dal successivo, cominciando dal valore 1 e proseguendo verso destra), comunque preso un insieme S non vuoto di alcuni di tali punti, esiste sempre un punto di S che è più a sinistra di tutti gli altri punti di S.

3.1 Principio di induzione

Supponiamo di avere un predicato $P(n)$ nella variabile n, con la variabile che assume valori nell'insieme $\mathbb{N}$ dei numeri naturali. Se volessimo dimostrare che $P(n)$ è vero per ogni valore della variabile n, non potremmo procedere con una verifica per tutti i valori di n, che sono infiniti.

Per esempio dato il predicato $P(n) =$ "$(n+1)^2 > n+2$" possiamo notare che per $n = 1$ è vero (perché $4 > 3$), per $n = 2$ è vero (perché $9 > 4$), per $n = 3$ è vero (perché $16 > 5$), ma come possiamo essere certi che $P(n)$ sia vero per ogni valore di n nell'insieme dei numeri naturali?

Una soluzione a questo problema è fornita dal cosiddetto *Principio di induzione*.

Teorema 66 [**Principio di induzione**] *Sia $P(n)$ un predicato nella variabile n, il cui universo (ossia l'insieme dei valori che la variabile può assumere) sia l'insieme $\mathbb{N}$ dei numeri naturali. Se sono vere le due seguenti ipotesi:*

1. *Il predicato $P(n)$ è vero per il valore $n = 1$ (in termini formali: $P(1)$ è vero);*
2. *Ogni volta che il predicato $P(n)$ è vero per un valore $n = k$, allora esso è anche vero per il valore successivo $k + 1$ (in termini formali: $P(k) \Rightarrow P(k + 1)$)*

allora $P(n)$ è vero per tutti i valori della variabile n.

Dimostrazione Per assurdo supponiamo vere le ipotesi 1 e 2 e falsa la tesi: quindi supponiamo che vi sia qualche valore della variabile n che rende falso $P(n)$. Costruiamo l'insieme (non vuoto) contenente tutti i numeri naturali che rendono falso $P(n)$:

$$S = \{k \mid k \text{ è un numero naturale per il quale } P(k) \text{ è falso}\}$$

Per l'Assioma del minimo, esiste un $s \in S$ minimo in S: quindi s è un numero naturale e inoltre $P(s)$ è falso. Per l'ipotesi 1, certamente $s \neq 1$, quindi $s > 1$ e dunque $s - 1 > 0$. Allora $s - 1$ è un numero naturale (quindi è uno dei possibili valori della variabile n): poiché $s - 1 < s$ (ed s è il minimo in S) si deduce che $s - 1 \notin S$, ossia $P(s - 1)$ è vero. Per l'ipotesi 2, sarà vero anche $P((s - 1) + 1) = P(s)$, contraddizione perché $P(s)$ è falso. □

Osservazione 67 Da ora in poi adotteremo la seguente convenzione. Generalizziamo i concetti somma e di prodotto di numeri naturali anche al caso di 1 solo addendo o 1 solo fattore: in questo caso il risultato dell'operazione sarà considerato uguale, per convenzione, all'unico addendo o fattore coinvolto nell'operazione.

Esempio 68 Diamo un esempio di applicazione del principio di induzione. **Formula di Gauss:** Dimostriamo che per ogni naturale n

$$1 + 2 + 3 + \cdots + n = \sum_{k=1}^{n} k = \frac{n(n + 1)}{2}$$

Si tratta di applicare il principio di induzione al predicato: $P(n)$ ="la somma dei primi n numeri naturali consecutivi è $= n(n+1)/2$". Basta verificare le ipotesi 1 e 2 del principio di induzione:

- $P(1)$ è vero, perché la somma del primo naturale è 1 (vedere convenzione precedente) ed in effetti $1 = 1(1+1)/2$.
- Se supponiamo vero $P(k)$ ="la somma dei primi k numeri naturali consecutivi è $= k(k+1)/2$", dimostriamo che è vero anche $P(k+1)$ ="la somma dei primi $(k+1)$ numeri naturali consecutivi è $= (k+1)(k+2)/2$".

  Ma la somma dei primi $(k+1)$ numeri naturali consecutivi si ottiene sommando la somma dei primi k naturali consecutivi (che per ipotesi è $k(k+1)/2$) con il numero $(k+1)$, ottenendo alla fine: $k(k+1)/2 + (k+1) = [k(k+1) + 2(k+1)]/2 = (k+1)(k+2)/2$, come si voleva.

Vediamo un'altra applicazione del principio di induzione che serve a calcolare il numero dei sottoinsiemi di un insieme finito:

Teorema 69 *Il numero dei sottoinsiemi di un insieme finito non vuoto di cardinalità n è 2^n.*

Dimostrazione Si tratta di applicare il principio di induzione al predicato: $P(n)$ ="Il numero dei sottoinsiemi di un insieme finito non vuoto di cardinalità n è 2^n" per dimostrare che tale predicato é vero per ogni valore naturale di n. Basta verificare le ipotesi 1 e 2 del principio di induzione:

1. $P(1)$ è vero, perché il numero dei sottoinsiemi di un insieme finito non vuoto A di cardinalità 1 è $2^1 = 2$ (i sottoinsiemi sono infatti solo $\emptyset, A$)

2. Se per un certo valore $n = k$ supponiamo vero $P(k)$ ="Il numero dei sottoinsiemi di un insieme finito non vuoto di cardinalità k è 2^k", dimostriamo che è vero anche $P(k+1)$ ="il numero dei sottoinsiemi di un insieme finito non vuoto di cardinalità $(k+1)$ è 2^{k+1}" . Dato l'insieme finito non vuoto A di cardinalità $(k+1)$, fissiamo un elemento $a \in A$ e consideriamo l'insieme $B = A - \{a\}$ di cardinalità k: poiché supponiamo vero $P(k)$ possiamo affermare

che il numero dei sottoinsiemi di B è 2^k. Per contare i sottoinsiemi di A, li dividiamo in 2 categorie:

1. I sottoinsiemi di A che non contengono l'elemento a;
2. I sottoinsiemi di A che contengono l'elemento a.

Quelli della categoria 1 non sono altro che i sottoinsiemi di B, quindi per ipotesi sono in numero di 2^k. Quelli della categoria 2 si ottengono ciascuno prendendone uno della categoria 1 e inserendo nel sottoinsieme l'elemento a, quindi sono anch'essi in numero di 2^k. In totale i sottoinsiemi di A sono in numero di $2^k + 2^k = 2k + 1$, quindi anche $P(k+1)$ è vero, come si voleva. Si conclude, applicando il principio di induzione, che $P(n)$ è vero per ogni valore naturale n, e si ottiene la tesi del teorema. □

Esercizi

1. Dimostrare che la somma dei primi n interi positivi dispari è n^2
2. Dimostrare che per ogni n naturale positivo, $n < 2^n$.
3. Dimostrare che $n^3 + n$ è divisibile per 3, per ogni intero positivo n
4. Dimostrare che $1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} + 1$
5. Progressione geometrica. Dimostrare che per ogni numero reale r (ragione) e per ogni intero naturale n si ha

$$1 + r + r^2 + r^3 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}$$

Il principio di induzione può essere enunciato anche nella seguente forma

Teorema 70 (Principio di induzione II forma) *Sia $P(n)$ un predicato nella variabile n (con universo= $\mathbb{N}$). Se sono vere le seguenti ipotesi:*

1. *$P(1)$ è vero;*
2. *Comunque fissato un valore k, ogni volta che $P(1), P(2), \ldots, P(k)$ sono veri, necessariamente anche $P(k+1)$ è vero;*

allora $P(n)$ è vero per ogni valore n.

Dimostrazione Supponiamo per assurdo che esista qualche numero naturale n che renda falso $P(n)$, e raccogliamo tali numeri in un insieme non vuoto:

$$S = \{n \in \mathbb{N} \mid P(n) \text{ è falso}\}$$

Per il principio del minimo esiste in S un valore minimo $m \in S$ (quindi in particolare $P(m)$ è falso). Per l'ipotesi 1 certamente $m > 1$, dunque possiamo considerare i numeri naturali minori di m:

$$1, 2, \ldots, m-1$$

Tali numeri non appartengono ad S (perché m è il minimo in S) dunque $P(1), P(2), \ldots, P(m-1)$ sono veri. Applicando l'ipotesi 2 al valore $k = m-1$, si ottiene che necessariamente anche $P(k+1)$ è vero, cioè $P(m)$ è vero, contraddizione. □

Definizione 71 *Dato un insieme A, si definisce* successione ad elementi in A *una qualunque funzione f che ha come dominio l'insieme $\mathbb{N}$ dei numeri naturali e come codominio l'insieme A*

$$f\colon \mathbb{N} \to A$$

In pratica f associa ad ogni numero naturale n un elemento $f(n)$ dell'insieme A: se indichiamo tale elemento $f(n)$ con il simbolo a_n otteniamo $f(1) = a_1, f(2) = a_2, f(3) = a_3 \ldots$, ossia una successione può essere pensata come una sequenza: $a_1, a_2, a_3, \ldots$.

Esempio 72 Costruiamo una successione di numeri naturali:

$$a_1, a_2, a_3, \ldots, a_n, \ldots$$

con le seguenti regole:

- definiamo $a_1 = 1$, $a_2 = 5$,
- per ogni indice $n > 2$ definiamo $a_n = 5a_{n-1} - 6a_{n-2}$.

Per esempio il termine a_3 si calcola così: $a_3 = 5a_2 - 6a_1 = 25 - 6 = 19$ e così via. Dimostriamo che per ogni numero naturale n è vero il seguente predicato:

$$P(n) = \text{“}a_n = 3^n - 2^n\text{”}$$

Utilizziamo la II forma del Principio di induzione, verificando se sono vere le ipotesi 1, 2.

- $P(1) = \text{“}a_1 = 3^1 - 2^1\text{”}$ è vero perché $a_1 = 1$.
- Fissato a piacere un valore k, supponiamo che $P(1), P(2), \ldots, P(k)$ siano veri, e dimostriamo che necessariamente anche $P(k+1)$ è vero. La nostra tesi è che $P(k+1) = \text{“}a_{k+1} = 3^{k+1} - 2^{k+1}\text{”}$ è vero. Ma per come sono stati costruiti i termini della successione, si ha $a_{k+1} = 5a_k - 6a_{k-1}$

  Per ipotesi $P(k-1) = \text{“}a_{k-1} = 3^{k-1} - 2^{k-1}\text{”}$, e $P(k) = \text{“}a_k = 3^k - 2^k\text{”}$ sono veri, dunque, sostituendo:

$$\begin{aligned} a_{k+1} = 5a_k - 6a_{k-1} = 5(3^k - 2^k) - 6(3^{k-1} - 2^{k-1}) = \\ = 5 \cdot 3^k - 5 \cdot 2^k - 6 \cdot 3^{k-1} + 6 \cdot 2^{k-1} = \\ = 5 \cdot 3 \cdot 3^{k-1} - 5 \cdot 2 \cdot 2^{k-1} - 6 \cdot 3^{k-1} + 6 \cdot 2^{k-1} = \\ = 15 \cdot 3^{k-1} - 10 \cdot 2^{k-1} - 6 \cdot 3^{k-1} + 6 \cdot 2^{k-1} = \\ = (15-6) \cdot 3^{k-1} - (10-6) \cdot 2^{k-1} = 9 \cdot 3^{k-1} - 4 \cdot 2^{k-1} = \\ = 3^2 \cdot 3^{k-1} - 2^2 \cdot 2k - 1 = 3^{k+1} - 2^{k+1} \end{aligned}$$

  e si ottiene la tesi.

Nell'esempio precedente abbiamo esaminato la costruzione di una successione di numeri naturali in cui si conoscono alcuni valori iniziali dei primi termini (nell'esempio si conoscevano il primo termine $a_1 = 1$ e il secondo termine $a_2 = 5$) e si definisce il valore di un termine generico a_n con una formula che lo fa dipendere da alcuni termini che lo precedono (nell'esempio

il termine generico a_n dipendeva dai due termini che lo precedono a_{n-1} e a_{n-2} secondo la formula $a_n = 5a_{n-1} - 6a_{n-2}$). Un tale tipo di successione è detto *successione ricorsiva*.

Naturalmente in una successione ricorsiva uno degli obiettivi è quello di potere calcolare il termine generico a_n con una *formula chiusa*, cioè con una formula che faccia dipendere a_n solo dall'indice n (e non dai termini che lo precedono). Nell'esempio precedente se volessimo calcolare il termine a_{100} con la formula ricorsiva $a_n = 5 \cdot a_{n-1} - 6 \cdot a_{n-2}$, dovremmo calcolare prima $a_3 = 5 \cdot 5 - 6 \cdot 1 = 19$, poi $a_4 = 5 \cdot 19 - 6 \cdot 5 = 65$, e così via e tale calcolo sarebbe piuttosto lungo. Invece la formula chiusa (trovata applicando il Principio di induzione): $a_n = 3^n - 2^n$ ci permette di fare il calcolo immediatamente $a_{100} = 3^{100} - 2^{100} = \cdots$.

3.1.1 La successione dei numeri di Fibonacci

La successione dei numeri di Fibonacci è una successione ben nota in Matematica e Informatica. Originariamente è stata concepita dal matematico Leonardo Pisano, detto Fibonacci per dare una legge matematica che descrivesse l'evoluzione nel tempo di una popolazione di conigli che segue le seguenti regole formali:

1. all'inizio vi è una coppia di conigli troppo piccoli per essere fertili;
2. dopo un mese la coppia diventa fertile e dopo un altro mese genera una nuova coppia di conigli, la quale impiega un mese per diventare fertile e un altro mese per generare una nuova coppia di conigli non fertile (nel frattempo anche la coppia iniziale genera una coppia di conigli ogni mese) e così via. (in pratica ogni coppia di conigli dalla nascita impiega un mese per diventare fertile, un altro mese per generare una nuova coppia di conigli e da quel momento genera ogni mese una nuova coppia di conigli).
3. La terza ipotesi (puramente formale) è che i conigli sono immortali.

Indichiamo con F_n il numero di coppie di conigli alla fine del mese numero n. Quindi $F_1 = 1$ (vi è solo la coppia iniziale); $F_2 = 1$ (vi è solo la coppia iniziale, che è diventata fertile); $F_3 = 2$ (la coppia iniziale genera una seconda coppia); $F_3 = 3$ (la coppia iniziale genera una terza coppia, e la seconda coppia diventa fertile); $F_3 = 5$ (la coppia iniziale genera una quarta coppia, e la seconda coppia genera una quinta coppia) etc. Si vede che la successione $F_1, F_2, F_3, \ldots, F_n, \ldots$ è una successione ricorsiva definita dai valori iniziali $F_1 = 1$, $F_2 = 1$, e per ogni $n > 2$ definita da $F_n = F_{n-1} + F_{n-2}$ (quindi ogni termine è la somma dei due termini che lo precedono). Infatti al mese numero n sono presenti tutte le coppie che erano presenti un mese prima (che sono in numero di F_{n-1}) più le coppie generate dalle coppie presenti due mesi precedenti che sono ora fertili (e che sono in numero di F_{n-2}).

3.1.2 La torre di Hanoi

Un altro esempio di successione deriva da un famoso gioco, quello delle *Torri di Hanoi*. Questo gioco segue le seguenti regole: ci sono aste, che indichiamo con A, B, C nelle quali si possono inserire n dischi (bucati al centro) di n diametri diversi. Il gioco inizia con tutti i dischi incolonnati su una delle aste (diciamo l'asta A) in ordine di grandezza decrescente (dal basso verso l'alto), in modo da formare un cono.

Lo scopo del gioco è portare tutti dischi su un'asta diversa da quella iniziale, potendo spostare solo un disco alla volta e potendo mettere un disco solo sopra un altro disco più grande, mai sopra uno più piccolo. Secondo una leggenda (probabilmente inventata dalla ditta che per prima ha messo in commercio il gioco) in un tempio indù alcuni monaci sono costantemente impegnati a spostare su tre colonne di diamante 64 dischi d'oro secondo le regole della Torre di Hanoi : quando i monaci completeranno il lavoro, il mondo finirà. Indichiamo con a_n il numero di mosse necessario per risolvere il gioco quando il numero di dischi è n. Per esempio per un disco solo ($n = 1$), basta 1 mossa (si sposta l'unico disco dal paletto A al paletto C) quindi $a_1 = 1$. Per due dischi ($n = 2$) bastano 3 mosse (si sposta il disco più piccolo da A a B, il disco più grande da A a C, il disco più piccolo da B a C). Ma ci si rende conto che, man mano che il numero dei dischi aumenta, il lavoro risulta sempre più complicato da gestire. In questo ci

viene in aiuto la ricorsione. Infatti conoscendo il sistema per spostare 3 dischi, possiamo ottenere lo spostamento di 4 sfruttando quanto ottenuto in precedenza. Infatti si può:

1. spostare 3 dischi dalla colonna A alla colonna B usando la colonna C come colonna di supporto;
2. spostare il disco più grande rimanente dalla colonna A alla colonna C.
3. spostare i 3 dischi dalla colonna B alla colonna C utilizzando la colonna A (ormai vuota) come colonna d'appoggio.

Questo ci dà un metodo per risolvere il problema per $n = 4$. Quindi una procedura analoga alla precedente ci permette di spostare 5 dischi e poi 6 e poi 7, etc. Vediamo come questo si traduce in numero di mosse effettuate.

Studiamo la successione $a_1, a_2, a_3, \ldots, a_n, \ldots$ che indica il numero delle mosse necessarie a risolvere il problema nel caso di $1, 2, 3, \ldots, n, \ldots$ dischi. Dimostriamo che il termine generico a_n dipende dal termine precedente a_{n-1} (se $n > 1$) secondo la formula ricorsiva $a_n = 2a_{n-1} + 1$. Infatti se il numero dei dischi è n, per risolvere il gioco possiamo operare così:

1. spostiamo $n-1$ dischi (tutti tranne il più grande) da A a B utilizzando C come colonna d'appoggio.
2. spostiamo il disco grande da A a C.
3. spostiamo $n-1$ dischi (tutti tranne il più grande) da B a C utilizzando la colonna A come colonna d'appoggio.

Per la fase 1 impieghiamo a_{n-1} mosse (perché i dischi da spostare sono in numero di $n-1$); per la fase 2 impieghiamo una mossa; per la fase 3 impieghiamo di nuovo a_{n-1} mosse (perché i dischi da spostare sono in numero di $n-1$). In totale il numero a_n di mosse è $a_{n-1} + 1 + a_{n-1} = 2a_{n-1} + 1$, come si voleva dimostrare.

Possiamo allora dire che la successione $a_1, a_2, a_3, \ldots, a_n, \ldots$ è una successione ricorsiva, dove il valore iniziale è $a_1 = 1$, e dove si pone $a_n = 2a_{n-1} + 1$ per ogni $n > 1$. Troviamo una formula chiusa per calcolare il termine generico a_n.

Teorema 73 *La successione* $a_n = 2a_{n-1} + 1$ *è descritta in forma chiusa dall'espressione* $a_n = 2^n - 1$

Dimostrazione Dimostriamo (utilizzando il principio di induzione nella I forma) che per ogni numero naturale n è vero il predicato $P(n) =$ "$a_n = 2n - 1$".

Infatti $P(1)$ è vero perché $a_1 = 1$ ed in effetti $1 = 2^1 - 1$.

Supponiamo vero $P(k)$ per un certo valore $n = k$ (quindi supponiamo vero $a_k = 2^k - 1$) e dimostriamo vero $P(k+1)$: la tesi è dunque che $a_{k+1} = 2^{k+1} - 1$. Ma per la regola vista sopra, a_{k+1} dipende dal termine precedente a_k secondo la regola $a_{k+1} = 2a_k + 1$, dunque si ha $a_{k+1} = 2a_k + 1 = 2(2^k - 1) + 1 = 2^{k+1} - 1$, cioè la tesi. □

Esempio 74 Nella leggenda dei monaci, se $n = 64$ è il numero di dischi da spostare, e se ogni mossa si compie in un secondo, il numero di mosse necessarie per completare il gioco è $a_{64} = 2^{64} - 1$ ed il tempo occorrente per eseguirle è di quasi 6 miliardi di anni.

3.2 Ricerca di una formula chiusa per una successione ricorsiva

Supponiamo di avere una successione definita in modo ricorsivo: sarebbe utile trovare una formula (detta formula chiusa) che esprima il termine generico a_n della successione in funzione di n e non in funzione dei termini precedenti (naturalmente tale formula dovrebbe soddisfare anche le condizioni iniziali, cioè i valori iniziali dei primi termini che sono in genere già fissati): una formula di questo tipo permetterebbe di valutare a_n direttamente, senza prima calcolare tutti i termini che lo precedono.

La formula che lega ogni termine della successione ad alcuni termini che lo precedono è detta *relazione ricorsiva*. Nel caso di relazioni ricorsive troppo generiche, è difficile trovarne una formula chiusa, quindi esamineremo solo alcuni casi più semplici.

Una relazione ricorsiva è detta *relazione ricorsiva omogenea* di grado k se è del tipo seguente:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

dove $c_1, c_2, \ldots, c_k$ sono dei numeri reali (detti coefficienti della relazione). Come si vede, in tale tipo di relazione ricorsiva il termine generico a_n della successione dipende dai k termini che lo precedono (che sono $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$).

Esempio 75 In un esempio precedente, si è studiata la successione costruita mediante la seguente relazione ricorsiva

$$a_n = 5a_{n-1} - 6a_{n-2}$$

che è una relazione ricorsiva omogenea di grado 2 (con coefficienti $c_1 = 5$, $c_2 = -6$): il termine generico a_n della successione dipende dai due termini che lo precedono (che sono a_{n-1}, a_{n-2}).

Anche la successione di Fibonacci è definita da una relazione ricorsiva omogenea di grado 2, poiché la relazione è la seguente:

$$F_n = F_{n-1} + F_{n-2}$$

(i coefficienti sono dunque $c_1 = 1$, $c_2 = 1$).

Per semplicità ci limiteremo a cercare una formula chiusa solo per le successioni ricorsive definite mediante una relazione ricorsiva omogenea di grado 1 o 2 .

3.2.1 Relazioni ricorsive omogenee di grado 1

In questa sezione diamo un metodo per calcolare la forma chiusa di un'equazione ricorsiva omogenea di grado 1.

Teorema 76 *Sia a_n una successione ricorsiva definita da una relazione ricorsiva omogenea di primo grado della forma:*

$$a_n = ca_{n-1}$$

per $n > 1$ (dove c è un coefficiente reale) e con valore iniziale $a_1 = b$ (dove b è un numero reale). Si ha allora:

$$a_n = bc^{n-1}$$

per ogni numero naturale n.

Dimostrazione Ragioniamo per induzione. Il teorema è vero per $n = 1$, perché $a_1 = b = bc^0 = bc^{1-1}$.

Inoltre se è vera per $n = k$, ossia se $a_k = bc^{k-1}$, allora $a_{k+1} = ca_k = cbc^{k-1} = bc^k$ quindi il teorema è vero anche per $n = k + 1$. Quindi il teorema è vero per ogni $n \in \mathbb{N}$. □

Esempio 77 Se una successione ricorsiva è definita dalla relazione ricorsiva omogenea di grado 1:

$$a_n = 5a_{n-1}$$

per $n > 1$ con valore iniziale $a_1 = 3$ si ha allora: $a_n = 3 \cdot 5^{n-1}$ per ogni numero naturale n (formula chiusa). Per esempio per calcolare il termine a_{10} basta calcolare $a_{10} = 3 \cdot 5^9$ (senza bisogno di calcolare i termini precedenti da a_1 fino ad a_9).

3.2.2 Relazioni ricorsive omogenee di grado 2

Supponiamo che una successione ricorsiva sia definita da una relazione ricorsiva omogenea di grado 2 della forma:

$$a_n = c_1a_{n-1} + c_2a_{n-2}$$

per $n > 2$ (dove c_1, c_2 sono coefficienti reali) e con valori iniziale fissati a_1, a_2. La relazione ricorsiva data può essere anche scritta nel modo seguente:

$$a_n - c_1a_{n-1} - c_2a_{n-2} = 0$$

e dunque anche nel modo seguente:

$$a_n + ba_{n-1} + ca_{n-2} = 0$$

(dove si è posto $b = -c_1, c = -c_2$).

Teorema 78 *La successione $a_n = r^n$ è una soluzione non nulla della relazione ricorsiva*

$$a_n + ba_{n-1} + ca_{n-2} = 0$$

per ogni numero naturale $n > 2$ se e solo se il numero r è una soluzione dell'equazione di 2^o grado $x^2 + bx + c = 0$.

Dimostrazione Se $a_n = r^n$ per ogni $n > 2$ è una soluzione della relazione ricorsiva data si ha:

$$r^n + br^{n-1} + cr^{n-2} = 0$$

per ogni numero naturale $n > 2$. Essendo $r > 0$ per ipotesi, si può dividere per r^{n-2} e si ottiene:

$$r^2 + br + c = 0$$

quindi r deve essere una soluzione dell'equazione $x^2 + bx + c = 0$.

Viceversa se r è una soluzione dell'equazione $x^2 + bx + c = 0$, per ogni numero naturale $n > 2$ moltiplicando per r^{n-2} l'uguaglianza $r^2 + br + c = 0$ si ha $r^n + br^{n-1} + cr^{n-2} = 0$, quindi $a_n = r^n$ è una soluzione della relazione ricorsiva data per ogni numero naturale $n > 2$. □

L'equazione

$$x^2 + bx + c = 0$$

e detta *equazione caratteristica* della relazione ricorsiva $a_n + ba_{n-1} + ca_{n-2} = 0$

Le soluzioni dell'equazione caratteristica permettono di trovare una formula chiusa per la successione ricorsiva, come ora vedremo distinguendo due casi: l'equazione ha due soluzioni distinte oppure ne ha due coincidenti.

Caso 1:

Teorema 79 *Sia* $a^n + ba^{n-1} + ca^{n-2} = 0$ *una successione ricorsiva omogenea di II grado. Se l'equazione caratteristica* $x^2 + bx + c = 0$ *ha due soluzioni distinte non nulle* r_1 *e* r_2*, fissati a piacere due numeri reali* c_1*,* c_2*, la successione*

$$a_n = c_1 r_1^n + c_2 r_2^n$$

è ancora una soluzione della relazione ricorsiva data, per ogni numero naturale $n > 2$*.*

Dimostrazione Per il Teorema 78 si ha che r_1^n , r_2^n sono entrambe soluzioni della relazione ricorsiva $a_n + ba_{n-1} + ca_{n-2} = 0$ per ogni numero naturale $n > 2$ dunque:

$$r_1^n + br_1^{n-1} + cr_1^{n-2} = 0$$
$$r_2^n + br_2^{n-1} + cr_2^{n-2} = 0$$

per ogni numero naturale $n > 2$

E allora si ha sostituendo all'equazione la successione $a_n = c_1 r_1^n + c_2 r_2^n$:

$$c_1 r_1^n + c_2 r_2^n + b(c_1 r_1^{n-1} + c_2 r_2^{n-1}) + c(c_1 r_1^{n-2} + c_2 r_2^{n-2}) =$$
$$= c_1(r_1^n + br_1^{n-1} + cr_1^{n-2}) + c_2(r_2^n + br_2^{n-1} + cr_2^{n-2}) = 0$$

per ogni numero naturale $n > 2$ il che dimostra che in effetti la successione

$$a_n = c_1 r_1^n + c_2 r_2^n$$

è ancora una soluzione della relazione ricorsiva data, per ogni numero naturale $n > 2$.

Quello che è più interessante (ma di cui omettiamo la dimostrazione) è che tutte le soluzioni della relazione ricorsiva data sono della forma trovata sopra: $a_n = c_1 r_1^n + c_2 r_2^n$. □

Quindi per trovare in questo Caso 1 una formula chiusa per la successione ricorsiva si può operare in questo modo:

- si scrive l'equazione caratteristica e si cercano le soluzioni distinte non nulle r_1 e r_2

- si scrive il termine generico a_n della successione con la formula chiusa $a_n = c_1 r_1^n + c_2 r_2^n$ (quindi come funzione di n) con due numeri reali c_1, c_2 che possono a priori essere scelti a piacere, ma che in effetti devono essere scelti imponendo che rendano valida la formula chiusa anche per i valori iniziali a_1, a_2 (che sono fissati)

Esempio 80 Nel caso della successione di Fibonacci così definita: $F_1 = 1$, $F_2 = 1$ (valori iniziali) e con relazione ricorsiva $F_n = F_{n-1} + F_{n-2}$ per ogni numero naturale $n > 2$ (quindi $F_n - F_{n-1} - F_{n-2} = 0$ per ogni $n > 2$), l'equazione caratteristica è $x^2 - x - 1 = 0$ che ha come soluzioni $r_1 = \frac{1-\sqrt{5}}{2}$ e $r_2 = \frac{1+\sqrt{5}}{2}$. Poiché esse sono distinte e non nulle, la formula chiusa per il calcolo del generico termine della successione di Fibonacci sarà:

$$F_n = c_1 r_1^n + c_2 r_2^n$$

con i numeri reali c_1 e c_2 che si possono a priori scegliere a piacere. Ma in effetti dobbiamo imporre che tali numeri rendano valida la formula chiusa anche per i valori iniziali $F_1 = 1$, $F_2 = 1$ (che sono fissati). Sostituendo tali valori nella formula chiusa si ottiene il seguente sistema nelle incognite c_1, c_2:

$$1 = F_1 = c_1 r_1^1 + c_2 r_2^1 = c_1 \left(\frac{1-\sqrt{5}}{2}\right) + c_2 \left(\frac{1+\sqrt{5}}{2}\right)$$

$$1 = F_2 = c_1 r_1^2 + c_2 r_2^2 = c_1 \left(\frac{1-\sqrt{5}}{2}\right)^2 + c_2 \left(\frac{1+\sqrt{5}}{2}\right)^2$$

le cui soluzioni si trovano con facili calcoli e sono:

$$c_1 = \frac{1}{\sqrt{5}}$$

$$c_2 = -\frac{1}{\sqrt{5}}$$

Sostituendo si ottiene alla fine la seguente formula chiusa per il generico numero di Fibonacci:

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right]$$

Caso 2:

Teorema 81 *Sia $a^n + ba^{n-1} + ca^{n-2} = 0$ una successione ricorsiva omogenea di II grado. Se l'equazione caratteristica $x^2 + bx + c = 0$ ha due soluzioni coincidenti non nulle $r_1 = r_2 = r$, allora fissati a piacere due numeri reali c_1, c_2, la successione:*

$$a_n = (c_1 + c_2 n)r^n$$

è ancora una soluzione della relazione ricorsiva data, per ogni numero naturale $n > 2$.

Dimostrazione Come è noto dall'algebra elementare se le due soluzioni sono coincidenti, $x^2 + bx + c = (x - r)^2 = x^2 - 2rx + r^2$ dunque $c = r^2$ e $b = -2r$. Per il Teorema 78 si ha che r^n è soluzione della relazione ricorsiva:

$$a_n + ba_{n-1} + ca_{n-2} = 0$$

per ogni numero naturale $n > 2$. Dunque:

$$r^n + br^{n-1} + cr^{n-2} = 0$$

per ogni numero naturale $n > 2$.

Dimostriamo che la successione $(c_1 + c_2 n)r^n$ è soluzione dell'equazione ricorsiva.

$$(c_1 + c_2 n)r^n + b(c_1 + c_2(n-1))r^{n-1} + c(c_1 + c_2(n-2)r^{n-2} =$$
$$= c_1(r^n + br^{n-1} + cr^{n-2}) + c_2^n(r^n + br^{n-1} + cr^{n-2}) - bc_2 r^{n-1} - 2cc_2 r^{n-2} =$$
$$= -bc_2 r^{n-1} - 2cc_2 r^{n-2} = (2r)c_2 r^{n-1} - 2r^2 c_2 r^{n-2} = 0$$

il che dimostra che in effetti la successione:

$$a_n = (c_1 + c_2 n)r_n$$

è ancora una soluzione della relazione ricorsiva data, per ogni numero naturale $n > 2$.

Ma anche in questo caso quello che è più interessante (ma di cui omettiamo la dimostrazione) è che tutte le soluzioni della relazione ricorsiva data sono della forma trovata sopra:

$$a_n = (c_1 + c_2 n)r^n$$

□

Quindi per trovare in questo Caso 2 una formula chiusa per la successione ricorsiva si può operare in questo modo:

- si scrive l'equazione caratteristica e si cercano le soluzioni coincidenti non nulle $r_1 = r_2 = r$;
- si scrive il termine generico a_n della successione con la formula chiusa $a_n = (c_1 + c_2 n)r^n$ (quindi come funzione di n) con due numeri reali c_1, c_2 che possono a priori essere scelti a piacere, ma che in effetti devono essere scelti imponendo che rendano valida la formula chiusa anche per i valori iniziali a_1, a_2 (che sono fissati)

Esempio 82 Nel caso della successione ricorsiva definita da: $a_1 = 0$, $a_2 = 1$ (valori iniziali), e con relazione ricorsiva $a_n = 4a_{n-1} - 4a_{n-2}$ per ogni numero naturale $n > 2$ (quindi $a_n - 4a_{n-1} + 4a_{n-2} = 0$ per ogni $n > 2$), l'equazione caratteristica è:

$$x^2 - 4x + 4 = 0$$

che ha 2 soluzioni coincidenti $r_1 = r_2 = 2$. La formula chiusa per il calcolo del generico termine della successione sarà:

$$a_n = (c_1 + c_2 n)r^n = (c_1 + c_2 n)2^n$$

con i numeri reali c_1 e c_2 che si possono a priori scegliere a piacere. Ma in effetti dobbiamo imporre che tali numeri rendano valida la formula chiusa anche per i valori iniziali $a_1 = 0$, $a_2 = 1$ (che sono fissati). Sostituendo tali valori nella formula chiusa si ottiene il seguente sistema nelle incognite c_1, c_2:

$$0 = a_1 = (c_1 + c_2)^2$$

$$1 = a_2 = (c_1 + c_2 \cdot 2)2^2$$

le cui soluzioni si trovano con facili calcoli e sono:

$$c_1 = \frac{-1}{4}$$

$$c2 = \frac{1}{4}$$

Sostituendo si ottiene alla fine la seguente formula chiusa per il generico elemento a_n:

$$a_n = (\frac{-1}{4} + \frac{1}{4}n)2^n$$

Sostituendo 4 con 2^2 si ottiene più sinteticamente: $a_n = (-1 + n)2^{n-2}$

Capitolo 4

Calcolo combinatorio

In questo capitolo trattiamo di metodi che permettono di contare gli elementi di insiemi di oggetti definiti in base a delle proprietà combinatoriche. Molti di questi problemi di conteggio vengono risolti mediante il seguente principio delle scelte multiple.

4.1 Principio delle scelte multiple

Il *principio delle scelte multiple* serve per contare gli elementi di un insieme finito, almeno in alcuni casi particolari. Partiamo da un esempio.

Esempio 83 Sia A l'insieme dei numeri naturali di 2 cifre (decine e unità) con cifre scelte fra i valori $1, 2, 3, 4$, e tali che la cifra delle decine sia minore di quella delle unità. Supponiamo di volere contare il numero di elementi di A, ossia conoscerne la cardinalità.

Notiamo che ogni elemento di A dipende dai valori di 2 variabili: la cifra x_1 delle decine e la cifra x_2 delle unità: quindi contare gli elementi di A equivale a contare le coppie di valori delle 2 variabili x_1, x_2.

Possiamo allora utilizzare il seguente metodo di calcolo: fissiamo un primo valore della variabile x_1, e in corrispondenza contiamo quanti sono i valori della variabile x_2; poi fissiamo un secondo valore della variabile x_1, e in corrispondenza contiamo quanti sono i valori della variabile x_2; continuiamo a procedere in questo modo (fissando ogni volta un valore della variabile x_1 e in corrispondenza contando quanti sono i valori della variabile x_2) fino ad esaurire tutti i possibili valori della variabile x_1. Sommando tutti i numeri ottenuti otterremo il numero degli elementi di A.

Più in dettaglio, fissato il valore $x_1 = 1$ (quindi la cifra delle decine è $= 1$) otteniamo in corrispondenza 3 valori di x_2 (valori della cifra delle unità che sono $2, 3, 4$), analogamente fissato il valore $x_1 = 2$ otteniamo in corrispondenza 2 valori di x_2 (che sono $3, 4$), fissato il valore $x_1 = 3$ otteniamo in corrispondenza 1 valore di x_2 (che è 4), fissato il valore $x_1 = 4$ otteniamo in corrispondenza 0 valori di x_2. In totale il numero di coppie di valori x_1, x_2(e quindi il numero di elementi di A) è la somma $3 + 2 + 1 + 0 = 6$.

Ora facciamo un altro esempio, con una situazione particolare.

Esempio 84 Sia A l'insieme dei numeri naturali di 2 cifre (decine e unità) con cifre scelte fra i valori $1, 2, 3, 4, 5, 6$ e tali che la cifra delle decine sia diversa da quella delle unità.

Come nell'esempio precedente, possiamo notare che ogni elemento dipende dai valori di 2 variabili: la cifra x_1 delle decine e la cifra x_2 delle unità. La variabile x_1 può assumere 6 valori distinti $1, 2, 3, 4, 5, 6$. Fissato un valore di x_1, il numero dei valori immagini di x_2 è costantemente uguale a 5 (sono tutti i valori 1,2,3,4,5,6 tranne quello scelto per x). Utilizzando il metodo precedente, si ottiene che il numero di elementi di A è la somma $5 + 5 + 5 + 5 + 5 + 5 = 6 \cdot 5 = 30$. Dunque rispetto all'esempio precedente il calcolo è stato più immediato: per ottenere il numero di elementi di A abbiamo calcolato il prodotto del numero dei valori possibili di x_1 per il numero dei valori possibili di x_2 (questo però solo perché, fissato un valore di x_1, il numero dei valori immagini di x_2 rimaneva costante, anche modificando il valore di x_1).

Da questo esempio possiamo dedurre il cosiddetto principio delle scelte multiple per 2 variabili:

Principio delle scelte multiple per 2 variabili

Sia A un insieme finito. Se:

- ogni elemento di A dipende dal valore di 2 variabili x_1, x_2;
- il numero di valori possibili di x_1 è uguale a h_1:
- fissato un valore di x_1, il numero di valori possibili di x_2 è costantemente uguale ad h_2

allora il numero di elementi di A è uguale al prodotto $h_1 h_2$.

Con ragionamenti simili ai precedenti si ottiene il principio delle scelte multiple per un numero qualunque di variabili:

Principio delle scelte multiple per k variabili

Se A è un insieme finito, e se:

- ogni elemento dell'insieme finito A dipenda dai valori di n variabili $x_1, x_2, \ldots, x_n$;
- il numero di possibili valori di x_1 é uguale ad h_1;
- fissato un valore di x_1, il numero di valori possibili di x_2 è costantemente uguale a h_2;
- fissato un valore di x_1 e di x_2, il numero di valori possibili di x_3 é costantemente uguale a h_3;
- $\cdots$

- fissato un valore di $x_1, x_2, \ldots, x_{n-1}$, il numero dei valori possibili di x_n é costantemente uguale ad h_n,

allora il numero degli elementi di A è uguale al prodotto $h_1 h_2 \cdots h_n$.

Vediamo alcune applicazioni del principio delle scelte multiple.

Teorema 85 *Siano A, B due insiemi finiti rispettivamente con $|A| = n$, $|B| = m$, allora il numero di tutte le funzioni $f : A \to B$ è $|B|^{|A|} = m^n$.*

Dimostrazione Se $\{a_1, a_2, \ldots, a_n\}$ sono gli elementi di A, ognuna di tali funzioni dipende dalle n variabili seguenti:

- x_1=valore dell'immagine in B dell'elemento a_1;
- x_2=valore dell'immagine in B dell'elemento a_2;
- $\cdots$
- x_n=valore dell'immagine in B dell'elemento a_n.

La variabile x_1 ha m valori possibili (gli m elementi di B); fissato un valore di x_1, la variabile x_2 ha m valori possibili (di nuovo gli m elementi di B); fissato un valore di x_1 e un valore di x_2, la variabile x_3 ha m valori possibili (di nuovo gli m elementi di B); etc; infine fissato un valore di x_1, uno di x_2, ..., uno di x_{n-1}, la variabile x_n ha m valori possibili (sempre gli m elementi di B). Per il principio delle scelte multiple, il numero delle possibili funzioni $f : A \to B$ è il prodotto $m \cdot m \cdot \cdots \cdot m$ (con n fattori), quindi è la potenza m^n. □

Esempio 86 Se $A = \{a, b\}$, $B = \{1, 2, 3\}$, il numero delle possibili funzioni $f : A \to B$ è $3^2 = 9$, mentre il numero delle possibili funzioni $f : B \to A$ è $2^3 = 8$.

Teorema 87 *Siano A, B due insiemi finiti rispettivamente con $|A| = n$, $|B| = m$. Allora il numero delle funzioni iniettive $f : A \to B$ è $m(m-1)(m-2)\cdots(m-n+1)$.*

Dimostrazione Sappiamo già che nel caso $n > m$ tale numero è 0 perché (per un Teorema dimostrato in precedenza) non esiste in questo caso nessuna funzione iniettiva da A a B. Quindi supponiamo $n < m$. Se $\{a_1, a_2, \ldots, a_n\}$ sono gli elementi di A, ognuna di tali funzioni iniettive dipende dalle n variabili seguenti:

- x_1=valore dell'immagine in B dell'elemento a_1;
- x_2=valore dell'immagine in B dell'elemento a_2;
- $\cdots$
- x_n=valore dell'immagine (in B) dell'elemento a_n.

La variabile x_1 ha m valori possibili (gli m elementi di B); fissato un valore di x_1, la variabile x_2 ha $m-1$ valori possibili (gli m elementi di B escluso quello scelto come immagine di a_1); fissato un valore di x_1 e uno di x_2, la variabile x_3 ha $m-2$ valori possibili (gli m elementi di B meno quelli scelti come immagini di a_1, a_2); etc.; fissato un valore di x_1, uno di x_2,$\cdots$, uno di x_{n-1}, la variabile x_n ha $m-(n-1) = m-n+1$ valori possibili (gli m elementi di B meno quelli scelti come immagini di $a_1, a_2, \ldots, a_{n-1}$). Per il principio delle scelte multiple, il numero delle possibili funzioni iniettive $f : A \to B$ è il prodotto $m(m-1)(m-2)\cdots(m-n+1)$, quindi è il prodotto in ordine decrescente dei numeri naturali da m ad $m-n+1$ (supponendo sempre $n < m$). □

Esempio 88 Se $A = \{a, b, c, d\}$, $B = \{1, 2, 3, 4, 5, 6\}$, $|A| = 4$, $|B| = 6$ il numero delle possibili funzioni iniettive $f : A \to B$ è $6 \cdot 5 \cdot 4 \cdot 3 = 360$.

Il problema di contare il numero delle funzioni surgettive fra insiemi finiti sarà affrontato in seguito, nell'ambito della teoria dei numeri di Stirling.

Siano A, B due insiemi finiti rispettivamente con $|A| = n$, $|B| = m$. Vogliamo contare il numero di tutte le possibili funzioni biunivoche $f : A \to B$. Sappiamo già che nel caso $n \neq m$ tale numero è 0 perché (per un Teorema dimostrato in precedenza) non esiste in questo caso nessuna funzione biunivoca da A in B. Quindi supponiamo $n = m$.

Teorema 89 *Siano A, B due insiemi finiti con $|A| = |B| = n$. Il numero di funzioni biunivoche $f: A \to B$ è $n(n-1)(n-2)\cdot\cdots\cdot 2\cdot 1 = n!$.*

Dimostrazione Per un teorema già dimostrato, sappiamo che, sotto l'ipotesi $A = B$, una funzione iniettiva è sempre anche surgettiva, quindi biunivoca: basta allora contare solo le funzioni iniettive da A a B. Applicando la formula precedente (con $n = m$) si ottiene che il numero delle possibili funzioni biunivoche $f : A \to B$ è il prodotto $n(n-1)\cdots 2\cdot 1$ □

Tale numero (ottenuto moltiplicando tutti i numeri naturali consecutivi da 1 ad n) è detto *fattoriale di n* ed è indicato con il simbolo $n!$. Quindi:

$$n! = n(n-1)\cdots 2\cdot 1 = 1\cdot 2\cdots (n-1)n$$

rappresenta il numero delle funzioni biunivoche fra 2 insiemi finiti di eguale cardinalità n.

Esempio 90 Se $A = \{1,2,3,4,5\}$, $B = \{6,7,8,9,10\}$, il numero delle funzioni biunivoche $f : A \to B$ è $5! = 1\cdot 2\cdot 3\cdot 4\cdot 5 = 120$.

Esercizi

1. Le sedie di un auditorium possono essere etichettate con una lettera e un intero positivo minore o uguale a 100. Quant'è il più grande numero do sedie che può essere etichettato in maniera differente?
2. Quante stringhe di lunghezza 7 di bit $\{0,1\}$ si possono costruire?
3. Quante targhe di macchine diverse si possono costruire se le targhe sono fatte di una sequenza di tre lettere seguite da 3 cifre?

4.2 Calcolo combinatorio

Il calcolo combinatorio è quella parte della teoria degli insiemi che studia i diversi modi di combinare gli elementi di un insieme finito.

4.2.1 Disposizioni semplici e con ripetizione

Siano n, m due numeri naturali qualunque. Sia poi A un insieme di cardinalità n, contenente gli n elementi distinti $a_1, a_2, \ldots, a_n$.

Definizione 91 *Chiamiamo* disposizione di classe m degli n elementi $a_1, a_2, \ldots, a_n$ *(o* disposizione degli n elementi $a_1, a_2, \ldots, a_n$ presi ad m ad m*) un qualunque modo di scegliere ordinatamente m fra gli n elementi $a_1, a_2, \ldots, a_n$ (quindi 2 disposizioni si distinguono fra loro non solo per gli m elementi scelti ma anche per il loro ordine).*

Una disposizione è detta semplice *se gli m elementi scelti sono tutti distinti (e in questo caso necessariamente deve essere $n \geq m$) oppure* con ripetizione *se è possibile (ma non obbligatorio) ripetere qualche elemento più volte (e in questo caso n, m possono essere arbitrari) .*

Indicheremo con il simbolo $D_{n,m}$ l'insieme di tutte le possibili disposizioni semplici di classe m degli n elementi $a_1, a_2, \ldots, a_n$, e con il simbolo $D^r_{n,m}$ l'insieme di tutte le possibili disposizioni con ripetizione di classe m degli n elementi $a_1, a_2, \ldots, a_n$ (nel simbolo, l'insieme A degli elementi non è indicato esplicitamente: d'altronde per le considerazioni che faremo, la natura degli elementi $a_1, a_2, \ldots, a_n$ non avrà influenza). Ovviamente ogni disposizione semplice è una particolare disposizione con ripetizione, quindi, come insiemi, si ha la seguente inclusione $D_{n,m} \subset D^r_{n,m}$.

Esempio 92 *Se $A = \{a, b, c\}$ (quindi $n = 3$) e se fissiamo $m = 2$ si ha:* $D_{3,2} = \{ab, ba, ac, ca, bc, cb\}$; $D^r_{3,2} = \{ab, ba, ac, ca, bc, cb, aa, bb, cc\}$

4.2.2 Numero delle disposizioni

Contiamo le disposizioni con ripetizione di classe m di n elementi $a_1, a_2, \ldots, a_n$. Ognuna di tali disposizioni dipende dai valori delle seguenti m variabili $x_1, x_2, \ldots, x_m$:

- x_1=valore dell'elemento nella prima posizione della disposizione;

- x_2= valore dell'elemento nella seconda posizione della disposizione;
- $\cdots$
- x_m= valore dell'elemento nell' ultima posizione della disposizione (la posizione numero m).

La variabile x_1 ha n valori possibili (gli n elementi $a_1, a_2, \ldots, a_n$); fissato un valore di x_1, la variabile x_2 ha n valori possibili (sempre gli n elementi $a_1, a_2, \ldots, a_n$); $\cdots$; fissato un valore di x_1, uno di x_2, ..., uno di x_{m-1}, la variabile x_m ha n valori possibili (sempre gli n elementi $a_1, a_2, \ldots, a_n$). Per il principio delle scelte multiple, il numero delle possibili disposizioni con ripetizione di $D^r_{n,m}$ è il prodotto $n \cdot n \cdot \cdots \cdot n$ (con m fattori), quindi è la potenza n^m:

$$D^r_{n,m} = n^m$$

Contiamo ora le disposizioni semplici di classe m di n elementi $a_1, a_2, \ldots, a_n$. Ovviamente nel caso $n < m$ non esiste nessuna di tali disposizioni semplici (essendo gli elementi dati in numero minore del numero m di quelli da scegliere, si è obbligati a delle ripetizioni):

$$D_{n,m} = \emptyset$$

nel caso $n < m$.

Quindi supponiamo di essere nel caso $n \geq m$.

Ogni disposizione semplice di classe m degli n elementi $a_1, a_2, \ldots, a_n$ dipende dai valori di m variabili $x_1, x_2, \ldots, x_m$, il cui significato è lo stesso di quello considerato nel caso delle disposizioni semplici. La variabile x_1 ha n valori possibili (gli n elementi $a_1, a_2, \ldots, a_n$); fissato un valore di x_1, la variabile x_2 ha $(n-1)$ valori possibili (gli n elementi $a_1, a_2, \ldots, a_n$ meno quello scelto come valore di x_1); $\cdots$; fissato un valore di x_1, uno di x_2, $\cdots$, uno di x_{m-1}, la variabile x_m ha $n-(m-1) = n-m+1$ valori possibili (gli n elementi $a_1, a_2, \ldots, a_n$ meno gli $m-1$ elementi scelti come valore di $x_1, x_2, \ldots, x_{m-1}$). Per il principio delle scelte multiple, il numero delle possibili disposizioni semplici di $D_{n,m}$ è il prodotto $n(n-1)(n-2)\cdots(n-m+1)$ (sempre nell'ipotesi che sia $n \geq m$):

$$D_{n,m} = n(n-1)(n-2)\cdots(n-m+1)$$

Esaminiamo alcune terminologie particolari relative alla teoria delle disposizioni.

1. **Permutazioni** Nel caso particolare $n = m$, le disposizioni semplici di n elementi presi ad n ad n sono dette *permutazioni* degli n elementi dati: esse rappresentano in pratica tutti i modi diversi di disporre in ordine gli n elementi dati. Il numero delle permutazioni di n elementi si ricava come caso particolare dalla formula della disposizioni semplici ponendo $n = m$: le permutazioni di n elementi sono dunque in numero di
$$n(n-1)(n-2)\cdots 1 = n!$$

   Esempio 93 *Se* $A = \{1, 2, 3, 4\}$*, le permutazioni di* $1, 2, 3, 4$ *sono in numero di* $4! = 24$*, ed esse costituiscono l'insieme*
$$D_{4,4} = \{1234, 1432, 2341, 4132, \ldots\}$$
   contenente appunto i 24 *modi diversi di disporre in ordine gli elementi* $1, 2, 3, 4$*.*

2. **Parole** Nel linguaggio informatico, le disposizioni con ripetizione degli n elementi $a_1, a_2, \ldots, a_n$ presi ad m ad m sono spesso chiamate *parole di lunghezza* m *sull'alfabeto* $a_1, a_2, \ldots, a_n$ (gli elementi $a_1, a_2, \ldots, a_n$ sono dette lettere dell'alfabeto): secondo quanto dimostrato quando abbiamo calcolato il numero delle disposizioni di n elementi presi ad m ad m, il numero delle parole di lunghezza m su un alfabeto di n lettere è n^m.

   Esempio 94 *Le parole di lunghezza 4 sull'alfabeto* $\{0, 1\}$ *sono le seguenti* $2^4 = 16$ *disposizioni con ripetizione dei* 2 *elementi* $0, 1$ *presi a* 4 *a* 4*:*
$$\{0000, 1111, 0001, 0010, 0100, 1000, 0011, 0101, 0110,$$
$$1010, 1100, 1001, 1110, 1101, 1011, 0111\}$$
   Le parole di lunghezza 8 sono in numero di $2^8 = 256$. Le parole binarie di 8 caratteri sono chiamati in informatica byte. Queste 256 disposizioni costituisce un modo di codificare in binario 256 possibili caratteri (codice ASCII).

4.3 Combinazioni

Definizione 95 *Siano n, m due numeri naturali qualunque. Sia poi A un insieme di cardinalità n, contenente gli n elementi distinti $a_1, a_2, \ldots, a_n$. Chiamiamo* combinazione di classe m degli n elementi *(o* combinazione degli n elementi presi ad m ad m*) un qualunque modo di scegliere m fra gli n elementi, non tenendo conto dell'ordine di scelta (quindi 2 combinazioni si distinguono fra loro solo per gli m elementi scelti e non per il loro ordine).*

Una combinazione è semplice *se gli elementi scelti sono tutti distinti (e in questo caso necessariamente deve essere $n \geq m$) oppure* con ripetizione *se è possibile ripetere qualche elemento più volte.*

Indicheremo con $C_{n,m}$ l'insieme di tutte le possibili combinazioni semplici di classe m degli n elementi, e con $C^r_{n,m}$ l'insieme di tutte le possibili combinazioni con ripetizione di classe m degli n elementi. Ovviamente ogni combinazione semplice è una particolare combinazione con ripetizione, quindi si ha $C_{n,m} \subset C^r_{n,m}$.

Esempio 96 *Se $A = \{a, b, c, d\}$ (quindi $n = 4$) e se fissiamo $m = 3$ si ha:*

$$C_{4,3} = \{abc, abd, acd, bcd\}$$

$$C^r_{4,3} = \{abc, abd, acd, bcd, aab, aac, aad, bbc, bba,$$
$$bbd, cca, ccb, ccd, dda, ddb, ddc, aaa, bbb, ccc, ddd\}$$

4.3.1 Numero delle combinazioni semplici

Calcoliamo la cardinalità di $C_{n,m}$ ossia il numero delle combinazioni semplici di n elementi $a_1, a_2, \ldots, a_n$ presi ad m ad m. Ragionando come nel caso delle disposizioni semplici, si deduce che nel caso $n < m$ non esiste nessuna di tali combinazioni semplici:

$$C_{n,m} = \emptyset \text{ se } n < m$$

Quindi supponiamo di essere nel caso $n \geq m$. Consideriamo l'insieme $D_{n,m}$ delle disposizioni semplici degli n elementi presi ad m ad m: sappiamo che ha cardinalità

$$n(n-1)(n-2)\cdots(n-m+1)$$

Poiché nelle combinazioni l'ordine degli elementi non conta, possiamo suddividere l'insieme delle disposizioni $D_{n,m}$ in sottoinsiemi, ponendo in ciascun sottoinsieme le disposizioni che coinvolgono m elementi fissati fra gli n elementi dati: è ovvio che le diverse disposizioni poste nello stesso sottoinsieme corrispondono ad 1 sola combinazione (per esempio se $A = \{a, b, c, d\}$, $n = 4$, $m = 3$ potremmo fissare i 3 elementi a, b, c e considerare le disposizioni che coinvolgono solo a, b, c, cioè $abc, acb, bac, bca, cab, cba$: esse sono 6 diverse disposizioni ma rappresentano 1 sola combinazione). Contare il numero delle combinazioni equivale a contare il numero dei sottoinsiemi in cui abbiamo suddiviso $D_{n,m}$. Ma in ognuno di tali sottoinsiemi vi sono le disposizioni che coinvolgono m elementi fissati e queste non sono altro che le permutazioni di questi m elementi: sappiamo già che esse sono in numero di $m!$. Dunque ognuno dei sottoinsiemi in cui abbiamo ripartito $D_{n,m}$ contiene lo stesso numero $m!$ di disposizioni. In totale il numero delle combinazioni semplici di n elementi $a_1, a_2, \ldots, a_n$ presi ad m ad m si otterrà dividendo la cardinalità di $D_{n,m}$ per $m!$, ottenendo alla fine, se $n \geq m$

$$C_{n,m} = \frac{D_{n,m}}{P_m} = \frac{n(n-1)(n-2)\cdots(n-m+1)}{m!}$$

Tale numero (intero nonostante la rappresentazione sotto forma di frazione) è detto *coefficiente binomiale* ed è indicato con il simbolo:

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

Esempio 97 *Se* $A = \{a, b, c, d, e, f\}$ *(quindi* $n = 6$*) e se* $m = 3$*, le combinazioni semplici dei* 6 *elementi presi a* 3 *a* 3 *sono in numero di*

$$\binom{6}{3} = \frac{6 \cdot 5 \cdot 4}{3!} = 20$$

Esempio 98 *Le combinazioni del Superenalotto sono le combinazioni semplici di* 90 *numeri presi a* 6 *a* 6*, quindi sono in numero di*

$$\binom{90}{6} = \frac{90 \cdot 89 \cdot 88 \cdot 87 \cdot 86 \cdot 85}{6!} = 622.614.630$$

4.3.2 Significato insiemistico del coefficiente binomiale

Se $A = \{a_1, a_2, \ldots, a_n\}$, possiamo notare che sostanzialmente il concetto di combinazione semplice degli n elementi $a_1, a_2, \ldots, a_n$ presi ad m ad m coincide con quello di sottoinsieme di cardinalità m contenuto nell'insieme A di cardinalità n (essendo gli elementi scelti nella combinazione tutti distinti e non tenendo conto del loro ordine). Per esempio le combinazioni semplici dei 3 elementi a, b, c presi a 2 a 2:

$$\{ab, ac, bc\}$$

corrispondono sostanzialmente a tutti i sottoinsiemi di cardinalità 2 dell'insieme $\{a, b, c\}$ di cardinalità 3: $\{a, b\}, \{a, c\}, \{b, c\}$

Per quanto dimostrato nella teoria delle combinazioni semplici, se fissiamo due numeri naturali n, m (con $n \geq m$), il coefficiente binomiale rappresenta dunque anche il numero dei sottoinsiemi di cardinalità m che sono contenuti in un insieme A di cardinalità n.

4.3.3 Numero delle combinazioni con ripetizione

Vogliamo ora contare il numero delle combinazioni con ripetizione di n elementi $a_1, a_2, \ldots, a_n$ presi ad m ad m, ossia la cardinalità di $C^r_{n,m}$. Per ottenere tale risultato abbiamo bisogno però di alcuni risultati preliminari.

Fissiamo un naturale r e consideriamo tutte le parole di lunghezza r sull'alfabeto $\{0, 1\}$: sappiamo che esse sono in numero di 2^r. Fissiamo poi un naturale $s \leq r$ e contiamo le parole di lunghezza r sull'alfabeto $\{0, 1\}$ che contengono la lettera 1 esattamente s volte. Ognuna di tali parole dipende da due variabili:

x_1=scelta delle s posizioni (fra le r disponibili) in cui inserire la lettera 1

x_2=scelta delle posizioni in cui inserire la lettera 0.

I valori possibili di x_1 corrispondono alle combinazioni semplici di r posizioni prese ad s ad s (perché la scelta di s posizioni fra le r disponibili

non tiene conto dell'ordine di scelta e non è possibile ripetere una casella più volte), quindi sono in numero di $\binom{r}{s}$. Fissato un valore per x_1 (cioè fissata una scelta delle s posizioni, fra le r disponibili, in cui inserire la lettera 1), per il valore di x_2 vi è una scelta obbligata (le rimanenti $(r-s)$ posizioni devono tutte contenere 0) ossia il numero dei valori possibili di x_2 è 1. Per il principio delle scelte multiple, il numero delle parole di lunghezza r sull'alfabeto $\{0,1\}$ che contengono la lettera 1 esattamente s volte coincide allora con il coefficiente binomiale $\binom{r}{s}$. Siamo ora in grado di determinare la cardinalità di $C^r_{n,m}$ ossia il numero delle combinazioni con ripetizione di n degli elementi presi ad m ad m. Siano $a_1, a_2, \ldots, a_n$ gli n elementi.

Considerando che l'ordine degli elementi non è importante, una generica combinazione con ripetizione di $C^r_{n,m}$ si può rappresentare nella forma:

$$a_1, a_1, \ldots, a_1, a_2, a_2, \ldots, a_2, \ldots, a_n, a_n, \ldots, a_n$$

dove a_1 compare m_1 volte (anche 0 volte, se non compare), a_2 compare m_2 volte, $\cdots$, a_n compare m_n volte, e dove ovviamente la somma $m_1 + m_2 + \cdots + m_n$ coincide con m (visto che la combinazione coinvolge esattamente m elementi fra gli n elementi dati). Possiamo costruire, a partire da tale combinazione con ripetizione, una opportuna parola sull'alfabeto $\{0,1\}$ nel modo seguente:

$$00\cdots0100\cdots01\cdots100\cdots0$$

dove gli zeri consecutivi all'inizio della parola sono in numero di m_1, dopo di essi vi è un 1 che funge da separatore, il secondo settore di zeri consecutivi contiene un numero m_2 di zeri, di seguito vi è un altro 1 che funge da separatore, e così procedendo fino all'ultimo separatore 1 seguito da altri zeri consecutivi in numero di m_n. Per esempio se $n = 4$, se gli elementi sono a_1, a_2, a_3, a_4 e se $m = 10$, a partire dalla seguente combinazione con ripetizione dei 4 elementi presi a 10 a 10:

$$a_1a_1a_2a_3a_3a_3a_4a_4a_4a_4$$

si può costruire la seguente parola sull'alfabeto $\{0,1\}$:

$$0010100010000$$

La parola costruita ha un numero di 1 (separatori) uguale ad $(n-1)$, ed un numero di 0 uguale alla somma $m_1 + m_2 + \cdots + m_n$, cioè uguale ad m. In

totale la lunghezza della parola è $(n-1)+m = n+m-1$. Se indichiamo con B l'insieme di tutte le parole sull'alfabeto $\{0,1\}$ di lunghezza $n+m-1$ in cui la lettera 1 compare esattamente $n-1$ volte, il procedimento precedente permette di costruire una funzione $f : C^r_{n,m} \to B$ che associa appunto ad ogni combinazione dell'insieme $C^r_{n,m}$ una parola dell'insieme B. Dal ragionamento fatto nella premessa precedente, sappiamo che B ha cardinalità

$$\binom{n+m-1}{n-1}$$

Ora dimostriamo che la funzione f è biunivoca.

Per dimostrare che f è iniettiva basta osservare che, date due combinazioni diverse in $C^r_{n,m}$, in esse vi sarà qualche elemento a_i che compare un numero diverso di volte nelle 2 combinazioni, quindi le 2 parole corrispondenti sull'alfabeto $\{0,1\}$ saranno diverse, perché nel settore corrispondente all'elemento a_i vi sarà un numero diverso di 0 fra 2 separatori.

Per dimostrare che f è surgettiva, data una parola qualunque in B, è facile (invertendo la costruzione precedente) trovare una combinazione di $C^r_{n,m}$ di cui la parola data sia la corrispondente mediante la funzione f: basta cominciare a leggere la parola da sinistra verso destra, isolare il primo settore di 0 consecutivi (seguiti da un 1), e prendere nella combinazione un numero di a_1 uguale al numero di tali 0 e così via.

Per la teoria delle funzioni biunivoche fra insiemi finiti, possiamo allora concludere che il numero delle combinazioni con ripetizione di n elementi $a_1, a_2, \ldots, a_n$ presi ad m ad m è il seguente:

$$|C^r_{n,m}| = |B| = \binom{n+m-1}{n-1}$$

4.3.4 Proprietà del coefficiente binomiale

Abbiamo visto che, fissati i numeri naturali n, m, (con $m \geq n$) il coefficiente binomiale rappresenta il numero delle combinazioni semplici di n elementi presi ad m ad m, ed anche il numero dei sottoinsiemi di cardinalità m con-

tenuti in un insieme di cardinalità n. Fissato il numero n, i valori possibili di m sono $m = 1, 2, \ldots, n$.

Ma tenendo conto del significato insiemistico, possiamo estendere per convenzione il valore del coefficiente binomiale anche al caso $m = 0$, definendo $\binom{n}{0} = 1$, coerentemente con l'osservazione che esiste 1 solo sottoinsieme di cardinalità 0 (quello vuoto) contenuto in un insieme di cardinalità n. Dunque i possibili coefficienti binomiali con n fissato sono i seguenti:

$$\binom{n}{0} = 1, \binom{n}{1}, \cdots, \binom{n}{n-1}, \binom{n}{n}$$

Notare che si ha

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

quindi i 2 valori estremi (il primo e l'ultimo) sono ambedue uguali a 1.

Notiamo anche sperimentalmente che i coefficienti binomiali

$$\binom{n}{0}, \binom{n}{1}, \cdots, \binom{n}{n-1}, \binom{n}{n}$$

sembrano coincidere a coppie. Per esempio per $n = 5$ facendo i calcoli si ottiene:

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

Daremo in seguito una giustificazione di ciò.

Costruiremo ora una formula alternativa per il calcolo di $\binom{n}{m}$ (ma all'inizio valida solo nel caso $m \neq 0$, $m \neq n$). Nella formula originale:

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

supponendo che sia $m \neq 0, m \neq n$, moltiplichiamo numeratore e denominatore per $(n-m)!$, ottenendo la nuova formula:

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

$$= \frac{n(n-1)\cdots(n-m+1)(n-m)\cdots\cdot 2\cdot 1}{m!(n-m)!} =$$

$$= \frac{n!}{m!(n-m)!}$$

Otteniamo dunque la formula alternativa:

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

(se $m \neq 0, m \neq n$).

Tale formula non ha senso nei casi $m = 0$, $m = n$, perché contiene un termine 0! al quale non abbiamo attribuito significato. Ma possiamo dare significato alla formula anche nei casi $m = 0$, $m = n$, definendo convenzionalmente $0! = 1$, per ritrovare i valori già noti:

$$\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{n!} = 1$$

$$\binom{n}{n} = \frac{n!}{n!(n-n)!} = \frac{n!}{n!} = 1$$

Dimostriamo ora il seguente risultato:

Teorema 99 *Se n è un numero naturale, comunque preso un intero m con $0 \leq m \leq n$ si ha:*

$$\binom{n}{m} = \binom{n}{n-m}$$

Dimostrazione Usiamo la formula alternativa per sviluppare il secondo membro ed arrivare al primo:

$$\binom{n}{n-m} = \frac{n!}{(n-m)!(n-(n-m)!} = \frac{n!}{(n-m)!m!} = \frac{n!}{m!(n-m)!} = \binom{n}{m}$$

□

Dal Teorema precedente si ha che, fissato il numero naturale n e facendo variare $m = 0, 1, \ldots, n$, i coefficienti binomiali:

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \cdots, \binom{n}{n-1}, \binom{n}{n}$$

sono uguali a coppie simmetriche (equidistanti rispetto al centro della successione):

$$\binom{n}{0} = \binom{n}{n}, \quad \binom{n}{1} = \binom{n}{n-1}, \cdots = \text{ etc} \cdots$$

(il primo coincide con l'ultimo, il secondo con il penultimo etc.)

Esempio 100 *Se $n = 5$ i coefficienti binomiali $\binom{n}{m}$ con $m = 0, 1, 2, 3, 4, 5$,sono uguali a coppie:*

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

Possiamo disporre i coefficienti binomiali in una struttura triangolare (detta triangolo di Tartaglia-Pascal) in cui in ogni riga si sistemano i coefficienti che hanno n fissato ed m variabile da 0 ad n. Per esempio le prime 4 righe del triangolo sono:

$$\binom{1}{0} = 1, \binom{1}{1} = 1$$

$$\binom{2}{0} = 1, \binom{2}{1} = 2, \binom{2}{2} = 1$$

$$\binom{3}{0} = 1, \binom{3}{1} = 3, \binom{3}{2} = 3, \binom{3}{3} = 1$$

$$\binom{4}{0} = 1, \binom{4}{1} = 4, \binom{4}{2} = 6, \binom{4}{3} = 4, \binom{4}{4} = 1$$

Notiamo che in ogni riga ogni termine (tranne quelli estremi) sembra potersi ottenere come somma dei 2 termini che lo sovrastano nella riga superiore: per esempio

$$\binom{3}{2} = \binom{2}{1} + \binom{2}{2}$$

$$\binom{4}{2} = \binom{3}{1} + \binom{3}{2}$$

Ciò non è casuale ma dipende dalla seguente formula :

Teorema 101 *Per ogni* $n \in \mathbb{N}$*, per ogni* $0 \leq m \leq n$

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

Dimostrazione Sviluppiamo il secondo membro, usando la formula alternativa per il calcolo del coefficiente binomiale:

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

$$= \frac{(n-1)!}{(m-1)!(n-1-(m-1))!} + \frac{(n-1)!}{m!(n-m-1)!} =$$

$$= \frac{(n-1)!}{(m-1)!(n-m)!} + \frac{(n-1)!}{m!(n-m-1)!}$$

Per calcolare il minimo comune denominatore delle 2 frazioni, è utile osservare che $(m-1)!m = m!$ e $(n-m-1)!(n-m) = (n-m)!$, dunque il comune denominatore è $m!(n-m)!$ e sviluppando i calcoli si ottiene:

$$\frac{m(n-1)! + (n-m)(n-1)!}{m!(n-m)!} =$$

$$= \frac{(m+n-m)(n-1)!}{m!(n-m)!} =$$

$$= \frac{n(n-1)!}{m!(n-m)!} =$$

$$= \frac{n!}{m!(n-m)!} = \binom{n}{m}$$

□

La formula dimostrata nel Teorema precedente permette di ricavare i termini di un riga del triangolo di Tartaglia-Pascal (tranne i 2 estremi che sono sempre uguali ad 1) conoscendo quelli della riga superiore e sommandoli a 2 a 2. Per esempio dalla conoscenza della riga numero 4:

$$\binom{4}{0} = 1, \binom{4}{1} = 4, \binom{4}{2} = 6, \binom{4}{3} = 4, \binom{4}{4} = 1$$

si possono ricavare subito i termini della riga numero 5:

$$\binom{5}{0} = 1, \binom{4}{1} = 1 + 4 = 5, \binom{5}{2} = 4 + 6 = 10$$

$$\binom{5}{3} = 6 + 4 = 10, \binom{5}{4} = 4 + 1 = 5, \binom{5}{5} = 1$$

e poi quella della riga 6 e così via.

4.4 Partizioni e numeri di Stirling

Dato un insieme non vuoto A, si chiama partizione di A un qualunque insieme di sottoinsiemi di A che soddisfano le seguenti proprietà:

1. sono sottoinsiemi non vuoti;
2. due qualunque di questi sottoinsiemi sono disgiunti (cioè hanno intersezione vuota, ossia non hanno elementi in comune);
3. la loro unione coincide con l'insieme A.

Esempio 102 *Se* $A = \{1, 2, 3, 4, 5, 6, 7\}$*, esempi di partizioni di* A *sono:*

$$\{\{1\}, \{2, 3, 4\}, \{5\}, \{6, 7\}\}$$

$$\{\{1, 2, 3, 7\}, \{6\}, \{4, 5\}\}$$

$$\{\{1, 3, 5, 7\}, \{2, 4, 6\}\}$$

(la prima è una partizione di A *in* 4 *sottoinsiemi, la seconda in* 3 *sottoinsiemi, la terza in* 2 *sottoinsiemi)*

Esempio 103 *Se* A *è l'insieme dei numeri naturali, esempi di partizioni di* A *sono:*

$$\{\{\textit{numeri naturali pari}\}, \{\textit{numeri naturali dispari}\}\}$$

$$\{\{1, 2\}, \{3, 4\}, \{5, 6\}, \ldots\}$$

(la prima è una partizione di A *in* 2 *sottoinsiemi, la seconda in un numero infinito di sottoinsiemi)*

Sia ora A un insieme finito di cardinalità n, e consideriamo le partizioni di A in m sottoinsiemi (dove m è un naturale fissato): ovviamente m può avere valore minimo $m = 1$ e valore massimo $m = n$. Il numero di tutte le possibili partizioni di A in m sottoinsiemi è chiamato *numero di Stirling* ed è indicato con $S(n, m)$ (sempre con $1 \leq m \leq n$).

Calcoliamo alcuni valori di $S(n, m)$. Per i valori estremi $m = 1$ ed $m = n$ si ha $S(n, 1) = 1$ (vi è una sola partizione di A in 1 sottoinsieme, in cui questo sottoinsieme è A stesso) e si ha $S(n, n) = 1$ (vi è una sola partizione di A in n sottoinsiemi, in cui ognuno di questi sottoinsiemi contiene un singolo elemento di A). Si ha $S(3, 2) = 3$: infatti se per esempio $A = \{a, b, c\}$ ha cardinalità $n = 3$, le partizioni possibili di A in 2 sottoinsiemi sono le 3 seguenti:

$$\{\{a\}, \{b, c\}\}, \{\{b\}, \{a, c\}\}, \{\{c\}, \{a, b\}\}$$

Si ha invece $S(4, 2) = 7$ perché se per esempio $A = \{a, b, c, d\}$ ha cardinalità $n = 4$, le partizioni possibili di A in 2 sottoinsiemi sono le 7 seguenti:

$$\{\{a\}, \{b, c, d\}\}, \{\{b\}, \{a, c, d\}\}, \{\{c\}, \{a, b, d\}\}, \{\{d\}, \{a, b, c\}$$

$$\{\{a, b\}, \{c, d\}\}, \{\{a, c\}, \{b, d\}\}, \{\{a, d\}, \{b, c\}\}$$

Possiamo sistemare i numeri di Stirling $S(n, m)$ nel triangolo di Stirling, in cui nella generica riga numero n vi sono i valori con n fissato ed m che varia da 1 ad n. Tenendo conto che i valori estremi di ogni riga sono $= 1$, si ha:

$$S(1, 1) = 1$$

$$S(2, 1) = 1 S(2, 2) = 1$$

$$S(3, 1) = 1 S(3, 2) = 3 S(3, 3) = 1$$

$$S(4, 1) = 1 S(4, 2) = 7 S(4, 3) = ? S(4, 4) = 1$$

$$S(5, 1) = 1 S(5, 2) = ? S(5, 3) = ? S(5, 4) = ? S(5, 5) = 1$$

e così via (come si vede alcuni valori dei numeri di Stirling sono ancora da determinare).

Vi è una relazione molto stretta fra i numeri di una riga e quelli della riga precedente, che può servire per calcolare facilmente i numeri di Stirling. Tale relazione è espressa dalla seguente formula:

Teorema 104

$$S(n,m) = S(n-1,m-1) + mS(n-1,m)$$

Dimostrazione Ricordiamo che $S(n,m)$ é il numero delle partizioni di un insieme di cardinalità n in m sottoinsiemi. Sia quindi $A = \{a_1, a_2, \ldots, a_{n-1}, a_n\}$ un insieme di cardinalità n. Poniamo poi $B = A - \{a_n\}$: notiamo che B ha cardinalità $n-1$. Le partizioni di A in m sottoinsiemi possono essere suddivise in 2 categorie:

1. le partizioni in cui l'elemento a_n è da solo in uno dei sottoinsiemi della partizione;
2. le partizioni in cui l'elemento a_n è insieme con altri elementi in uno dei sottoinsiemi della partizione.

Le partizioni della categoria 1) si ottengono fissando una partizione di B in $m-1$ sottoinsiemi (tale scelta si può effettuare in $S(n-1,m-1)$ modi diversi) e poi aggiungendo il sottoinsieme $\{a_n\}$: quindi le partizioni della categoria 1) sono in numero di $S(n-1,m-1)$. Le partizioni della categoria 2) si ottengono fissando una partizione di B in m sottoinsiemi (tale scelta si può effettuare in $S(n-1,m)$ modi diversi) e poi inserendo l'elemento a_n in uno degli m sottoinsiemi della partizione (questa scelta si può effettuare in m modi diversi): quindi, per il principio delle scelte multiple, le partizioni della categoria 2) sono in numero uguale al prodotto $mS(n-1,m)$. Il numero totale $S(n+1,m)$ delle partizioni dell'insieme A di cardinalità $n+1$ in m sottoinsiemi si ottiene sommando il numero delle partizioni delle 2 categorie, e si ottiene la formula voluta. □

La formula permette di calcolare tutti i numeri di Stirling di una riga, conoscendo quelli della riga precedente. Per esempio: $S(4,3) = S(3,2) + 3S(3,3) = 6$ (tale valore completa la riga numero 4); $S(5,2) = S(4,1) + 2S(4,2) = 15$, $S(5,3) = S(4,2)+3S(4,3) = 25$, $S(5,4) = S(4,3)+4S(4,4) = 10$ (completamento della riga 5) e così via per le righe successive.

4.5 Principio dei cassetti

Si basa sul seguente risultato di insiemistica: se A, B sono insiemi finiti, con $A = n$, $B = m$, e se $n > m$, comunque data una funzione $f : A \to B$, esistono sempre almeno 2 elementi diversi in A che hanno in B lo stesso corrispondente mediante f (tale risultato è ovvio perché sappiamo che, se $n > m$, la funzione f certamente non è iniettiva). Se pensiamo ad A come un insieme di n oggetti, a B come un insieme di m cassetti, e alla funzione f come un modo di inserire ogni oggetto in un cassetto, il principio afferma semplicemente che se il numero di oggetti è maggiore di quello dei cassetti, certamente esistono almeno 2 oggetti diversi che saranno inseriti nello stesso cassetto.

Vediamo un paio di applicazioni del principio dei cassetti:

Esempio 105 Il problema delle strette di mano. Supponiamo che A sia un insieme di n persone che si riuniscono, e che ognuna stringa la mano ad alcune altre (al limite anche a nessuna o a tutte le altre). Si può allora concludere con certezza che esistono sempre almeno 2 persone diverse che hanno stretto la mano allo stesso numero di persone. Infatti se B è l'insieme dei numeri interi da 0 ad $(n-1)$, possiamo definire una funzione $f : A \to B$, associando ad ogni persona il numero di strette di mano. Ovviamente però non può avvenire contemporaneamente che i valori 0 e $(n-1)$ siano corrispondenti di elementi di A (se esiste una persona che ha stretto le mani a tutte le altre, non ne esiste una che non ha stretto le mani a nessuno). Quindi possiamo restringere il codominio B, sostituendolo con un insieme C ottenuto togliendo da B quel numero (0 oppure $(n-1)$) che non è corrispondente di nessun elemento di A. Otteniamo così una funzione $f : A \to C$, dove $A = n$, $C = n - 1 < n$: applicando il principio dei cassetti si ha la tesi.

Esempio 106 Il problema del bersaglio Si supponga di colpire con 101 colpi (tutti a segno) un bersaglio quadrato con il lato di lunghezza 70 cm. Allora certamente esistono almeno 2 colpi sul bersaglio che distano meno di 10 cm. Infatti basta suddividere il bersaglio in 100 quadrati, ognuno con il lato di lunghezza 7 cm., considerare l'insieme A dei 101 colpi e l'insieme B dei 100 quadrati, e definire poi la funzione $f : A \to B$ che associa ad ogni colpo di A il quadrato in cui esso cade. Per il principio dei cassetti (essendo

la cardinalità 101 di A maggiore della cardinalità 100 di B) esistono almeno 2 colpi che cadono nello stesso quadrato, e geometricamente la loro distanza non è superiore alla lunghezza della diagonale che è uguale a $7\sqrt{2}$ cioè circa $9,9$ cm.

4.6 Principio della somma

Siano A, B insiemi finiti con $A = n$, $B = m$.

Se A, B non hanno elementi comuni, cioè se $A \cap B = \emptyset$, è ovvio che la cardinalità dell'unione $A \cup B$ coincide con la somma delle singole cardinalità dei 2 insiemi, perché l'elenco degli elementi distinti di $A \cup B$ si ottiene semplicemente elencando consecutivamente gli elementi di A e di B:

$$|A \cup B| = n + m = |A| + |B|$$

Questa formula esprime il cosiddetto *principio della somma* per 2 insiemi).

E' ovvio che tale principio si può generalizzare ad un numero qualunque di insiemi: se $A_1, A_2, \ldots, A_n$ sono n insiemi finiti, e se a 2 a 2 hanno intersezione vuota, si ha allora:

$$A_1 \cup A_2 \cup \cdots A_n = |A_1| + |A_2| + \cdots + |A_n|$$

la precedente formula esprime il principio della somma per n insiemi.

4.7 Principio di inclusione-esclusione

Siano A, B insiemi finiti con $|A| = n$, $|B| = m$.

Se A, B hanno qualche elemento in comune, cioè se $A \cap B \neq \emptyset$, il principio della somma non è più valido, perché la somma delle singole cardinalità di A e B non coincide con la cardinalità dell'unione $A \cup B$, in quanto nella somma delle cardinalità gli elementi comuni sarebbero erroneamente contati 2 volte.

Si deve quindi modificare la formula nel modo seguente:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Questa formula è il cosiddetto *principio di inclusione-esclusione per 2 insiemi.*

E' ovvio che il principio della somma diventa un caso particolare del principio di inclusione-esclusione nel caso che sia $A \cap B = \emptyset$ (perché in tale caso la cardinalità di $A \cap B$ è 0).

Tale principio di inclusione-esclusione si può estendere facilmente a più di 2 insiemi. Se per esempio sono dati 3 insiemi finiti A, B, C, per calcolare la cardinalità della loro unione, usando le proprietà insiemistiche dell'unione e dell'intersezione (in particolare la proprietà distributiva) e usando più volte il principio di inclusione-esclusione valido per 2 insiemi, si ha:

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

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

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

(notando che $(A \cap C) \cap (B \cap C) = A \cap B \cap C$)

$$= |A| + |B| + |C| - [|A \cap B + |A \cap C| + |B \cap C|] + |A \cap B \cap C|$$

e si ottiene quindi la formula del *principio di inclusione-esclusione nel caso di 3 insiemi finiti*:

$$|A \cup B \cup C| = |A| + |B| + |C| - [|A \cap B| + |A \cap C| + |B \cap C|] + |A \cap B \cap C|$$

Esiste una formula generale per il caso di n insiemi (che si dimostra con il principio di induzione, ma della quale omettiamo la dimostrazione): se sono dati n insiemi finiti $A_1, A_2, \ldots, A_n$, la cardinalità della loro unione si calcola con la formula

$$|A_1 \cup A_2 \cup \cdots A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \alpha_4 + \cdots \pm \alpha_n$$

dove α_1 è la somma delle cardinalità dei singoli insiemi; α_2 è la somma delle cardinalità di tutte le possibili intersezioni a 2 a 2 degli insiemi; α_3 è la somma delle cardinalità di tutte le possibili intersezioni a 3 a 3 degli insiemi; etc.; α_n è la cardinalità dell'intersezione di tutti gli insiemi: l'ultimo addendo é preceduto da un segno $+$ se n è dispari, da un segno $-$ se n è pari (*principio di inclusione-esclusione per n insiemi*).

4.8 Uso del principio di inclusione-esclusione

Esistono un uso positivo e un uso negativo del principio di inclusione-esclusione.

Uso positivo del principio di inclusione-esclusione:
Sia dato un insieme finito A ed n diverse proprietà $P_1, P_2, \ldots, P_n$ che possono (o non possono) essere soddisfatte dagli elementi di A. Se vogliamo contare il numero degli elementi di A che soddisfano *almeno una* delle n proprietà, ciò equivale a costruire per ogni $i = 1, 2, \ldots, n$ l'insieme A_i degli elementi di A che soddisfano la proprietà P_i, e calcolare la cardinalità dell'unione $A_1 \cup A_2 \cup \cdots A_n$, servendosi della formula del principio di inclusione-esclusione.

Esempio 107 *Sia A l'insieme dei numeri naturali di 5 cifre con cifre scelte fra $1, 2, 3, 4, 5, 6$. Risolviamo il problema di contare il numero degli elementi di A che soddisfano almeno una delle seguenti 3 proprietà:*

P_1. *La prima cifra è 2;*

P_2. *Le prime 3 cifre sono uguali fra loro;*

P_3. *L'ultima cifra è 3.*

Dobbiamo allora costruire gli insiemi degli elementi di A che soddisfano singolarmente le 3 proprietà:

$$A_1 = \{x \in A \mid \text{ la prima cifra è } 2\}$$

$$A_2 = \{x \in A \mid \text{ le prime } 3 \text{ cifre sono uguali fra loro }\}$$

$$A_3 = \{x \in A \mid \text{ l'ultima cifra è } 3 \}$$

e calcolare, con la formula del principio di inclusione-esclusione:

$$A_1 \cup A_2 \cup A_3 = (|A_1| + |A_2| + |A_3|) - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + |A_1 \cap A_2 \cap A_3|$$

Servendoci del principio delle scelte multiple si ottengono i valori:

$$|A_1| = 6^4, \qquad |A_2| = 6^3, \qquad |A_3| = 6^4$$

$$|A_1 \cap A_2| = 6^2, \qquad |A_1 \cap A_3| = 6^3, \qquad |A_2 \cap A_3| = 6^2 <$$
$$|A_1 \cap A_2 \cap A_3| = 6$$

Quindi la risposta al problema è:

$$|A_1 \cup A_2 \cup A_3| = 6^4 + 6^3 + 6^4 - (6^2 + 6^3 + 6^2) + 6 =$$

$$1296 + 216 + 1296 - (36 + 216 + 36) + 6 = 2526$$

Viceversa, esiste anche un uso negativo del principio di inclusione-esclusione.

Uso negativo del principio di inclusione-esclusione:
Sia dato un insieme finito A ed n diverse proprietà $P_1, P_2, \ldots, P_n$ che possono (o non possono) essere soddisfatte dagli elementi di A. Se vogliamo contare il numero degli elementi di A che non soddisfano *nessuna* delle n proprietà, ciò equivale a costruire per ogni $i = 1, 2, \ldots, n$ l'insieme A_i degli elementi di A che soddisfano la proprietà P_i, e calcolare la cardinalità del complementare dell'unione $A_1 \cup A_2 \cup \cdots \cup A_n$, cioè calcolare la differenza

$$|A| - |A_1 \cup A_2 \cup \cdots \cup A_n|$$

usando la formula del principio di inclusione-esclusione.

Esempio 108 *Se le proprietà sono quelle dell'esempio precedente, il numero degli elementi di A che non soddisfano nessuna delle proprietà P_1, P_2, P_3 sarà:*

$$|A| - |A_1 \cup A_2 \cup A_3| = 6^5 - 2526 = 5250$$

Esempio 109 [Il problema della segretaria distratta] Supponiamo di avere n lettere (per n destinatari diversi) e le n buste corrispondenti (con il nome del destinatario già stampato), e di effettuare un imbustamento mettendo ogni lettera in una busta (lettere diverse in buste diverse).
Quesito: in quanti modi diversi si può effettuare un imbustamento totalmente errato, cioè in cui nessuna lettera vada nella busta corrispondente? Possiamo numerare la lettere e le buste da 1 ad n (lettera e busta corrispondente con lo stesso numero) e rappresentare ogni imbustamento come una funzione biunivoca

$$f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

L'insieme A di tutti gli imbustamenti coincide con l'insieme di tutte le suddette funzioni biunivoche, di cardinalità $n!$. Ogni imbustamento totalmente errato è una funzione $f \in A$ che non soddisfa nessuna delle seguenti n proprietà:

$$f(1) = 1; f(2) = 2; \ldots; f(n) = n$$

Possiamo allora usare la forma negativa del principio di inclusione-esclusione. Costruiamo quindi gli n insiemi:

$$A_1 = \{f \in A \mid f(1) = 1\}$$

$$A_2 = \{f \in A \mid f(2) = 2\};$$

$$\ldots;$$

$$A_n = \{f \in A \mid f(n) = n\}$$

La risposta al quesito sarà:

$$|A| - |A_1 \cup A_2 \cup \cdots \cup A_n|$$

Per il principio di inclusione-esclusione si ha:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \alpha_4 + \cdots \pm \alpha_n$$

dove α_1 è la somma delle cardinalità dei singoli insiemi; α_2 è la somma delle cardinalità di tutte le possibili intersezioni a 2 a 2 degli insiemi; α_3 è la somma delle cardinalità di tutte le possibili intersezioni a 3 a 3 degli insiemi; $\ldots$; α_n è la cardinalità dell'intersezione di tutti gli insiemi, preceduta da un segno $+$ se n è dispari, da un segno $-$ se n è pari. Calcoliamo la cardinalità di A_1: esso contiene le funzioni biunivoche $f: \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ tali che $f(1) = 1$. Con il principio delle scelte multiple si ottiene che $|A_1| = (n-1)!$. Con ragionamenti analoghi si ottiene:

$$|A_2| = |A_3| = \ldots = |A_n| = (n-1)!$$

dunque α_1 è la somma di n addendi tutti uguali ad $(n-1)!$, ossia

$$\alpha_1 = (n-1)! \cdot n = n!$$

Ragionando in modo simile si ottiene che $|A_1 \cap A_2| = (n-2)!$, e ciò vale per la cardinalità dell'intersezione di 2 qualunque degli insiemi. Il numero

di possibili intersezioni a 2 a 2 corrispondono alle combinazioni semplici di n insiemi presi a 2 a 2, quindi sono in numero di $\binom{n}{2}$. Dunque α_2 è la somma di $\binom{n}{2}$ addendi tutti uguali ad $(n-2)!$.

Si ha allora:

$$\alpha_2 = (n-2)!\binom{n}{2} = (n-2)!\frac{n!}{2!(n-2)!} = \frac{n!}{2!}$$

Con ragionamenti analoghi si ha:

$$\alpha_3 = \frac{n!}{3!} \qquad \alpha_4 = \frac{n!}{4!} \qquad \dots \qquad \alpha_n = \frac{n!}{n!} = 1$$

Dunque il numero di imbustamenti totalmente errati é:

$$|A| - |X_1 \cup X_2 \cup \cdots \cup X_n| = n! - (n! - \frac{n!}{2!} + \frac{n!}{3!} - \frac{n!}{4!} + \cdots \pm 1) = \frac{n!}{2!} - \frac{n!}{3!} + \frac{n!}{4!} - \cdots \pm 1$$

(dove l'ultimo addendo 1 ha il segno + se n é pari, il segno − se n è dispari).

Esempio 110 *Se il numero delle lettere (e delle buste) è $n = 5$, il numero di imbustamenti totalmente errati è:*

$$\frac{5!}{2!} - \frac{5!}{3!} + \frac{5!}{4!} - \frac{5!}{5!} = 60 - 20 + 5 - 1 = 44$$

(su un totale di $5! = 120$ imbustamenti in totale).

Esercizi sul principio di Inclusione-esclusione

Esercizio 1: In un'urna vi sono palline colorate di 6 colori diversi, fra i quali il giallo e il rosso, in modo che vi siano almeno 8 palline per ogni colore (le palline dello stesso colore sono identiche e non distinguibili una dall'altra). Si pescano a caso 8 palline e le si inserisce in un sacchetto

- quanti sono i possibili diversi contenuti del sacchetto?;
- Fra i diversi contenuti del sacchetto, calcolare quanti sono quelli che non soddisfano né l'una né l'altra delle seguenti condizioni: tutte le palline hanno un colore diverso dal giallo; esattamente 2 palline hanno colore rosso.

Soluzione: I diversi contenuti del sacchetto sono le combinazioni con ripetizione di 6 colori presi a 8 a 8, in numero di $\binom{n+m-1}{n-1} = \binom{13}{5}$. Se X è l'insieme di tali combinazioni, se Y è l'insieme di quelle che non contengono il giallo, e se Z è l'insieme di quelle che contengono esattamente 2 volte il rosso, applicando il principio di inclusione-esclusione (forma negativa) la risposta al secondo quesito è:

$$|X| - |Y \cup Z| = |X| - [|Y| + |Z| - |Y \cap Z|]$$

dove $X = \binom{13}{5}$, $Y = \binom{12}{4}$, $Z = \binom{10}{4}$, $Y \cap Z = \binom{9}{3}$, tenendo conto che Y contiene le combinazioni con ripetizione di 5 colori a 8 a 8; gli elementi di Z sono tante quante le combinazioni con ripetizione di 5 colori a 6 a 6; gli elementi di $Y \cap Z$ sono tante quante le combinazioni con ripetizione di 4 colori a 6 a 6.

Esercizio 2: Si considerino l'insieme $A = \{b, c, d, e, i\}$ e l'insieme $B = \{3, 4, 5, 6, 7, 8, 9, 10\}$. Calcolare il numero delle funzioni $f : A \to B$ tali che almeno una delle consonanti di A abbia immagine dispari in B.

Soluzione: Si può applicare il principio di inclusione-esclusione in forma positiva: se X è l'insieme di tutte le funzioni $f : A \to B$ e se Y, Z, T sono i sottoinsiemi di X delle funzioni f tali che $f(b)$ (rispettivamente $f(c), f(d)$) sono dispari, la risposta al quesito è:

$$|Y \cup Z \cup T| = |Y| + |Z| + |T| - [|Y \cap Z| + |Y \cap T| + |Z \cap T|] + |Y \cap Z \cap T| =$$

$$= 4 \cdot 8^4 + 4 \cdot 8^4 + 4 \cdot 8^4 - [4^2 \cdot 8^3 + 4^2 \cdot 8^3 + 4^2 \cdot 8^3] + 4^3 \cdot 8^2$$

(dove i risultati numerici si ottengono con un opportuno uso del principio delle scelte multiple).

Esercizio 3: Calcolare il numero delle matrici 3×4 ad elementi in $\{0, 1, 2\}$ tali che nella terza colonna non vi sono due caselle adiacenti contenenti entrambe il valore 2.

Soluzione: Si può applicare il principio di inclusione-esclusione in forma negativa: se A è l'insieme delle matrici 3×4 ad elementi $0, 1, 2$, e se X, Y

sono rispettivamente i sottoinsiemi di A formati dalle matrici in cui la 1^a e la 2^a casella, la 2^a e la 3^a casella della terza colonna contengono entrambe il valore 2, la risposta al quesito è: $|A| - |X \cup Y|$, dove $|A| = 3^{12}$ e dove

$$|X \cup Y| = |X| + |Y| - |X \cap Y| = 3^{10} + 3^{10} - 3^9$$

Esercizio 4: Calcolare il numero delle parole di lunghezza 6 sull'alfabeto $A = \{a, e, i, o, u, m, n, p, q, r\}$ tali che almeno 4 lettere della parola in posizioni consecutive siano vocali.

Soluzione: Si può applicare il principio di inclusione-esclusione, costruendo gli insiemi X, Y, Z dove X contiene le parole in cui le prime 4 lettere sono vocali, Y contiene le parole in cui le lettere dalla 2^a alla 5^a sono vocali, Z contiene le parole in cui le ultime 4 lettere sono vocali, e calcolare (utilizzando anche il principio delle scelte multiple):

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - [|X \cap Y| + |X \cap Z| + |Y \cap Z|] + |X \cap Y \cap Z| =$$

$$= 5^4 \cdot 10^2 + 5^4 \cdot 10^2 + 5^4 \cdot 10^2 - [5^5 \cdot 10 + 5^6 + 5^5 \cdot 10] + 5^6$$

Esercizio 5: Un espositore è formato da 5 file di 10 contenitori ciascuna: in ogni contenitore può essere messo un prodotto, scelto fra 7 prodotti diversi, oppure può essere lasciato vuoto. Calcolare il numero delle diverse configurazioni dell'espositore in cui non vi sono 3 file consecutive tutte vuote.

Soluzione: Si può usare il principio di esclusione-esclusione in forma negativa. Considerando l'insieme A di tutte le possibili configurazioni dell'espositore (di cardinalità 8^{50} perché per ognuno dei 50 contenitori vi sono 8 possibilità) e costruendo gli insiemi X, Y, Z dove X contiene le configurazioni in cui le prime 3 file sono vuote, Y contiene le configurazioni in cui le file dalla 2^a alla 4^a sono vuote, Z contiene le configurazioni in cui le ultime 3 file sono vuote, la risposta è: $|A| - |X \cup Y \cup Z|$, dove $A = 8^{50}$ e dove:

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - [|X \cap Y| + |X \cap Z| + |Y \cap Z|] + |X \cap Y \cap Z| =$$

$$= 8^{20} + 8^{20} + 8^{20} - [8^{10} + 1 + 8^{10}] + 1.$$

Esercizio 6: Si consideri l'insieme $A = \{1, 2, 3, 4, 5, 6, 7\}$. Contare il numero di funzioni $f : A \to A$ tali che almeno uno dei numeri pari di A abbia immagine dispari.

Soluzione: Si può usare il principio di inclusione-esclusione: se X, Y, Z sono gli insiemi delle funzioni $f : A \to A$ tali che rispettivamente $f(2)$, $f(4)$, $f(6)$ siano dispari, la risposta al quesito é:

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - (|X \cap Y| + |X \cap Z| + |Y \cap Z|) + |X \cap Y \cap Z| =$$
$$= 4 \cdot 7^6 + 4 \cdot 7^6 + 4 \cdot 7^6 - 4^2 \cdot 7^5 + 4^2 \cdot 7^5 + 4^2 \cdot 7^5 + 4^3 \cdot 7^4$$

(per calcolare ognuna delle cardinalità a secondo membro si può usare il principio delle scelte multiple

Esercizio 5: Considerato l'insieme $A = \{x \mid x \text{ è intero positivo} < 16\}$ ed il prodotto cartesiano $A \times A$, calcolare il numero degli elementi $(x, y) \in A \times A$ che non soddisfano nessuna delle seguenti condizioni:

1. Il prodotto xy è dispari;
2. $x < 8$;
3. $y > 4$.

Soluzione: Si può usare il principio di inclusione in forma negativa. Se X, Y, Z sono rispettivamente i sottoinsiemi di $A \times A$ contenenti gli elementi che soddisfano $1, 2, 3$ la risposta al quesito è:

$$|A \times A| - |X \cup Y \cup Z|$$

dove $A \times A = 15^2$ e dove:

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| + |X \cap Z| + |Y \cap Z| + |X \cap Y \cap Z| =$$
$$= 8^2 + 7 \cdot 15 + 15 \cdot 11 - 4 \cdot 8 + 8 \cdot 6 + 7 \cdot 11 + 4 \cdot 6$$

Dati 2 numeri naturali a, b diremo che b *è divisore di* a (o che a *è multiplo di* b o ancora che b *divide* a) se esiste un numero naturale c tale che $a = b \cdot c$: in tale caso scriveremo il simbolo $b \mid a$. Per esempio $2 \mid 8$ perché esiste il numero naturale $c = 4$ tale che $8 = 2 \cdot 4$.

Capitolo 5

Divisibilità

Dati due numeri naturali a, b diremo che b *è divisore di* a (o che a *è multiplo di* b o ancora che b *divide* a) se esiste un numero naturale c tale che $a = b \cdot c$: in tal caso scriveremo il simbolo $b \mid a$. Per esempio $2 \mid 8$ perché esiste il numero naturale $c = 4$ tale che $8 = 2 \cdot 4$.

5.1 Algoritmo della divisione fra i numeri naturali

E' ben noto che, dati 2 numeri interi positivi, si possa dividere il primo (dividendo) per il secondo (divisore) trovando un quoziente e un resto. Dimostreremo formalmente tale proprietà:

Teorema 111 (Algoritmo della divisione) *Comunque dati due numeri naturali a, b (detti rispettivamente dividendo e divisore), esistono due numeri interi $q, r \geq 0$ (detti rispettivamente quoziente e resto) tali che $a = b \cdot q + r$ con $r < b$. Inoltre il quoziente q e il resto r sono unici.*

Dimostrazione

Dimostrazione dell'esistenza di q, r: si consideri l'insieme di tutte le differenze della forma $a - bx$, con x che varia fra gli interi ≥ 0, limitandosi a quelle differenze che danno un risultato ≥ 0:

$$S = \{z \mid z = a - bx, \text{ con } x \text{ intero} \geq 0, \text{ e con } z \geq 0\}$$

L'insieme S è non vuoto: infatti almeno la differenza $a - b \cdot 0 = a$ è elemento di S, perché $a > 0$. Possiamo osservare che S contiene certamente un elemento minimo: infatti se S non contiene lo 0 allora S è sottoinsieme di $\mathbb{N}$ ed S contiene un elemento minimo per l'Assioma del minimo; se invece S contiene lo 0, è ovvio che 0 è il suo minimo.
Sia dunque s il minimo in S. Per costruzione di S si ha che s è un intero ≥ 0, ed inoltre $s = a - bx$ con x intero ≥ 0. Da cui $a = bx + s$, e basta scegliere $r = s$ e $q = x$ per avere l'esistenza di q ed r.
Resta però da verificare che $r < b$: se per assurdo fosse $r \geq b$, si avrebbe $r - b \geq 0$, $r - b = (a - bq) - b = a - b(q + 1)$, con $q + 1 \neq 0$ (perché $q = x \geq 0$) dunque il numero $r - b$ sarebbe una delle differenze che appartengono ad S; ma si avrebbe anche $r - b < r$ (perché $b > 0$), contraddizione perché r è il minimo in S.
Dimostrazione dell'unicità di q, r: se $a = bq + r = bq_1 + r_1$ (con q, r, q_1, r_1 interi ≥ 0 e con $r < b$, $r_1 < b$) le tesi sono che $r = r_1$, $q = q_1$.
Tesi $r = r_1$: se per assurdo fosse $r \neq r_1$ e se per esempio fosse $r > r_1$ (se è al contrario $r < r_1$ si ragiona in modo simile) si avrebbe $r - r_1 > 0$, $r - r_1 = b(q_1 - q)$, dunque $q_1 - q > 0$, ossia $q_1 - q \geq 1$, $r - r_1 = b(q_1 - q) > b$; ma si ha anche $r \geq r - r_1 = b(q_1 - q) \geq b$, contraddizione perché $r < b$.
Tesi $q = q_1$: avendo già dimostrato la prima tesi, si ha $bq = a - r = a - r_1 = bq_1$, dunque $q = q_1$. □

Il prossimo Teorema fornisce un criterio per stabilire quando un numero naturale b è divisore di un numero naturale a.

Teorema 112 *Siano dati due numeri naturali a, b. Allora si ha:*

$b \mid a \iff$ *dividendo a per b (con l'algoritmo della divisione) si ottiene resto* 0

Dimostrazione Dimostriamo la doppia implicazione:

$\Rightarrow$: Per ipotesi esiste un numero naturale c tale che $a = bc$. Dividiamo a per b ottenendo due numeri interi $q, r \geq 0$ (quoziente e resto) tali che $a = bq + r$,

con $r < b$; ma si ha anche:

$$a = bq + r = bc + 0 \text{ con } 0 < b$$

e per l'unicità del resto nella divisione di a per b si ottiene $r = 0$ (tesi).

$\Leftarrow$: Per ipotesi se dividiamo a per b otteniamo resto 0, quindi $a = bq + r$ con $r = 0$, ossia $a = bq$, con q (quoziente) numero intero ≥ 0; ma si può notare che q è certamente positivo (perché a, b lo sono) quindi $a = bq$ con q numero naturale e si ottiene la tesi $b \mid a$. □

5.2 Massimo comune divisore

Definizione 113 *Dati due naturali a, b, si chiama* massimo comune divisore di a e b *e di indica con* $\mathrm{mcd}(a, b)$ *un numero naturale d tale che:*

1. *$d \mid a$, $d \mid b$ (quindi d è divisore comune di a, b);*
2. *d è multiplo di tutti i divisori comuni di a, b*

Ovviamente dalla proprietà *2.* segue che d è anche il più grande dei divisori comuni di a e b.

Esempio 114 *Se $a = 24$, $b = 18$, i divisori comuni di a, b sono $1, 2, 3, 6$ e $d = 6$ è multiplo di tutti i divisori comuni, quindi $6 = \mathrm{mcd}(24, 18)$.*

Dimostreremo ora l'esistenza del massimo comune divisore di due qualunque numeri naturali a, b. Premettiamo una utile nozione.

Definizione 115 *Dati due numeri naturali a, b definiamo* combinazione lineare di a, b a coefficienti interi relativi *un qualunque numero intero relativo della forma $ax + by$ dove i numeri x, y (detti appunto coefficienti) variano fra i numeri interi relativi.*

Per esempio se $a = 4$, $b = 6$, esempi di combinazioni lineari di 4 e 6 a coefficienti interi relativi sono i seguenti numeri: $4 \cdot 5 + 6 \cdot (-2) = 8$; $4 \cdot (-7) + 6 \cdot 2 = -16$, $4 \cdot (-3) + 6 \cdot 2 = 0$.

Teorema 116 [**Teorema di esistenza del massimo comune divisore**] *Comunque presi due numeri naturali a, b, esiste sempre il loro massimo comune divisore.*

Dimostrazione Costruiamo l'insieme S di tutte le possibili combinazioni lineari di a, b a coefficienti interi relativi che siano positive:

$$S = \{z \mid z = ax + by, \text{ con } x, y \in \mathbb{Z}; z > 0\}$$

L'insieme S é non vuoto perché contiene per esempio almeno l'elemento $a = a \cdot 1 + b \cdot 0$, e l'elemento $b = a \cdot 0 + b \cdot 1$. Per l'Assioma del minimo esiste in S un elemento minimo d: in particolare d è un intero > 0 e d è combinazione lineare di a, b della forma $d = ax + by$ per opportuni valori $x, y \in \mathbb{Z}$. Dimostriamo che d è il massimo comune divisore di a, b che cercavamo, verificando che d soddisfa le proprietà *1.* e *2.* della definizione di massimo comune divisore di a, b.

1. Dimostriamo che $d \mid a$ e che $d \mid b$. Per l'Algoritmo della divisione fra numeri naturali, possiamo dividere a per d ottenendo $a = dq + r$, con q, r interi ≥ 0, ed $r < d$. Per il Teorema precedente, per dimostrare che $d \mid a$, basta dimostrare che il resto r è $= 0$. Se per assurdo fosse $r > 0$ sarebbe $r = a - dq = a - (ax + by)q = a(1 - xq) + b(-yq)$ e si otterrebbe che anche r è combinazione lineare (positiva)di a, b, cioè $r \in S$, con $r < d$ ed d minimo in S, contraddizione. In modo molto simile si dimostra che $d \mid b$.

2. Dimostriamo che d è multiplo di qualunque divisore comune s di a, b: ma se s è divisore comune di a, b esisteranno due numeri naturali c, v tali che $a = sc$, $b = sv$, da cui si ricava $d = ax + by = scx + svy = s(cx + vy)$ ossia d è multiplo di s, come si voleva dimostrare.

Poiché d soddisfa le proprietà *1.* e *2.* della definizione di massimo comune divisore, si conclude che d è il massimo comune divisore di a, b e si ottiene la tesi. □

Osserviamo che nel corso della dimostrazione del Teorema di esistenza del $\mathrm{mcd}(a,b)$ si è anche dimostrato che il $\mathrm{mcd}(a,b)$ è combinazione lineare dei numeri a,b con coefficienti interi relativi, dunque esistono due opportuni numeri interi relativi x,y tali che $\mathrm{mcd}(a,b) = ax+by$. Per esempio se $a=14$, $b=10$, esaminando i divisori comuni di a,b è facile verificare che $\mathrm{mcd}(14,10)=2$: come coefficienti x,y si possono allora scegliere per esempio i valori $x=-2$, $y=3$ (infatti $ax+by = 14\ (-2)+10\cdot 3 = 2 = \mathrm{mcd}(14,10)$). Notiamo anche che i coefficienti x,y non sono unici (nell'esempio precedente vanno bene per esempio anche i valori $x=8, y=-11$, in quanto $ax+by = 14\cdot 8+10\cdot(-11) = 2 = \mathrm{mcd}(14,10)$).

Problema:

Dati i numeri naturali a,b, come calcolare degli interi relativi x,y tali che $\mathrm{mcd}(a,b) = ax+by$?

La soluzione al Problema enunciato è nell'Algoritmo Euclideo delle divisioni successive, che illustreremo in seguito. Premettiamo un risultato preliminare:

Teorema 117 *Siano a,b numeri naturali e sia $a=bq+r$ la divisione di a per b, con q,r interi ≥ 0, ed $r<b$. Allora:*

1. *se $r>0$ si ha $\mathrm{mcd}(a,b) = \mathrm{mcd}(b,r)$;*
2. *se $r=0$ si ha $\mathrm{mcd}(a,b) = b$*

Dimostrazione *1.* Supponiamo $r>0$ e poniamo $d=\mathrm{mcd}(a,b)$. La tesi è che $d=\mathrm{mcd}(b,r)$.
Dimostriamo dapprima che d è divisore comune di b,r. Essendo $d=\mathrm{mcd}(a,b)$, sappiamo già che $d \mid a$, $d \mid b$ (quindi esistono numeri naturali c,v tali che $a=dc$, $b=dv$); essendo già vero che $d \mid b$, si deve solo dimostrare che $d \mid r$: ma $r = a-bq = dc-dvq = d(c-vq)$ quindi $d \mid r$. Resta poi da dimostrare che d è multiplo di ogni divisore comune z di b,r: ma in questo caso esistono numeri naturali f,g tali che $b=zf$, $r=zg$, da cui si ricava $a=bq+r=zfq+zg=z(fq+g)$ ossia $z \mid a$, quindi z è divisore comune di a,b. Ma per ipotesi $d=\mathrm{mcd}(a,b)$ quindi d è multiplo di tutti i divisori

comuni di a, b, e si conclude in particolare che d è multiplo di z, come si voleva.
2. Supponiamo $r = 0$ e dimostriamo la tesi $mcd(a, b) = b$. Ovviamente b è divisore sia di a (perché $a = bq$) che di b (perché $(b = b \cdot 1)$, dunque è divisore comune di a, b. Resta da verificare che b è multiplo di ogni divisore comune z di a, b: ma ciò è ovvio, perché, essendo z divisore di b, si ha che b è multiplo di z. □

5.2.1 Algoritmo Euclideo delle divisioni successive

L'algoritmo consiste in una successione di divisioni effettuate secondo le regole seguenti:

- La prima divisione si ottiene dividendo a per b.
- Data una generica divisione dell'algoritmo, la divisione successiva si effettua solo se il resto della precedente è >0, e nella divisione successiva il dividendo coincide con il divisore della divisione precedente, mentre il divisore coincide con il resto della divisione precedente.
- L'algoritmo ha termine quando una divisione ha resto = 0.

Schematizzando:

divisione 1

$$a = bq_1 + r_1 \text{ con } q_1, r_1 \text{ interi } \geq 0, r_1 < b$$

divisione 2 (se $r_1 > 0$)

$$b = r_1q_2 + r_2 \text{ con } q_2, r_2 \text{ interi } \geq 0, r_2 < r_1$$

divisione 3 (se $r_2 > 0$)

$$r_1 = r_2q_3 + r_3 \text{ con } q_3, r_3 \text{ interi } \geq 0, r_3 < r_2$$

divisione 4 (se $r_3 > 0$)

$$r_2 = r_3q_4 + r_4 \text{ con } q_4, r_4 \text{ interi } \geq 0, r_4 < r_3$$

...

Osserviamo che l'algoritmo ha termine dopo un numero finito di divisioni: se infatti per assurdo così non fosse, si otterrebbe una successione infinita di divisioni tutte con resto > 0, ma, essendo i resti legati dalla relazione $r_1 > r_2 > r_3 > r_4 > \cdots$, l'insieme di tutti questi resti sarebbe un insieme S di numeri naturali senza minimo, in contraddizione con l'Assioma del buon ordinamento.

5.3 Numeri primi

Sia a un qualunque numero naturale. Dall'eguaglianza $a = a \cdot 1$ segue che $a, 1$ sono in ogni caso divisori di a (detti *divisori banali di* a).

Definiamo *numero primo* un numero naturale $a > 1$ i cui unici divisori sono i divisori banali $1, a$.

Osservazione 118 Osserviamo che, nella definizione data, il numero naturale 1 non è considerato primo. Il motivo di questa esclusione del numero 1 dai numeri primi sarà chiarito nella dimostrazione del Teorema di fattorizzazione unica.

Osservazione 119 Nell'agosto del 2008 è stato trovato il più grande numero primo attualmente conosciuto (esso ha quasi 13.000.000 cifre in base 10). Utili notizie possono essere trovate sul sito www.mersenne.org.

5.3.1 Fattorizzazione in primi

Dimostreremo che i numeri primi sono come i mattoni elementari con cui si possono costruire tutti i numeri naturali > 1, nel senso che ogni numero naturale > 1 è prodotto di numeri primi e tale rappresentazione è sotto certi aspetti unica. Ricordiamo che per convenzione il termine "prodotto" si intende eventualmente anche con un solo fattore (nel quale caso il risultato del

prodotto è l'unico fattore coinvolto). Premettiamo un risultato preliminare sui numeri primi:

Teorema 120 *Se p è un numero primo e se p é divisore del prodotto di due numeri naturali ab allora p è divisore di almeno uno dei fattori a, b.*

Dimostrazione Per assurdo supponiamo che p non sia divisore né di a né di b. Essendo per ipotesi $p \mid ab$ esiste un numero naturale t tale che $pt = ab$. Poniamo $d = \mathrm{mcd}(p, a)$. Essendo $d \mid p$, $d \mid a$ ed essendo p numero primo, si ha $d = 1$ oppure $d = p$. Ma non può essere $d = p$ (perché d è divisore di a mentre p non lo è) dunque è $d = 1$. Per una proprietà del $\mathrm{mcd}(p, a)$, esistono due interi relativi x, y tali che $d = 1 = px+ay$. Moltiplicando ambo i membri per b e tenendo conto che $pt = ab$ si ha: $b = pbx+aby = pbx+pty = p(bx+ty)$ e si ottiene $p \mid b$ (contraddizione). □

Osservazione 121 Il risultato ora dimostrato si può estendere facilmente al caso del prodotto di 3 o più fattori. Per esempio se il numero primo p è divisore di un prodotto abc di tre numeri naturali a, b, c allora, utilizzando la proprietà associativa del prodotto, si può osservare che p sarà divisore del prodotto $(ab)c$ dei due fattori ab, c dunque (utilizzando la proprietà precedente valida per due fattori) si otterrà $p \mid ab$ oppure $p \mid c$, e di nuovo applicando la proprietà precedente sarà $p \mid a$ oppure $p \mid b$ oppure $p \mid c$ quindi p sarà divisore di almeno uno dei tre fattori a, b, c. Con ragionamenti analoghi si ottiene che se un numero primo p è divisore del prodotto di n numeri naturali, allora p è divisore di almeno uno degli n fattori (qualunque sia il numero n di fattori).

Teorema 122 [**Teorema di fattorizzazione unica**] *Ogni numero naturale $a > 1$ è fattorizzabile come prodotto di numeri primi (al limite con 1 solo fattore) e tale fattorizzazione è unica (a meno dell'ordine dei fattori), nel senso che, se sono date due fattorizzazioni dello stesso a in prodotto di numeri primi:*

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

dove tutti i p_i e i q_j sono numeri primi. Allora:

- *$r = s$ (il numero dei fattori primi nelle due fattorizzazioni è uguale);*

- *riordinando opportunamente i fattori, si ha* $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_r$ *(cioè i fattori coincidono ordinatamente nelle due fattorizzazioni)*

Dimostrazione

Esistenza della fattorizzazione: Supponiamo per assurdo che esistano numeri naturali non fattorizzabili nel prodotto di numeri primi, e costruiamo l'insieme S di tali numeri:

$$S = \{x \mid x \in \mathbb{N}, x > 1, x \text{ non é fattorizzabile nel prodotto di numeri primi}\}$$

L'insieme non vuoto S, per l'Assioma del minimo, contiene un elemento minimo $s \in S$: sarà $s \in \mathbb{N}$, $s > 1$, s non fattorizzabile nel prodotto di numeri primi. In particolare s non è un numero primo (altrimenti s sarebbe fattorizzabile nel prodotto di numeri primi, con un solo fattore) quindi s ha un divisore non banale b, con $b \neq 1$, $b \neq s$. Esiste allora un naturale c tale che $s = bc$, e ovviamente anche $c \neq 1$, $c \neq s$. In totale si ha $1 < b < s$, $1 < c < s$, ed essendo s il minimo in S, si deduce che $b, c \notin S$, dunque b, c sono entrambi fattorizzabili nel prodotto di numeri primi, ma allora anche $a = bc$ sarebbe fattorizzabile nel prodotto di numeri primi, contraddizione.

Unicità della fattorizzazione: Sia a un numero naturale > 1 e siano date due fattorizzazioni di a in prodotto di numeri primi:

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

(dove tutti i p_i e i q_j sono numeri primi)

Le tesi sono allora le seguenti:

- $r = s$ (il numero dei fattori primi nelle due fattorizzazioni è uguale);
- riordinando opportunamente i fattori, si ha $p_1 = q_1$, $p_2 = q_2$, ... , $p_r = q_r$ (cioè i fattori coincidono ordinatamente nelle due fattorizzazioni).

Dall'eguaglianza $a = p_1(p_2 \cdots p_r) = q_1 q_2 \cdots q_s$ segue che p_1 è divisore del prodotto $q_1 q_2 \cdots q_s$. Per l'Osservazione nella precedente lezione, il numero

primo p_1 è divisore di almeno uno dei fattori $q_1, q_2, \ldots, q_s$ e, riordinando opportunamente i fattori, possiamo fare in modo che $p_1 \mid q_1$. Essendo q_1 primo, le possibilità per il suo divisore p_1 sono $p_1 = 1$ oppure $p_1 = q_1$. Ma allora $p_1 = q_1$ (perché per definizione di numero primo si ha $p_1 > 1$). Dividendo ambo i membri dell'eguaglianza per p_1 si ottiene l'eguaglianza: $p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$, e si può iterare il ragionamento ottenendo $p_2 = q_2$ (riordinando di nuovo opportunamente i fattori). La tesi 2. è dunque dimostrata. Dimostriamo ora la tesi 1: se per assurdo la supponessimo falsa, si avrebbe $r \neq s$. Supponiamo per esempio che sia $r > s$ (se $r < s$ si ragiona in modo simile): dopo s passi del precedente procedimento iterativo, dividendo per ps, si avrebbe alla fine l'eguaglianza: $p_{s+1} p_{s+2} \cdots p_r = 1$, contraddizione perché i numeri primi p_i sono tutti > 1. □

Illustriamo una conseguenza del Teorema di fattorizzazione unica:

Teorema 123 *La radice quadrata di un numero primo p è un numero non razionale.*

Dimostrazione Per assurdo supponiamo $\sqrt{p} = a/b$ dove a, b sono naturali. Si ha $p = a^2/b^2$, $b^2 p = a^2$. Nel caso $a = 1$, si ha $b^2 p = 1$, contraddizione perché $p > 1$. Nel caso $b = 1$ si ha $p = a^2 = aa$, contraddizione perché il primo p avrebbe un divisore a non banale. Infine nel caso $a > 1$, $b > 1$, fattorizziamo a, b in prodotto di primi:

$$a = p_1 p_2 \cdots p_r$$

$$b = q_1 q_2 \cdots q_s$$

da cui si avrebbe:

$$b_2 p = q_1 q_1 q_2 q_2 \cdots q_s q_s p = a_2 = p_1 p_1 p_2 p_2 \cdots p_r p_r$$

e per il Teorema di fattorizzazione unica sarebbe uguale il numero di fattori primi nelle due fattorizzazioni, ottenendo l'eguaglianza $2_s + 1 = 2_r$, contraddizione perché $2_s + 1$ è dispari, 2_r è pari. □

Illustriamo un'altra conseguenza del Teorema di fattorizzazione unica:

Teorema 124 *I numeri primi sono infiniti.*

Dimostrazione Per assurdo supponiamo che l'insieme dei numeri primi contenga un numero finito di elementi, e sia $p_1, p_2, \ldots, p_k$ l'elenco completo di tutti i numeri primi. Consideriamo il seguente numero naturale ottenuto sommando 1 al prodotto di tutti i numeri primi:

$$a = (p_1 p_2 \cdots p_k) + 1$$

Sicuramente questo numero non è primo perchè è diverso da tutti quelli elencati. Per il Teorema di esistenza della fattorizzazione, a si può scomporre in fattori primi e se p è uno qualunque dei suoi fattori primi si ha ovviamente $p \mid a$, ossia esiste un numero naturale c tale che $pc = a = (p_1 p_2 \cdots p_k) + 1$, da cui $1 = pc - (p_1 p_2 \cdots p_k)$. Ma p coinciderà con uno dei p_i (perché per assurdo $p_1, p_2, \ldots, p_k$ sono tutti i possibili numeri primi), dunque nel secondo membro dell'eguaglianza precedente si può mettere in evidenza il fattore comune p, e si conclude che p è divisore di 1, contraddizione perché $p > 1$. □

5.3.2 Criteri di primalità

Abbiamo definito numero primo un numero intero $p > 1$ che non ha fra i numeri naturali dei divisori diversi da 1 e p stesso. Un numero intero > 1 che non è primo sarà detto *numero composto*.

Dato un numero naturale $n > 1$, come verificare se n è un numero primo?

Possiamo procedere con il seguente algoritmo: elenchiamo i numeri naturali da 2 ad $(n-1)$:

$$2, 3, \ldots, (n-1)$$

e per ognuno di essi verifichiamo se è un divisore di n (basta dividere n per tale numero e verificare se il resto è 0). Se in tutte queste divisioni otteniamo sempre resto diverso da 0, concludiamo che nessuno dei numeri $2, 3, \ldots, (n-1)$ è un divisore di n, dunque n ha solo $1, n$ come divisori e cioè n è un numero primo; se invece in almeno una di queste divisioni il resto è 0, allora abbiamo trovato un divisore di n diverso da 1 e da n, dunque concludiamo che n è un numero composto.

Esempio 125 *Il numero $n = 7$ è un numero primo?*
Dividiamo 7 successivamente per $2, 3, 4, 5, 6$ ottenendo i resti $1, 1, 3, 2, 1$ che sono tutti diversi da 0, e concludiamo che 7 ha solo $1, 7$ come divisori e cioè 7 è un numero primo.
Il numero $n = 9$ è un numero primo?
Dividiamo 9 successivamente per $2, 3, 4, 5, 6, 7, 8$ e ci accorgiamo che dividendo 9 per 3 si ottiene resto 0, dunque 3 è un divisore di 9 diverso da 1 e 9, ossia 9 è un numero composto.

Tale algoritmo si può rendere più efficiente con la seguente:

Proposizione 126 *Se $n > 1$ è un numero composto, fra i numeri $2, 3, \ldots, n-1$ il più piccolo divisore di n è sicuramente non maggiore di $\sqrt{n}$.*

Dimostrazione Fra i numeri $2, 3, \ldots, n-1$ sia d il divisore più piccolo di n e supponiamo per assurdo che sia $d > \sqrt{n}$; essendo d divisore di n, esiste un intero c (sempre fra $2, 3, \ldots, n-1$) tale che $n = cd$, e poiché d è il divisore più piccolo di n, si ha $c \geq d$, quindi $c > \sqrt{n}$; ma allora $n = cd > \sqrt{n}\sqrt{n} = n$, cioè $n > n$, contraddizione. □

In base alla Proposizione 126, basta cercare un eventuale divisore di n fra i numeri $2, 3, \ldots, n-1$ che sono $\leq \sqrt{n}$: se tale divisore esiste, n è composto, altrimenti è primo.

Esempio 127 *Il numero $n = 101$ è un numero primo? Se adoperassimo l'algoritmo iniziale, dovremmo cercare un eventuale divisore di n fra i numeri $2, 3, \ldots, 100$ (che sono 99), quindi effettuare 99 divisioni; ma sfruttando l'Osservazione, ci possiamo limitare ai soli numeri $\leq \sqrt{n}$ cioè ai numeri $2, 3, 4, 5, 6, 7, 8, 9, 10$ (solo 9 divisioni): poiché tutte le divisioni di 101 per tali numeri danno resto diverso da 0, concludiamo che $n = 101$ è un numero primo.*

Un criterio di primalità è il seguente:

Proposizione 128 *se il numero intero $n > 1$ non ha fra i suoi divisori nessun numero primo $\leq \sqrt{n}$, allora n è certamente primo.*

Dimostrazione Se n è un numero composto, come visto nella Proposizione 126, n ha, fra i numeri $2, 3, \ldots, n-1$, un divisore $d \leq \sqrt{n}$; essendo d un intero > 1, per il Teorema di Fattorizzazione Unica d è prodotto di numeri primi (tutti divisori di d, e tutti $\leq \sqrt{n}$); tutti questi numeri sono a maggior ragione divisori di n. □

In base a tale criterio di primalità, per verificare se un numero intero $n > 1$ è primo potremmo procedere nel modo seguente: dividere n per tutti i numeri primi $\leq \sqrt{n}$ e se tutte le divisioni avessero resto diverso da 0 potremmo concludere che n è primo.

Esempio 129 *Per il numero* $n = 101$ *esaminato sopra basterebbe dividere* 101 *per* $2, 3, 5, 7$ *(sono i numeri primi* $\leq \sqrt{101}$*) e poiché tutte queste divisioni danno resto diverso da 0 potremmo concludere che* 101 *è primo (utilizzando solo* 4 *divisioni invece delle* 9 *divisioni considerate sopra).*

Però per applicare tale criterio di primalità dovremmo avere un elenco completo di tutti i numeri primi $\leq \sqrt{n}$. Un tale elenco si può ottenere con il *crivello di Eratostene*: si scrivono i numeri > 1 e $\leq \sqrt{n}$ e si cancellano dapprima i multipli di 2 $(4, 6, 8, 10, \ldots)$; poi si cancellano i numeri multipli del successivo numero rimasto in elenco (che è 3); così si procede cancellando sempre i numeri multipli del successivo numero rimasto in elenco. Alla fine nell'elenco restano solo i numeri primi $\leq \sqrt{n}$.