Dispense di Aritmetica

Dikran Dikranjan e Maria Silvia Lucido

Dipartimento di Matematica e Informatica
Università di Udine
via delle Scienze 200, I-33100 Udine

settembre 2003

Queste dispense nascono per il corso di Aritmetica.
Nel capitolo 1 viene presentato il concetto di insieme e di appartenenza, le operazioni tra insiemi, la definizione di insieme finito e un esempio di insieme infinito, i numeri naturali con una loro importante proprietà, il principio di induzione.
Nel capitolo 2 vengono illustrate le relazioni su insiemi. Tra queste occupa un posto fondamentale la definizione di applicazione. Vengono poi introdotte anche le relazioni di equivalenza, i coefficienti binomiali, le relazioni d'ordine e preordine e i reticoli.

Nel capitolo 3 vengono introdotti le prime nozioni riguardanti l'*aritmetica*, ovvero lo studio dei numeri. All'interno dell'insieme dei numeri interi, si da' la definizione di divisibilità e di numero primo. I numeri primi saranno poi gli "atomi" con i quali si costruiscono tutti i numeri interi. Si danno le nozioni di massimo comun divisore e di minimo comune multiplo. Inoltre viene formalizzata con l'algoritmo di Euclide, la divisione euclidea che si impara alle scuole elementari. Si enuncia e si dimostra il Teorema Fondamentale dell'Aritmetica, che garantisce che ogni numero intero si può fattorizzare in modo essenzialmente unico come prodotto di primi. Si definisce nell'insieme dei numeri interi una relazione di equivalenza, la *congruenza modulo* n, per un fissato numero intero n. Questa relazione è compatibile con le operazioni di somma e prodotto dei numeri interi. Per questo ritroveremo spesso nei successivi corsi di Algebra (e non solo) l'insieme delle sue classi di equivalenza.
Con questi strumenti verranno poi spiegati i criteri di divisibilità per 3, 9, 11 e 101, alcuni dei quali noti fino dalle scuole elementari.
Negli ultimi due paragrafi di questo capitolo viene dimostrato un Teorema di Fermat (non l'ultimo...) e una sua generalizzazione dovuta ad Eulero. Viene poi studiata la funzione di Eulero, che conta quanti sono i numeri naturali coprimi con n e minori di n, per un fissato numero naturale n.

Nel capitolo 4 vengono presentati gli altri insiemi di numeri, ovvero i numeri razionali, reali e complessi. I numeri reali vengono solo accennati perché sono oggetto di studio approfondito dei corsi di Analisi. Maggiore attenzione viene invece dedicata ai numeri complessi, alle operazioni definite su di essi e alla loro interpretazione geometrica.

Questo conclude la parte basilare della Teoria che costituisce il corso di Aritmetica. Seguono due capitoli di complementi sugli insiemi e sull'aritmetica, in cui vengono presentati alcuni risultati che richiedono talvolta delle dimostrazioni un po' più complesse delle precedenti.

Il capitolo 5 contiene complementi alla teoria degli insiemi che riguardano innanzitutto insiemi ordinati, prodotti cartesiani e equipotenza di insiemi (finiti o infiniti). Cominciamo

rilevando l'importanza delle applicazioni in tali questioni. Gli insiemi ordinati offrono un linguaggio flessibile e universale, indispensabile sia nei settori della matematica pura (Algebra, Analisi e Geometria), che di quella applicata (Informatica Teorica, Ottimizzazione, Matematica Finanziaria). Concludiamo il capitolo con un paragrafo che contiene un elenco di tutti gli assiomi necessari per sviluppare correttamente la teoria degli insiemi. Questa appendice, assieme ad una parte degli esercizi, denotati con * possono essere tralasciati durante una prima lettura del testo. Una parte degli assiomi è stata "assorbita" durante i corsi di Aritmetica e Analisi 1 (l'esistenza di un insieme, di unioni, di coppie e l'insieme delle parti). Qui diamo particolare enfasi all'assioma della scelta (che permette di dimostrare l'esistenza di un buon ordine su ogni insieme) e dell'assioma dell'infinito (che permette di dimostrare l'esistenza di $\mathbb{N}$). Dimostriamo anche il lemma di Zorn, uno dei mezzi universali per stabilire l'esistenza di oggetti con proprietà ottimali in Algebra, Analisi e Geometria. Per dare la possibilità di esercitarsi nell'applicazione di quest'arma potente abbiamo incluso diversi esercizi il cui svolgimento richiede il Lemma di Zorn.
Nel capitolo 7 vengono introdotti i numeri primi di Fermat e di Mersenne. Vengono inoltre dati alcuni cenni sulla distribuzione dei numeri primi.

Concludono le dispense due capitoli di esercizi, suddivisi in esercizi sugli insiemi ed esercizi sull'aritmetica.

Contents

1 Insiemi

1.1 Il concetto di insieme e appartenenza

Il concetto di insieme e appartenenza "$\in$" sono primitivi e non verranno definiti rigorosamente. Un insieme X è determinato dai suoi elementi x, scriveremo $x \in X$ e leggeremo x *appartiene a* X. Scriveremo spesso anche $X = \{x : \text{vale } P(x)\}$, dove $P(x)$ è qualche proprietà che descrive gli elementi di X. Nel caso in cui X abbia un numero finito di elementi $x_1, x_2, \ldots, x_n$ scriveremo $X = \{x_1, x_2, \ldots, x_n\}$ (cioè X è determinato dalla lista dei suoi elementi, è importante ribadire che questi elementi sono a due a due distinti). In tal caso X si dice un *insieme finito* e il numero n dei suoi elementi si denota anche con $|X|$.
Vediamone subito qualche esempio.

Esempio 1.1 a) L'insieme di tutti gli studenti dell'Università di Udine.
b) L'insieme di tutte le rette del piano.
c) L'insieme delle lettere dell'alfabeto inglese.
d) L'insieme dei colori dell'arcobaleno.

Vediamo ora qualche esempio numerico.

Esempio 1.2 a) L'insieme $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$ dei numeri naturali.
b) L'insieme $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots\}$ dei numeri interi.
c) L'insieme $\mathbb{Q}$ dei numeri razionali.
d) L'insieme $\mathbb{R}$ dei numeri reali.
e) L'insieme $\mathbb{R}_+ = \{x \in \mathbb{R} : x > 0\}$ dei numeri reali positivi.
f) L'insieme dei numeri primi $\mathbb{P} = \{2, 3, 5, \ldots\}$.

Esempio 1.3 a) L'insieme $\{0, 2, 4, \ldots\}$ dei numeri naturali pari si può scrivere anche così:

$$\{x \in \mathbb{N} : x = 2y \text{ per qualche } y \in \mathbb{N}\}.$$

b) L'insieme $\mathbb{R}_+ = \{x \in \mathbb{R} : x > 0\}$ dei numeri reali positivi.

Essendo ogni insieme completamente determinato dai suoi elementi, due insiemi X e Y coincidono, cioè $X = Y$, se hanno gli stessi elementi, ovvero, per ogni $x \in X$ vale anche $x \in Y$ e per ogni $y \in Y$ vale anche $y \in X$. Se per due insiemi X e Y è verificata solamente la prima delle implicazione, cioè per ogni $x \in X$ vale anche $x \in Y$, diremo che X è *sottoinsieme* di Y (oppure X è contenuto in Y), e lo denoteremo con il simbolo $X \subseteq Y$. In questa circostanza diremo anche Y *contiene* X e lo denoteremo con il simbolo $Y \supseteq X$.
La condizione $x \notin \emptyset$ determina un insieme $\emptyset$, privo di elementi, che chiameremo *l'insieme vuoto*. Ovviamente, vale $\emptyset \subseteq X$ per ogni insieme X. Infatti, basta trovare una proprietà P tale che nessun elemento di X soddisfa P. Per esempio:

$$\emptyset = \{x \in \mathbb{N} : 2x = 5\}, \qquad \emptyset = \{x \in \mathbb{Q} : x^2 = 2\},$$
$$\emptyset = \{x \in \mathbb{R} : x^4 = -11\}, \qquad \emptyset = \{x \in X : x \neq x\}.$$

Gli elementi di un insieme possono avere natura del tutto arbitraria. In particolare, possono essere insiemi essi stessi. Per esempio, se X ed Y sono insiemi, possiamo considerare l'insieme $Z = \{X, Y\}$, che ha come elementi X e Y. Se abbiamo n insiemi $A_1, \ldots, A_n$, possiamo considerare l'insieme $Z = \{A_1, \ldots, A_n\}$. Spesso ci riferiamo a Z dicendo anche "Z è una *famiglia* di insiemi" ("famiglia" e "insieme" sono sinonimi). Ecco un esempio di una famiglia infinita di insiemi. Per ogni $x \in \mathbb{R}$ sia A_x l'intervallo $]x, x+1[$ in $\mathbb{R}$. Allora gli insiemi A_x, al

variare di x in $\mathbb{R}$ formano una famiglia infinita di insiemi, che denoteremo con $\{A_x : x \in \mathbb{R}\}$. Analogamente, quando si ha una famiglia di insiemi A_i, indiciata con gli elementi i di un insieme di indici I, scriveremo $\{A_i : i \in I\}$.
Dato un insieme X consideriamo la famiglia $\mathcal{P}(X)$ di tutte le parti (sottoinsiemi) di X. Questa famiglia si chiama *l'insieme delle parti* di X. Si noti che $\mathcal{P}(\emptyset)$ non è più vuoto, essendo $\mathcal{P}(\emptyset) = \{\emptyset\}$. Si veda inoltre che $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

Esercizio 1.4 *Si descriva l'insieme* $\mathcal{P}(\{1, 2, 3\})$.

Esercizio 1.5 *Siano* A *e* B *due insiemi. Si dimostri che* $A \subseteq B$ *se e solo se* $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

1.2 Unione e intersezione

Siano X ed Y due insiemi. L'*unione* di X e Y è l'insieme $X \cup Y$ che ha come elementi tutti gli x tali che valga $x \in X$ oppure $x \in Y$. In altre parole,

$$X \cup Y = \{x : x \in X \text{ o } x \in Y\}.$$

Non è difficile vedere che

$$X \subseteq X \cup Y \text{ e } Y \subseteq X \cup Y. \tag{1}$$

L'unione $X \cup Y$ è il più piccolo insieme che soddisfa la proprietà (1). Infatti se Z soddisfa (1), ovvero, se $X \subseteq Z$ e $Y \subseteq Z$, allora anche $X \cup Y \subseteq Z$. Infatti, se $x \in X \cup Y$, allora si ha $x \in X$ o $x \in Y$ e in entrambi casi segue $x \in Z$.

L'operazione unione gode delle seguenti proprietà:

(1) (commutativa) $X \cup Y = Y \cup X$ per ogni coppia di insiemi X e Y;

(2) (associativa) $(X \cup Y) \cup Z = X \cup (Y \cup Z)$ per ogni terna di insiemi X, Y e Z;

(3) $A \cup A = A$ per ogni insieme A.

L'*intersezione* di due insiemi X e Y è l'insieme $X \cap Y$ che ha come elementi tutti gli x tali che vale $x \in X$ *e* $x \in Y$. In altre parole,

$$X \cap Y = \{x : x \in X \text{ e } x \in Y\}.$$

Possiamo descrivere l'intersezione anche come

$$X \cap Y = \{x \in X : x \in Y\} = \{x \in Y : x \in X\}.$$

Due insiemi X e Y si dicono *disgiunti* se $X \cap Y = \emptyset$.
Non è difficile vedere che

$$X \cap Y \subseteq X \text{ e } X \cap Y \subseteq Y. \tag{2}$$

Esercizio 1.6 *Dimostrare che l'intersezione* $X \cap Y$ *è il più grande insieme che soddisfa la proprietà (2). Più precisamente, se* Z *soddisfa (2), ovvero, se* $Z \subseteq X$ *e* $Z \subseteq Y$*, allora anche* $Z \subseteq X \cap Y$.

L'operazione intersezione gode delle seguenti proprietà:

(1) (commutativa) $X \cap Y = Y \cap X$ per ogni coppia di insiemi X e Y;

(2) (associativa) $(X \cap Y) \cap Z = X \cap (Y \cap Z)$ per ogni terna di insiemi X, Y e Z;

(3) $A \cap A = A$ per ogni insieme A.

Si può definire l'unione di una famiglia arbitraria di insiemi $\mathcal{F}$ ponendo $\bigcup_{A\in\mathcal{F}} A = \{x : x \in A \text{ per qualche } A \in \mathcal{F}\}$.

Esempio 1.7 L'insieme dei reali $\mathbb{R}$ si può vedere come un'unione (infinita) di suoi intervalli $\mathbb{R} = \bigcup_{x\in\mathbb{Z}}]x, x+2[$. Questa uguaglianza resta vera se gli intervalli $]x, x+2[$ di lunghezza 2 vengono sostituiti con gli intervalli $]x, x+1[$ di lunghezza 1?

Come nel caso dell'unione, si può definire l'intersezione di una famiglia arbitraria di insiemi, ponendo $\bigcap_{A\in\mathcal{F}} A = \{x : x \in A \text{ per ogni } A \in \mathcal{F}\}$.
Vediamo ora alcuni esempi di intersezioni infinite.

Esempio 1.8 $\bigcap_{n=1}^{\infty}]n, +\infty[= \emptyset$. Supponiamo per assurdo che questa intersezione non sia vuota, allora esiste un elemento $x \in \mathbb{R}$ che appartiene a $\bigcap_{n=1}^{\infty}]n, +\infty[$. Sia n_0 la parte intera di x ($n_0 = [x]$). Allora x non appartiene all'insieme $]n_0+1, \infty[$ e pertanto non può appartenere a quell'intersezione.

Esercizio 1.9 *Si provi che* $\bigcap_{n=1}^{\infty}]-\frac{1}{n}, +\frac{1}{n}[= \{0\}$.

Svolgimento. Per dimostrare l'uguaglianza tra due insiemi, si dimostra l'inclusione del primo nel secondo e del secondo nel primo, nota come *doppia inclusione*. Nel nostro caso $0 \in]-\frac{1}{n}, +\frac{1}{n}[$ per ogni $n \in \mathbb{N}$, $n \geq 1$. Questo dimostra l'inclusione "$\supseteq$". Dimostriamo quindi che $\bigcap_{n=1}^{\infty}]-\frac{1}{n}, +\frac{1}{n}[\subseteq \{0\}$. Sia $x \in \bigcap_{n=1}^{\infty}]-\frac{1}{n}, +\frac{1}{n}[$. Se $x \neq 0$, sia $|x^{-1}| = |x|^{-1}$ il modulo del suo inverso. Sia $n_0 = [|x^{-1}|]$, allora $n_0 \leq |x^{-1}| < n_0 + 1$, da cui si ricava $|x| > \frac{1}{n_0+1}$ e quindi $x \notin]-\frac{1}{n_0+1}, +\frac{1}{n_0+1}[$. Pertanto se $x \neq 0$ non può appartenere a quella intersezione, da cui si deduce che l'unico elemento contenuto nell'intersezione è 0. □

Verifichiamo ora le *leggi distributive* dell'intersezione rispetto all'unione e dell'unione rispetto all'intersezione.

Proposizione 1.10 *Siano A, B e C tre insiemi, allora valgono:*

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

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

Dimostrazione. i) Sia $x \in (A \cap B) \cup C$, allora o $x \in (A \cap B)$ oppure $x \in C$, cioè o $x \in A$ e $x \in B$ oppure $x \in C$. Se x appartiene ad A e a B, allora $x \in A \cup C$ e $x \in B \cup C$. Se $x \in C$, allora $x \in A \cup C$ e $x \in B \cup C$. Pertanto in ogni caso $x \in (A \cup C) \cap (B \cup C)$.
Supponiamo ora $x \in (A \cup C) \cap (B \cup C)$. Allora $x \in A \cup C$ e $x \in B \cup C$. Se x non appartiene a C, allora da $x \in A \cup C$ si ricava che $x \in A$ e da $x \in B \cup C$ si ricava che x deve stare anche in B. Quindi o $x \in C$ oppure $x \in A \cap B$, cioè $x \in (A \cap B) \cup C$.
ii) Si lascia per esercizio. □

Definizione 1.11 Una famiglia $\{A : A \in \mathcal{F}\}$ di sottoinsiemi non vuoti A di un insieme X è una *partizione di X* se

i) $X = \bigcup_{A\in\mathcal{F}} A$,

ii) $A \cap B = \emptyset$ se $A, B \in \mathcal{F}$ e $A \neq B$.

Vediamone qualche esempio.

Esempio 1.12 *i)* Sia X un insieme. Allora $\{\{x\} : x \in X\}$ è una partizione di X.
ii) Consideriamo i seguenti insiemi $X = \{$studenti dell'Università di Udine$\}$, $F = \{$facoltà presenti presso l'Università di Udine$\}$ e sia $X_f = \{$studenti iscritti alla facoltà $f \in F\}$. Allora $\{X_f : f \in F\}$ è una partizione di X.
iii) L'insieme $\{[n, n+1[: n \in \mathbb{Z}\}$ è una partizione di $\mathbb{R}$.

Esercizio 1.13 *Provare che qualunque siano gli insiemi S e T risulta*
a) $\mathcal{P}(S \cap T) = \mathcal{P}(S) \cap \mathcal{P}(T)$
b) $\mathcal{P}(S) \cup \mathcal{P}(T) \subseteq \mathcal{P}(S \cup T)$
c) $\mathcal{P}(S) \cup \mathcal{P}(T) = \mathcal{P}(S \cup T)$ *se e solo se* $S \subseteq T$ *oppure* $T \subseteq S$.

Svolgimento. *a)* $\mathcal{P}(S \cap T) \subseteq \mathcal{P}(S)$ e $\mathcal{P}(S \cap T) \subseteq \mathcal{P}(T)$ per l'Esercizio 1.5. Per dimostrare l'altra inclusione basta notare che ogni $A \in \mathcal{P}(S) \cap \mathcal{P}(T)$ è contenuto sia in S sia in T, e quindi $A \subseteq S \cap T$ per l'Esercizio 1.6.
b) Sia $A \in \mathcal{P}(S) \cup \mathcal{P}(T)$, allora $A \in \mathcal{P}(S)$ oppure $A \in \mathcal{P}(T)$, cioè $A \subseteq S$ oppure $A \subseteq T$, in ogni caso $A \subseteq S \cup T$. L'inclusione può essere stretta. Infatti se per esempio $S = \{0, 1, 2\}$, $T = \{0, 3\}$ e $A = \{1, 3\}$, si ha $A \in \mathcal{P}(S \cup T)$, ma $A \notin \mathcal{P}(S) \cup \mathcal{P}(T)$.
c) Se, per esempio, $S \subseteq T$, $S \cup T = T$ e $\mathcal{P}(S) \cup \mathcal{P}(T) = \mathcal{P}(T)$. Viceversa supponiamo che $\mathcal{P}(S) \cup \mathcal{P}(T) = \mathcal{P}(S \cup T)$ e che $S \not\subseteq T$. Pertanto esiste $s \in S \setminus T$. Considero $A = \{s\} \cup T \subseteq S \cup T$. Allora $A \notin \mathcal{P}(T)$ e quindi $A \in \mathcal{P}(S)$, cioè $T \subseteq S$. □

1.3 Differenza di insiemi

La *differenza* di due insiemi X e Y (detta anche *complementare di Y in X*) è l'insieme $X \setminus Y$ che ha come elementi tutti gli $x \in X$ tali che $x \notin Y$. In altre parole

$$X \setminus Y = \{x : x \in X \text{ e } x \notin Y\}. \tag{3}$$

Esempio 1.14 i) Il complementare di $\mathbb{Q}$ in $\mathbb{R}$ è l'insieme dei numeri irrazionali.
ii) Il complementare dei numeri pari in $\mathbb{N}$ è l'insieme dei numeri dispari.
iii) Il complementare dei numeri dispari nell'insieme dei numeri primi $\mathbb{P}$ è $\{2\}$.

È facile vedere che $X \setminus X = \emptyset$ per ogni insieme X. Più precisamente, si ha:

Lemma 1.15 $X \setminus Y = \emptyset$ *se e solo se* $X \subseteq Y$.

Dimostrazione. Sia $X \setminus Y = \emptyset$. Se $x \in X$, allora non possiamo avere $x \notin Y$, altrimenti $x \in X \setminus Y$ contrariamente all'ipotesi $X \setminus Y = \emptyset$. Questo dimostra l'inclusione $X \subseteq Y$.
Viceversa, se $X \subseteq Y$, allora non esiste un elemento $x \in X$ tale che $x \notin Y$. Pertanto, la proprietà (3) definisce l'insieme vuoto. □

Esercizio 1.16 $X \setminus Y = X$ *se e solo se* X *e* Y *sono disgiunti.*

Vediamo ora alcune proprietà della differenza:

Proposizione 1.17 (Leggi di de Morgan) *Sia X un insieme e $A \in \mathcal{P}(X)$ e $\mathcal{F} \subseteq \mathcal{P}(X)$. Si dimostri che*

i) $A \setminus \bigcap_{B \in \mathcal{F}} B = \bigcup_{B \in \mathcal{F}} (A \setminus B)$;

ii) $A \setminus \bigcup_{B \in \mathcal{F}} B = \bigcap_{B \in \mathcal{F}} (A \setminus B)$.

DIMOSTRAZIONE. i) Se $x \in A \setminus \bigcap_{B\in\mathcal{F}} B$, allora $x \in A$ ed esiste $B_0 \in \mathcal{F}$ tale che $x \notin B_0$. Pertanto $x \in A \setminus B_0$ e quindi a maggior ragione $x \in \bigcup_{B\in\mathcal{F}}(A \setminus B)$. Supponiamo viceversa $x \in \bigcup_{B\in\mathcal{F}}(A \setminus B)$, allora esiste B_0 tale che $x \in A \setminus B_0$. Pertanto $x \notin B_0$ e quindi $x \notin \bigcap_{B\in\mathcal{F}} B$, cioè $x \in A \setminus \bigcap_{B\in\mathcal{F}} B$.
ii) La dimostrazione è analoga. □

Esercizio 1.18 *Siano S, T e V insiemi. Provare che valgono le proprietà distributive della differenza rispetto all'intersezione e all'unione:*
a) $(S \cap T) \setminus V = (S \setminus V) \cap (T \setminus V)$,
b) $(S \cup T) \setminus V = (S \setminus V) \cup (T \setminus V)$.
c) Mostrare con un esempio che non valgono per la differenza le proprietà associativa e commutativa.

SUGGERIMENTI. c) Siano a, b, c tre elementi distinti di un insieme X. Si prendano ad esempio gli insiemi $S = \{a, b\}$, $T = \{a, c\}$ e $V = \{b, c\}$. Allora $(S \setminus T) \setminus V = \emptyset \neq S \setminus (T \setminus V) = \{b\}$ e $S \setminus T \neq T \setminus S$. □

Esercizio 1.19 *Siano A e B due insiemi. Si dimostri che $\{A \setminus B, B \setminus A, A \cap B\}$ è una partizione di $A \cup B$.*

Esercizio 1.20 *Siano A e B due insiemi finiti. Si dimostri che $|A \cup B| = |A| + |B| - |A \cap B|$.*

Esercizio 1.21 *Siano A, B e C tre insiemi finiti. Si dimostri che*

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

1.4 Un esempio di insieme: i numeri naturali e il principio di induzione

I numeri interi maggiori o uguali a 0 si dicono *numeri naturali* e si denotano con il simbolo $\mathbb{N}$.

Assiomi di Peano. Il matematico italiano *Peano* (1858-1932) ha proposto la seguente descrizione dell'insieme $\mathbb{N}$ dei numeri naturali a partire dei concetti di base $\mathbb{N}$, 0 e s (successore):

(P1) $0 \in \mathbb{N}$;

(P2) se $n \in \mathbb{N}$, allora anche $s(n) \in \mathbb{N}$;

(P3) se $n \in \mathbb{N}$, allora $s(n) \neq 0$;

(P4) se l'insieme E contiene 0 ed ha la proprietà che assieme ad ogni $n \in E$ anche $s(n) \in E$, allora $\mathbb{N} \subseteq E$;

(P5) s è iniettiva.

La più importante proprietà dei numeri naturali è senz'altro il seguente:

Assioma del buon ordinamento: *ogni insieme non vuoto di numeri naturali possiede un elemento minimo.*

Si usa la parola *assioma* perché su questa proprietà (assieme a poche altre) si può fondare una precisa definizione di $\mathbb{N}$. Un'importante applicazione del principio del buon ordinamento è la seguente proposizione.

Proposizione 1.22 (Principio di induzione) *Supponiamo che S sia un sottoinsieme di $\mathbb{N}$ tale che $0 \in S$ e per ogni $x \in S$ si ha che anche $x+1 \in S$. Allora $S = \mathbb{N}$.*

DIMOSTRAZIONE. Supponiamo per assurdo che S non sia tutto $\mathbb{N}$. Allora l'insieme $\mathbb{N} \setminus S$ degli elementi di $\mathbb{N}$ che non stanno in S è diverso dal vuoto. Quindi per l'assioma del buon ordinamento ammette un elemento minimo, cioè esiste $m \in \mathbb{N} \setminus S$, e poiché $0 \in S$, si avrà $m > 0$. Pertanto $m - 1 \geq 0$ e $m - 1 \in S$. Allora, per ipotesi, si dovrebbe avere anche $m \in S$. Questa contraddizione prova la proposizione. □

Proposizione 1.23 Principio di induzione (prima forma) *Per ogni $n \in \mathbb{N}$, consideriamo un'asserzione $A(n)$ e supponiamo che*
i) $A(0)$ sia vera;
ii) se $A(k)$ è vera, allora anche $A(k+1)$ è vera.
Allora l'asserzione $A(n)$ è vera per ogni $n \in \mathbb{N}$.

Proposizione 1.24 Principio di induzione (seconda forma) *Per ogni $n \in \mathbb{N}$, consideriamo un'asserzione $A(n)$ e supponiamo che*
i) $A(0)$ sia vera;
ii) per ogni $m > 0$, se $A(k)$ è vera per ogni $0 \leq k < m$, allora anche $A(m)$ è vera.
Allora l'asserzione $A(n)$ è vera per ogni $n \in \mathbb{N}$.

Esercizio 1.25 *Si dimostrino le proposizioni 1.23 e 1.24.*

Un'ultima osservazione sul Principio di Induzione: nelle Proposizioni 1.23 e 1.24 si può sostituire nelle ipotesi $A(0)$ con $A(n_0)$, per qualche $n_0 \in \mathbb{N}$ e la tesi sarà quindi *$A(n)$ è vera per ogni $n \geq n_0$, $n \in N$.*

Esercizio 1.26 *Usando il principio di induzione, provare che per ogni numero naturale $n \geq 1$ risulta:*

(a) $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$.

(b) $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

(c) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$.

(d) $1^4 + 2^4 + 3^4 + \ldots + n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$.

(e) $1^5 + 2^5 + 3^5 + \ldots + n^5 = \frac{n^2(n+1)^2(2n^2+2n-1)}{12}$.

(f) $1^6 + 2^6 + 3^6 + \ldots + n^6 = \frac{n(n+1)(2n+1)(3n^4+6n^3-3n+1)}{42}$.

(g) $1^7 + 2^7 + 3^7 + \ldots + n^7 = \frac{n^2(n+1)^2(3n^4+6n^3-n^2-4n+2)}{24}$.

Esercizio 1.27 *Usando il principio di induzione, provare che per ogni numero naturale n risulta:*

$$\frac{1}{2^0} + \frac{1}{2^1} + \frac{1}{2^2} + \ldots + \frac{1}{2^n} = 2 - \frac{1}{2^n}.$$

Nel seguito scriveremo la somma $a_1 + a_2 + \ldots + a_n$ brevemente $\Sigma_{k=1}^{n} a_k$, dove l'indice k varia da 1 a n e può essere sostituito da qualunque altro carattere, per esempio $\Sigma_{i=1}^{n} a_i$ o $\Sigma_{j=1}^{n} a_j$. In particolare, la somma del punto (c) dell'Esercizio 1.26 è $\Sigma_{k=1}^{n} k^3$. Diamo ora alcune regole di calcolo che possono essere utili nel seguito.

Esercizio 1.28 *Sia $m > 2$ un numero naturale e sia assegnato un numero reale $a_{k\nu}$ per ogni coppia k, ν con $2 \leq k \leq m$ e $2 \leq \nu \leq k$. Allora $\sum_{k=2}^{m} \left(\sum_{\nu=2}^{k} a_{k\nu} \right) = \sum_{\nu=2}^{m} \left(\sum_{k=\nu}^{m} a_{k\nu} \right)$.*

SUGGERIMENTI. Si può dimostrare per induzione su m. Altrimenti, basta applicare la legge associativa e la legge commutativa per l'operazione + e notare che le somme sono estese sullo stesso insieme di numeri. □

Questa "regola di scambio" è molto utile quando ogni addendo è della forma $a_{k\nu} = c_\nu d_{k\nu}$ e la somma $S_\nu = \sum_{k=\nu}^{m} d_{k\nu}$ ha una forma semplice. In tale caso si avrà $\sum_{k=2}^{m} \left(\sum_{\nu=2}^{k} a_{k\nu} \right) = \sum_{\nu=2}^{m} c_\nu S_\nu$.

Esercizio 1.29 *Scrivere nella forma abbreviata tutte le somme degli esercizi 1.26 e 1.27.*

Esercizio 1.30 *Usando il principio di induzione, provare che:*

(a) $\Sigma_{k=1}^{n} \frac{1}{\sqrt{k}} \geq \sqrt{n}$ *per ogni numero naturale* $n \geq 1$*;*

(b) $\Sigma_{k=1}^{n} \frac{1}{n+k} \geq \frac{7}{12}$ *per ogni numero naturale* $n \geq 2$*;*

(c) $\Sigma_{k=2}^{n} \frac{1}{k^2-1} = \frac{3}{4} - \frac{2n+1}{2n(n+1)}$ *per ogni numero naturale* $n \geq 2$ *;*

(d) $\Sigma_{k=1}^{n} kq^{k-1} = \frac{nq^{n+1} - (n+1)q^n + 1}{(1-q)^2}$*, dove q è un numero razionale fisso diverso da 1, per ogni* $n \geq 1$.

Esercizio 1.31 *Siano n e $a_1 < a_2 < \ldots < a_n$ numeri naturali. Provare che* $(\Sigma_{k=1}^{n} a_k)^2 \leq \Sigma_{k=1}^{n} a_k^3$.

SUGGERIMENTI. Ragionando per induzione su n supponiamo di avere $(\Sigma_{k=1}^{n-1} a_k)^2 \leq \Sigma_{k=1}^{n-1} a_k^3$. Allora

$$\Sigma_{k=1}^{n-1} a_k \leq \Sigma_{k=1}^{a_{n-1}} k = \frac{(1 + a_{n-1}) a_{n-1}}{2} \leq \frac{a_n(a_n - 1)}{2}. \qquad (*)$$

Da (*) si ricava $2\left(\Sigma_{k=1}^{n-1} a_k\right) + a_n \leq a_n^2$ e di conseguenza $2a_n\left(\Sigma_{k=1}^{n-1} a_k\right) + a_n^2 \leq a_n^3$. Aggiungendo ad entrambi i membri $(\Sigma_{k=1}^{n-1} a_k)^2$ si ha $(\Sigma_{k=1}^{n} a_k)^2 \leq (\Sigma_{k=1}^{n-1} a_k)^2 + a_n^3$. L'ipotesi induttiva ci permette di proseguire l'uguaglianza $(\Sigma_{k=1}^{n-1} a_k)^2 + a_n^3 \leq \Sigma_{k=1}^{n} a_k^3$. □

La seconda forma del Principio di Induzione è molto più flessibile. Tuttavia, i seguenti esercizi evidenziano anche i suoi limiti.

Esercizio 1.32 *Dimostrare che tutti i cavalli sono bianchi.*

SVOLGIMENTO. Basterà dimostrare che tutti cavalli sono dello stesso colore. Poiché tutti abbiamo visto almeno un cavallo bianco, la tesi segue immediatamente. Sia $A(n)$ l'affermazione "in ogni insieme di n cavalli tutti i cavalli sono dello stesso colore". Ovviamente, $A(1)$ è vera. Ora supponiamo che sia vera $A(k)$ per tutti i $k < n$. Siano $C_1, \ldots, C_n$ dei cavalli. Allora per l'ipotesi induttiva tutti i cavalli $C_1, \ldots, C_{n-1}$ sono dello stesso colore (diciamo bianchi). Ora applichiamo l'ipotesi induttiva ai cavalli $C_2, C_3, \ldots, C_{n-2}, C_{n-1}, C_n$ e ne deduciamo che anch'essi sono dello stesso colore, che per forza deve essere il colore di C_{n-1}. Pertanto, tutti i cavalli $C_1, \ldots, C_n$ sono dello stesso colore e quindi $A(n)$ è stata dimostrata. □

Esercizio 1.33 *Trovare l'errore nello svolgimento dell'esercizio precedente.*

SUGGERIMENTI. L'errore consiste nell'applicazione scorretta del principio di induzione nella seconda forma. Nel passaggio da $k < n$ a n si sfrutta implicitamente il fatto che $n > 2$ (dove ?), in particolare che $A(2)$ è vera. □

1.5 Prodotti cartesiani finiti

Siano X e Y due insiemi non vuoti. Un *coppia ordinata* (x, y) consiste di un elemento $x \in X$ e un elemento $y \in Y$. É importante il fatto che nella coppia ordinata le due componenti x e y abbiano posizioni ben determinate – prima e seconda componente. Il *prodotto cartesiano* $X \times Y$ di X per Y è l'insieme di tutte le coppie ordinate (x, y), dove $x \in X$ e $y \in Y$.
Nel caso $X = Y$ l'insieme di tutte le coppie (x, x) con $x \in X$ si denota con Δ_X e si chiama *diagonale* di $X \times X$. Scriveremo X^2 per denotare $X \times X$.
Siano $A_1, A_2, \ldots, A_n$ degli insiemi non vuoti. Definiamo il prodotto cartesiano $A_1 \times A_2 \times \ldots \times A_n$ come l'insieme che ha come elementi tutte le n-uple ordinate $(a_1, a_2, \ldots, a_n)$ con $a_1 \in A_1$, $a_2 \in A_2$, ..., $a_n \in A_n$. Se tutti gli insiemi $A_1, A_2, \ldots, A_n$ coincidono con un dato insieme A, scriveremo brevemente A^n per il prodotto cartesiano $A_1 \times A_2 \times \ldots \times A_n$.

2 Relazioni e funzioni

In questo capitolo introduciamo la definizione di relazione e studiamo vari tipi di relazioni binarie, che godono di certe proprietà.

Definizione 2.1 Siano X ed Y insiemi non vuoti. Una *relazione binaria* tra X e Y è un sottoinsieme R di $X \times Y$.

Un primo importantissimo esempio di relazione binaria è l'*applicazione*. La definizione intuitiva di applicazione è nata nell'ambito degli insiemi di numeri, o altri oggetti concreti, dove la "regola" di "calcolare" $f(x)$ a partire da x può avere senso.
Intuitivamente, un'*applicazione* $f : X \to Y$ tra due insiemi X e Y è una regola che permette di assegnare ad *ogni* elemento $x \in X$ un *unico* elemento $f(x)$ di Y. Le due parole evidenziate sono le parole chiave per definire poi rigorosamente un'applicazione tra due insiemi. Notiamo infatti che la posizione $f : \mathbb{R} \to \mathbb{R}$ definita da $f(x) = \log x$ non è un'applicazione perché non è definita su ogni elemento di $\mathbb{R}$.
Vediamo ora alcuni esempi:

Esempio 2.2 (a) Sia X un insieme non vuoto. L'applicazione $id_X : X \to X$ definita dalla regola $id_X(x) = x$ per ogni $x \in X$ si dice *identità* (o *applicazione identica*) di X.

(b) Sia X un insieme non vuoto. Allora $f : X \to \mathcal{P}(X)$ definita da $f(x) = \{x\}$ è un'applicazione.

(c) Sia $X = \{\text{studenti dell'Università di Udine}\}$, allora $f : X \to \mathbb{N}$ che associa ad ogni studente il suo numero di matricola, è un'applicazione.

(d) Se $X = \{\text{rette del piano}\}$, allora $f : X \to \mathbb{R} \cup \{\infty\}$ che associa ad ogni retta il suo coefficiente angolare è un'applicazione.

Un'importante esempio di applicazioni sono senza dubbio le funzioni numeriche.

Esempio 2.3

(a) La funzione quadrata $f : \mathbb{R} \to \mathbb{R}$ definita da $f(x) = x^2$.

(b) La funzione logaritmica $f : \mathbb{R}_+ \to \mathbb{R}$ definita da $f(x) = \log x$.

(c) La funzione radice quadrata $f : \mathbb{R}_+ \to \mathbb{R}_+$ definita da $f(x) = \sqrt{x}$.

Il *grafico* $G(f)$ di una funzione (applicazione) $f : X \to Y$ si definisce come l'insieme di tutte le coppie $(x, f(x)) \in X \times Y$ con $x \in X$, ovvero

$$G(f) = \{(x, y) \in X \times Y : y = f(x)\}.$$

Chiaramente, il grafico della funzione quadrata $f : \mathbb{R} \to \mathbb{R}$ al punto (a) dell'esempio 2.3 è la parabola $\{(x, y) \in \mathbb{R}^2 : y = x^2\}$ nel piano $\mathbb{R}^2$, mentre il grafico dell'applicazione identica $id_X : X \to X$ è la diagonale Δ_X di $X \times X$.
Non è difficile verificare che il grafico $G(f)$ è un sottoinsieme del prodotto cartesiano $X \times Y$ con le seguenti proprietà:

(A1) per ogni $x \in X$ esiste una coppia $(x, y) \in G(f)$;

(A2) se $(x, y) \in G(f)$ e $(x, y') \in G(f)$, allora $y = y'$.

2.1 Definizione rigorosa di applicazione

Proponiamo ora una forma astratta del tutto rigorosa basata sulle proprietà (A1) e (A2) del grafico $G(f)$ di un'applicazione, descritte nel paragrafo precedente.

Definizione 2.4 Siano X e Y due insiemi non vuoti. Un applicazione $f : X \to Y$ è un sottoinsieme G del prodotto cartesiano $X \times Y$ (una relazione) con le proprietà (A1) e (A2), ovvero

(A1) per ogni $x \in X$ esiste una coppia $(x, y) \in G$;

(A2) se $(x, y) \in G$ e $(x, y') \in G$, allora $y = y'$.

L'insieme X si dice *dominio* dell'applicazione f e l'insieme Y si dice *codominio* dell'applicazione f. Si noti che ogni applicazione, nel senso della Definizione 2.4, determina una "regola" che permette di "calcolare" $f(x) \in Y$ come l'unico elemento $y \in Y$ tale che $(x, y) \in Y$.
Per $A \subseteq X$ l'insieme $f(A) = \{f(a) : a \in A\}$ è l'*immagine* di A. Se $a \in X$, $f(a) = f(\{a\})$ si chiama *immagine di a secondo f* (o *valore di f in a*). L'insieme $f(X)$ di tutte le immagini degli elementi di X si chiama *immagine dell'applicazione* f.
Per $b \in Y$ l'insieme $\{x \in X : f(x) = b\}$ si chiama *immagine inversa di b* o *antimmagine di b* e si denota con $f^{-1}(b)$. Chiaramente, $f^{-1}(b) \neq \emptyset$ se e solo se $b \in f(X)$. Per $B \subseteq Y$ l'insieme $\{x \in X : f(x) \in B\}$ si chiama *immagine inversa di B* e si denota con $f^{-1}(B)$.

Definizione 2.5 Siano X, Y due insiemi non vuoti. L'insieme di tutte le funzioni da X in Y si denota con $Y^X = \{f : X \to Y,\ f \text{ funzione }\}$.

La seguente definizione introduce tre proprietà molto importanti delle applicazioni.

Definizione 2.6 Un applicazione $f : X \to Y$ si dice:

(a) *iniettiva*, se per ogni $x, y \in X$ l'uguaglianza $f(x) = f(y)$ implica $x = y$;

(b) *suriettiva*, se per ogni $y \in Y$ esiste un $x \in X$ tale che $f(x) = y$;

(c) *biiettiva*, se f è iniettiva e suriettiva.

Chiaramente, $f : X \to Y$ è iniettiva se e solo se elementi distinti di X hanno immagini distinte in Y. In altre parole, f è iniettiva se e solo se $f^{-1}(b)$ contiene al più un elemento. D'altra parte, f è suriettiva se e solo se $f(X) = Y$.

Esempio 2.7 Sia X un insieme non vuoto. Allora l'applicazione id_X è biiettiva, quindi, iniettiva e suriettiva.

Esercizio 2.8 *Si dica quale delle applicazioni definite negli esempi 2.2 e 2.3 sono iniettive, suriettive o biiettive.*

Esercizio 2.9 *Sia $f : \mathbb{R} \to \mathbb{R}$ una delle seguenti funzioni. Si dica quale di queste funzioni è iniettiva, suriettiva o biiettiva.*
i) $f(x) = 2^x$; *ii)* $f(x) = 3x^2 - \sqrt{5}$; *iii)* $f(x) = sen(x)$;
iv) $f(x) = \begin{cases} x \text{ se } x < 0 \\ x^2 \text{ se } x \geq 0. \end{cases}$

Teorema 2.10 (Teorema di Cantor) *Non esiste un'applicazione suriettiva $f : X \to P(X)$, dove X è un insieme non vuoto.*

DIMOSTRAZIONE. Supponiamo che esista un'applicazione suriettiva $f : X \to P(X)$. Sia $A = \{x \in X : x \notin f(x)\}$. Allora per la suriettività di f esiste $x_0 \in X$ con $f(x_0) = A$. Ma per x_0 e A non valgono ne' $x_0 \in A$, ne' $x_0 \notin A$ – assurdo. □

Vogliamo sottolineare il ruolo importante delle applicazioni rispetto agli insiemi. A questo scopo faremo vedere come, a partire dalle applicazioni, si possano definire:

(a) l'insieme delle parti $\mathcal{P}(X)$;

(b) le relazioni binarie;

(c) i prodotti cartesiani;

(d) gli insiemi finiti/infiniti.

L'insieme delle parti $\mathcal{P}(X)$ è in biiezione con l'insieme 2^X di tutte le funzioni $X \to \{0, 1\}$. Infatti, per $A \in \mathcal{P}(X)$ consideriamo la funzione caratteristica

$$\chi_A(x) = \begin{cases} 1, \text{ se } x \in A \\ 0, \text{ se } x \in X, x \notin A \end{cases}.$$

Allora definiamo $\varphi(A) = \chi_A$. Si vede facilmente, che φ è una biiezione (vedi l'Esercizio 6.17) che permette di identificare $\mathcal{P}(X)$ con l'insieme 2^X delle funzioni caratteristiche.
Le relazioni binarie si possono definire facilmente tramite le applicazioni, facendo uso di (a). Infatti, sia $R \subseteq X \times X$ una relazione su X. Allora l'applicazione $\chi_R : X \times X \to \{0, 1\}$ ci permette di dire che per $x, y \in X$ si ha xRy se e solo se $\chi_R(x, y) = 1$. In altre parole, la relazione R si può "codificare" tramite un'applicazione $X \times X \to \{0, 1\}$. Nel paragrafo 2.2 vedremo come la distinzione tra insiemi finiti/infiniti si possa fare esclusivamente tramite applicazioni. Nel paragrafo 5.1 verranno definiti gli ordini su un'insieme X a partire da un'applicazione $f : \mathcal{P}(X) \setminus \{\emptyset\} \to X$ con la proprietà $f(A) \in A$ per ogni $A \in \mathcal{P}(X) \setminus \{\emptyset\}$. Nel paragrafo 5.2 le applicazione si usano allo scopo di definire in modo efficace prodotti cartesiani anche di famiglie infinite di insiemi.
Nei successivi corsi di Algebra vedremo come il concetto primario dell'algebra, l'**operazione**, non è altro che un'applicazione $A \times A \to A$.

2.2 Insiemi finiti e infiniti.

Diremo che un insieme X è *finito*, se X è vuoto o esiste un numero naturale $n > 0$ e una biiezione $\{1, 2, \ldots, n\} \to X$. Diremo in tal caso che X ha cardinalità n e scriveremo $|X| = n$. Non è difficile dimostrare per induzione su $n = |X|$ che ogni iniezione $X \to X$ di un insieme finito X è anche una suriezione.
Nel paragrafo 1.4 è stata introdotta la funzione successore s che non è suriettiva, quindi l'insieme $\mathbb{N}$ non è finito. Non è difficile vedere che se abbiamo a disposizione solamente la coppia $(\mathbb{N}, s)$ e sappiamo che (P3) e (P4) degli Assiomi di Peano valgono per qualche elemento $0 \in \mathbb{N}$, allora $\{0\} = \mathbb{N} \setminus s(\mathbb{N})$ e quindi 0 è univocamente determinato dalla coppia $(\mathbb{N}, s)$. L'esistenza di una coppia $(\mathbb{N}, s)$ che soddisfi gli assiomi di Peano descritti sopra non è scontata. Vedremo in seguito quali sono le condizioni che garantiscono l'esistenza di tale coppia $(\mathbb{N}, s)$.
Un insieme X si dice *infinito*, se esiste un'applicazione iniettiva, ma non suriettiva $f : X \to X$. Pertanto, un insieme infinito non è finito. Chiaramente, $\mathbb{N}$ è infinito. Dimostriamo ora che l'esistenza di un qualunque insieme infinito permette di costruire la coppia $(\mathbb{N}, s)$ dei numeri naturali $\mathbb{N}$ e la funzione successore s (vedi anche l'Esercizio 6.38 dove si dimostra che ogni insieme infinito contiene una copia di $\mathbb{N}$, assumendo l'esistenza di $\mathbb{N}$).

Teorema 2.11 *Sia X un insieme infinito. Allora esiste una coppia $(\mathbb{N}, s)$ che soddisfa gli assiomi di Peano e un'applicazione iniettiva $h : \mathbb{N} \to X$.*

Dimostrazione. Sia $f : X \to X$ un'applicazione iniettiva, ma non suriettiva a sia $x \in X \setminus f(X)$. Sia $\mathcal{A}$ la famiglia di tutti i sottoinsiemi A di X contenenti x e tali che $f(A) \subseteq A$. Non è difficile vedere che l'insieme $C = \bigcap_{A \in \mathcal{A}} A$ soddisfa $f(C) \subseteq C$ (essendo ovviamente $f(C) \subseteq A$ per ogni $A \in \mathcal{A}$). Quindi, $C \in \mathcal{A}$ in quanto $x \in C$. Pertanto C è il più piccolo elemento di $\mathcal{A}$. Sia $s : C \to C$ la restrizione di f a C. Ovviamente s è iniettiva. Dimostriamo che la coppia (C, s) soddisfa (1) e (2) relativamente all'elemento $x \in C$. Infatti, $x \notin s(C)$ è ovvia. Per vedere che vale (2) si noti che ogni insieme $E \subseteq C$ con la proprietà $x \in E$ e $s(E) \subseteq E$ necessariamente appartiene a $\mathcal{A}$ in quanto $f(E) = s(E) \subseteq E$. Quindi $E = C$ per la proprietà di C di essere il più piccolo elemento di $\mathcal{A}$. Quindi la coppia (C, s) soddisfa gli assiomi di Peano. Ora come $h : C \to X$ possiamo prendere l'inclusione. □

Teorema 2.12 *Un insieme X è infinito se e solo se esiste un'applicazione iniettiva $h : \mathbb{N} \to X$.*

Dimostrazione. Se X è infinito, la tesi segue dalla dimostrazione teorema precedente (vedi anche l'Esercizio 6.38). Supponiamo che esista un'applicazione iniettiva $h : \mathbb{N} \to X$. Allora possiamo scrivere $X = h(\mathbb{N}) \cup Y$, dove $Y = X \setminus h(\mathbb{N})$. Sia $s : \mathbb{N} \to \mathbb{N}$ l'applicazione definita da $s(n) = n + 1$. Allora l'applicazione $f : X \to X$, che coincide con $h \circ s \circ h^{-1}$ su $h(\mathbb{N})$ ed è l'identità su Y, è iniettiva, ma non suriettiva. □

2.3 Composizione di applicazioni

Siano $f : X \to Y$ e $g : Y \to Z$ due applicazioni tali che il dominio di g coincide con il codominio di f. La *composizione* di f e g è l'applicazione $g \circ f : X \to Z$ definita da $(g \circ f)(x) = g(f(x))$ per ogni $x \in X$. La composizione $g \circ f$ è detta spesso anche *applicazione composta* (o *applicazione prodotto*) di f per g.
Vediamo ora come la composizione di applicazioni preservi la proprietà di essere iniettiva o suriettiva.

Lemma 2.13 *Siano $f : X \to Y$ e $g : Y \to Z$ due applicazioni.*

(1) se f e g sono suriettive, allora anche $g \circ f$ è suriettiva;

(2) se f e g sono iniettive, allora anche $g \circ f$ è iniettiva.

DIMOSTRAZIONE. i) Per dimostrare la suriettività di $g \circ f$, prendiamo un elemento $z \in Z$ del codominio e vogliamo dimostrare che esiste $x \in X$ tale che $g(f(x)) = z$. Poiché g è suriettiva, esiste $y \in Y$ tale che $g(y) = z$. Inoltre poiché f è suriettiva, esiste $x \in X$ tale che $y = f(x)$. Pertanto sostituendo y nella precedente uguaglianza, otteniamo proprio $z = g(y) = g(f(x))$, cioè $z = (g \circ f)(x)$.
ii) Per dimostrare che $g \circ f$ è iniettiva, supponiamo $(g \circ f)(x) = (g \circ f)(y)$ e mostriamo che allora $x = y$. Dal fatto che g è iniettiva e che $g(f(x)) = g(f(y))$, otteniamo $f(x) = f(y)$. Dal fatto che pure f è iniettiva, otteniamo ora $x = y$. □

Possiamo parzialmente invertire questo risultato. In generale non è vero che se $g \circ f$ è iniettiva o suriettiva allora anche g ed f lo sono. Infatti

Esempio 2.14 Sia $X = \mathbb{R} \setminus \{0\}$ e sia $f : X \to X$ definita da $f(x) = x^2$. Sia ora $g : X \to \mathbb{R}$ definita da $g(y) = \log(|y|)$. Allora $g \circ f$ è suriettiva, ma f non è suriettiva.

Esempio 2.15 Sia $f : \mathbb{N} \to \mathbb{Z}$ la funzione *immersione*, cioè $f(x) = x$ e sia $g : \mathbb{Z} \to \mathbb{Z}$ la funzione $g(x) = x^2$. Allora $g \circ f$ è iniettiva, mentre g non lo è.

Vediamo quindi come possiamo invertire il risultato precedente.

Lemma 2.16 *Siano $f : X \to Y$ e $g : Y \to Z$ due applicazioni.*

(1) se $g \circ f$ è suriettiva, allora anche g è suriettiva;*

(2) se $g \circ f$ è iniettiva, allora anche f è iniettiva.*

DIMOSTRAZIONE. (1*) Se $g \circ f$ è suriettiva, per ogni $z \in Z$ esiste $x \in X$ tale che $(g \circ f)(x) = g(f(x)) = z$. Sia dunque $y = f(x)$, allora $g(y) = g(f(x)) = z$. Questo dimostra che g è suriettiva.
(2*) Siano $x, y \in X$ tali che $f(x) = f(y)$. Allora $(g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y)$. Dalla iniettività di $g \circ f$, otteniamo $x = y$. □

Definizione 2.17 Un applicazione $f : X \to Y$ si dice *invertibile*, se esiste un applicazione $g : Y \to X$ tale che $g(f(x)) = x$ per ogni $x \in X$ e $f(g(y)) = y$ per ogni $y \in Y$.

L'applicazione g di questa definizione di dice *inversa di* f. Un'applicazione $g : Y \to X$ è inversa dell'applicazione $f : X \to Y$ se e solo se $g \circ f = id_X$ e $f \circ g = id_Y$. Si vede facilmente dalla definizione, che l'applicazione inversa di un'applicazione invertibile f è unica. Infatti se g' fosse un'altra inversa, allora per ogni $y \in Y$ si avrebbe $g(y) = x = g'(y)$ per l'unico $x \in X$ con $f(x) = y$; pertanto $g' = g$. Denoteremo con f^{-1} tale unica inversa.

Lemma 2.18 *Ogni applicazione biiettiva è invertibile.*

DIMOSTRAZIONE. Sia $f : X \to Y$ un applicazione biiettiva. Per ogni $y \in Y$ esiste $x \in X$ tale che $f(x) = y$, poiché f è suriettiva. In più, tale x è unico perché f è anche iniettiva. Poniamo $g(y) = x$. Adesso è chiaro che $f(g(y)) = f(x) = y$ per ogni $y \in Y$ per la definizione di g. D'altra parte, per ogni $x \in X$ si ha $g(f(x)) = x$ sempre per la definizione di g. □

Teorema 2.19 *Un'applicazione è invertibile se e solo se è biiettiva.*

DIMOSTRAZIONE. Sia $f : X \to Y$ un'applicazione. Abbiamo dimostrato nel Lemma 2.18 che se f è biiettiva, allora f è invertibile. Ora resta da vedere che se f è invertibile, allora f è biiettiva. Per ipotesi esiste un'applicazione $g : Y \to X$ tale che $g \circ f = id_X$ e $f \circ g = id_Y$. Per l'esempio 2.7 $g \circ f$ è iniettiva, quindi per (2^*) del Lemma 2.16 concludiamo che f è iniettiva. Analogamente, l'Esempio 2.7 ci garantisce che $f \circ g$ è suriettiva, quindi per (1^*) del Lemma 2.16 concludiamo che f è suriettiva. Essendo iniettiva e suriettiva, f risulta biiettiva. □

Le applicazioni biiettive $X \to X$ di un insieme X si dicono anche *permutazioni* di X.

Esercizio 2.20 *Verificare che il numero di tutte le applicazioni iniettive di un insieme finito X con n elementi in un insieme Y con m elementi è uguale a $m \cdot (m-1) \cdot \ldots \cdot (m-n+1)$.*

SVOLGIMENTO. Prima di cominciare notiamo che l'asserto è banalmente vero per $m < n$, perché in tal caso non ci sono applicazioni iniettive di X in Y, mentre il numero $m \cdot (m-1) \cdot \ldots \cdot (m-n+1)$ è uguale a 0 essendo il fattore $(m-m) = 0$. Pertanto, assumeremo nel seguito che $m \geq n$.
Poiché X è un insieme finito, possiamo numerare i suoi elementi, cioè $X = \{x_1, x_2, ..., x_n\}$. Allora contiamo quali sono le possibili immagini di x_1 in Y tramite una applicazione iniettiva. Possiamo scegliere tra tutti gli m elementi di Y. Ci sono pertanto m scelte. Ora l'immagine di x_2 può essere un qualsiasi elemento di Y, eccetto l'immagine di x_1, perché l'applicazione deve essere iniettiva. Pertanto si hanno $m-1$ scelte per l'immagine di x_2. Proseguendo in questo modo, le possibili scelte per le immagini dell'elemento x_i (una volta scelte le immagini degli elementi x_j, $1 \leq j < i$) sono $m(m-1)(m-2)...(m-i+1)$. Concludiamo con x_n, da cui segue l'enunciato. □

Questo esercizio dà subito come corollario:

Esercizio 2.21 *Sia X un insieme finito con n elementi. Si dimostri che il numero di tutte le permutazioni di X è $n! = 1 \cdot 2 \cdot \ldots \cdot n$.*

Esercizio 2.22 *Sia f una funzione da un insieme A in sé. Si supponga che $f \circ f \circ f = id_A$. Si può concludere che f è biiettiva?*

SVOLGIMENTO. $f \circ (f \circ f) = id_A$ implica che f è suriettiva e che $f \circ f$ è iniettiva, quindi nuovamente f è iniettiva. Allora f è biiettiva. □

Esercizio 2.23 *Sia f una funzione da un insieme A in sé e sia $f_* : \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$ la funzione così definita $f_*(B) = f(B) = \{f(b) : b \in B\}$. Si provi che*

(a) f è iniettiva se e solo se f_* è iniettiva,

(b) f è suriettiva se e solo se f_* è suriettiva.

SVOLGIMENTO. a) Supponiamo che f_* sia iniettiva. Siano $a, b \in A$ tali che $f(a) = f(b)$, allora $f_*(\{a\}) = f(\{a\}) = \{f(a)\} = \{f(b)\} = f(\{b\}) = f_*(\{b\})$. Poiché f_* è iniettiva, si avrà $\{a\} = \{b\}$ e quindi $a = b$.
Sia ora f iniettiva. Supponiamo $f_*(B) = f_*(C)$, con $B, C \in \mathcal{P}(A)$. Supponiamo per assurdo che B non sia contenuto in C. Allora esiste un elemento $b \in B \setminus C$. Poiché $f(b) \in f(B) = f_*(B) = f_*(C) = f(C)$, esiste un elemento $c \in C$ tale che $f(b) = f(c)$, da cui $b = c \in C$, in

contraddizione con quanto supposto. Quindi $B \subseteq C$ e analogamente si prova $C \subseteq B$, da cui la tesi $B = C$.
b) Supponiamo f_* suriettiva. Sia $y \in A$, considero $C = \{y\}$, esiste B tale che $f(B) = C$, con $B \neq \emptyset$. Pertanto esiste $b \in B$ tale che $f(b) = c$.
Sia ora f suriettiva e $C \subseteq A$. Allora $f^{-1}(C) \neq \emptyset$ e pertanto $f(f^{-1}(C)) = f_*(f^{-1}(C)) = C$. □

Esercizio 2.24 *Sia $f : X \longrightarrow Y$ una funzione e $B \subseteq Y$.*
a) Si provi che $f(f^{-1}(B)) \subseteq B$,
b) Si costruisca un esempio per cui $f(f^{-1}(B)) \neq B$.
c) Quando vale $f(f^{-1}(B)) = B$?

Svolgimento. a) Sia $x \in f^{-1}(B)$, allora, per definizione di immagine inversa, si ha che $f(x) \in B$.
b) Basta prendere una funzione non suriettiva, per esempio $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ tale che $f(x) = x^2$ e un insieme non contenuto nell'immagine di f, per esempio $B = \{1, 2\}$. Allora $f^{-1}(B) = \{1, -1\}$ e $f(f^{-1}(B)) = \{1\} \neq B$.
c) Quando f è suriettiva. Se $b \in B$, esiste $x \in A$ tale che $b = f(x)$ e quindi $x \in f^{-1}(B)$. □

Esercizio 2.25 *Sia A insieme e B sottoinsieme di A, $\emptyset \neq B \neq A$.*
Sia $f : \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$ la funzione così definita $f(X) = B \setminus X$ per ogni $X \in \mathcal{P}(A)$.
a) Si provi che f non è né iniettiva né suriettiva,
b) si descriva $f^{-1}(\{B\})$.

Svolgimento. a) f non è suriettiva perché $f(X) \subseteq B$, pertanto $f(X) \neq A$, per ogni $X \in \mathcal{P}(A)$. f non è iniettiva perché $A \neq B$ e $f(A) = \emptyset = f(B)$.
b) $f^{-1}(\{B\}) = \mathcal{P}(A \setminus B)$. □

Esercizio 2.26 *Sia A insieme e B sottoinsieme di A, $\emptyset \neq B \neq A$.*
Sia $f : \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$ la funzione così definita $f(X) = B \cap X$.
a) f è iniettiva?
b) f è suriettiva? Se no, se ne trovi l'immagine.
c) si descriva $f^{-1}(\{B, A, \emptyset\})$.

Svolgimento. a) No, perché $A \neq B$ e $f(A) = B = f(B)$.
b) No, perché $f(X) \subseteq B$ e quindi $A \neq f(X)$ per ogni $X \in \mathcal{P}(A)$. Allora $f(\mathcal{P}(A)) \subseteq \mathcal{P}(B)$, ma anzi coincidono poiché se $X \in \mathcal{P}(B)$ si ha $f(X) = X$.
c) $f^{-1}(B) = \{X \in \mathcal{P}(A) : X \supseteq B\}$, $f^{-1}(A) = \emptyset$, $f^{-1}(\emptyset) = \{X \in \mathcal{P}(A) : X \cap B = \emptyset\} = \mathcal{P}(A \setminus B)$. □

Esercizio 2.27 *i) Siano $f_1 : X \to Y$ e $f_2 : X \to Y$ due funzioni. Sia $g : Y \to Z$ una funzione iniettiva, allora g è* cancellabile a sinistra*, cioè se $g \circ f_1 = g \circ f_2$, allora $f_1 = f_2$.*

ii) Siano $g_1 : Y \to Z$ e $g_2 : Y \to Z$ due funzioni. Sia $f : X \to Y$ una funzione suriettiva, allora f è cancellabile a destra*, cioè se $g_1 \circ f = g_2 \circ f$, allora $g_1 = g_2$.*

Svolgimento. i) Per ipotesi $(g \circ f_1)(x) = g(f_1(x)) = g(f_2(x)) = (g \circ f_2)(x)$ per ogni $x \in X$. Poiché g è iniettiva, si deduce $f_1(x) = f_2(x)$ per ogni $x \in X$, che prova $f_1 = f_2$.
ii) Per ipotesi $(g_1 \circ f)(x) = g_1(f(x)) = g_2(f(x)) = (g_2 \circ f)(x)$ per ogni $x \in X$. Sia ora $y \in Y$, allora, poiché f è suriettiva, esiste $x \in X$ tale che $y = f(x)$ e quindi $g_1(y) = g_1(f(x)) = g_2(f(x)) = g_2(y)$. Questo prova $g_1 = g_2$. □

Esercizio 2.28 *Sia $f: X \to Y$ un'applicazione. Allora f è iniettiva se e solo se esiste una funzione $g: Y \to X$ tale che $g \circ f = id_X$.*

SVOLGIMENTO. Se esiste una funzione $g: Y \to X$ tale che $g \circ f = id_X$, allora nuovamente f è iniettiva per il Lemma 2.16, dato che id_Y è iniettiva. Supponiamo pertanto che f sia iniettiva. Poiché nella definizione di applicazione si suppone che X non sia vuoto, esiste $x_0 \in X$. Inoltre, poiché f è iniettiva, per ogni $y \in f(X)$ esiste un unico $x \in X$ tale che $f(x) = y$. Definiamo pertanto $g: Y \to X$ ponendo $g(y) = g(f(x)) = x$ se $y = f(x) \in f(X)$ e $g(y) = x_0$, se $y \notin f(X)$. Allora $g(f(x)) = x$ per ogni $x \in X$. $\square$

La controparte di questo esercizio che caratterizza le applicazioni suriettive sarà dimostrata più tardi

Esercizio 2.29 *Sia $f: \mathbb{R} \to \mathbb{R}$ l'applicazione definita da*
$f(x) = \begin{cases} x + \frac{x+1}{x-1}, & \text{se } x \neq 1 \\ 0 \text{ se } & x = 1. \end{cases}$
Si determini se f è iniettiva e se f è suriettiva.

2.4 Relazioni di equivalenza

Definizione 2.30 Una relazione binaria R su un insieme X si dice *relazione di equivalenza*, se sono verificate le seguenti proprietà:
1) (riflessiva) $(x, x) \in R$ per ogni $x \in R$;
2) (simmetrica) $(x, y) \in R$ implica $(y, x) \in R$ per ogni coppia $x, y \in X$;
3) (transitiva) $(x, y) \in R$ e $(y, z) \in R$ implicano $(x, z) \in R$ per ogni terna $x, y, z \in X$;

Nel seguito scriveremo brevemente xRy al posto di $(x, y) \in R$.

Ogni relazione di equivalenza R definisce le *classi di equivalenza* $[a]_R$, per $a \in X$, nel modo seguente:

$$[a]_R = \{x \in X : xRa\}.$$

Si noti che $a \in [a]_R$ per la proprietà 1), pertanto le classi $[a]_R$ sono non vuote. Se due classi di equivalenza $[a]_R$ e $[b]_R$ hanno elementi in comune, allora esse coincidono. Infatti, supponiamo che $[a]_R \cap [b]_R \neq \emptyset$. Poiché ogni $x \in [a]_R$ soddisfa xRz, dove $z \in [a]_R \cap [b]_R$, e quindi xRb e $x \in [b]_R$; analogamente si dimostra che $[b]_R \subseteq [a]_R$. Quindi risulta una partizione di X in classi di equivalenza (vedi la definizione 1.11)

$$X = \bigcup_{a \in X} [a]_R.$$

Proviamo anzi che questo risultato si può invertire.

Teorema 2.31 *Esiste una corrispondenza biunivoca tra le relazioni di equivalenza definite su un insieme X e le partizioni di X.*

DIMOSTRAZIONE. Abbiamo già dimostrato che ogni relazione di equivalenza su X definisce una partizione di X. Supponiamo ora di avere una partizione $\mathcal{L} = \{X_i : i \in I\}$ di X. Definiamo una relazione di equivalenza su X nel modo seguente: $xR_{\mathcal{L}}y$ se e solo se $x, y \in X_i$ per uno stesso insieme X_i di $\mathcal{L}$. Vediamo che tale relazione è di equivalenza.
-riflessiva: poiché $\mathcal{L}$ è una partizione, ogni elemento $x \in X$ appartiene a qualche X_i, $i \in I$, quindi $xR_{\mathcal{L}}x$.

-simmetrica: se $xR_{\mathcal{L}}y$, allora x, y appartengono allo stesso insieme X_i, pertanto vale anche $yR_{\mathcal{L}}x$.
-transitiva: se $xR_{\mathcal{L}}y$ e $yR_{\mathcal{L}}z$, allora $x, y \in X_i$ per qualche $i \in I$ e $y, z \in X_j$ per qualche $j \in I$. Poiché $\mathcal{L}$ è una partizione, avremo $X_i \cap X_j = \emptyset$ se $i \neq j$. Nel nostro caso $y \in X_i \cap X_j$, che non può pertanto essere vuota. Allora $i = j$ e $x, y, z \in X_i$, quindi $xR_{\mathcal{L}}z$.
Ora, data un'equivalenza R, si consideri la partizione in classi di equivalenza $\mathcal{L}_R = \{[a]_R : a \in X\}$ definita prima. Allora la relazione di equivalenza $R_{\mathcal{L}_R}$ costruita a partire da $\mathcal{L}_R$ coincide con R: infatti $aR_{\mathcal{L}_R}b$ se e solo se $a, b \in [a]_R$ se e solo se aRb. D'altra parte, per ogni partizione $\mathcal{L}$ di X la relazione di equivalenza $R_{\mathcal{L}}$ genera, tramite le sue classi di equivalenza, la partizione di partenza $\mathcal{L}$. Questo conclude la dimostrazione. □

Esempio 2.32 Sia $f : X \to Y$ un'applicazione. Allora la relazione binaria R_f definita da

$$xR_fy \text{ se e solo se } f(x) = f(y)$$

è una relazione di equivalenza.

Ora vedremo che ogni relazione di equivalenza su un insieme X può essere di questa forma.

Teorema 2.33 *Sia X un insieme non vuoto e sia R una relazione di equivalenza su X. Allora esiste un'applicazione $f : X \to Y$ tale che R coincide con la relazione R_f.*

Dimostrazione. Sia Y l'insieme delle classi di equivalenza $\{[x]_R : x \in X\}$. Definiamo $f : X \to Y$ con $f(x) = [x]_R$. Non è difficile verificare che $R = R_f$. □

L'insieme delle classi di equivalenza $\{[x]_R : x \in X\}$ si dice *insieme quoziente di X modulo la relazione di equivalenza R* e si denota con X/R.

Esercizio 2.34 *Calcolare il numero delle relazioni di equivalenza su un insieme di 2,3,4 o 5 elementi.*

Suggerimenti. Grazie al Teorema 2.31, è sufficiente calcolare il numero delle partizioni su un insieme di 2,3,4 o 5 elementi. Si lasciano al lettore i primi 3 casi (le risposte sono 2,5 e 15 rispettivamente). Sia ora $X = \{a, b, c, d, e\}$. Contiamo le partizioni di X:
- 1 del tipo $\{\{a\}, \{b\}, \{c\}, \{d\}, \{e\}\}$;
- 1 del tipo $\{a, b, c, d, e\}$,
- 5 del tipo $\{\{a\}, \{b, c, d, e\}\}$,
- 10 del tipo $\{\{a, b\}, \{c, d, e\}\}$,
- 10 del tipo $\{\{a\}, \{b\}, \{c, d, e\}\}$,
- 15 del tipo $\{\{a, b\}, \{c, d\}, \{e\}\}$,
- 10 del tipo $\{\{a, b\}, \{c\}, \{d\}, \{e\}\}$;

per un totale di 52 partizioni e relazioni di equivalenza. □

2.5 Partizioni e coefficienti binomiali

Ci proponiamo adesso di calcolare il numero di tutte le partizioni di un insieme X di n elementi. Per avere una visione più chiara della situazione vediamo ogni partizione di X come una colorazione di X (in altre parole, vedremo classi di equivalenza come "colori")

Il mondo in bianco e nero. Sia $n \geq 1$ un numero naturale e sia X un insieme di n elementi. Allora il numero di tutte le colorazioni di X in due colori, bianco e nero, è uguale

a 2^n. Infatti ogni colorazione di X si potrebbe considerare come applicazione $\mathbf{c} : X \to \mathcal{C}$, dove $\mathcal{C}$ è l'insieme dei due colori $\{bianco, nero\}$ in modo di poter vedere il valore $\mathbf{c}(x)$ assunto in $x \in X$ come il colore (bianco o nero) di x. Notiamo che ogni colorazione $\mathbf{c}$ di X è completamente determinata dall'insieme $B_\mathbf{c} = \{x \in X : \mathbf{c}(x) = bianco\}$ dei punti bianchi di $\mathbf{c}$ poiché l'insieme $N_\mathbf{c} = \{x \in X : \mathbf{c}(x) = nero\}$ dei punti neri di $\mathbf{c}$ è precisamente il complemento $X \setminus B_\mathbf{c}$ di $B_\mathbf{c}$ (per chi preferisce vedere il mondo in nero, aggiungiamo, che anche l'insieme $N_\mathbf{c}$ determina completamente la colorazione $\mathbf{c}$). Inoltre, le colorazioni costanti sono le due colorazioni monocolore:

(1) $\mathbf{b} : X \to \mathcal{C}$ con $B_\mathbf{b} = X$ e $N_\mathbf{b} = \emptyset$ (cioè tutto bianco)

(2) $\mathbf{n} : X \to \mathcal{C}$ con $N_\mathbf{n} = X$ e $B_\mathbf{n} = \emptyset$ (cioè tutto nero).

Le colorazioni suriettive sono quelle che hanno effettivamente tutti e due i colori (cioè non sono monocolore) e sono quindi $2^n - 2$.
Osserviamo che ad ogni colorazione $\mathbf{c}$ in due colori corrisponde una partizione di X in due parti disgiunte $B_\mathbf{c}$ e $N_\mathbf{c}$, ma ad ogni partizione di X in due insiemi disgiunti Y e Z corrispondono *due* colorazioni di X che danno la partizione $X = Y \cup Z$. Per ogni k con $0 \leq k \leq n$ il numero delle colorazioni $\mathbf{c}$, con insieme "bianco" $B_\mathbf{c}$ consistente precisamente di k elementi, è uguale al numero delle k-uple non ordinate in X, che denoteremo nel seguito con C_k^n. In particolare, $C_0^n = C_n^n = 1$. Notiamo che se l'insieme "bianco" $B_\mathbf{c}$ ha k elementi, allora l'insieme "nero" $N_\mathbf{c}$ consiste di $n-k$ elementi. Analogamente, il numero delle colorazioni $\mathbf{c}$, con insieme "nero" $N_\mathbf{c}$ di k elementi, è uguale a C_k^n. Poiché le colorazioni con k elementi bianchi sono precisamente le colorazioni con $n - k$ elementi neri, si ricava l'uguaglianza

$$C_k^n = C_{n-k}^n. \tag{1}$$

La formula

$$C_k^n = C_k^{n-1} + C_{k-1}^{n-1}. \tag{2}$$

si ricava contando le colorazioni con k elementi bianchi di X fissando un elemento $x_0 \in X$. Presentando X come $X' \cup \{x_0\}$ (dove X' è il complemento di $\{x_0\}$ in X) vediamo che ci sono C_k^{n-1} colorazioni di X con k elementi bianchi in X' (cioè diversi da x_0) e C_{k-1}^{n-1} colorazioni con k elementi bianchi di cui uno è x_0 (queste corrispondono alle colorazioni di X' con $k-1$ elementi bianchi). Alla fine, ponendo come sempre $0! = 1$, si può dimostrare che

$$C_k^n = \frac{n!}{k! \cdot (n-k)!} \tag{3}$$

per induzione su n. (Per $n = 1$ è ovvio, se $n > 1$ si supponga (3) vera per $n-1$ e si applichi (2).) Il numero C_k^n va chiamato anche *coefficiente binomale* e denotato anche con $\binom{n}{k}$ (ma per motivi tipografici qui preferiamo la forma C_k^n). Il nome "coefficiente binomiale" proviene dalla formula *binomiale*

$$(a+b)^n = \sum_{k=0}^{n} C_k^n a^{n-k} b^k \tag{4}$$

che si dimostra facilmente per induzione applicando (2). Ponendo in (4) $a = -b = 1$ si ha

$$\sum_{k=0}^{n} (-1)^k C_k^n = 0. \tag{5}$$

I coefficienti binomiali si possono disporre in un triangolo illimitato (*triangolo di Tartaglia–Pascal*) dove (1) e (2) hanno un interpretazione geometrica elegante:

$$
\begin{array}{ccccccccccc}
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
. & . & . & . & . & . & . & . & . & . & .
\end{array}
$$

Il primo e l'ultimo coefficiente binomiale su ogni riga del triangolo sono uguali a 1, mentre ogni coefficiente binomiale all'interno del triangolo è somma dei due coefficienti binomiali che gli stanno immediatamente sopra.

Abbiamo calcolato il numero $V_m^n = n(n-1)\dots(n-m+1) = m! \cdot C_m^n$ di tutte le applicazioni iniettive di un insieme finito X con n elementi in un insieme Y con $m > n$ (vedi l'Esercizio 2.20). ,

2.6 Relazioni di ordine e preordine

Definizione 2.35 Una relazione binaria R in un insieme X si dice *relazione di preordine*, se R è riflessiva e transitiva.

Chiaramente, ogni relazione di equivalenza è anche una relazione di preordine. Più precisamente, una relazione di preordine è una relazione di equivalenza se e solo se è simmetrica.

Definizione 2.36 Una relazione di preordine R in un insieme X si dice *relazione di ordine*, se è verificata anche la seguente proprietà

- (antisimmetrica) $(x, y) \in R$ e $(y, x) \in R$ implicano $x = y$ per ogni coppia $x, y \in X$.

Esempio 2.37 Sia X un insieme non vuoto. Allora:
a) la relazione $A \leq B$ in $\mathcal{P}(X)$ definita da

$$A \leq B \text{ se e solo se } B \subseteq A$$

è una relazione di ordine.
b) la relazione $A \preceq B$ in $\mathcal{P}(X)$ definita da

$$A \preceq B \text{ se e solo se la differenza } B \setminus A \text{ è finita}$$

è una relazione di preordine.

Una relazione di (pre)ordine si denota al solito con $\leq$, $\prec$ ecc. Un insieme dotato di una relazione d'ordine si dice un *insieme ordinato* e due elementi x, y di un insieme ordinato $(X, \leq)$ si dicono *confrontabili* se $x \leq y$ oppure $y \leq x$.

Definizione 2.38 Sia $\leq$ un ordine su di un insieme X e Y un sottoinsieme non vuoto di X.

- l'ordine $\leq$ si dice *totale*, se per ogni coppia $x, y \in X$ vale $x \leq y$ o $y \leq x$.
- un elemento $y \in Y$ si dice *minimo di* Y, se $y \leq z$ per ogni $z \in Y$; analogamente un elemento y di Y si dice *massimo di* Y, se $y \geq z$ per ogni $z \in Y$;

- un elemento $y \in Y$ si dice *minimale di* Y, se per ogni $z \in Y$ si ha che $z \leq y$ implica $y = z$; analogamente un elemento y di Y si dice *massimale di* Y, se per ogni $z \in Y$ si ha che $y \leq z$ implica $y = z$;

- un elemento $y \in Y$ si dice *minorante di* Y, se per ogni $z \in Y$ si ha che $y \leq z$; analogamente un elemento y di Y si dice *maggiorante di* Y, se per ogni $z \in Y$ si ha che $z \leq y$;

- un elemento x di X si dice *estremo inferiore di* Y *in* X, se x è il massimo dei minoranti di Y; analogamente un elemento x di X si dice *estremo superiore di* Y *in* X, se x è il minimo dei maggioranti di Y;

- l'ordine $\leq$ si dice *buono*, se ogni sottoinsieme non vuoto Y di X ha un elemento minimo.

Esercizio 2.39 *Dimostrare che ogni insieme non vuoto parzialmente ordinato e finito ammette elementi massimali ed elementi minimali.*

SUGGERIMENTI. Ragionare per induzione. □

Esercizio 2.40 *Sia $\leq$ un ordine su un insieme X e Y un sottoinsieme non vuoto di X. Si provi che:*
a) se Y ha un minimo (massimo), esso è unico;
b) se Y ha un estremo superiore (inferiore) in X, esso è unico.

SVOLGIMENTO. a) Sia a un minimo di X. Se b è un altro minimo, allora $a \leq b$ e $b \leq a$, e pertanto per la proprietà antisimmetrica $a = b$.
b) segue da a) e dalla definizione di estremo superiore (inferiore). □

Esercizio 2.41 *Si provi che se A è totalmente ordinato e $a \in A$, allora a è massimo di A se e solo se a è un elemento massimale di A.*

SVOLGIMENTO. Se a è massimo, $a \geq x$ per ogni $x \in A$, pertanto se si ha $a \leq b$ si conclude che $a = b$, cioè massimale.
Viceversa supponiamo a massimale. Sia b un elemento di A, poiché l'ordine è totale $a \leq b$ oppure $b \leq a$. Se $a \leq b$, dal fatto che a è massimale si deduce che $a = b$, pertanto in ogni caso si ha $b \leq a$. □

Esercizio 2.42 *Sia $\mathbb{N}$ l'insieme dei numeri naturali. Si dimostri che $\mathbb{N}$ con la relazione di divisione ($n|m$ se e solo se esiste $r \in \mathbb{N}$ tale che $m = rn$) è un insieme parzialmente ordinato che ammette massimo e minimo.*

SVOLGIMENTO. Riflessiva: $n|n$ perché $n = 1n$,
antisimmetrica: $n|m$ e $m|n$ implicano $m = rn = r(qm)$, cioè $rq = 1$ e $r, q \in \mathbb{N}$ implicano $r = q = 1$, cioè $m = n$,
transitiva: $n|m$ e $m|l$ implicano $l = qm = q(rn) = (rq)n$, cioè $n|l$.
Il minimo deve essere un elemento x di $\mathbb{N}$ tale che $x|n$ per ogni $n \in \mathbb{N}$, cioè $x = 1$. Il massimo y invece deve essere tale che $n|y$ per ogni $n \in \mathbb{N}$, cioè $y = 0$. □

Sia $(A, \leq)$ un insieme parzialmente ordinato. Un sottoinsieme C di A si dice una *catena*, se $(C, \leq)$ è totalmente ordinato. La *lunghezza* della catena C è il numero cardinale $|C|$.

Esercizio 2.43 *Individuare tutte le catene di lunghezza 4 nell'insieme ordinato per divisibilità di tutti i divisori di 20. Dimostrare che le catene di lunghezza 2 sono 12.*

SUGGERIMENTI. Le catene di lunghezza 4 sono tre: $\{1, 2, 4, 20\}$, $\{1, 2, 10, 20\}$ e $\{1, 5, 10, 20\}$. Infine notiamo che tra tutte le coppie (non ordinate!) di due divisori distinti di 20, solo $\{2, 5\}$, $\{5, 4\}$ e $\{4, 10\}$ non formano una catena. □

2.7 Reticoli

Definizione 2.44 Un insieme ordinato $(X, \leq)$ si dice *reticolo* se per ogni coppia $a, b \in X$ l'insieme $\{a, b\}$ ammette estremo superiore, denotato con $a \vee b$, e estremo inferiore, denotato con $a \wedge b$.
Se X ha anche elemento minimo e massimo, essi si denotano solitamente con 0 e 1, rispettivamente. In tal caso il reticolo si dice *limitato* e si denota con $(L, \wedge, \vee, 0, 1)$.

Ogni insieme totalmente ordinato è banalmente un reticolo.

Esercizio 2.45 *Dimostrare che ogni reticolo finito è limitato.*

Esercizio 2.46 *Sia X un insieme non vuoto. L'insieme parzialmente ordinato $(\mathcal{P}(X), \subseteq)$ è un reticolo limitato.*

Esercizio 2.47 *Sia $(X, \leq)$ un reticolo, allora sull'insieme X^X definiamo un ordine parziale nel modo seguente:*

$$f, g \in X^X \quad f \prec g \quad \Longleftrightarrow \quad f(x) \leq g(x) \quad \textit{per ogni} \quad x \in X.$$

Si dimostri che $(X^X, \prec)$ è un reticolo.

SVOLGIMENTO. Dimostriamo che dati due elementi f, g di X^X, questi ammettono massimo e minimo. Definiamo la funzione $h(x) = f(x) \vee g(x)$: è ben definita perché X è un reticolo e $f(x), g(x)$ sono due elementi del reticolo. Allora $h = f \vee g$. Analogamente per l'estremo inferiore. □

Esercizio 2.48 *Sia $(X, \leq)$ un reticolo e a un suo elemento massimale, allora a è massimo.*

SVOLGIMENTO. Se a è massimale, allora se $a \leq x$, si ha $a = x$ per ogni $x \in X$. Sia dunque $z \in X$ e sia $b = a \vee z$. Allora $b \geq a$, quindi $a = b$, cioè $a \geq z$. Concludiamo che a è massimo. □

Esercizio 2.49 *Dimostrare che l'insieme ordinato $(\mathbb{N}^*, |)$ è un reticolo. E' limitato?*

SVOLGIMENTO. Si ha $n \wedge m = M.C.D.(m, n)$ e $n \vee m = m.c.m.(n, m)$ in entrambi casi. $(\mathbb{N}^*, |)$ non è limitato perché non ammette massimo che avevamo dimostrato essere lo zero di $\mathbb{N}$. □

Esercizio 2.50 *Si dia un esempio di un reticolo che ha un sottoinsieme ordinato che non è un reticolo.*

SVOLGIMENTO. Consideriamo l'insieme Y di tutti i divisori di 15, ordinato per divisibilità: $Y = \{1, 3, 5, 15\}$ e $a \preceq b$ se e solo se $a|b$. $(Y, |)$ è un reticolo e non è totalmente ordinato perché $3 \not| 5$ e $5 \not| 3$. Il sottoinsieme parzialmente ordinato $X = \{3, 5\}$ non è un reticolo perché $3 \vee 5 = 15$ non esiste in X. □

3 I numeri interi e l'aritmetica

L'insieme dei numeri interi $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}$ è il sistema numerico che si impara ad usare fin dalle scuole inferiori, così come l'addizione e la moltiplicazione definite su $\mathbb{Z}$. Riterremo pertanto note le proprietà delle due operazioni fondamentali, che verranno comunque riprese in seguito, e anche la relazione di $\leq$ (*minore o uguale di*) in base alla quale $\mathbb{Z}$ viene *ordinato linearmente*.

La divisione in $\mathbb{Z}$: Dati due numeri interi a e b si dice che a *divide* b (o, a *è divisore di* b) se esiste $c \in \mathbb{Z}$ tale che $b = ac$ e scriviamo $a|b$. Chiaramente,
a) $a|0$ per ogni $a \in \mathbb{Z}$, mentre $0|a$ solo per $a = 0$.
b) $\pm 1|b$ e $\pm b|b$ per ogni $b \in \mathbb{Z}$.
Allora "a divide b" definisce una relazione binaria in $\mathbb{Z}$ che scriveremo $a|b$. Se $a|b$, diremo che a è *divisore di* b.
Se $a|b$ e $b|a$ diremo che a *è associato a* b e lo denoteremo con $a \sim b$. È facile vedere che $\sim$ è una relazione di equivalenza in $\mathbb{Z}$. L'insieme $\{1, -1\}$ coincide con la classe di equivalenza di 1. Più in generale, la classe di equivalenza di $a \in \mathbb{Z}$ coincide con $\{a, -a\}$, ovvero $b \sim a$ se e solo se $b = \pm a$. Poiché ogni $b \in \mathbb{Z}$ ha come divisori $a = \pm 1$ e $a = \pm b$, questi divisori sono chiamati *divisori impropri* di b. Un divisore a di b si dice *proprio* se non è improprio.
Denoteremo con $\mathbb{Z}^*$ l'insieme dei numeri interi non nulli.

3.1 I numeri primi

Un numero $b \in \mathbb{Z}^*$ si dice *primo*, se $p \neq \pm 1$ e p non ha divisori propri. I numeri primi servono come "atomi" dai quali si possono ottenere (in modo unico!) tutti gli altri numeri di $\mathbb{Z}$ tramite moltiplicazioni. É chiaro che un numero intero $m > 1$ non è primo se e solo se $m = ab$ con $1 < a < m$ e $1 < b < m$.
Il seguente metodo, detto *crivello di Eratostene*, consente di determinare i numeri primi minori di un numero assegnato n (ragionevolmente piccolo, nel caso 40). Scriviamo in ordine tutti gli interi da 2 a 40. Il primo intero 2 risulta primo non potendo avere dei divisori propri < 2 nella lista. Mettiamolo nella lista dei primi e cancelliamo poi con un tratto / di penna tutti i numeri pari > 2 (cioè, i multipli di 2 maggiori di 2). Il primo intero che rimane è 3, che risulta primo per lo stesso motivo di 2. Aggiungiamo 3 alla lista dei numeri primi e cancelliamo con un tratto \ di penna tutti i numeri multipli di 3. Il più piccolo intero che rimane, 5, è primo. Aggiungiamo 5 alla lista, cancelliamo poi con tratto — di penna tutti i numeri multipli di 5 e così via.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29
~~30~~ 31 ~~32~~, ~~33~~ ~~34~~ ~~35~~ ~~36~~ ~~37~~ ~~38~~

Così i primi minori di 40 risultano essere $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$ e 37.

Esercizio 3.1 *Determinare i numeri primi minori di 250.*

Per determinare se un numero $a > 0$ è primo, si può controllare se è divisibile per qualche primo minore di a. In realtà basta verificarlo su un insieme più piccolo. Infatti:

Esercizio 3.2 *Se un numero intero $a > 0$ non è primo, allora a ha divisori primi p minori o uguali a $\sqrt{a}$.*

Osserviamo inoltre che il crivello di Eratostene ci permette di dire, al passo corrispondente a p, quali sono i numeri primi fino a $(p + 2)^2 - 1$, se p è un numero primo dispari. Infatti se il più piccolo primo che divide un numero intero a è $q > p$, si avrà $q \geq p + 2$, da cui

$a \geq q^2 > (p+2)^2 - 1$. Quindi, per esempio, considerando solo i primi 11 primi, cioè tutti i primi minori o uguali a 31, si possono calcolare tutti i primi minori di 1000. Ci si può quindi chiedere se questo procedimento può terminare dopo un numero finito di passi, ed ottenere quindi tutti i numeri primi. Il Teorema 3.16 ci dara' la risposta.
Quello che abbiamo fatto finora è stato di capire se certi numeri interi sono primi o no. Vediamo ora come si possono "costruire" numeri primi.

Esercizio 3.3 *Si verifichi che il polinomio $f(x) = x^2 + x + 17$ è un generatore di primi per $x \in \mathbb{N}$, $x \leq 15$.*

Il polinomio definito nel precedente Esercizio 3.3 è un caso particolare di una definizione più generale che vedremo più avanti (vedi l'Esercizio 8.8).

3.2 Massimo comun divisore e minimo comune multiplo

Definizione 3.4 Il *massimo comun divisore* d dei numeri interi a e b è definito come un divisore comune di a e b (cioè $d|a$ e $d|b$) per il quale risulti $d'|d$ per ogni altro divisore comune d' di a e b.

Chiaramente, se d è massimo comun divisore di a e b, lo è anche $-d$. Quindi, il massimo comun divisore è determinato solo a meno del segno. Tuttavia, spesso prendiamo in considerazione il massimo comun divisore *positivo* (a, b) di a e b, che coincide anche con il più grande di tutti i divisori comuni di a e b. Diremo che a e b *sono coprimi* se $(a, b) = 1$.

Definizione 3.5 Il *minimo comune multiplo* m dei numeri interi a e b è definito come un multiplo comune di a e b (cioè, $a|m$ e $b|m$) per il quale risulta $m|m'$ per ogni altro multiplo comune m' di a e b.

Chiaramente, se m è minimo comune multiplo di a e b, lo è anche $-m$. Quindi, il minimo comune multiplo è determinato solo a meno del segno. Tuttavia, spesso prendiamo in considerazione il minimo comune multiplo *positivo* $mcm(a, b)$ di a e b, che coincide anche con il più grande di tutti i multipli comuni di a e b.

Vediamo ora alcune altre proprietà dei divisori e del massimo comun divisore.

Lemma 3.6 *(d_1) Se $c|a$ e $c|b$, allora $c|ka + mb$ per ogni scelta di $k, m \in \mathbb{Z}$.*
(d_2) Se $a|a'$ e $b|b'$, allora $ab|a'b'$.
(d_3) Se $d|a$, $d|b$ e $d = ka + mb$, allora d è massimo comun divisore di a e b (cioè, $d = \pm(a, b)$).
(d_4) Se $d = (a, b)$, allora $a = da_1$ e $b = db_1$, con $a_1, b_1 \in \mathbb{Z}$, coprimi.

Dimostrazione. (d_1) Siano $a = cx$ e $b = cy$, con $x, y \in \mathbb{Z}$. Allora $ka + mb = c(kx + my)$, quindi $c|ka + mb$.
(d_2) Se $a' = ax$ e $b' = by$, allora $a'b' = ab(xy)$. (d_3) Sia d' un divisore comune di a e b. Allora $d'|d$ per il punto (d_1). Quindi d è massimo comun divisore di a e b.
(d_4) Sia $d' = (a_1, b_1)$. Allora $d'|a_1$ e $d'|b_1$, quindi $dd'|da_1 = a$ e $dd'|db_1 = b$ per il punto (d_2). Quindi dd' è un divisore comune di a e b. Quindi $dd'|d$. Poiché $d|dd'$, si conclude che $dd' = \pm d$, cioè, $d' = 1$. □

3.3 La divisione euclidea

Vedremo che una via per stabilire l'esistenza del massimo comune divisore è la proprietà che permette di eseguire la "divisone con resto" (detta anche *divisone euclidea*) nel modo seguente:

Teorema 3.7 *Se $a, b \in \mathbb{Z}$ e $b \neq 0$, possiamo trovare $q, r \in \mathbb{Z}$ tali che $a = q \cdot b + r$ e $0 \leq r < |b|$.*

DIMOSTRAZIONE. Si considera prima il caso $a \geq 0$ e $b > 0$. Allora, per ogni $0 \leq a < b$ possiamo prendere $q = 0$ e $r = a$. Se $a = b$ si prende semplicemente $q = 1$ e $r = 0$. Supponiamo ora $a > b$ e che tali q ed r si possano trovare per $a - 1$, cioè $a - 1 = qb + r$ con $q \in \mathbb{Z}$ e $0 \leq r < b$. Se $r < b - 1$, allora con $0 \leq r' = r + 1 < b$ abbiamo $a = aq + r'$. Se invece $r = b - 1$, allora $a = (q + 1)b$.
Lasciamo al lettore la facile riduzione del caso di a o b negativi al caso $a \geq 0$ e $b > 0$. □

La divisione con resto è rilevante per i numeri interi, ma non per $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, perché essi sono campi, e quindi la divisibilità $b|a$ c'è sempre quando $b \neq 0$ (poiché esiste l'inverso b^{-1} di b e quindi $a = b(b^{-1}a)$).

Teorema 3.8 *Se $a, b \in \mathbb{Z}$ e $b \neq 0$, esiste il massimo comun divisore d di a e b ed ha la forma $d = ua + vb$, con $u, v \in \mathbb{Z}$.*

DIMOSTRAZIONE. Per il Teorema 3.7 esistono $q_1, r_1 \in \mathbb{Z}$ con $a = q_1 \cdot b + r_1$ e $r_1 < b$. Se $r_1 = 0$ abbiamo $b|a$ e quindi $d = b = 0 \cdot a + 1 \cdot b$.
Se $r_1 > 0$ possiamo continuare, esistono $q_2, r_2 \in \mathbb{Z}$ con $b = q_2 \cdot r_1 + r_2$ e $0 \leq r_2 < r_1$. Se $r_2 > 0$ possiamo continuare, esistono $q_3, r_3 \in \mathbb{Z}$ con $r_1 = q_3 \cdot r_2 + r_3$ e $0 \leq r_3 < r_2$; e così via. Si costruiscono in questo modo due successioni di interi

$$q_1, q_2, \ldots, q_k, \ldots, \text{ e } b > r_1 > r_2 > \ldots > r_k > \ldots \qquad (*)$$

tali che

$$r_{s-1} = q_{s+1} r_s + r_{s+1}. \qquad (1)$$

Chiaramente, la successione degli r_k dovrebbe fermarsi allo 0 dopo al più b passi, cioè esiste k con $r_{k+1} = 0$. Allora $r_{k-1} = q_{k+1} r_k$, quindi $r_k | r_{k-1}$. Supponiamo $k - 1 > s > 1$ e $r_k | r_{k-s+1}$ e $r_k | r_{k-s}$, dimostreremo che allora r_k divide anche r_{k-s-1}. Infatti, basta applicare (1), poiché $r_{k-s-1} = q_{k-s+1} r_{k-s} + r_{k-s+1}$ e $r_k | r_{k-s+1}$ e $r_k | r_{k-s}$ per ipotesi. Adesso con $s = k - 2$ e $s = k - 1$ ricaviamo $r_k | r_2$ e $r_k | r_1$. Ma allora $r_k | b = q_2 \cdot r_1 + r_2$ e $r_k | a = q_1 \cdot b + r_1$.
Ora notiamo che $r_1 = a - q_1 b$ è combinazione lineare di a e b con coefficienti interi. Supponiamo che $r_1, \ldots, r_s$ (per $1 \leq s < k$) siano combinazioni lineari di a e b, cioè, per $1 \leq s < k$ esistono $A_s, B_s \in \mathbb{Z}$ tali che $r_s = A_s a + B_s b$. Allora $r_{s+1} = r_{s-1} - q_{s+1} r_s = A_{s+1} a + B_{s+1} b$, dove $A_{s+1} = A_{s-1} - q_{s+1} A_s$ e $B_{s+1} = B_{s-1} - q_{s+1} B_s$. In particolare, con $s = k$, si ha $r_k = A_k a + B_k b$. Allora, per il punto (d_3) del Lemma 3.6 , r_k è massimo comun divisore di a e b. □

Corollario 3.9 *Sia p primo. Se p non divide un numero intero a, allora p e a sono coprimi.*

DIMOSTRAZIONE. Per il Teorema 3.8 esiste il massimo comun divisore $d = (p, a)$. Supponiamo per assurdo che p ed a non siano coprimi Poiché $d|p$ e p è primo, avremo come unica possibilità $d = \pm p$. Ma poiché $d|a$, e $p|d$, risulterà $p|a$ – assurdo. □

Esercizio 3.10 *Trovare il massimo comun divisore d di 142 e 96 nella forma $d = 142u + 96v$. Lo stesso per 212 e 176.*

Per trovare il massimo comun divisore d tra due numeri naturali a e b e la sua espressione come combinazione lineare di a e b, costruiamo una tabella a 3 colonne. Nella prima riga mettiamo $1, 0, a$ e nella seconda $0, 1, b$ e poi mostriamo come si costruisce una riga, conoscendo le due precedenti.

1	0	a
0	1	b
$\dots$	$\dots$	$\dots$
x	y	z
x'	y'	z'
$x - qx'$	$y - qy'$	r

dove $z = qz' + r$ e q è il quoziente della divisione di z per z'.

Allora ogni riga di questa tabella soddisfa $ax + by = z$: infatti le prime due righe la soddisfano e se due righe la soddisfano, allora la successiva, per costruzione la soddisfa:
$a(x - qx) + b(y - qy') = ax - by + q(ax' - by') = z - qz' = r$.
Poiché nell'ultima colonna i valori continuano a diminuire, tale tabella si concluderà con $z = 0$ e la penultima riga ci darà le informazioni richieste.

Esempio

1	0	156
0	1	84
1	-1	72
-1	2	12
7	-13	0

Allora si avrà $12 = MCD(156, 84)$ e $12 = -1 \cdot 156 + 2 \cdot 84$ e $0 = 7 \cdot 156 - 13 \cdot 84$.

Lemma 3.11 *Se $a, b, c \in \mathbb{Z}$, c e a sono coprimi e $c|ab$, allora $c|b$.*

Dimostrazione. Essendo $1 = (a, c)$ possiamo scrivere, per il Teorema 3.8 $1 = ua + vc$ con opportuni $u, v \in \mathbb{Z}$. Moltiplicando per b si trova $b = uab + vcb$. Poiché $c|ab$ e $c|c$, il punto (d_1) del Lemma 3.6 implica $c|b$. □

Vediamo ora una caratterizzazione importante dei numeri primi, cioè un numero è primo se e solo se ogniqualvolta divide il prodotto di due numeri, in realtà divide già uno dei due numeri.

Proposizione 3.12 *Un numero intero $p \neq 0, \pm 1$ è primo se e solo se per ogni coppia $a, b \in \mathbb{Z}$ con $p|ab$ si ha $p|a$ o $p|b$.*

Dimostrazione. Sia p primo e si supponga che $p|ab$. Se p non divide a, allora p e a sono coprimi per il Corollario 3.9. Quindi, per il Corollario 3.14, $p|ab$ implica $p|b$.
Supponiamo adesso che p non sia primo. Quindi esistono dei divisori propri a e b di p con $p = ab$. In tal caso p non divide né a né b, ma ovviamente $p|ab$. □

Il minimo comune multiplo può essere definito anche utilizzando la definizione del massimo comun divisore.

Teorema 3.13 *Se $a, b \in \mathbb{Z}^*$ e d è un massimo comun divisore di a e b, allora $m = \frac{ab}{d}$ è un minimo comune multiplo di a e b.*

DIMOSTRAZIONE. Per il punto (d_4) del Lemma 3.6 possiamo scrivere $a = da_1$ e $b = db_1$, con $a_1, b_1 \in \mathbb{Z}$, coprimi. Allora $m = a_1 b = b_1 a$ risulta ovviamente un multiplo comune di a e b. Sia m' un altro multiplo comune di a e b. Allora da $a|m'$ e $b|m'$ si deduce $m' = ax$ e $m' = by$ con $x, y \in Z$. Quindi, $ax = by$ e di conseguenza $da_1 x = db_1 y$. Cancellando $d \neq 0$ si ha

$$a_1 x = b_1 y. \tag{2}$$

Per il Lemma 3.11 e $(a_1, b_1) = 1$ possiamo concludere che $a_1|y$ e $b_1|x$. Quindi, $y = a_1 y_1$ e $x = b_1 x_1$ con opportuni $z_1, y_1 \in \mathbb{Z}$. Pertanto, $m' = ax = ab_1 x_1 = mx_1$ e quindi $m|m'$. □

Corollario 3.14 *Se a e b sono coprimi, allora $mcm(a, b) = |ab|$. In particolare, se $a|c$ e $b|c$, e a e b sono coprimi, allora anche $ab|c$.*

3.4 Il teorema fondamentale dell'aritmetica

In questo paragrafo enunciamo e dimostriamo il Teorema fondamentale dell'Aritmetica che garantisce la fattorizzazione unica in prodotto di numeri primi nel senso seguente. Se $p_1 p_2 \dots p_k = q_1 q_2 \dots q_s$ e $p_1, p_2, \dots, p_k$, $q_1, q_2, \dots, q_s$ sono dei numeri primi, allora $s = k$ e dopo una permutazione opportuna dei primi $p_1, p_2, \dots, p_k$ si ha $p_1 = \pm q_1, \dots, p_k = \pm q_k$.

Teorema 3.15 *Tutti i numeri non invertibili di $\mathbb{Z}^*$ hanno una fattorizzazione unica in prodotto di numeri primi.*

DIMOSTRAZIONE. Per un numero intero $a \neq 0, \pm 1$ dimostriamo che a ha una fattorizzazione unica in prodotto di numeri primi. Basta considerare il caso $a > 0$. Ragioniamo per induzione su a. Il caso $a = 2$ è banale perché 2 è primo. Supponiamo $a > 2$. Se a è primo, abbiamo finito. Altrimenti esistono b e c in $\mathbb{Z}$ con $a = bc$ e $1 < b < a$, $1 < c < a$. Per l'ipotesi induttiva, entrambi b e c, essendo > 1, sono prodotti di numeri primi. Così abbiamo dimostrato l'esistenza della fattorizzazione di a in prodotto di numeri primi.
Per dimostrare l'unicità supponiamo che $a = p_1 \dots p_n = q_1 \dots q_s$ siano due fattorizzazioni di a in prodotto di numeri primi. Ragioniamo per induzione su n. Se $n = 1$, avremo $p_1 = q_1 \dots q_s$, che implica $s = 1$ poiché p_1 è primo. Supponiamo adesso $n > 1$. Allora p_1 divide il prodotto $q_1 \dots q_s$ e quindi divide uno dei fattori, diciamo q_1. Poiché q_1 è primo, concludiamo che $q_1 = \pm p_1$. Dopo la cancellazione, abbiamo $p_2 \dots p_n = \pm q_2 \dots q_s$. Poiché l'elemento $a' = p_2 \dots p_n$ è prodotto di un numero di primi inferiore ad n, l'ipotesi induttiva ci dice che la sua fattorizzazione deve essere unica a meno di permutazione dei fattori, cioè si può supporre $s = n$ e $q_2 = \pm p_2, \dots, q_s = \pm p_n$. □

Sia $a > 1$, allora il teorema principale dell'aritmetica ci permette di scrivere $a = p_1^{k_1} \dots p_s^{k_s}$, con $p_1, \dots, p_s$ numeri primi distinti. In questa forma l'unicità della fattorizzazione si può esprimere così: se $a = q_1^{m_1} \dots q_t^{m_t}$ è un'altra fattorizzazione di a, con $q_1, \dots, q_t$ numeri primi distinti, allora $t = s$, esiste un'opportuna permutazione dei primi $p_1, p_2, \dots, p_s$ con $q_1 = \pm p_1$, $\dots, q_s = \pm p_s$ e $m_1 = k_1, \dots, m_s = k_s$. Poiché $a > 0$, possiamo considerare fattorizzazioni con $p_i > 0$ e $q_j > 0$, perciò avremo $q_1 = p_1, \dots, q_s = p_s$, in altre parole, gli insiemi dei primi $\{p_1, \dots, p_s\}$ e $\{q_1, \dots, q_t\}$ coincidono (quindi $t = s$) e dopo un riordino dei primi (per esempio in ordine crescente), coincidono persino le s-uple $(p_1, \dots, p_s)$ e $(q_1, \dots, q_s)$ e le s-uple $(m_1, \dots, m_s)$ e $(k_1, \dots, k_s)$.
Tuttavia, in certe situazione ci converrà usare anche fattorizzazioni $a = p_1^{k_1} \dots p_s^{k_s}$, con $p_1, \dots, p_s$ numeri primi distinti, permettendo di avere anche $k_i = 0$ per alcuni $i = 1, 2, \dots, s$.

Questo diventa comodo quando si lavora con più numeri $a, b, c, ...$ per permettere un confronto tra loro. Scriviamo così

$$a = p_1^{k_1} \dots p_s^{k_s},\ b = p_1^{m_1} \dots p_s^{m_s} \text{ e } c = p_1^{l_1} \dots p_s^{l_s} \tag{4}$$

con $p_1, \dots, p_s$ numeri primi distinti e $k_i \geq 0, m_i \geq 0$ e $l_i \geq 0$ per ogni $i = 1, 2, \dots, s$. Prima di tutto, osserviamo che per il Corollario 3.14, $c|a$ se e solo se $l_i \leq k_i$ per ogni $i = 1, 2, \dots, s$. In particolare, $c|a$ e $c|b$ se e solo se $l_i \leq k_i$ e $l_i \leq m_i$ per ogni $i = 1, 2, \dots, s$. In altre parole, se e solo se $l_i \leq \min\{k_i, m_i\}$ per tutti gli $i = 1, 2, \dots, s$. Per questo, il massimo comun divisore c di a e b è determinato da $l_i = \min\{k_i, m_i\}$ per tutti gli $i = 1, 2, \dots, s$.
Analogamente si ragiona per vedere che il minimo comune multiplo c di a e b deve avere $l_i = \max\{k_i, m_i\}$ per ogni $i = 1, 2, \dots, s$ (o basta applicare la formula $MCD(a, b) = \frac{ab}{(a,b)}$).
Possiamo ora rispondere alla domanda posta all'inizio del paragrafo sui numeri primi e cioè quanti numeri primi esistono.

Teorema 3.16 (Euclide) *Esistono infiniti numeri primi.*

DIMOSTRAZIONE. Supponiamo che $p_1, p_2, \dots, p_n$ siano tutti i numeri primi e consideriamo il numero $N = p_1 p_2 \dots p_n + 1$. Poiché $p_1, p_2, \dots, p_n$ non dividono N (perché?), N deve essere primo e quindi coincide con uno dei $p_1, p_2, \dots, p_n$ - assurdo. □

Possiamo addirittura "specializzare" la forma dei numeri primi, chiedendo per esempio quanti primi di un certo tipo esistono, come nei seguenti esercizi.

Esercizio 3.17 *Si dimostri che esistono infiniti numeri primi della forma* $3k + 2$.

SVOLGIMENTO. Supponiamo che $p_0 = 2$, $p_1, p_2, \dots, p_n$ siano tutti i numeri primi del tipo $3k + 2$ e consideriamo il numero $N = 3p_1 p_2 \dots p_n + 2$. Poiché 3 non divide N, i divisori primi di N sono dispari e del tipo $3k + 1$ e $3k + 2$. Prodotto di numeri del tipo $3k + 1$ è dello stesso tipo, quindi almeno uno dei divisori primi q di N è del tipo $3k+2$. Di conseguenza, q coincide con uno dei $p_0, p_1, p_2, \dots, p_n$ - assurdo, perché nessun p_i può dividere N. □

Esercizio 3.18 *Si dimostri che:*
a) esistono infiniti numeri primi della forma $6k + 5$*;*
b) esistono infiniti numeri primi della forma $4k + 3$.

3.5 Congruenze in $\mathbb{Z}$

Sia $m > 1$ un intero. Introduciamo nell'insieme $\mathbb{Z}$ la relazione binaria $a \equiv_m b$ detta *congruenza modulo* m. Diremo, per definizione, che a *è congruo* a b *modulo* m se m divide la differenza $a - b$. Verifichiamo innanzitutto che $\equiv_m$ è una relazione di equivalenza su $\mathbb{Z}$:

- $a \equiv_m a$ per ogni $a \in \mathbb{Z}$ poiché m divide $0 = a - a$;
- se $a \equiv_m b$, allora anche $b \equiv_m a$ per ogni coppia $a, b \in \mathbb{Z}$ (poiché $m|a - b$ implica $m|b - a = -(a - b)$;
- se $a \equiv_m b$ e $b \equiv_m c$, allora anche $a \equiv_m c$ (poiché $m|a - b$ e $m|b - c$ implica $m|a - c = (a - b) + (b - c)$).

Vediamo ora quali m sono rilevanti. Ovviamente, per $m = 0$ si ha $a \equiv_0 b$ se e solo se $a = b$, quindi la congruenza $\equiv_0$ coincide con la solita uguaglianza "=". Per $m = \pm 1$ abbiamo $a \equiv_m b$ per ogni coppia a, b. Quindi, $\equiv_m$ ha una sola classe di equivalenza. Per finire, notiamo che $m|a - b$ se e solo se $-m|a - b$, quindi le relazioni $\equiv_m$ e $\equiv_{-m}$ coincidono. Per questi motivi in seguito considereremo solo $m > 1$.
Denotiamo con $[a]_m$ la classe di equivalenza di a, in altre parole,

$$[a]_m = \{x \in Z : \text{ esiste } y \in \mathbb{Z} \text{ con } x = a + my\} = \{\ldots, a - 2m, a - m, a, a + m, \ldots\}$$

cioè $[a]_m$ è la progressione aritmetica bilaterale di ragione m e punto iniziale a.
Si noti che la classe $[a]_m$ è *infinita*, mentre ci sono solo un numero finito di classi di equivalenza. Infatti, questo segue subito dal seguente ovvio lemma:

Lemma 3.19 *Sia r il resto di a modulo m (i.e., $a = qm + r$, con $0 \leq r < m$). Allora $a \equiv_m r$.*

Adesso è chiaro che l'insieme

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m - 1]_m\}$$

presenta tutte le classi di equivalenza modulo m e queste classi sono a due a due distinte (perché $k \not\equiv_m r$ quando $0 \leq k < m$ e $0 \leq r < m$).
Se $n|m$, allora $a \equiv_m b$ implica $a \equiv_n b$. Se $(n, m) = 1$, allora $a \equiv_{mn} b$ se e solo se $a \equiv_m b$ a $a \equiv_n b$. Infatti, $m|a - b$ e $n|a - b$ implicano $mn|a - b$ poiché m e n sono coprimi (Corollario 3.14).
Le seguenti proprietà delle congruenze sono collegate alle operazioni algebriche in $\mathbb{Z}$:

Lemma 3.20 *i) se $a \equiv_m a'$ e $b \equiv_m b'$, allora anche $a + b \equiv_m a' + b'$ e $ab \equiv_m a'b'$.*

ii) se $ac \equiv_m bc$ e $(c, m) = 1$, allora anche $a \equiv_m b$.

Dimostrazione. i) Sia ha $m|a - a'$ e $m|b - b'$. Allora (d_1) del Lemma 3.6 ci permette di concludere che $m|(a - a') + (b - b') = (a + b) - (a' - b')$, quindi $a + b \equiv_m a' + b'$. Per quanto riguarda il prodotto presentiamo la differenza $ab - a'b'$ come $ab - ab' + ab' - a'b' = a(b - b') + b'(a - a')$. Di nuovo il punto (d_1) del Lemma 3.6 ci permette di concludere che $m|a(b - b') + b'(a - a') = ab - a'b'$. Quindi $ab \equiv_m a'b'$.
ii) Dai fatti che m divide $ac - bc = (a - b)c$ ed $(m, c) = 1$, segue m divide $a - b$ per il Lemma 3.11. □

Usando le classi di equivalenza, possiamo scrivere (a) anche nel modo seguente:
(a*) se $[a]_m = [a']_m$ e $[b]_m = [b']_m$, allora $[a + b]_m = [a' + b']_m$ e $[ab]_m = [a'b']_m$.
La proprietà (a*) ci permette di introdurre in $\mathbb{Z}_m$ due operazioni algebriche nel modo seguente:

$$[a]_m + [b]_m = [a + b]_m \text{ e } [a]_m[b]_m = [ab]_m. \qquad (*)$$

Infatti, (a*) garantisce che la somma $[a + b]_m$ dipende solamente dalle classi $[a]_m$ e $[b]_m$ e non dai singoli rappresentanti a, b.

Esercizio 3.21 *Dimostrare per induzione che:*
(a) l'ultima cifra di 7^{4n+1} è 7.
(b) le ultime due cifre di 5^{n+2} sono 25.
(c) l'ultima cifra di 2^{4n+3} è 8.
(d) l'ultima cifra di 3^{4n+1} è 3.
(e) l'ultima cifra di 4^{2n+3} è 4.

(f) l'ultima cifra di 3^{4n+3} *è 7.*
(g) l'ultima cifra di 7^{4n+2} *è 9.*
(h) l'ultima cifra di 9^{2n+1} *è 9.*
(i) l'ultima cifra di 6^{n+3} *è 6.*

3.6 Equazioni congruenziali

Consideriamo equazioni congruenziali di primo grado ad una variabile. cioè, dati $m > 1$, a e b numeri interi fissati, cerchiamo le soluzioni $x \in \mathbb{Z}$ della congruenza

$$ax \equiv_m b \qquad (1).$$

Ovviamente, se x_0 è una soluzione di (1), lo sono anche tutti gli $x \equiv_m x_0$.
Sia $d = (a, m)$. Allora (1) ha soluzione se e solo se d divide anche b. Infatti, se (1) vale per x, allora m divide la differenza $ax - b$. Quindi, d divide la differenza $ax - b$ e anche a. Quindi, d divide b.
Supponiamo adesso che d divida b e quindi $b = db_1$ per qualche $b_1 \in \mathbb{Z}$. Per $(a, m) = d$ si trovano numeri interi u, v tali che $d = au + mv$. Ma allora

$$b = db_1 = (au + mv)b_1 = a(ub_1) + mvb_1 \equiv_m a(ub_1).$$

Pertanto $x_0 = ub_1$ è una soluzione di (1). Verifichiamo ora che gli elementi del tipo $x_0 + n \cdot m/d$, al variare di $n \in \mathbb{Z}$, sono tutte soluzioni di (1). Infatti

$$a(x_0 + n \cdot \frac{m}{d}) = ax_0 + n \cdot \frac{am}{d} \equiv_m b + n \cdot m \cdot \frac{a}{d} \equiv_m b,$$

poiché $d|a$ e quindi $a/d \in \mathbb{Z}$.

Applichiamo questo procedimento ad un caso concreto.

Esercizio 3.22 *Risolvere l'equazione congruenziale* $143x \equiv_{57} 17$.

Svolgimento. Dividendo 143 per 57 troviamo $143 = 2 \cdot 57 + 29$, poi $57 = 29 + 28$ e $29 = 28 + 1$. Di qui $1 = 29 - 28 = 29 - (57 - 29) = 2 \cdot 29 - 57 = 2 \cdot (143 - 2 \cdot 57) - 57 = 2 \cdot 143 - 5 \cdot 57$. Quindi $x \equiv_{57} 2 \cdot 17 = 34$.
Un modo più veloce di lavorare è di sostituire subito 143 con il suo resto 29 modulo 57, cioè lavorare in partenza con l'equazione congruenziale $29x \equiv_{57} 17$. Adesso con $29 \equiv_{57} -28$ e $17 \equiv_{57} -40$ si trova l'equazione congruenziale $-28x \equiv_{57} -40$. Poiché 4 e 57 sono coprimi possiamo cancellare 4 e si trova $-7x \equiv_{57} -10$ e di conseguenza

$$7x \equiv_{57} 10. \qquad (*)$$

Poiché $57 = 8 \cdot 7 + 1$, abbiamo $8 \cdot 7 \equiv_{57} -1$. Quindi, moltiplicando (*) per 8 si trova $8 \cdot 7x \equiv_{57} 80$ e pertanto $-x \equiv_{57} 23$ e $x \equiv_{57} -23 \equiv_{57} 34$. □

Esercizio 3.23 *Trovare tutte le soluzioni in* $\mathbb{Z}_{126}$ *della seguente equazione congruenziale*

$$30x \equiv_{126} 42$$

Svolgimento. Osserviamo che $MCD(30, 126) = 6$ divide 42. Pertanto

$$42 = 6 \cdot 7 = (126 - 30 \cdot 4) \cdot 7 \equiv_{126} 30 \cdot (-28),$$

da cui si ricava che le soluzioni sono del tipo $x = -28 + z \cdot 126/6$. Quindi se cerchiamo tutte le soluzioni in $\mathbb{Z}_{126}$, queste sono 14, 35, 56, 77, 98, 119. □

Esercizio 3.24 *Trovare tutti gli interi positivi minori di 100 che soddisfano la seguente equazione congruenziale* $17x \equiv_{29} 3$

SVOLGIMENTO. Si vede facilmente che gli interi che soddisfano quella congruenza sono del tipo $x = 36 + 29z$ e pertanto si avrà $x = 7, 36, 65, 94$. □

Esercizio 3.25 *Si trovi il minimo numero naturale n per cui risulti simultaneamente*

$$n \equiv_7 2 \quad n \equiv_6 1 \quad n \equiv_5 0$$

SVOLGIMENTO. Dalla prima congruenza ricaviamo $n = 2 + 7\lambda$, per qualche $\lambda \in \mathbb{Z}$, che sostituita nella seconda porge $n = 2 + 7\lambda \equiv_6 1$. Pertanto $7\lambda \equiv_6 1 - 2$, cioè $\lambda \equiv_6 5$ e quindi esiste $k \in \mathbb{Z}$ tale che $\lambda = 5 + 6k$. Sostituendo si ottiene $n = 2 + (5 + 6k)7 = 37 + 42k$ che sostituita nell'ultima dà

$$37 + 42k \equiv_5 0 \quad \Rightarrow \quad 2 + 2k \equiv_5 0 \quad \Rightarrow \quad k \equiv_5 -1 \equiv_5 4,$$

usando il Lemma 3.20, in quanto (2,5)=1.
Allora esiste $h \in \mathbb{Z}$ tale che $k = 4 + 5h$ e quindi $n = 37 + 42k = 37 + 42(4 + 5h) = 205 + 210h$. Le soluzioni intere sono quindi del tipo $n = -5 + 210m$ e pertanto si avrà $n = 205$. □

Esercizio 3.26 *Risolvere le seguenti equazioni congruenziali:*
a) $4x \equiv_{17} -3$*;* *b)* $29x + 3 \equiv_{12} 0$*;* *c)* $3x - 8 \equiv_{13} 0$*;* *d)* $7x \equiv_{19} 4$*;* *e)* $37x \equiv_{117} 25$*;* *f)*$13x \equiv_{153} 178$*;* *g)*$18x \equiv_{51} 5$

Esercizio 3.27 *Trovare i numeri interi x che soddisfano le equazioni congruenziali:*

$$x \equiv 2(mod\ 3),\ \ x \equiv 1(mod\ 4)\ \text{ e }\ x \equiv 3(mod\ 5).$$

Esercizio 3.28 *Determinare le ultime due cifre di* 7^{1996} *e le ultime tre cifre di* 7^{1983}*.*

SUGGERIMENTI. Notare che $7^4 \equiv_{25} 1$ e $7^4 \equiv_8 1$. Quindi $7^4 \equiv_{100} 1$ e quindi le ultime due cifre di 7^{4k} sono $\ldots 01$. Dalla congruenza $7^4 \equiv_{25} 1$ dedurre che $7^{20} \equiv_{125} 1$. Di conseguenza $7^{20} \equiv_{1000} 1$. □

Esercizio 3.29 *Trovare il resto del numero* 341^{17} *modulo 72.*

$$341^{17} \equiv_{72} (-19)^{17} \equiv_{72} -(19)^{16} \cdot 19 \equiv_{72} -((19)^2)^8 \cdot 19 \equiv_{72} -(1)^8 \cdot 19 \equiv_{72} 53.$$

3.7 Criteri di divisibilità per 3, 9, 11, 101

Sia $m > 1$ intero. Per ogni numero intero positivo a possiamo trovare il resto a_0 nella divisione per m, $a = q_1 m + a_0$. Adesso possiamo trovare il resto a_1 di q_1 modulo m per avere $q_1 = q_2 m + a_1$ e di conseguenza $a = q_2 m^2 + a_1 m + a_0$. Proseguendo in questo modo otteniamo una successione di resti $a_0, a_1, a_2, a_3, \ldots$ e di dividendi $q_1 > q_2 > \ldots$ tali che $q_i = q_{i+1} m + a_i$ per ogni $i = 1, 2, \ldots$ e quindi

$$a = a_0 + a_1 m + a_2 m^2 + a_3 m^3 + \ldots + a_i m^i + \ldots + a_k m^k + q_{k+1} m^{k+1}.$$

Poiché la successione q_i decresce strettamente, avremo $q_{k+1} = 0$ per un certo k, per il quale si avrà

$$a = a_0 + a_1 m + a_2 m^2 + a_3 m^3 + \ldots + a_i m^i + \ldots + a_k m^k.$$

I resti $a_0, a_1, a_2, a_3, \ldots a_k$ si chiamano *cifre* di a in base m. In particolare, con $m = 10$ si hanno le cifre decimali.

Proposizione 3.30 *Siano $a_0, a_1, a_2, a_3, \ldots, a_k$ le cifre decimali di a e sia $S = a_0 + a_1 + a_2 + \ldots + a_k$. Allora $a \equiv_9 S$. In particolare:*
(a) a è divisibile per 3 se e solo se S è divisibile per 3;
(b) a è divisibile per 9 se e solo se S è divisibile per 9.

DIMOSTRAZIONE.(a) Ovviamente $10 \equiv_9 1$, quindi $10^i \equiv_9 1$ per ogni $i = 1, 2, \ldots, k$. Moltiplicando per a_i si ricava $a_i 10^i \equiv_9 a_i$ per ogni $i = 1, 2, \ldots, k$. Sommando si ricava $a = a_0 + a_1 10 + a_2 10^2 + \ldots + a_k 10^k \equiv_9 S$. Ora (b) segue immediatamente da (a). □

Proposizione 3.31 *Siano $a_0, a_1, a_2, a_3, \ldots, a_k$ le cifre decimali di a e sia $S = a_0 - a_1 + a_2 + \ldots + (-1)^k a_k = \Sigma_{i=0}^{k} (-1)^i a_i$. Allora $a \equiv_{11} S$. In particolare a è divisibile per 11 se e solo se S è divisibile per 11.*

DIMOSTRAZIONE. Poiché $10 \equiv_{11} -1$, si ha $10^i \equiv_{11} (-1)^i$ per ogni $i = 1, 2, \ldots, k$. Moltiplicando per a_i si ricava $a_i 10^i \equiv_{11} (-1)^i a_i$ per ogni $i = 1, 2, \ldots, k$. Sommando si ricava $a = a_0 + a_1 10 + a_2 10^2 + \ldots + a_k 10^k \equiv_{11} S$. La seconda affermazione segue dalla prima. □

Proposizione 3.32 *Siano $a_0, a_1, a_2, a_3, \ldots, a_n$ le cifre decimali di a e sia $S = a_1 a_0 - a_3 a_4 + \ldots + (-1)^k a_{2k+1} a_{2k} + \ldots\ldots + (-1)^{[n/2]} a_{2[n/2]+1} a_{2[n/2]} =$*
$= \Sigma_{k=0}^{[n/2]} (-1)^k a_{2k+1} a_{2k}$.
Allora $a \equiv_{101} S$. In particolare a è divisibile per 101 se e solo se S è divisibile per 101.

DIMOSTRAZIONE. Ovviamente $100 \equiv_{101} -1$, quindi $100^i \equiv_{101} (-1)^i$ per ogni $i = 1, 2, \ldots, k$. Pertanto
$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \ldots + a_i \cdot 10^i + \ldots + a_k \cdot 10^k \equiv_{101}$
$a_0 + a_1 \cdot 10 - a_2 + a_3 \cdot 10 + a_4 + a_5 \cdot 10 - \ldots (-1)^k (a_{2k+1} + a_{2k} \cdot 10) + \ldots\ldots + (-1)^{[n/2]} (a_{2[n/2]+1} + a_{2[n/2]} \cdot 10$.
La seconda affermazione segue dalla prima. □

3.8 I teoremi di Fermat e Eulero

Il seguente importante teorema è dovuto a Fermat. Vedremo più avanti come questo sia un caso particolare di un teorema più generale dovuto ad Eulero.

Teorema 3.33 (Piccolo teorema di Fermat) *Sia p un numero primo. Allora $a^p \equiv_p a$ per ogni numero intero a.*

DIMOSTRAZIONE. Se $p|a$, avremo $a \equiv_p 0$ e $a^p \equiv_p 0$, quindi la congruenza $a^p \equiv_p a$ vale.
Possiamo quindi supporre che p non divida a. Allora p e a sono coprimi, quindi la congruenza $a^p \equiv_p a$ è equivalente ad $a^{p-1} \equiv_p 1$, che dimostreremo. Sia $R = \{1, 2, \ldots, p-1\}$ l'insieme dei resti diversi da 0 modulo p. Definiamo un'applicazione $\alpha : R \to R$ nel modo seguente. Per $k \in R$ eseguiamo la divisione con resto di ak per p. Si ricava così un resto r_k soddisfacente $ak = qp + r_k$, e quindi $0 \leq r_k < p$ e

$$ak \equiv_p r_k \text{ per } k = 1, 2, \ldots p-1. \tag{1}$$

Poiché k e a sono entrambi coprimi con p, p non può dividere ak e concludiamo che $r_k \neq 0$ in (1). Pertanto possiamo definire $\alpha(k) := r_k \in R$. Se $r_k = r_i$ per $i, k \in R$ avremo da (1) $ak \equiv_p r_k = r_i \equiv_p ai$, e quindi $ak \equiv_p ai$. Poiché a è coprimo con p, lo possiamo cancellare.

Quindi $k \equiv_p i$ e per la definizione di R, $k = i$. Abbiamo così verificato che α è un applicazione iniettiva. Quindi l'immagine $\alpha(R)$ dovrà avere $p-1$ elementi come R stesso. Essendo $\alpha(R)$ anche un sottoinsieme di R, avremo $\alpha(R) = \{r_1, r_2, \ldots, r_{p-1}\} = R$. In particolare, il prodotto $r_1 \cdot r_2 \cdot \ldots \cdot r_{p-1}$ coincide con $1 \cdot 2 \cdot \ldots \cdot (p-1)$, cioè

$$r_1 \cdot r_2 \cdot \ldots \cdot r_{p-1} = (p-1)!. \tag{2}$$

Moltiplicando le $p-1$ congruenze in (1) otteniamo $a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv_p r_1 \cdot r_2 \cdot \ldots \cdot r_{p-1}$. Ora (2) ci permette di sostituire $r_1 \cdot r_2 \cdot \ldots \cdot r_{p-1}$ con $(p-1)!$ in questa congruenza e ottenere $a^{p-1} \cdot (p-1)! \equiv_p (p-1)!$. Essendo $(p-1)!$ coprimo con p possiamo cancellare $(p-1)!$ e ricavare $a^{p-1} \equiv_p 1$. □

Esercizio 3.34 *Sia p un numero primo e a un intero coprimo con p. Allora per il teorema di Fermat esiste un numero naturale $n > 0$ con la proprietà $a^n \equiv_p 1$. Sia k il più piccolo di tali n, allora k ha le seguenti proprietà*
a) $a^{qk} \equiv_p 1$ per ogni intero $q \geq 0$;
b) se $a^n \equiv_p 1$ per un intero $n \geq 0$, allora k divide n.

SUGGERIMENTI. a) Basta elevare $a^k \equiv_p 1$ per la potenza q. Per dimostrare b), si divida n per k con resto r, cioè $n = qk + r$, con $0 \leq r < k$. Adesso per a) avremo $1 \equiv_p a^n = a^{qk+r} = a^{qk} \cdot a^r \equiv_p 1 \cdot a^r$. Di conseguenza $a^r \equiv_p 1$. Per la scelta di k si ha $r = 0$, cioè k divide n. □

Nel seguito denoteremo con $o_p(a)$ il numero k definito nell'Esercizio 3.34.

Esercizio 3.35 *Sia p un numero primo e a un intero coprimo con p. Dimostrare che:*
a) $o_p(a)$ divide $p-1$;
b) se $p > 2$, allora $a^{\frac{p-1}{2}} \equiv_p \pm 1$.
c) se $a^{\frac{p-1}{2}} \equiv_p -1$ allora $o_p(a) = p-1$.

SUGGERIMENTI.(a) Applicare il Teorema di Fermat e b) dell'Esercizio 3.34. (b) Poiché p è primo e divide $a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$, concludiamo che p divide uno dei due fattori. □

Esercizio 3.36 *Dimostrare che 67, 97, 193 e 257 sono numeri primi. Calcolare (a) $o_{67}(2)$, (b) $o_{97}(2)$, (c) $o_{193}(2)$ e (d) $o_{257}(2)$.*

SUGGERIMENTI. Per verificare che 67 sia primo basta controllare che nessun primo $p < \sqrt{67}$ (cioè, $p = 2, 3, 5$ e 7 divide 67). Si procede analogamente con 97, 193 e 257.
(a) Da $2^6 \equiv_{67} -3$ ricavare, elevando al quadrato, $2^{12} \equiv_{67} 9$ e $2^{24} \equiv_{67} 14$. Moltiplicando la prima e l'ultima congruenza si ricava $2^{30} \equiv_{67} 25$. Ora moltiplicare per 8 per ottenere $2^{33} \equiv_{67} -1$ (e quindi, e $2^{33} \not\equiv_{67} 1$). Per gli altri divisori propri 6 e 22 di 66 abbiamo $2^6 \not\equiv_{67} 1$ e $2^{22} \not\equiv_{67} 1$. D'altra parte, dall'Esercizio precedente sappiamo che $o_{67}(2)$ divide 66. Questo ci permette di scrivere $o_{67}(2) = 66$ perché ogni divisore proprio di 66 divide uno dei divisori 6, 22 e 33.
(b) Da $2^9 \equiv_{97} 27$ e $2^7 \equiv_{97} 31$ ricavare moltiplicando $2^{16} \equiv_{97} 61 \equiv_{97} -36$ e elevando al quadrato $2^{32} \equiv_{97} 35$. Moltiplicando le ultime due congruenze si ottiene $2^{48} \equiv_{97} 1$. Poiché $2^{16} \not\equiv_{97} 1$ e $2^{24} \not\equiv_{97} 1$ (spiegare perché!) si conclude che $o_{97}(2) = 48$.
(c) Per 193 notare che partendo da $2^{10} \equiv_{193} 59$ e moltiplicando tre volte per 4, ricavando $2^{12} \equiv_{193} 43$ si ottiene $2^{14} \equiv_{193} -21$. Pertanto $2^{16} \equiv_{193} -84$ e (elevando al quadrato) $2^{32} \equiv_{193} 108$. Moltiplicando le due congruenze si ottiene $2^{48} \equiv_{193} -1$, che permette di affermare $o_{193}(2) = 96$.
(d) Per $257 = 2^8 + 1$ si ha $2^8 \equiv_{257} -1$ e quindi $2^{16} \equiv_{257} 1$. Adesso $o_{257}(2) = 16$. □

3.9 Funzione di Eulero

Definizione 3.37 Poniamo $\varphi(1) = 1$ e per un numero naturale $n > 1$ poniamo $\varphi(n)$ uguale al numero dei numeri naturali k coprimi con n e soddisfacenti $1 \leq k \leq n$.

La funzione $\varphi(n)$ è nota come *funzione di Eulero* o *funzione totiente.*

Lemma 3.38 *Siano m e n due numeri naturali coprimi tra loro. Allora $\varphi(m{\cdot}n) = \varphi(m){\cdot}\varphi(n)$.*

DIMOSTRAZIONE. Dobbiamo dimostrare $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ per ogni coppia di numeri naturali m ed n coprimi tra loro. In altre parole, bisogna vedere che ci sono precisamente $\varphi(m) \cdot \varphi(n)$ numeri interi x tra 1 ed mn coprimi con mn. Poiché m ed n sono coprimi tra loro, basta assicurarsi che x sia coprimo con m e coprimo con n. Infatti, se x è coprimo con mn, ovviamente x è coprimo anche con m e con n. Viceversa, se x è coprimo con m e coprimo con n, allora ogni divisore comune d di x e mn, essendo $(x, m) = 1$, deve essere coprimo con m. Quindi, d dovrebbe dividere n e di conseguenza $d = \pm 1$ poiché anche $(x, n) = 1$.
Possiamo scrivere ogni numero naturale x tra 1 ed mn come

$$x = ym + z, \text{ con } 1 \leq z \leq m, 0 \leq y < n. \tag{2}$$

Infatti, dividiamo x per m con il resto: $x = qm + r$ con $0 \leq r < m$. Se $r > 0$ poniamo $y = q$ e $z = r$, se $r = 0$, poniamo $y = q - 1$ e $z = m$. Notiamo che x dato da (2) è coprimo con m se e solo se z è coprimo con m. Perciò fissiamo da ora in poi un arbitrario z con $1 \leq z \leq m$, coprimo con m. Ora vogliamo chiarire per *quanti* valori di y, $0 \leq y < n$, il numero x determinato da (2) sia coprimo con n. Dividendo x per n con il resto ricaviamo $x = qn + r_y$, dove $0 \leq r_y < n$. Notiamo che se $y \neq y'$, allora anche $r_y \neq r_{y'}$, poiché $r_y = r_{y'}$ implica $ym \equiv_n y'm$. Poiché $(m, n) = 1$, questo implica $y \equiv_n y'$ e di conseguenza, $y = y'$. Abbiamo così verificato che $(x, n) = 1$ se e solo se $(r_y, n) = 1$. Poiché tra $r_0, r_1, \ldots, r_{n-1}$ ci sono precisamente $\varphi(n)$ resti coprimi con n, ci saranno $\varphi(n)$ dei numeri definiti in (2) coprimi con n (per z fisso!). Quindi, per ogni z fissato precisamente $\varphi(n)$ tra i numeri x definiti da (2) sono coprimi con n. Quindi, in totale ci sono $\varphi(m) \cdot \varphi(n)$ numeri x tra 1 e mn coprimi con mn. □

Lemma 3.39 *Sia p un numero primo e sia $n > 0$ un numero naturale. Allora $\varphi(p^n) = p^n - p^{n-1}$.*

DIMOSTRAZIONE. Basta contare quanti sono i numeri $k \leq p^n$ che *non sono* coprimi con p^n. Allora k non è coprimo con p^n se e solo se k è divisibile per p. Quindi $k = pk_1$ per qualche $k_1 \in \mathbb{Z}$. Ora $k \leq p^n$ implica $k_1 \leq p^{n-1}$. Ci sono p^{k-1} numeri k tra 1 e p^k che non sono coprimi con p^n, da cui $\varphi(p^n) = p^n - p^{n-1}$. □

Gli ultimi due lemmi permettono di dimostrare:

Teorema 3.40 *Se $m = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_s^{n_s}$ è la decomposizione di m in prodotto di potenze di numeri primi tra loro diversi, allora*

$$\varphi(m) = (p_1^{n_1} - p^{n_1-1})(p_2^{n_2} - p_2^{n_2-1}) \cdot \ldots \cdot (p_s^{n_s} - p_s^{n_s-1}) = m(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_s}).$$

Esercizio 3.41 *Dimostrare la formula*

$$n = \sum_{d|n} \varphi(d).$$

SVOLGIMENTO. Si faccia induzione sul numero s di primi che compaiono nella fattorizzazione di n in primi. Se $s = 1$, allora $n = p^k$ e

$$\sum_{d|n} \varphi(d) = \sum_{i=0}^{k} \varphi(p^i) = 1 + \sum_{i=1}^{k} p^{i-1}(p-1) = 1 + (p-1)(1 + p + \ldots + p^{k-1}) = p^k.$$

Sia ora $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_s^{k_s}$ e poniamo $m = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_{s-1}^{k_{s-1}}$. Allora i divisori di n sono tutti i divisori di m e poi tutti i divisori del tipo dp_s^i, ove d divide m e $0 < i \leq k_s$. Possiamo applicare l'ipotesi induttiva ad m e quindi

$$\sum_{d|n} \varphi(d) = \sum_{d|m} \varphi(d) + \sum_{d|m} \left(\sum_{i=1}^{k_s} \varphi(dp^i) \right) = m + \sum_{d|m} \left(\sum_{i=1}^{k_s} \varphi(d)\varphi(p^i) \right) =$$

$$m + \sum_{d|m} \varphi(d) \left(\sum_{i=1}^{k_s} \varphi(p^i) \right) = m + \left(\sum_{d|m} \varphi(d) \right) (p_s^{k_s} - 1) = m + m \cdot p_s^{k_s} - m = n.$$

□

Il seguente fatto, noto come teorema di Eulero, si dimostra in modo analogo al piccolo teorema di Fermat e come preannunciato ne è una generalizzazione.

Teorema 3.42 Teorema di Eulero *Se $a > 1$ e $m > 1$ sono due numeri naturali coprimi, allora $a^{\varphi(m)} \equiv 1 (mod\, m)$.*

DIMOSTRAZIONE. Sia $R = \{1, \ldots, m-1\}$ l'insieme dei resti coprimi con m modulo m. Definiamo un'applicazione $\alpha : R \to R$ nel modo seguente. Per $k \in R$ dividiamo ak per m con resto. Si ricava così un resto r_k soddisfacente $ak = qp + r_k$, e quindi $0 \leq r_k < m$ e

$$ak \equiv_m r_k \text{ per } k = 1, 2, \ldots m-1. \tag{1}$$

Poiché k ed a sono entrambi coprimi con m, m è coprimo con ak e concludiamo che $r_k \in R$. Pertanto possiamo definire $\alpha(k) := r_k \in R$. Se $r_k = r_i$ per $i, k \in R$ avremo da (1) $ak \equiv_m r_k = r_i \equiv_m ai$, e quindi $ak \equiv_m ai$. Poiché a è coprimo con m, lo possiamo cancellare. Quindi $k \equiv_m i$ e per la definizione di R, $k = i$. Abbiamo così verificato che α è un applicazione iniettiva. Quindi l'immagine $\alpha(R)$ dovrà avere $\varphi(m)$ elementi come R stesso. Essendo $\alpha(R)$ anche un sottoinsieme di R, avremo $\alpha(R) = \{r_1, \ldots, r_{\varphi(m)}\} = R$. In particolare, il prodotto $r_1 \cdot \ldots \cdot r_{\varphi(m)}$ coincide con il prodotto Π di tutti i resti in R, cioè

$$r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} = \Pi. \tag{2}$$

Moltiplicando le $\varphi(m)$ congruenze in (1) otteniamo $a^{\varphi(m)} \cdot \Pi \equiv_m r_1 \cdot \ldots \cdot r_{\varphi(m)}$. Ora (2) ci permette di sostituire $r_1 \cdot \ldots \cdot r_{\varphi(m)}$ con Π in questa congruenza e ottenere $a^{\varphi(m)} \cdot \Pi \equiv_m \Pi$. Essendo Π coprimo con m possiamo cancellare Π e ricavare $a^{\varphi(m)} \equiv_m 1$. □

Vediamo ora un altro modo per risolvere le equazioni congruenziali del tipo $ax \equiv_m b$, nel caso in cui $(a, m) = 1$. Si ha infatti, grazie al teorema di Eulero, che $a^{\varphi(m)} \equiv_m 1$, da cui si ricava $a(a^{\varphi(m)-1}b) \equiv_m b$, per cui una soluzione si ottiene immediatamente ponendo $x_0 = a^{\varphi(m)-1}b$. Se si vuole ottenere una soluzione dell'equazione congruenziale anche nel caso generale usando il teorema di Eulero, ci si può poi ridurre al caso appena visto "dividendo" l'equazione per $d = (a, m)$.

4 I numeri razionali, reali e complessi

4.1 I numeri razionali e reali

Denoteremo con il simbolo $\mathbb{Q}$ l'insieme dei numeri razionali, cioè $\mathbb{Q} = \{\frac{a}{b} \text{ con } a, b \in \mathbb{Z}, b \neq 0\}$. Anche in questo caso si supporranno note le proprietà dell'addizione e della moltiplicazione definite su $\mathbb{Q}$ e le proprietà dell'usuale ordinamento $\leq$ definito su $\mathbb{Q}$. Vogliamo solo osservare che in $\mathbb{Q}$ vale la seguente proprietà:

Proprietà di densità: dati $x, y \in \mathbb{Q}$, tali che $x < y$, esiste $z \in \mathbb{Q}$ tale che $x < z < y$. Basterà infatti prendere $z = \frac{x+y}{2}$.

Questa proprietà non vale in $\mathbb{Z}$, ma in compenso in $\mathbb{Q}$ non vale una proprietà analoga all'assioma del buon ordinamento. Infatti l'insieme dei numeri razionali positivi non ammette minimo.

I numeri reali $\mathbb{R}$ sono già stati introdotti nei corsi di Analisi. Osserviamo solamente che anche in $\mathbb{R}$ sono definite le operazioni addizione e moltiplicazione e un ordinamento. Supponiamo noto il fatto che si può immaginare $\mathbb{Q}$ come un sottoinsieme di $\mathbb{R}$.
Denotiamo con $]a, b[$ l'intervallo aperto di estremi a e b, cioè $]a, b[= \{x \in \mathbb{R} : a < x < b\}$ e con $[a, b]$ l'intervallo chiuso di estremi a e b, cioè $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$.
Inoltre

$$[a, b[= \{x \in \mathbb{R} : a \leq x < b\}, \qquad]a, b] = \{x \in \mathbb{R} : a < x \leq b\},$$
$$]-\infty, b] = \{x \in \mathbb{R} : x \leq b\}, \qquad]-\infty, b[= \{x \in \mathbb{R} : x < b\},$$
$$[a, +\infty[= \{x \in \mathbb{R} : x \geq a\}, \qquad]a, +\infty[= \{x \in \mathbb{R} : x > a\}.$$

Ricordiamo una definizione, per poter descrivere una proprietà importante di $\mathbb{R}$.

Definizione 4.1 Un sottoinsieme S di $\mathbb{R}$ si dice *limitato superiormente* se ammette *maggioranti*, vale a dire se esiste un elemento $a \in \mathbb{R}$ tale che $x \leq a$ per ogni $x \in S$.

In $\mathbb{R}$ vale la seguente proprietà, che non vale in $\mathbb{Q}$.
Proprietà di completezza: se S è un sottoinsieme di $\mathbb{R}$, non vuoto e limitato superiormente, allora l'insieme dei maggioranti di S ha minimo. Questo minimo si dice l'*estremo superiore*.

Tra le conseguenze della completezza, citiamo le seguenti:

(a) $\mathbb{Q}$ è denso in $\mathbb{R}$, cioè se $x, y \in \mathbb{R}$ e $x < y$, allora esiste $z \in \mathbb{Q}$ tale che $x < z < y$;

(b) ogni numero reale è l'estremo superiore di un insieme di numeri razionali;

(c) ogni numero reale non negativo è un quadrato, cioè per ogni $a \in \mathbb{R}$, $a \geq 0$, esiste $b \in \mathbb{R}$ tale che $b^2 = a$.

Il seguente esercizio dà un'idea di come si potrebbe dimostrare il punto (a).

Esercizio 4.2 *Dimostrare che per ogni numero reale ρ esiste un numero intero $n \geq \rho$.*

Svolgimento. Ragioniamo per assurdo e supponiamo che per qualche numero reale ρ si abbia $n < \rho$ per ogni $n \in \mathbb{Z}$. Quindi l'insieme $\mathbb{Z}$ è superiormente limitato. Sia σ l'estremo superiore di $\mathbb{Z}$, allora $\sigma - 1$, essendo minore di σ non è più un limite superiore per $\mathbb{Z}$, pertanto $\sigma - 1 \leq n$ per qualche $n \in \mathbb{Z}$ e quindi $\sigma \leq n + 1$, assurdo poiché σ è un limite superiore per $\mathbb{Z}$. $\square$

Definizione 4.3 Per ogni numero reale ρ denotiamo con $[\rho]$ l'unico numero intero n determinato da $n \leq \rho < n+1$.

Per l'esercizio precedente, questa definizione è corretta.

Esercizio 4.4 *Dimostrare che non esistono numeri razionali il cui quadrato è 2.*

SVOLGIMENTO. Supponiamo che esista un numero razionale r con $r^2 = 2$. Allora $r \neq 0$ e quindi possiamo scrivere $r = a/b$, dove a e b sono interi, non entrambi pari (altrimenti possiamo semplificare la frazione). Ora $(a/b)^2 = 2$ ci dà $a^2 = 2b^2$, di conseguenza a^2 è pari, e quindi anche a è pari. Sia $a = 2a_1$, con un intero a_1. Allora $4a_1^2 = 2b^2$. Di conseguenza $2a_1^2 = b^2$, e quindi b^2 è pari. Questo implica che anche b è pari, assurdo. $\square$

L'Esercizio 4.4 ci permette di asserire che l'insieme $\mathbb{Q}$ è strettamente contenuto in $\mathbb{R}$. Gli elementi di tale insieme $\mathbb{R} \setminus \mathbb{Q}$ si dicono *numeri irrazionali*.

Esercizio 4.5 *Usando il principio di induzione, provare che per ogni $x \in \mathbb{R}$, tale che $x \geq -1$ e per ogni $n \in \mathbb{N}$ risulta $(1+x)^n \geq 1 + nx$.*

Esercizio 4.6 *Dimostrare che la media aritmetica è maggiore o uguale alla media geometrica. cioè, dati $a_i \in \mathbb{R}$, con $a_i > 0$, per $i = 1, 2, \ldots, n$ si dimostri che*

$$\sqrt[n]{a_1 \cdot a_2 \cdot \ldots \cdot a_n} \quad \leq \quad \frac{a_1 + a_2 + \ldots + a_n}{n}.$$

SVOLGIMENTO. Eleviamo tutto alla n e quindi dobbiamo dimostrare la seguente proprietà $A(n)$

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n \ \leq \ \left(\frac{a_1 + a_2 + \ldots + a_n}{n}\right)^n \text{ vale per ogni } n\text{-upla } a_1, \ldots, a_n \text{ in } \mathbb{R}_+.$$

E' facile verificare che $A(1)$ ed $A(2)$ sono vere. Verifichiamo ora che $A(t)$ implica $A(2t)$ per ogni $t \geq 1$. Infatti, siano $a_1, a_2, \ldots, a_{2t}$ numeri reali positivi. Essendo $A(t)$ vera si ha

$$a_1 \cdot a_2 \cdot \ldots \cdot a_t \quad \leq \quad \left(\frac{a_1 + a_2 + \ldots + a_t}{t}\right)^t, \tag{1}$$

ma anche

$$a_{t+1} \cdot a_{t+2} \cdot \ldots \cdot a_{2t} \quad \leq \quad \left(\frac{a_{t+1} + a_{t+2} + \ldots + a_{2t}}{t}\right)^t, \tag{2}$$

Moltiplichiamo tra loro le disuguaglianze (1) e (2)

$$a_1 \cdot a_2 \cdot \ldots \cdot a_t \cdot a_{t+1} \cdot a_{t+2} \cdot \ldots \cdot a_{2t} \leq \quad \left(\frac{a_1 + a_2 + \ldots + a_t}{t}\right)^t \cdot \left(\frac{a_{t+1} + a_{t+2} + \ldots + a_{2t}}{t}\right)^t \tag{3}$$

Considerando ora i due fattori del secondo membro della disuguaglianza così ottenuta e utilizzando $A(2)$ già dimostrata, sia ha (prima utilizzo $A(2)$ e poi elevo alla t)

$$\left(\frac{a_1 + a_2 + \ldots + a_t}{t}\right)^t \cdot \left(\frac{a_{t+1} + a_{t+2} + \ldots + a_{2t}}{t}\right)^t \ \leq$$

$$\leq \left(\frac{a_1 + a_2 + \ldots + a_t + a_{t+1} + a_{t+2} + \ldots + a_{2t}}{2t}\right)^{2t}.$$

Mettendo assieme l'ultima disuguaglianza e la disuguaglianza (3), si ottiene la tesi.
Adesso supponiamo $m > 2$ e $V(k)$ vera per tutti i k con $1 \leq k < m$. Consideriamo due casi. Se $m = 2t$, allora $2 \leq t < m$ e quindi possiamo supporre che $A(t)$ sia vera. Per il fatto appena dimostrato, questo implica anche $A(2t)$ vera. Si ottiene, dunque, la tesi nel caso m pari.
Supponiamo ora $m = 2t - 1$, allora $2 < m$ e quindi $2 \leq t = (m+1)/2 < m$. Possiamo supporre che $A(t)$ sia vera. Per il fatto appena dimostrato, questo implica anche $A(2t)$ vera. La applicheremo ai numeri $a_1, a_2, \ldots, a_{2t-1}, s$, dove $s = \frac{a_1+a_2+\ldots+a_{2t-1}}{2t-1}$ è la media aritmetica. La disuguaglianza per il caso di $2t$ fattori ci dà:

$$a_1 \cdot a_2 \cdot \ldots \cdot a_{2t-1} \cdot s \leq \left(\frac{(a_1 + a_2 + \ldots + a_{2t-1}) + s}{2t} \right)^{2t}.$$

Ora $a_1 + a_2 + \ldots + a_{2t-1} = s(2t-1)$ e quindi sostituisco nel secondo membro della precedente disuguaglianza e divido tutto per s, ottenendo

$$\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_{2t-1} \cdot s}{s} \leq \left(\frac{s(2t-1) + s}{s \cdot 2t} \right)^{2t} = \frac{s^{2t}}{s}.$$

Eliminando s e risostituendo l'espressione per s otteniamo

$$a_1 \cdot a_2 \cdot \ldots \cdot a_{2t-1} \leq s^{2t-1} = \left(\frac{a_1 + a_2 + \ldots + a_{2t-1}}{2t-1} \right)^{2t-1}.$$

□

Esercizio 4.7 *Si dimostri che*

$$\frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_n}} \leq \sqrt[n]{a_1 \cdot a_2 \cdot \ldots \cdot a_n}.$$

SUGGERIMENTI. Si usi l'Esercizio 4.6. □

4.2 I numeri complessi

Nell'insieme delle coppie ordinate dei numeri reali $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ definiamo due operazioni di addizione e moltiplicazione ponendo, per ogni $z = (a, b), z' = (a', b') \in \mathbb{C}$:

$$z + z' = (a + a', b + b') \qquad z \cdot z' = (aa' - bb', ab' + ba').$$

Valgono le seguenti proprietà per ogni $z = (a, b), z' = (a', b'), z'' = (a'', b'') \in \mathbb{C}$:

A1. $z + (z' + z'') = (z + z') + z''$ (associativa dell'addizione);
A2. $z + z' = z' + z$ (commutativa dell'addizione);
A3. $z + (0, 0) = z$ (elemento neutro dell'addizione);
A4. $(a, b) + (-a, -b) = (0, 0)$ (opposto);
M1. $z \cdot (z' \cdot z'') = (z \cdot z') \cdot z''$ (associativa della moltiplicazione);
M2. $z \cdot z' = z \cdot z'$ (commutativa della moltiplicazione) ;
M3. $z \cdot (1, 0) = z$ (elemento neutro della moltiplicazione);
M4. $(a, b) \cdot (a/(a^2 + b^2), -b/(a^2 + b^2)) = (1, 0)$ (inverso) ;
D1. $z \cdot (z' + z'') = z \cdot z' + z \cdot z''$ (distributiva della moltiplicazione rispetto all'addizione).

Allora $\mathbb{C}$, con queste due operazioni, risulta essere un campo che chiameremo il *campo complesso* e definiamo i suoi elementi *numeri complessi*.

L'applicazione $j : \mathbb{R} \longrightarrow \mathbb{C}$ tale che $j(a) = (a, 0)$ è un'applicazione iniettiva che conserva le somme e i prodotti. Questo ci permette di identificare i numeri reali con i numeri complessi della forma $(a, 0)$ e di pensare ad $\mathbb{R}$ come a un sottoinsieme (sottocampo) di $\mathbb{C}$.

Denotiamo con i l'elemento $(0, 1)$ di $\mathbb{C}$ e lo chiamiamo *unità immaginaria*. Osserviamo che $i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -1$, in base all'identificazione appena vista. Quindi i e' una radice quadrata di -1.
Ora ogni numero complesso si può scrivere nella forma seguente, utilizzando l'identificazione di $\mathbb{R}$ in $\mathbb{C}$.

$$z = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1) = (a, b) = a + bi.$$

In questo modo a si dice la *parte reale di* z e si denota $a = Re(z)$ e $b = Im(z)$ si dice la *parte immaginaria di* z. Con questa nuova notazione, risulterà più comodo operare utilizzando le usuali regole del calcolo letterale, ricordando che si ha $i^2 = -1$.

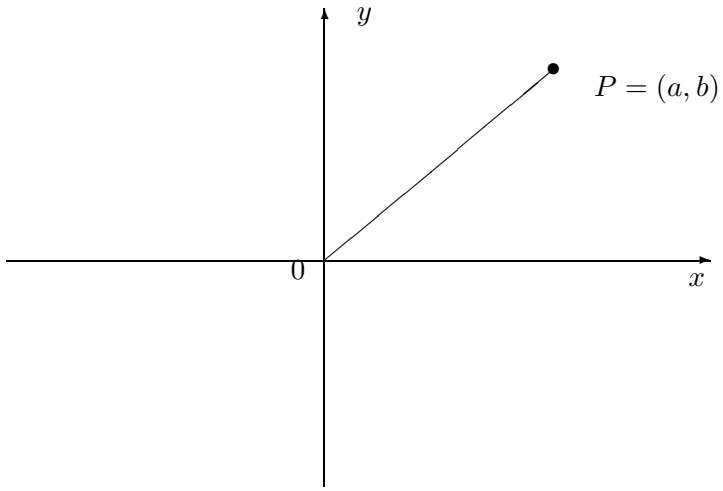
Esempio 4.8 $(1 + i\sqrt{2})(7 - i) = (7 + \sqrt{2}) + i(-1 + 7\sqrt{2})$,

$$\frac{1 + i3}{4 - i\sqrt{2}} = \frac{(1 + i3)(4 + i\sqrt{2})}{(4 - i\sqrt{2})(4 + i\sqrt{2})} = \frac{4 - 3\sqrt{2}}{18} + i\frac{12 + \sqrt{2}}{18}.$$

Definiamo la *coniugazione* di un elemento $z = a + ib$ come $\overline{z} = a - ib$. La coniugazione è un'applicazione che conserva le somme e i prodotti. Inoltre è un'applicazione involutoria, cioè $\overline{\overline{z}} = z$ e pertanto è biiettiva e la sua inversa coincide con la coniugazione stessa. Valgono inoltre le seguenti proprietà:

$$z + \overline{z} = 2Re(z) \in \mathbb{R}; \quad z - \overline{z} = 2iIm(z) \in i\mathbb{R}; \quad z \cdot \overline{z} = a^2 + b^2 \in \mathbb{R}.$$

Fissiamo ora un sistema di coordinate cartesiane ortogonali x, y su un piano che chiameremo *piano di (Argand)-Gauss*. Ogni numero complesso $a+ib$ si può rappresentare geometricamente con il punto P di coordinate (a, b). Questa assegnazione dà luogo ad una corrispondenza biunivoca tra i punti del piano di Gauss e i numeri complessi.



L'asse x è detto *asse reale* e l'asse y è detto *asse immaginario*. La distanza di $P = (a, b)$ dall'origine, cioè il numero reale non negativo $\rho = \sqrt{a^2 + b^2}$ è detto il *modulo* del numero complesso $z = a + ib$ e viene denotato con $|z|$. Il numero reale φ che misura l'angolo orientato

formato dal semiasse positivo delle x e dalla semiretta di origine 0 e passante per P viene detto *argomento* o *anomalia* di $z = a + ib$. Osserviamo che φ non è determinato se $P = 0$, cioè se $z = 0$. Concludiamo che un numero complesso diverso da zero individua univocamente il proprio modulo, ma determina il proprio argomento solo a meno di multipli interi di 2π. Osserviamo che $|z| = \sqrt{z \cdot \overline{z}}$ e quindi l'inverso del numero complesso z è

$$z^{-1} = \frac{\overline{z}}{|z|^2}.$$

Dalla definizione di seno e coseno si ha

$$a = \rho\ cos(\varphi), \quad b = \rho\ sen(\varphi), \quad z = \rho(cos(\varphi) + isen(\varphi)).$$

Questa è la *forma trigonometrica* del numero complesso z.
La scrittura in forma trigonometrica è molto utile per calcolare il prodotto di due numeri complessi $z = \rho(cos(\varphi) + isen(\varphi))$ e $z' = \rho'(cos(\varphi') + isen(\varphi'))$.

$$\begin{aligned} z \cdot z' &= \rho((cos(\varphi) + isen(\varphi)\rho'((cos(\varphi') + isen(\varphi') = \\ &= (\rho\rho')[(cos(\varphi)cos(\varphi') - sen(\varphi)sen(\varphi')) + i(cos(\varphi)sen(\varphi') + sen(\varphi)cos(\varphi'))] = \\ &= (\rho\rho')(cos(\varphi + \varphi') + sen(\varphi + \varphi')). \end{aligned}$$

Pertanto il prodotto di due numeri complessi ha per modulo il prodotto dei moduli e per argomento la somma degli argomenti. Questo semplice calcolo ha però come corollario una formula che si rivelerà molto utile.

Corollario 4.9 *Formula di De Moivre* *Se $z = \rho(cos(\varphi) + isen(\varphi))$ è un numero complesso scritto in forma trigonometrica, e $n \in \mathbb{N}$, allora*

$$z^n = \rho^n(cos(n\varphi) + isen(n\varphi))$$

Dimostrazione. La dimostrazione è per induzione su n e utilizza la formula del prodotto di due numeri complessi. □

Una conseguenza della formula di De Moivre è il calcolo delle soluzioni dell'equazione in $x^n = w$, $w \in \mathbb{C}$. Infatti z è soluzione di quest'equazione, e si dice che z è *radice n-esima* di w, se e solo se $z^n = w$. Pertanto se $0 \neq z = \rho(cos(\varphi) + isen(\varphi))$ e $0 \neq w = \tau(cos(\vartheta) + isen(\vartheta))$, dalla formula di de Moivre si deduce

$$\rho = \sqrt[n]{\tau} \qquad \varphi = (\vartheta + 2k\pi)/n, \quad k \in \mathbb{Z}.$$

Pertanto se

$$z_k = \sqrt[n]{\tau}\left(cos\left(\frac{\vartheta + 2k\pi}{n}\right) + isen\left(\frac{\vartheta + 2k\pi}{n}\right)\right)$$

si ha che z_k è un radice n-esima di w per ogni $k \in \mathbb{Z}$. Sia ora $k \in \mathbb{Z}$, facciamo la divisione con il resto tra k ed n, otteniamo $k = qn + r$, con $0 \leq r \leq n - 1$ e quindi $z_k = z_r$. Inoltre $z_k = z_h$ se e solo se $k - h \in n\mathbb{Z}$. Pertanto $z_0, z_1, z_2, \ldots, z_{n-1}$ sono n radici distinte di w. Abbiamo così provato

Lemma 4.10 *Ogni numero complesso $w \neq 0$ ammette n radici n-esime distinte, per ogni $0 \neq n \in \mathbb{N}$. Esse sono rappresentate nel piano di Argand-Gauss dai vertici di un poligono regolare di n lati inscritto nella circonferenza di centro 0 e raggio $\sqrt[n]{|w|}$.*

Osserviamo infine che $w = 0$ ha un'unica radice n-esima $z = 0$.

4.3 Interpretazione geometrica delle operazioni tra numeri complessi

Ci sono facili interpretazioni geometriche di tutte e tre le operazioni tra numeri complessi.
L'addizione corrisponde alla *traslazione*. Infatti, il punto $z+b$ si ottiene dal punto z tramite la traslazione definita dal vettore con inizio l'origine 0 e con punto finale il punto rappresentato da b.
Se a è un numero complesso con $|a| = 1$, allora la moltiplicazione per a corrisponde alla rotazione (in senso antiorario e con centro 0) di angolo φ uguale all'argomento di a. Se invece $r = |a|$ è arbitrario, ma positivo, allora la moltiplicazione per a corrisponde alla rotazione di centro 0 ed angolo φ seguita dalla dilatazione di centro 0 e coefficiente r.
La coniugazione corrisponde alla simmetria di asse $0x$.
La retta definita dall'origine e dal punto z è precisamente il luogo determinato da tutti i numeri complessi del tipo λz, dove $\lambda \in \mathbb{R}$. I punti del segmento $[0, z]$ sono ottenuti con $0 \leq \lambda \leq 1$, mentre quelli della semiretta con inizio z che non contiene l'origine 0, con $\lambda \geq 1$ (e quelli della semiretta con inizio 0 che non contiene z, con $\lambda \leq 0$). Il punto medio del segmento $[0, z]$ è proprio $\frac{1}{2}z$.

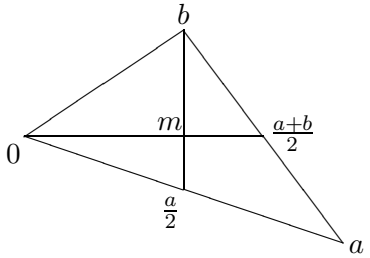
Esercizio 4.11 *Siano z_1 e z_2 due punti distinti del piano di Gauss-Argand. Determinare i numeri complessi che corrispondono ai punti della retta che passa per z_1 e z_2.*

SUGGERIMENTI. Traslando per $-z_1$ la retta l in questione diventa una retta che passa per l'origine e per il punto $z_2 - z_1$, ed è pertanto definita dai punti $\{\lambda(z_2 - z_1) : \lambda \in \mathbb{R}\}$. Ora traslando questa retta per z_1 troviamo che la retta l è definita dai punti $z_1 + \lambda(z_2 - z_1) = (1 - \lambda)z_1 + \lambda z_2$ per $\lambda \in \mathbb{R}$. I punti del segmento $[z_1, z_2]$ sono ottenuti con $0 \leq \lambda \leq 1$, ecc. □

Esercizio 4.12 *Siano z_1 e z_2 due punti distinti del piano di Gauss-Argand. Dimostrare che il punto medio del segmento $[z_1, z_2]$ corrisponde al punto $\frac{z_1+z_2}{2}$.*

Esercizio 4.13 *Usando queste espressioni delle rette dimostrare che le tre mediane di un triangolo si intersecano in un solo punto che le divide in rapporto $2 : 1$.*

SUGGERIMENTI. Rappresentiamo il triangolo nel piano di Gauss-Argand. Traslandolo possiamo supporre, senza ledere la generalità, che uno dei vertici coincida con l'origine 0 e pertanto i vertici del triangolo saranno 0, a e b con $a, b \in \mathbb{C}$. Usando gli esercizi precedenti, si vede facilmente che i punti della mediana che passa per 0 sono della forma $\mu\frac{a+b}{2}$, mentre i punti della mediana che passa per b sono della forma $\lambda\frac{a}{2} + (1 - \lambda)b$, dove $\mu, \lambda \in \mathbb{R}$. Il punto m dell'intersezione di queste due mediane corrisponde a valori di μ e λ che soddisfano $\lambda\frac{a}{2} + (1 - \lambda)b = \mu\frac{a+b}{2}$. Questo ci dà $(\mu/2 - \lambda/2)a + (\frac{\mu}{2} + \lambda - 1)b = 0$. Poiché i vettori a e b sono linearmente indipendenti, abbiamo $\mu/2 - \lambda/2 = 0$ e $\frac{\mu}{2} + \lambda - 1 = 0$. Di conseguenza $\mu = \lambda = 2/3$. Si noti che il punto di intersezione $m = \frac{a+b}{3}$ divide entrambe le mediane in rapporto $2 : 1$.



Analogamente si dimostra che la mediana che passa per il punto a passa anche per il punto m. $\square$

Esercizio 4.14 *Dimostrare che quattro punti a, b, c, d del piano di Gauss-Argand formano un parallelogramma se e solo se $a + c = b + d$.*

Esercizio 4.15 *Dimostrare che i punti medi dei quattro lati di un quadrangolo formano un parallelogramma.*

SUGGERIMENTI. Se a, b, c, d sono i quattro vertici di un quadrangolo, i punti medi sono $\frac{a+b}{2}$, $\frac{b+c}{2}$, $\frac{c+d}{2}$ e $\frac{d+a}{2}$. Ora basta applicare l'Esercizio precedente. $\square$

Esercizio 4.16 *Dimostrare che i punti medi di due lati opposti di un quadrangolo e i punti medi delle sue diagonali formano un parallelogramma.*

Esercizio 4.17 *Siano a e b due punti del piano di Gauss-Argand. Dimostrare che l'area del triangolo determinato da a, b e l'origine coincide con $\frac{1}{4}|b\overline{a} - a\overline{b}|$.*

SUGGERIMENTI. L'area S del triangolo coincide con il prodotto $\frac{|a|\cdot|b|\cdot\sin\varphi}{2}$, dove φ è l'angolo tra $0a$ e $0b$ in senso antiorario. L'angolo φ coincide anche con l'argomento del numero complesso $z = b/a$, perciò

$$\sin\varphi = \text{Im}\ \frac{z}{|z|} = \frac{z - \overline{z}}{2|z|i} = \frac{(b/a - \overline{b}/\overline{a})|a|}{2|b|i}.$$

Di conseguenza, $S = \frac{|a|^2\cdot(b/a - \overline{b}/\overline{a})}{4i} = \frac{\overline{a}b - a\overline{b}}{4i}$. Questo è il valore "algebrico" dell'area, che può essere negativo se $\varphi < 0$. Il valore assoluto dell'area è $\frac{|\overline{a}b - a\overline{b}|}{4}$. $\square$

4.4 Esercizi

Esercizio 4.18 *Esprimere nella forma $x + iy$ i seguenti numeri complessi $\frac{7-i6}{2+i3}$, $\frac{2i}{(2+i)^2}$.*

SVOLGIMENTO.

$$\frac{7 - i6}{2 + i3} = -\frac{4}{13} - i\frac{33}{13}; \qquad \frac{2i}{(2+i)^2} = \frac{8}{25} + i\frac{6}{25}.\square$$

Esercizio 4.19 *Si scrivano in forma trigonometrica $\frac{2-2i}{3+3i}$, $-7\sqrt{3}$, $(1 + i\sqrt{3})^2$.*

SVOLGIMENTO.

$$\frac{2 - 2i}{3 + 3i} = -\frac{2}{3}i = \frac{2}{3}\left(cos\left(\frac{3}{2}\pi\right) + isen\left(\frac{3}{2}\pi\right)\right); \qquad -7 = 7(cos\pi + isen(\pi));$$

$$(1 + i\sqrt{3})^2 = (1 - 3 + i2\sqrt{3}) = 4\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = 4\left(cos\left(\frac{2}{3}\pi\right) + isen\left(\frac{2}{3}\pi\right)\right).\square$$

Esercizio 4.20 *Si calcolino e si disegnino sul piano di Argand-Gauss le radici quarte dell'unità.*

SUGGERIMENTI. Le radici quarte dell'unità sono $i, -1, -i, 1$. $\square$

Esercizio 4.21 *Si calcolino $(1 + i)^6$, $(1 + i)^{86}$, $(1 + i\sqrt{3})^{42}$, $(\sqrt{3} - i)^{210}$.*

SVOLGIMENTO. Per fare questi calcoli ricordiamo che $(1/\sqrt{2} + i/\sqrt{2})$ è una radice ottava dell'unità, $cos(\pi/3) + isen(\pi/3)$ è radice sesta dell'unità e $cos(11\pi/6) + isen(11\pi/6)$ è radice dodicesima dell'unità.

$$(1+i)^6 = [\sqrt{2}(cos(\pi/4) + isen(\pi/4))]^6 = 8(cos(6\pi/4) + isen(6\pi/4) = -8i,$$

$$(1+i)^{86} = [(1+i)^2]^{43} = (2i)^{43} = -2^{43}i,$$

$$(1+i\sqrt{3})^{42} = [2(cos(\pi/3) + isen(\pi/3)]^{42} = 2^{42}[(cos(\pi/3) + isen(\pi/3)^6]^7 = 2^{42},$$

$(\sqrt{3} - i)^{210} = [2(cos(11\pi/6) + isen(11\pi/6))]^{210} =$
$= 2^{210}[(cos(11\pi/6) + isen(11\pi/6)^6]^{35} = 2^{210}(-1)^{35} = -2^{210}$. Un modo più veloce di fare questi calcoli è osservando che, per esempio $(1+i)^2 = 2i$ o che

$$(1+i\sqrt{3})^3 = 1 + 3\sqrt{3}i - 3 \cdot 3 - i3\sqrt{3} = -8,$$

o infine

$$(\sqrt{3} - i)^3 = 3\sqrt{3} - 9i - 3\sqrt{3} - i = 8i.\square$$

Esercizio 4.22 *Sia $z = \rho(cos(\varphi) + isen(\varphi)) \in \mathbb{C}$. Si scrivano in forma trigonometrica $\overline{z}$ e z^{-1}.*

SVOLGIMENTO.

$$\overline{z} = \rho(cos(-\varphi) + isen(-\varphi)) \qquad z^{-1} = \rho^{-1}(cos(-\varphi) + isen(-\varphi)).\square$$

Esercizio 4.23 *Si calcolino in $\mathbb{C}$ e si disegnino sul piano di Argand-Gauss le soluzioni delle seguenti equazioni $x^4 + i = 0$, $x^3 - 2i = 0$.*

SVOLGIMENTO. Sia $z = \rho(cos(\varphi) + isen(\varphi)) \in \mathbb{C}$ soluzione dell'equazione $x^4 + i = 0$. Allora

$$\rho^4 = 1, \quad 4\varphi = 3/2\pi + 2k\pi \quad \Longrightarrow \quad \rho = 1, \quad \varphi = 3\pi/8 + k\pi/2.\square$$

Sia ora $z = \rho(cos(\varphi) + isen(\varphi)) \in \mathbb{C}$ soluzione dell'equazione $x^3 = 2i$. Allora

$$\rho^3 = 2, \quad 3\varphi = \pi/2 + 2k\pi \quad \Longrightarrow \quad \rho = \sqrt[3]{2}, \quad \varphi = \pi/2 + 2k\pi/3.\square$$

Esercizio 4.24 *Si calcolino $(1-i)^{28}$, i^{-1}.*

Esercizio 4.25 *Si scrivano in forma trigonometrica i seguenti numeri complessi $3\sqrt{5}i$, $5 - 5i$.*

Esercizio 4.26 *Esprimere nella forma $x + iy$ i seguenti numeri complessi $\frac{1-i3}{3-i4}$, $\frac{(2-\sqrt{5}i)^2}{3i}$.*

Esercizio 4.27 *Calcolare (1-i)^{179}.*

SVOLGIMENTO. Sia $a = 1 - i$, allora $a^2 = -2i$ e $a^4 = -4$. Pertanto, $a^{179} = a^{4\cdot 44} \cdot a^2 \cdot a = 4^{44} \cdot (-2i) \cdot (1-i) = -2^{89}(1+i)$. $\square$

Esercizio 4.28 *Calcolare (1-i)^{79}.*

Esercizio 4.29 *Dimostrare che per ogni numero naturale $n \geq 1$ risulta:*

(a) $\binom{4n}{1} + \binom{4n}{5} + \binom{4n}{9} + \ldots \binom{4n}{4n-3} = \binom{4n}{3} + \binom{4n}{7} + \binom{4n}{11} + \ldots \binom{4n}{4n-1}$.

(b) $1 + \binom{12n+6}{4} + \binom{12n+6}{8} + \binom{12n+6}{12} + \ldots \binom{12n+6}{12n+4} = \binom{12n+6}{2} + \binom{12n+6}{6} + \binom{12n+6}{10} + \ldots \binom{12n+6}{12n+6}$.

SUGGERIMENTI. (a) Si applichi la formula del binomio per $(1+i)^{4n}$. $\square$

5 Complementi su Insiemi

5.1 Assioma della scelta e buoni ordini

Vogliamo dimostrare che ogni insieme non vuoto ammette una relazione di buon ordine. Ovviamente, ogni insieme finito X ammette un buon ordine, quello dato dalla biiezione $\{1, 2, \ldots, n\} \to X$, dove $n = |X|$ (vedi l'Esercizio 6.10 per il caso numerabile). Il caso generale è noto come

Teorema di Zermelo. *Ogni insieme non vuoto ammette una relazione di buon ordine.*

La dimostrazione di questo teorema richiede un'assioma detto l'Assioma della scelta. Esso può essere formulato in varie forme equivalenti. Solitamente si usa questa:

Assioma della scelta. *Sia $\{A_i\}_{i\in I}$ una famiglia di insiemi non vuoti con $I \neq \emptyset$. Allora esiste un'applicazione $f : I \to \bigcup_{i\in I} A_i$ tale che $f(i) \in A_i$ per ogni $i \in I$.*

Definizione 5.1 L'applicazione f con questa proprietà si chiama *funzione di scelta* per la famiglia $\{A_i\}_{i\in I}$.

Quindi, l'Assioma della scelta afferma che ogni famiglia non vuota di insiemi non vuoti ammette una funzione di scelta. Nel 1908 *Zermelo* propose una versione diversa dell'assioma della scelta, con la richiesta che gli insiemi A_i fossero a due a due disgiunti. *Russell* provò nello stesso anno che le due forme sono equivalenti.
In questo paragrafo utilizzeremo anche la seguente forma equivalente.

Lemma 5.2 *L'assioma della scelta è equivalente alla seguente affermazione:*
$(*)$ per ogni insieme non vuoto X esiste un'applicazione $f : \mathcal{P}(X)\setminus\{\emptyset\} \to X$ tale che $f(A) \in A$ per ogni $\emptyset \neq A \in \mathcal{P}(X)$.

Dimostrazione. Ovviamente, l'assioma della scelta implica $(*)$, prendendo come famiglia non vuota di insiemi non vuoti proprio $\mathcal{P}(X) \setminus \{\emptyset\}$. Per dimostrare che $(*)$ implica l'Assioma della scelta basta prendere una famiglia $\{A_i\}_{i\in I}$ di insiemi non vuoti con $I \neq \emptyset$. Sia $X = \bigcup_{i\in I} A_i$ e sia $j : I \to \mathcal{P}(X) \setminus \{\emptyset\}$ definita da $j(i) = A_i$. Allora $(*)$ applicata a X e composta con j, determina una funzione di scelta per la famiglia $\{A_i\}_{i\in I}$. □

Per capire bene la relazione tra l'Assioma della scelta e il Teorema di Zermelo vediamo che il Teorema di Zermelo implica l'Assioma della scelta. Infatti, se X è un'insieme non vuoto e $\leq$ è un buon ordine su X, allora basta porre $f(A) = \min A$ per ogni $A \in \mathcal{P}(X) \setminus \{\emptyset\}$. In altre parole, ogni buon ordine $\leq$ su X determina un'applicazione

$$f : \mathcal{P}(X) \setminus \{\emptyset\} \to X, \text{ tale che } f(B) \in B \text{ per ogni } B \subset X. \tag{1}$$

cioè una funzione scelta per la famiglia $\mathcal{P}(X) \setminus \{\emptyset\}$ (vedi l'Esercizio 6.45 per un'altra dimostrazione).
Possiamo ora dimostrare il Teorema di Zermelo.

Dimostrazione del Teorema di Zermelo. Sia X un insieme non vuoto. Per l'assioma della scelta esiste un'applicazione $g : \mathcal{P}(X) \setminus \{\emptyset\} \to X$ tale che $g(A) \in A$ per ogni $\emptyset \neq A \in \mathcal{P}(X)$. Sia $c : \mathcal{P}(X) \to \mathcal{P}(X)$ l'applicazione che manda ogni sottoinsieme A di X nel suo complemento $X \setminus A$. Allora la composizione $f = g \circ c$ è un'applicazione $\mathcal{P}(X) \setminus \{X\} \to X$ che soddisfa $f(B) \notin B$ per ogni $B \subseteq X$ distinto da X stesso. L'idea è di costruire un ordine $\leq$ su X tale che per ogni sottoinsieme proprio B di X, posto $x = f(B)$, B risulta essere il segmento iniziale $I(x) = \{y \in X : y < x\}$ di tutti gli elementi di X minori di x. Partendo da

questa idea, $x_0 = f(\emptyset)$ sarà l'elemento minimo di $\leq$ (essendo $I(x_0) = \emptyset$), $x_1 = f(\{x_0\})$ sarà il successore di x_0, $x_2 = f(\{x_0, x_1\})$ il successore di x_1, $x_3 = f(\{x_0, x_1, x_2\})$ sarà il successore di x_2 e così via. L'ordine $x_0 < x_1 < x_2 < \ldots < x_n$ è un buon ordine per ogni n.
Per rendere questo argomento rigoroso bisogna ragionare così. Abbiamo visto che esistono sottoinsiemi non vuoti A di X che ammettono un buon ordine $\leq_A$ per il quale per ogni $a \in A$ e per il segmento iniziale $I_A(a) := \{y \in A : y <_A x\}$ si ha $f(I_A(a)) = a$ (per esempio, $A = \{x_0, x_1, x_2, x_3\}$). Denotiamo con $\mathcal{A}$ la famiglia di tutti i sottoinsiemi A di X, con questa proprietà. Il nostro scopo è di dimostrare che $X \in \mathcal{A}$.

Passo 1. Dimostrare che se A e B appartengono ad $\mathcal{A}$, allora $A \subseteq B$ e l'ordine $\leq_B$ coincide con l'ordine $\leq_A$ su A, oppure $B \subseteq A$ e l'ordine $\leq_A$ coincide con l'ordine $\leq_B$ su B. Consideriamo $C = \{c \in A \cap B : I_A(c) = I_B(c)\})$ e dimostreremo che C coincide con A o B ragionando per assurdo. Cioè supponendo $A \not\subseteq B$ (risp. $B \not\subseteq A$) abbiamo $A \setminus C \neq \emptyset$ (risp. $B \setminus C \neq \emptyset$). Sia a il minimo elemento di $A \setminus C$ e sia b il minimo elemento di $B \setminus C$. Allora ogni $a' \in I_A(a)$ appartiene a B in quanto $a' < a$ e $a' \in A$. Analogamente $I_B(b) \subseteq A$. Pertanto $I_A(a) \subseteq A \cap B$ e $I_B(b) \subseteq A \cap B$. Ora dimostriamo che $I_A(a) \subseteq I_B(b)$. Sia $a' \in I_A(a)$. Allora $a' \in C \subseteq A \cap B$. Notiamo che $a' \neq b$ poiché $b \notin C$. Per l'Esercizio 6.14 gli elementi $a', b \in B$ sono confrontabili. Supponiamo $a' >_B b$. Allora $b \in I_B(a') = I_A(a')$ (perché $a' \in C$). Quindi $b \in A$ e $b <_A a' <_A a$. Di conseguenza $b \in C$, assurdo. Quindi, $a' <_B b$, cioè $a' \in I_B(b)$. Analogamente si dimostra che $I_B(b) \subseteq I_A(a)$. Ora l'uguaglianza $I_A(a) = I_B(b)$ implica $a = f(I_A(a)) = f(I_B(b)) = b$. Quindi $c = a = b \in A \cap B$ e $I_A(c) \subseteq I_B(c)$. Pertanto $c \in C$, assurdo. Questo dimostra che C coincide con A o B, di conseguenza abbiamo dimostrato la tesi del Passo 1. Inoltre, se $A \subseteq B$, A risulta essere il segmento iniziale di B determinato dal minimo elemento b di B che non appartiene ad A.

Passo 2. Sia $Y = \bigcup_{A \in \mathcal{A}} A$. Se $a, b \in Y$, allora per il Passo 1 esiste $A \in \mathcal{A}$, tale che $a, b \in A$. Poniamo $a \leq b$ se $a \leq_A b$. Dobbiamo ora verificare che questo definisce un buon ordine $\leq_Y$ in Y per il quale risulta $Y \in \mathcal{A}$. Sia M un sottoinsieme non vuoto di Y. Allora esiste $A \in \mathcal{A}$ tale che $M \cap A \neq \emptyset$. Quindi $M \cap A$ ha un elemento minimo m. Per provare che m è un elemento minimo di M, prendiamo $y \in M$. Se $y \in M \cap A$ ovviamente si ha $m \leq y$. Supponiamo $y \in M \setminus A$. Allora esiste $B \in \mathcal{A}$ tale che $y \in B$. Per il passo 1, $A \subseteq B$ (infatti, y ci fa vedere che $B \subseteq A$ non vale). Per il fatto che A è un segmento iniziale di B e per la scelta di m, concludiamo che $m < y$. Pertanto, m è un elemento minimo di M.

Passo 3. Se risulta $Y = X$, allora $(X, \leq_X)$ è ben ordinato. Supponiamo per assurdo che $Y \neq X$. Allora con $x = f(Y)$ poniamo $Z = Y \cup \{x\}$ e estendiamo l'ordine $\leq_Y$ di Y su Z ponendo $y \leq_Z x$ per tutti gli $y \in Y$. Con questo ordine $(Z, \leq_Z)$ è ben ordinato e appartiene a $\mathcal{A}$ in quanto $I_Z(x) = Y$ e $f(Y) = x$. Ma allora $x \in Z \subseteq Y$, assurdo. •

Ora possiamo usare l'assioma della scelta per dimostrare una proprietà delle applicazioni che risulta un'altra forma equivalente dell'assioma della scelta.

Teorema 5.3 *L'assioma della scelta è equivalente alla seguente proprietà: per ogni applicazione $f : X \to Y$ suriettiva esiste una funzione*[1] *$g : Y \to X$ tale che $f \circ g = id_Y$.*

Dimostrazione. Supponiamo che la proprietà sia verificata. Per verificare l'assioma della scelta usiamo la forma di Zermelo. Quindi basta provare che per ogni famiglia non vuota $\mathcal{A} = \{A_i\}_{i \in I}$ di insiemi non vuoti a due a due disgiunti esiste un'applicazione $h : I \to \bigcup_{i \in I} A_i$ tale che $h(i) \in A_i$ per ogni $i \in I$. Sia $X = \bigcup_{i \in I} A_i$ e sia $f : X \to \mathcal{A}$ l'applicazione definita da $f(a) = A_i$ per ogni $i \in I$ e $a \in A_i$. Allora f è suriettiva, e quindi esiste $g : \mathcal{A} \to X$ tale che

[1] Se esiste una tale g con $f \circ g = id_Y$, allora f è suriettiva perché la suriettività di $f \circ g$ (dato che id_Y è suriettiva) implica la suriettività di f. Analogamente, la iniettività di id_Y implica che g è iniettiva.

$f(g(A_i)) = A_i$ per ogni $i \in I$. Allora $a_i = g(A_i) \in A_i$ per ogni $i \in I$. Ora la composizione h dell'applicazione $I \to \mathcal{A}$, definita da $i \mapsto A_i$, e g serve come funzione scelta $h : I \to \bigcup_{i\in I} A_i$ desiderata.
Supponiamo che valga l'assioma della scelta e che $f : X \to Y$ sia un'applicazione suriettiva. Allora, dato $y \in Y$, esiste $x \in X$ tale che $f(x) = y$. Scelgo un tale $x \in f^{-1}(y)$ e definisco $g : Y \to X$ tramite $g(y) = x$ (quell'unico x che ho scelto). Quindi, per costruzione della g, si ha $f(g(y)) = f(x) = y$. □

Si noti che l'applicazione g è iniettiva. Quindi, questa proprietà si può enunciare anche così: *esiste un applicazione suriettiva $f : X \to Y$ se e solo se esiste un'applicazione iniettiva $g : Y \to X$.*

La seguente importante proprietà è nota come Lemma di Zorn. Essa trova molte applicazioni nell'Algebra e nell'Analisi per dimostrare l'esistenza di certi oggetti con proprietà estremali (vedi per esempio la dimostrazione del Teorema di Hartogs nel paragrafo 5.3). Per un'applicazione immediata si veda anche lo svolgimento degli Esercizi 6.48 e la dimostrazione del Lemma 5.13. Per poter enunciare il Lemma di Zorn, abbiamo prima bisogno di una definizione:

Definizione 5.4 Un insieme parzialmente ordinato $(A, \leq)$ si dice *induttivo* se ogni catena ha un maggiorante.

L'Esercizio 6.8 garantisce l'esistenza di insiemi induttivi, per esempio tutti gli insiemi parzialmente ordinati finiti.
Vedremo ora che la dimostrazione di questo lemma usa l'assioma della scelta. D'altra parte, si può dimostrare che il Lemma di Zorn implica l'assioma della scelta.

Lemma di Zorn. *Ogni insieme parzialmente ordinato e induttivo ammette elementi massimali.*

Dimostrazione. Sia $(X, \leq)$ un insieme ordinato induttivo. Supponiamo per assurdo che X non abbia elementi massimali e denotiamo con $\mathcal{B}$ la famiglia di tutti i sottoinsiemi superiormente limitati di X. Per la nostra ipotesi, $X \notin \mathcal{B}$ e ogni catena è superiormente limitata, quindi appartiene a $\mathcal{B}$.
Per ogni insieme $B \in \mathcal{B}$ denotiamo con $M(B)$ l'insieme (non vuoto) dei maggioranti di B e notiamo che $M(B) \not\subseteq B$. Infatti, ogni $b_0 \in M(B) \cap B$ è un elemento massimo di B. Poiché X non ha elementi massimali, esiste $x \in X$ con $x > b_0$ (altrimenti b_0 sarebbe massimale). Ora $x \in M(B) \setminus B$. Abbiamo così dimostrato che $M(B) \setminus B \neq \emptyset$ per ogni $B \in \mathcal{B}$. Sia f una funzione scelta definita per la famiglia $\{M(B) \setminus B : B \in \mathcal{B}\}$. Definiamo ora $g : \mathcal{B} \to X$ con $g(B) = f(M(B) \setminus B)$. Per $x_0 = f(X)$ (si noti che $X = M(\emptyset)$) il segmento iniziale $I(x_0)$ nell'insieme ben ordinato $(\{x_0\}, \leq)$ è vuoto e quindi $x_0 = g(I(x_0))$. Sia $\mathcal{A}$ la famiglia di tutti i sottoinsiemi $A \subseteq X$ tali che $(A, \leq)$ è ben ordinato e per ogni $a \in A$ si ha $a = g(I_A(a))$, dove $I_A(a)$ è il segmento iniziale in A determinato da a (ovviamente $I_A(a) \in \mathcal{B}$). Ovviamente, $\{x_0\} \in \mathcal{A}$, pertanto $\mathcal{A}$ non è vuoto.
Passo 1. Dimostrare che se A e $B \in \mathcal{A}$, allora $A \subseteq B$, oppure $B \subseteq A$. Poniamo $C = \{c \in A \cap B : I_A(c) = I_B(c)\}$ e dimostreremo che C coincide con A o B ragionando per assurdo. Sia a il minimo elemento di $A \setminus C$ e sia b il minimo elemento di $B \setminus C$. Vogliamo dimostrare che $I_A(a) = I_B(b)$. Sia $x \in I_A(a)$. Allora $x \in A$ e $x < a$ implica $x \in C$. Quindi $x \in B$ e $I_A(x) = I_B(x)$. Notiamo che $x \neq b$ poiché $b \notin C$. Per l'Esercizio 6.14 gli elementi $x, b \in B$ sono paragonabili. Supponiamo $x > b$. Allora da $I_A(x) = I_B(x)$ si avrebbe $b \in A$ e $b < x < a$. Di conseguenza $b \in C$, assurdo. Quindi, $x < b$, cioè $x \in I_B(b)$. Analogamente si dimostra che $I_B(b) \subseteq I_A(a)$. Ora l'uguaglianza $I_A(a) = I_B(b)$ implica $a = g(I_A(a)) = g(I_B(b)) = b$. Quindi

$c = a = b \in A \cap B$ e $I_A(c) = I_B(c)$. Pertanto $c \in C$, assurdo. Questo dimostra che C coincide con A o B, di conseguenza abbiamo dimostrato che $A \subseteq B$, oppure $B \subseteq A$.

Passo 2. Sia $Y = \bigcup_{A \in \mathcal{A}} A$. Allora Y è una catena in X in quanto per ogni coppia $a, b \in Y$, esistono $A \in \mathcal{A}$ e $B \in \mathcal{A}$ con $a \in A$ e $b \in B$. Per il Passo 1, $A \subseteq B$, oppure $B \subseteq A$. Pertanto si avrà $a, b \in A$ oppure $a, b \in B$. Quindi vale $a \leq b$ oppure $b \leq a$. Essendo Y una catena si ha $Y \in \mathcal{B}$. Poniamo $z = g(Y)$ e notiamo che $Z = Y \cup \{z\}$ risulta essere ben ordinato con l'ordine $\leq$ e $g(I_Z(z)) = z$. Quindi $Z \in \mathcal{A}$. Poiché Z contiene propriamente Y, questo contraddice la definizione di Y. □

5.1.1 Principio dell'induzione transfinita

In un insieme ben ordinato $(X, \leq)$ si può definire il concetto di *successore* di un elemento x, come il minimo elemento dell'insieme di tutti gli elementi $y > x$ di X. Analogamente, si può definire anche il concetto di successore $succ(Y)$ di un *sottoinsieme* $Y \neq X$ quale il minimo elemento del complemento di Y in X. D'altra parte, ogni elemento x determina anche l'insieme $I_X(x) := \{z \in X : z < x\}$, detto *segmento iniziale* (determinato da x), del quale risulta essere il successore.
Di particolare importanza è il seguente

Principio di induzione transfinita. *Se $(X, \leq)$ è un insieme ben ordinato con elemento minimo x_0 ed E è un sottoinsieme di X tale che*

(a) $x_0 \in E$

(b) E contiene tutti gli elementi $x \in X$ per i quali $I_X(x) \subseteq E$,

allora $E = X$.

Dimostrazione. Ragionando per assurdo supponiamo $E \neq X$. Allora l'insieme $X \setminus E \neq \emptyset$. Quindi, esiste un elemento minimo x di $X \setminus E$. Allora $y \in E$ per tutti gli $y < x$ in X. In altre parole, $I_X(x) \subseteq E$. Allora la condizione (b) implica $x \in E$, assurdo. □

Come caso particolare si ricava il principio di induzione. Infatti, poniamo $X = \mathbb{N}$ con l'usuale ordine $\leq$ in $\mathbb{N}$. Allora $(\mathbb{N}, \leq)$ risulta ben ordinato e in questo caso il principio di induzione transfinita coincide con il solito principio di induzione. Infatti, la condizione (b) nel caso di $\mathbb{N}$ è equivalente alla richiesta $n+1 \in E$ qualora $n \in E$ (si noti che in $\mathbb{N}$ ogni insieme superiormente limitato ha un elemento massimo, quindi $I_{\mathbb{N}}(x)$ ha un elemento massimo ovvero il predecessore di x).

5.2 Prodotti cartesiani

Siano X e Y due insiemi non vuoti. Per un elemento $x \in X$ e un elemento $y \in Y$ l'insieme $\{\{x\}, \{x, y\}\}$ si dice *coppia ordinata con prima coordinata x e seconda coordinata y* e si denota con (x, y). Non è difficile vedere che due coppie (x, y) e (x_1, y_1) coincidono se e solo se $x = x_1$ e $y = y_1$. Il *prodotto cartesiano* $X \times Y$ di X per Y è l'insieme di tutte le coppie ordinate (x, y), dove $x \in X$ e $y \in Y$.

5.2.1 Potenze cartesiani

Cominciamo con le potenze cartesiane, ovvero prodotti cartesiani di un insieme con se stesso. Nel caso $X = Y$ l'insieme di tutte le coppie (x, x) con $x \in X$ si denota con Δ_X e si chiama *diagonale* di $X \times X$. Scriveremo X^2 per denotare $X \times X$.

Siano A ed I due insiemi non vuoti. L'insieme di tutte le applicazioni $f : I \to A$ si denota con A^I. Discuteremo ora la possibilità di vedere l'insieme A^I come un prodotto cartesiano. Cominciamo con le potenze cartesiane finite.

Lemma 5.5 *Sia A un insieme non vuoto. Esiste una biiezione tra $A^{\{1,2\}}$ ed il prodotto cartesiano $A \times A$.*

DIMOSTRAZIONE. All'applicazione $f : \{1, 2\} \to A$ mettere in corrispondenza la coppia ordinata $(f(1), f(2))$ di $A \times A$. Questo definisce un'applicazione $\varphi : A^{\{1,2\}} \to A \times A$. Inoltre φ è invertibile, avendo come inversa l'applicazione $\psi : A \times A \to A^{\{1,2\}}$ che alla coppia $(a, b) \in A \times A$ associa l'applicazione $f : \{1, 2\} \to A$ definita da $f(1) = a$ e $f(2) = b$. □

La biiezione φ del Lemma 5.5 ci permette di identificare $A^{\{1,2\}}$ con il prodotto cartesiano $A \times A$ e scrivere più brevemente A^2. In questo modo non si distingue più tra una coppia ordinata di elementi di A ed un'applicazione $f : \{1, 2\} \to A$. Analogamente, per ogni $n > 1$ esiste una biiezione tra $A^{\{1,2,\ldots,n\}}$ ed il prodotto cartesiano $\underbrace{A \times A \times \ldots \times A}_{n \ \ volte}$ (vedi l'Esercizio 6.16). Grazie a questa biiezione identifichiamo l'insieme $A^{\{1,2,\ldots,n\}}$ con il suddetto prodotto cartesiano che scriviamo più brevemente A^n.

Analogamente, possiamo considerare un'applicazione $f : \mathbb{N} \to A$, cioè un elemento di $A^{\mathbb{N}}$, come una successione infinita $a_1, a_2, \ldots, a_n, \ldots$ di elementi di A. Questo dà una interpretazione della potenza cartesiana infinita $\underbrace{A \times A \times \ldots \times A \times \ldots}_{\text{infinite volte}}$. Nel caso generale, la potenza cartesiana A^I è semplicemente l'insieme di tutte le applicazioni $f : I \to A$.

5.2.2 Prodotti cartesiani di insiemi non necessariamente uguali

Nel caso di prodotti cartesiani di insiemi non necessariamente uguali bisogna ragionare così:

Lemma 5.6 *Siano A e B due insiemi non vuoti. Denotiamo con X l'insieme delle applicazioni $f : \{1, 2\} \to A \cup B$ con la proprietà $f(1) \in A$ e $f(2) \in B$. Trovare una biiezione tra X ed il prodotto cartesiano $A \times B$.*

DIMOSTRAZIONE. All'applicazione $f \in X$ mettere in corrispondenza la coppia ordinata $(f(1), f(2)) \in A \times B$. Questo definisce un'applicazione $\varphi : X \to A \times B$. Provare che φ è invertibile, avendo come inversa l'applicazione $\psi : A \times B \to X$ che alla coppia $(a, b) \in A \times B$ associa l'applicazione $f : \{1, 2\} \to A \cup B$ definita da $f(1) = a$ e $f(2) = b$. □

Grazie alla biiezione φ identifichiamo il prodotto cartesiano $A \times B$ con l'insieme delle applicazioni $f : \{1, 2\} \to A \cup B$ con la proprietà $f(1) \in A$ e $f(2) \in B$. Lo scopo di introdurre un tale punto di vista diventa chiaro quando si passa a prodotti cartesiani di più di due insiemi. Sia $n > 1$ e siano $A_1, A_2, \ldots, A_n$ degli insiemi non vuoti. Definiamo il prodotto cartesiano $A_1 \times A_2 \times \ldots \times A_n$ come l'insieme che ha come elementi tutte le n-uple ordinate $(a_1, a_2, \ldots, a_n)$ con $a_1 \in A_1$, $a_2 \in A_2$, …, $a_n \in A_n$ definite in modo analogo. Se tutti gli insiemi $A_1, A_2, \ldots, A_n$ coincidono con un dato insieme A, scriveremo brevemente A^n per il prodotto cartesiano $A_1 \times A_2 \times \ldots \times A_n$.

Ecco un altro modo di descrivere il suddetto prodotto cartesiano. Denotiamo con X l'insieme delle applicazioni $f : \{1, 2, \ldots, n\} \to A_1 \cup A_2 \cup \ldots \cup A_n$ con la proprietà $f(1) \in A_1$, $f(2) \in A_2$, …, $f(n) \in A_n$, che chiameremo *funzione di scelta* per la famiglia $A_1, \ldots, A_n$ (vedi anche la definizione 5.1). Allora esiste una biiezione tra X ed il prodotto cartesiano $A_1 \times A_2 \times \ldots \times$

A_n (vedi l'Esercizio 6.18). Grazie a questa biiezione identificheremo nel futuro il prodotto cartesiano $A_1 \times A_2 \times \ldots \times A_n$ con l'insieme delle funzioni di scelta per la famiglia $A_1, \ldots, A_n$. Sia $n > 1$ e siano $A_1, A_2, \ldots, A_n$ insiemi non vuoti. Per $i = 1, 2, \ldots, n$ definiamo la *proiezione* $p_i : A_1 \times A_2 \times \ldots \times A_n \to A_i$ con $p_i(a_1, a_2, \ldots, a_n) = a_i$. Queste applicazioni sono molto importanti per la definizione del prodotto cartesiano (vedi l'Esercizio 6.19).
Sia $\{A_i\}_{i \in I}$ una famiglia non vuota (cioè, $I \neq \emptyset$) di insiemi non vuoti A_i. Una *funzione di scelta* per questa famiglia è un'applicazione $f : I \to \bigcup_{i \in I} A_i$ tale che $f(i) \in A_i$ per ogni $i \in I$. Nel caso dei prodotti cartesiani finiti siamo riusciti a descrivere il prodotto cartesiano, a meno di una biiezione, come l'insieme di tutte le funzioni scelta (si vedano gli Esercizi 5.5-6.18). Nel caso di prodotto cartesiano di famiglie arbitrarie, questa resta l'unica strada da percorrere:

Definizione 5.7 Il *prodotto cartesiano* della famiglia $\{A_i\}_{i \in I}$, denotato con $\prod_{i \in I} A_i$, è l'insieme di tutte le funzioni di scelta della famiglia $\{A_i\}_{i \in I}$.

Esercizio 5.8 *Il prodotto cartesiano $\prod_{i \in I} A_i$ è non vuoto se I è finito.*

SUGGERIMENTI. Vedi l'Esercizio 6.20. □

Vediamo ora l'impatto dell'Assioma della scelta sui prodotti infiniti di insiemi. In generale, l'affermazione che il prodotto cartesiano $\prod_{i \in I} A_i$ sia non vuoto è ovviamente equivalente all'Assioma della scelta. Abbiamo costruito una funzione di scelta nel caso di I finito (Esercizio 6.22). Nonostante l'apparente "chiarezza" dell'esistenza della funzione scelta, l'Assioma della scelta non è dimostrabile a partire degli altri assiomi della teoria degli insiemi.
Analogamente a quanto fatto nel caso di prodotti finiti di insiemi, si può definire la proiezione anche nel caso infinito. Per $i \in I$ definiamo la *proiezione* $p_i : \prod_{i \in I} A_i \to A_i$ ponendo $p_i(f) = f(i)$ per ogni funzione di scelta $f \in \prod_{i \in I} A_i$.

5.3 Numeri cardinali.

In analogia con il caso di un insieme finito A, introduciamo qui un concetto di "misura" $|A|$ anche per insiemi infiniti A. Diremo che A e B sono *equipotenti*, e scriveremo $|A| = |B|$, se esiste una biiezione $A \to B$. Poiché è naturale avere $|A| \leq |B|$ per un sottoinsieme A di B, poniamo in generale $|A| \leq |B|$ se esiste un'applicazione iniettiva[2] $A \to B$. Scriveremo $|A| < |B|$ se vale $|A| \leq |B|$, ma non vale $|B| \leq |A|$. Nel seguente Teorema di Cantor-Bernstein vediamo che $|A| = |B|$ equivale alla validità simultaneamente di $|A| \leq |B|$ e $|B| \leq |A|$. Questo teorema fornisce anche un metodo utile alla determinazione di insiemi equipotenti.

Teorema di Cantor-Bernstein. *Siano S e T due insiemi non vuoti. Se esistono iniezioni $S \to T$ e $T \to S$, allora esiste anche una biiezione $S \to T$.*

DIMOSTRAZIONE. Per la dimostrazione di questo Teorema, avremo bisogno del seguente lemma che è praticamente un caso particolare del Teorema di Bernstein, nel quale uno degli insiemi è sottoinsieme dell'altro e la rispettiva iniezione è l'inclusione. Vedremo dopo, che il caso generale si deduce facilmente da questo caso.

`Lemma.` *Sia $f : X \to X$ un'applicazione iniettiva, ma non suriettiva. Allora per ogni sottoinsieme Y di X, tale che $f(X) \subseteq Y \subseteq X$, esiste una biiezione $h : Y \to X$.*

[2]D'altra parte, per il teorema 5.3, esiste un'applicazione suriettiva $A \to B$ se e solo se esiste un'applicazione iniettiva $B \to A$ (vedi anche l'Esercizio 6.36). Quindi, $|A| \leq |B|$ se e solo se esiste anche un un'applicazione suriettiva $B \to A$.

Cominciamo la dimostrazione del lemma. Per definire una biiezione $g : Y \to X$ basta definire una biiezione $s : Y \to f(X)$ e comporla con l'inversa di f su $f(X)$. Si consideri in X la relazione R così definita:

$$xRy \Leftrightarrow \text{ esistono } n, m \in \mathbb{N} \text{ con } \ f^n(x) = f^m(y).$$

Si dimostra facilmente che R è una relazione di equivalenza. Siano $\{C_i\}_{i\in I}$ le classi di equivalenza. Allora esse formano una partizione $X = \bigcup_{i\in I} C_i$ di X e, di conseguenza, una partizione $Y = \bigcup_{i\in I}(Y \cap C_i)$ di Y.
Fissiamo un $i \in I$ e notiamo che $Y \cap C_i \neq C_i$ accade se e solo se $C_i \not\subseteq Y$, e in particolare $C_i \not\subseteq f(X)$. Vediamo che esiste precisamente un elemento $z \in C_i \setminus f(X)$. Infatti se $z, z' \in C_i \setminus f(X)$, allora esistono $n, m \in \mathbb{N}$ con $f^n(z) = f^m(z')$. Per l'iniettività di f si può supporre che almeno uno tra n ed m sia 0. Per la scelta di z, z' deduciamo che tutte e due sono 0. Quindi $z = z'$ e pertanto $C_i = \{z\} \cup (f(X) \cap C_i)$. Poiché $C_i \supseteq Y \cap C_i \supseteq f(X) \cap C_i$, l'ipotesi $Y \cap C_i \neq C_i$ implica $Y \cap C_i = f(C_i)$. Pertanto la restrizione f_i di f su C_i risulta un biiezione $f_i : C_i \to Y \cap C_i$.
Ora definiamo un'applicazione $g : X \to Y$ nel modo seguente. Per $x \in X$ esiste un unico $i \in I$ tale che $x \in C_i$. Se $Y \cap C_i \neq C_i$, poniamo $g(x) = f(x)$, se $Y \cap C_i = C_i$, poniamo $g(X) = x$. Verifichiamo che

$$\text{per ogni } i \in I \text{ vale } g(C_i) = Y \cap C_i \text{ e } g^{-1}(Y \cap C_i) = C_i. \qquad (*)$$

Inoltre g definisce una biiezione tra C_i e $Y \cap C_i$. Questo è ovvio quando $Y \cap C_i = C_i$, perché allora la restrizione di g su C_i coincide con l'identità di C_i. Se $Y \cap C_i \neq C_i$, allora la restrizione di g su C_i coincide con la biiezione $f_i : C_i \to Y \cap C_i$. Questo dimostra $(*)$.
Per finire notiamo che g è suriettiva, in quanto $y \in Y$ appartiene a qualche $Y \cap C_i$ e quindi $y = g(x)$ per qualche $x \in C_i$, come visti sopra. Se $g(x) = g(z)$, allora esiste qualche i tale che $g(x) = g(z) \in Y \cap C_i$. Di nuovo, da $(*)$ e l'iniettività di g ristretta a C_i, concludiamo $x = z$.
Se $Y \cap C_i = C_i$, abbiamo ovviamente anche $|Y \cap C_i| = |C_i|$. Supponiamo che $C_i \not\subseteq Y$, in particolare $C_i \not\subseteq f(X)$. Notiamo che esiste precisamente un elemento $z \in C_i \setminus f(X)$. Infatti, se $z, z' \in C_i \setminus f(X)$, allora esistono $n, m \in \mathbb{N}$ con $f^n(z) = f^m(z')$. Per l'iniettività di f si può supporre che almeno uno tra n ed m sia 0. Per la scelta di z, z' deduciamo che tutte e due sono 0. Quindi $z = z'$. Per la dimostrazione del Teorema 2.11 esiste un'applicazione iniettiva $h : \mathbb{N} \to X$ con $h(0) = z$. Ora $C_i \setminus \{z\} \subseteq Y \cap C_i \subseteq C_i$, quindi $|Y \cap C_i| = |C_i| = |\mathbb{N}|$. A questo punto applichiamo l'Esercizio 6.47 che descrive come si può costruire una biiezione a partire da una famiglia opportuna di biiezioni. Nel nostro caso le biiezioni provengono dalle eguaglianze $|Y \cap C_i| = |C_i|$. La conclusione dell'Esercizio citato permette di concludere $|Y| = |X|$. Questo completa la dimostrazione del lemma.

Torniamo alla dimostrazione del Teorema di Cantor–Bernstein. Siano $r : S \to T$ e $q : T \to S$ due iniezioni. Allora basta applicare il lemma precedente per $X = S$, $Y = q(T)$ e $f = q \circ r$. □

L'idea usata nel Teorema di Cantor–Bernstein è costruire biiezioni a partire da applicazioni con proprietà più deboli, quali le iniezioni. Vediamo ora che ci sono iniezioni in abbondanza. Più precisamente, dati due insiemi S e T, si ha sempre la dicotomia $|S| \leq |T|$ oppure $|T| \leq |S|$.

Teorema di Hartogs. *Siano S e T due insiemi non vuoti. Allora esiste un'iniezione $S \to T$ oppure un'iniezione $T \to S$.*

Dimostrazione. Supponiamo che non esista un'iniezione $T \to S$. Per il Teorema 5.3 questo garantisce che non esiste nemmeno una suriezione $S \to T$. Dimostreremo che esiste una iniezione $S \to T$.

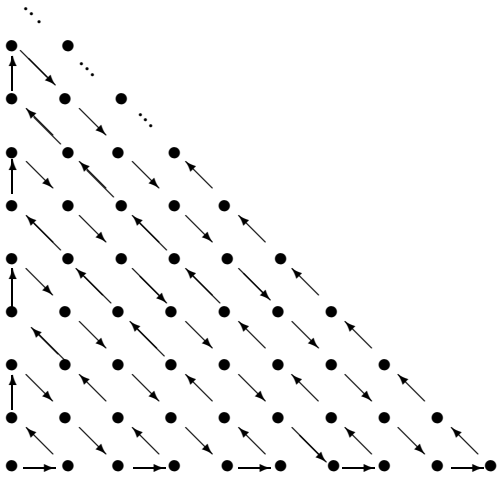
La famiglia $\mathcal{F}$ di tutte le applicazione iniettive $j_A : A \to T$, con $A \subseteq S$, è ordinata nel modo seguente: si pone $j_A \leq j_B$ per un'applicazione $j_B : B \to T$ se $A \subseteq B$ e $j_B(a) = j_A(a)$ per ogni $a \in A$. Dimostriamo ora che l'ordine $\leq$ di $\mathcal{F}$ è induttivo. Infatti, sia $\mathcal{C} = \{j_{B_i} : i \in I\}$ una catena in $\mathcal{F}$. Poniamo $B = \bigcup_{i\in I} B_i$ e definiamo $j_B : B \to T$ con $j_B(b) = j_{B_i}(b)$, se $b \in B_i$. La definizione è corretta, poiché se $b \in B_k$ per un altro $k \in I$, allora si ha $j_{B_i} \leq j_{B_k}$ oppure $j_{B_k} \leq j_{B_i}$. In entrambi casi $j_{B_k}(b) = j_{B_i}(b)$. Così abbiamo definito un elemento $j_B \in \mathcal{F}$ tale che $j_{B_i} \leq j_B$ per ogni $i \in I$. Quindi j_B è un maggiorante per la catena $\mathcal{C}$. Quindi $\mathcal{F}$ è induttivo. Pertanto $\mathcal{F}$ ha elementi massimali per il Lemma di Zorn. Sia $f = j_{B_0} : B_0 \to T$ un tale elemento massimale. Se $B_0 = S$ abbiamo costruito una iniezione $S \to T$. Supponiamo per assurdo che $B_0 \neq S$. Allora esiste un elemento $x \in S \setminus B_0$. Per la nostra ipotesi non esiste una suriezione $S \to T$. Quindi neanche $f : B_0 \to T$ è suriettiva (altrimenti si potrebbe facilmente estendere ad una suriezione $S \to T$). Pertanto $f(B_0) \neq T$ ed esiste $y \in T \setminus f(B_0)$. Ora si può estendere f a $B' = B_0 \cup \{x\}$ ponendo $j_{B'}(b) = b$ per tutti i $b \in B_0$ e $j_{B'}(x) = y$. Allora $j_{B'}$ è iniettiva e $j_{B_0} < j_{B'}$, che contraddice la massimalità di j_{B_0}. Questo assurdo dimostra l'uguaglianza $B_0 = S$. $\square$

Il Teorema di Hartogs garantisce che per due insiemi S e T si ha $|S| \leq |T|$ oppure $|T| \leq |S|$. In altre parole, i numeri cardinali sono sempre paragonabili. Il teorema di Cantor-Bernstein garantisce inoltre che, se abbiamo simultaneamente $|S| \leq |T|$ e $|T| \leq |S|$, allora $|S| = |T|$.
Per il teorema di Cantor vale $|X| < |\mathcal{P}(X)|$ (vedi Esercizio 2.10).

Definizione 5.9 Un insieme X si dice *numerabile*, se $|X| = |\mathbb{N}|$. La cardinalità dell'insieme $\mathcal{P}(\mathbb{N})$ è nota come *cardinalità del continuo* e si denota con $\mathfrak{c}$ (vedi la motivazione nell'Esercizio 6.54).

Lemma 5.10 $\mathbb{N} \times \mathbb{N}$ *è numerabile.*

Dimostrazione. A questo scopo troviamo un'applicazione iniettiva $h : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$. Definiamo h nel modo seguente: $h(0,0) = 0, h(1,0) = 1, h(0,1) = 2, h(0,2) = 3, h(1,1) = 4, h(2,0) = 5$, ecc. seguendo le frecce nel seguente diagramma



Poiché ovviamente esiste un'iniezione $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$, ora basta applicare il teorema di Cantor-Bernstein. $\square$

Il 7 Dicembre 1873 *Georg Cantor*, fondatore della Teoria degli Insiemi, (nato nel 1845 a S. Pietroburgo, morto nel 1918 a Halle) dimostrò che l'insieme dei numeri reali non è numerabile.

Aritmetica dei numeri cardinali infiniti. Definiamo adesso somma e prodotto di numeri cardinali seguendo il caso degli insiemi finiti. Ricordiamo che per insiemi finiti X, Y, si ha $|X| \cdot |Y| = |X \times Y|$ e $|X| + |Y| = |X \cup Y|$, se X e Y sono disgiunti.
Adesso estendiamo la definizione del prodotto dei numeri cardinali per due insiemi X, Y arbitrari ponendo $|X| \cdot |Y| := |X \times Y|$.
Se almeno uno degli insiemi X, Y è infinito poniamo per definizione $|X| + |Y| := |X| \cup |Y|$.
Bisogna notare che a differenza del caso degli insiemi finiti non si richiede più che i due insiemi X, Y siano *disgiunti*.

Teorema 5.11 *Se almeno uno degli insiemi X, Y è infinito, si ha $|X \cup Y| = \max\{|X|, |Y|\}$.*

Dimostrazione. Per il teorema di Hartogs possiamo supporre che $|X| \geq |Y|$. Si può dimostrare che per l'insieme infinito X esiste una partizione $X = X_1 \cup X_2$, tale che $|X_1| = |X_2| = |X|$ (vedi l'Esercizio 6.50). Quindi esiste un'iniezione $X \cup Y \to X_1 \cup X_2 = X$ e possiamo concludere che $|X \cup Y| \leq |X|$. Poiché ovviamente $|X \cup Y| \geq |X|$, il Teorema di Cantor-Bernstein ci permette di concludere che $|X \cup Y| = |X| = \max\{|X|, |Y|\}$. $\square$

Per quanto riguarda il prodotto abbiamo:

Teorema 5.12 *Se almeno uno degli insiemi X, Y è infinito, si ha $|X \times Y| = \max\{|X|, |Y|\}$.*

Per la dimostrazione del Teorema 5.12, abbiamo bisogno del seguente Lemma.

Lemma 5.13 ** *$|X \times X| = |X|$ per ogni insieme infinito X.*

Dimostrazione. Sia A_0 un sottoinsieme numerabile di X. Per il Lemma 5.10, esiste una biiezione $i_{A_0} : A_0 \times A_0 \to A_0$. Si consideri la famiglia $\mathcal{A}$ delle coppie (A, i_A), dove $A_0 \subseteq A \subseteq X$ e $i_A : A \times A \to A$ è una biiezione che estende i_{A_0}. Si consideri in $\mathcal{A}$ la relazione $\leq$ definita da $(A, i_A) \leq (B, i_B)$ se e solo se $A \subseteq B$ e $i_B \restriction_A$. Non è difficile provare che $\leq$ è un ordine per il quale $(\mathcal{A}, \leq)$ è un insieme ordinato induttivo. Per il Lemma di Zorn esiste un membro massimale $(M, i_M) \in \mathcal{A}$. Chiaramente $(M, i_M) \in \mathcal{A}$ implica

$$|M \times M| = |M|. \tag{1}$$

Se $|M| = |X|$, allora abbiamo anche $|X \times X| = |M \times M|$ (vedi l'Esercizio 6.22), e quindi l'uguaglianza (2) assieme alla nostra ipotesi implica $|X \times X| = |X|$. Supponiamo per assurdo che $|M| \neq |X|$. Poiché $|M| \leq |X|$, resta la sola possibilità $|M| < |X|$. D'altra parte $X = M \cup (X \setminus M)$, quindi $|X \setminus M| \geq |M|$ per il Teorema 5.11. Quindi possiamo trovare un sottoinsieme $N \subseteq X \setminus M$ con $|N| = |M|$. Ora $M' = M \cup N$ contiene M propriamente, e $M' \times M' = (M \times M) \cup D$, dove $D = (M \times N) \cup (N \times M) \cup (N \times N)$. Ora $|N \times M| = |M \times N| = |N \times N| = |M| = |N|$. Allora esiste una biiezione $D \to N$, che, assieme alla biiezione $i_M : M \times M \to M$ ci da' una biiezione $i_{M'} : M' \times M' \to M'$ che estende i_M. Quindi $(M', i_{M'}) \in \mathcal{A}$ e $(M, i_M) < (M', i_{M'})$, assurdo. Pertanto $|M| = |X|$. $\square$

Dimostrazione del Teorema 5.12. Per il teorema di Hartogs possiamo supporre che $|X| \geq |Y|$. Si può dimostrare che per l'insieme infinito X si ha $|X \times X| = |X|$ (vedi il Lemma 5.13). Allora $|X| \geq |X \times X| \geq |X \times Y| \geq |X|$.$\square$

Di conseguenza, se almeno uno degli insiemi X, Y è infinito la somma e il prodotto delle loro cardinalità coincidono:

$$|X| \cdot |Y| = |X| + |Y| = |X \times Y| = |X \cup Y| = \max\{|X|, |Y|\}. \tag{$*$}$$

Questo fatto rende molto facile l'aritmetica dei numeri cardinali infiniti. Per esempio, si può dimostrare per induzione che $|X_1 \times \ldots \times X_n| = |X_1 \cup \ldots \cup X_n| = \max\{|X_1|, \ldots, |X_n|\}$ e $|X^n| = |X|$ per ogni ogni numero naturale $n > 0$ se X e almeno uno degli insiemi $X_1, \ldots, X_n$ è infinito. Di conseguenza

$$|X_1| \cdot \ldots \cdot |X_n| = |X_1| + \ldots + |X_n| = \max\{|X_1|, \ldots, |X_n|\} \text{ e } |X|^n = |X|$$

(vedi l'Esercizio 6.43 per i casi concreti).
Poniamo $2^{|X|} = |2^X| = |\mathcal{P}(X)|$. Per il teorema di Cantor, si ha sempre $2^{|X|} > |X|$. Questo ci permette di trovare degli insiemi di cardinalità sempre più grandi.

Il primo numero cardinale infinito $|\mathbb{N}|$ si denota con $\aleph_0$, quello successivo con $\aleph_1$ ecc. Si ottiene così una successione infinita di numeri cardinali a partire da quelli finiti

$$0 < 1 < 2 < \ldots < n < \ldots < \aleph_0 < \aleph_1 < \ldots < \aleph_n < \ldots \tag{3}$$

5.4 Assiomi della teoria degli insiemi.

1. (Esistenza) Esiste un insieme.
2. (Estensionalità) Due insiemi coincidono se e solo se hanno gli stessi elementi.
3. (Separazione) Ad ogni proprietà P (di insiemi) e ad ogni insieme X corrisponde un[3] insieme Y che ha come elementi precisamente gli elementi y di X che possiedono la proprietà P.
4. (Esiste la coppia) Se X è un insieme e Y è un insieme, allora esiste un insieme Z che ha come elementi X e Y e non ha altri elementi.
5. (Unione) Per ogni insieme [4] X esiste l'insieme Y che ha come elementi gli z che appartengono ad almeno uno degli elementi dell'insieme X.
6. (Fondazione) Per ogni insieme $X \neq \emptyset$ esiste un insieme $Y \in X$ che non ha elementi comuni con X.
7. (L'insieme della parti) Per ogni insieme X esiste l'insieme $P(X)$ che ha come elementi i sottoinsiemi di X.
8. (Rimpiazzamento) Se R è una relazione binaria tra insiemi tale che ad ogni insieme x corrisponde al più un insieme y con xRy, allora per ogni insieme X esiste l'insieme $\{y : \text{ esiste } x \in X \text{ con } xRy\}$.
9. (Esiste un insieme infinito) Esiste un insieme induttivo.[5]

L'assioma della Fondazione serve per evitare insiemi patologici con $X \in X$, o catene discendenti infinite $\ldots \in X_3 \in X_2 \in X_1 \in X_0$. Per esempio, se $X = \mathcal{P}(A)$, allora $Y = \emptyset \in X$ non ha elementi comuni con X.

Paradosso di Russell. Nell'assioma di Separazione si definisce $Y = \{z \in X : z \text{ ha la proprietà } P\}$; il fatto di prendere tutti gli z in un *insieme* X è importante perché altrimenti si rischia di uscire fuori dell'ambito degli insiemi, come accade nel seguente paradosso di Russell.

[3] unico, per l'assioma precedente.
[4] che è meglio vedere in questo contesto come famiglia di insiemi.
[5] cioè un insieme X tale che se $z \in X$ allora anche $z \cup \{z\} \in X$.

Sia $\mathcal{P}$ la proprietà : "l'insieme non è elemento di se stesso". Allora la formazione $\mathfrak{M}$ che consiste di tutti gli insiemi che possiedono la proprietà $X \notin X$ non può essere un insieme (perché?).
Suggerimento: Notare che non è vero nè $\mathfrak{M} \in \mathfrak{M}$ nè $\mathfrak{M} \notin \mathfrak{M}$.
Per evitare questo paradosso è permesso solo di considerare l'insieme degli elementi di un certo insieme che possiedono una certa proprietà $\mathcal{P}$.

L'ipotesi del continuo. Chiaramente, la cardinalità del continuo $2^{\aleph_0}$ si trova nella successione (3) e $2^{\aleph_0} > \aleph_0$ per il Teorema di Cantor. Quindi, $2^{\aleph_0} \geq \aleph_1$. L'affermazione $2^{\aleph_0} = \aleph_1$ è nota come *Ipotesi del continuo*. In altre parole, l'Ipotesi del continuo afferma che ogni insieme non numerabile di numeri reali ha la cardinalità del continuo. I numerosi tentativi di provarla sono falliti per più di 70 anni. Infatti, Gödel ha dimostrato che l'Ipotesi del continuo è soddisfatta in alcuni modelli della teoria degli insiemi, mentre Paul Cohen ha dimostrato che l'Ipotesi del continuo non vale in altri modelli della teoria degli insiemi da lui costruiti tramite il celebre metodo del *forcing* introdotto da lui a questo proposito[6]. Di conseguenza, l'Ipotesi del continuo non è dimostrabile, ne è dimostrabile la sua negazione.

6 Esercizi su Insiemi

6.1 Esercizi e svolgimento di alcuni esercizi precedenti su insiemi

Esercizio 6.1 *Sia X un'insieme e sia $j_X : X \to \mathcal{P}(X)$ l'applicazione definita da $j_X(x) = \{x\}$. Dimostrare che j_X è sempre iniettiva.*

Esercizio 6.2 *Sia $f : X \to Y$ un'applicazione e sia $f_* : \mathcal{P}(X) \longrightarrow \mathcal{P}(Y)$ la funzione così definita $f_*(B) = f(B)$. Si provi che*

(a) $f_* \circ j_X = j_Y \circ f$;

(b) f è iniettiva se e solo se f_* è iniettiva,,

(c) f è suriettiva se e solo se f_* è suriettiva.

Svolgimento. (a) è ovvia.
(b) Se f_* è iniettiva, allora la composizione $f_* \circ j_X$ è iniettiva per il Lemma 2.13 e l'Esercizio precedente. Per (a) anche la composizione $j_Y \circ f$ è iniettiva. Ora dal Lemma 2.16 si conclude che f è iniettiva. Ora supponiamo che f sia iniettiva. Ragionando come nello svolgimento del punto (a) dell'Esercizio 2.23 si conclude che anche f_* è iniettiva.
(c) Supponiamo che f_* sia suriettiva. Allora esiste $A \in \mathcal{P}(X)$ con $f_*(A) = f(A) = Y$, quindi anche $f(X) = Y$ e pertanto f è suriettiva. Se invece f è suriettiva e $C \subseteq Y$, allora $f(f^{-1}(C)) = C$, quindi $C = f_*(f^{-1}(C))$. $\square$

Esercizio 6.3 *Sia $f : X \to Y$ un'applicazione e sia $f^* : \mathcal{P}(Y) \longrightarrow \mathcal{P}(X)$ la funzione così definita $f^*(B) = f^{-1}(B) = \{a \in X : f(a) \in B\}$. Si provi che*

(a) f^* è iniettiva se e solo se f è suriettiva,

(b) f^* è suriettiva se e solo se f è iniettiva.

[6]Questo teorema valse per Paul Cohen la medaglia Fields nel 1966, il premio più prestigioso attribuito nell'ambito della matematica.

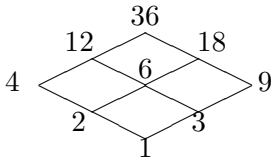
SVOLGIMENTO. (a) Supponiamo che f^* sia iniettiva. Allora essendo $f^*(Y) = f^*(f(X))$ concludiamo che $Y = f(X)$, cioè f è suriettiva. Viceversa, sia f suriettiva, cioè $Y = f(X)$. Allora $f_* \circ f^* = id_{\mathcal{P}(Y)}$ essendo $f(f^{-1}(B)) = B$ per ogni $B \in \mathcal{P}(Y)$. Quindi, f^* è iniettiva per il Lemma 2.16.
(b) Sia f^* suriettiva, e supponiamo per assurdo che esistano $x \neq y$ in X con $f(x) = f(y)$. Poiché f^* è suriettiva, esiste $B \in \mathcal{P}(Y)$ tale che $\{x\} = f^*(B)$. Ma $y \in f^*(B)$ e quindi si avrebbe $x = y$. Da questa contraddizione concludiamo che f è iniettiva. Supponiamo ora che f sia iniettiva e $A \in \mathcal{P}(X)$, allora $f^{-1}(f(A)) = A$, cioè $A = f^*(f(A))$. Questo dimostra che f^* è suriettiva. □

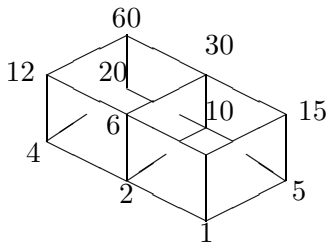
Esercizio 6.4 *Si considerino le relazioni binarie R_1, R_2, R_3 e R_4 nell'insieme $\mathbb{C}$ dei numeri complessi definite come segue:*
1) xR_1y se il numero $x - y$ è naturale;
2) xR_2y se il numero $x - y$ è razionale;
3) xR_3y se il numero $x - y$ è reale e $x - y \geq 0$;
4) xR_4y se la parte reale e la parte immaginaria del numero $x - y$ sono ≥ 0.
Si determini quali delle relazioni R_1, R_2, R_3 e R_4 sono relazioni di equivalenza, e quali sono ordini o preordini, specificando il tipo di ordine (buon ordine, ordine lineare ecc.).

6.2 Esercizi sugli insiemi parzialmente ordinati

Esercizio 6.5 *Si disegnino i diagrammi di Hasse degli insiemi parzialmente ordinati per divisibilità dei divisori di 36 e 60.*

SVOLGIMENTO.





□

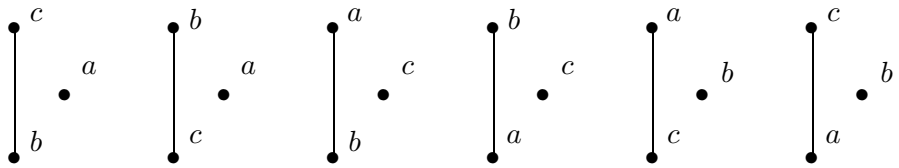
L'insieme ordinato dei divisori di 36 L'insieme ordinato dei divisori di 60

Esercizio 6.6 *Trovare il numero di tutti gli ordini di un insieme di 3 elementi.*

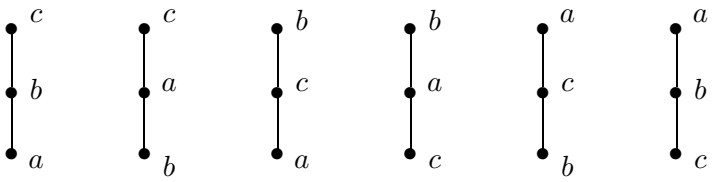
SVOLGIMENTO. Siano a, b, c i tre elementi distinti dell'insieme X. Allora i possibili ordini sono:

(1) nessuna coppia di elementi è confrontabile (l'ordine è discreto), cioè dati $x, y \in X$, con $x \neq y$ si ha $x \not\leq y$ e $y \not\leq x$;

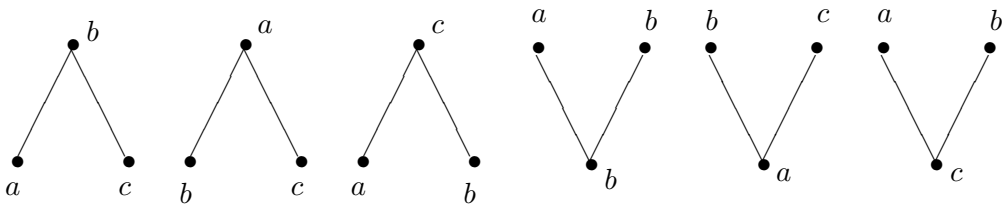
(2) due elementi sono confrontabili e il terzo non lo è con nessuno degli altri due: ci sono 6 ordini di questo tipo ($b \leq c$, $c \leq b$, $a \leq b$, $b \leq a$, $a \leq c$ e $c \leq a$):



(3) i tre elementi formano una catena: $a \leq b \leq c$, ci sono 6 ordini di questo tipo:



(4) esiste un massimo e l'insieme non è una catena: $a \leq b \geq c$ e ci sono 3 ordini di questo tipo oppure esiste un minimo e l'insieme non è una catena: $a \geq b \leq c$ e ci sono 3 ordini di questo tipo.



In totale ci sono 19 possibili ordinamenti su un insieme con 3 elementi. □

Esercizio 6.7 *Trovare il numero di tutti gli ordini di un insieme di 4 elementi.*

SUGGERIMENTI. Daremo un suggerimento. Gli ordini che hanno un elemento massimo o un elemento minimo sono facilmente riducibili all'Esercizio precedente. Resta da determinare il numero degli ordini che non hanno nè un elemento massimo nè un elemento minimo. Di questo tipo sono tutti gli ordini che hanno un elemento isolato (non confrontabile con gli altri elementi). Infine, resta un ultimo tipo di ordine, senza elementi isolati, nè minimi nè massimi. □

Esercizio 6.8 *Dimostrare che ogni insieme parzialmente ordinato e finito è induttivo.*

Esercizio 6.9 *Dimostrare che ogni reticolo finito è limitato.*

Esercizio 6.10 *Sia A un insieme non vuoto finito o numerabile. Dimostrare che A ammette una relazione di buon ordine.*

SUGGERIMENTI. Esiste, per ipotesi, una biiezione $f : I \to A$, dove $I = \{1, 2, \ldots, n\}$ o $I = \mathbb{N}$. In entrambi i casi I ammette un buon ordine $\leq$, che si trasporta su A ponendo per definizione $f(a) \leq f(b)$ qualora $a \leq b$ in I. □

Esercizio 6.11 *Sia X un insieme non vuoto. L'insieme parzialmente ordinato $(\mathcal{P}(X), \subseteq)$ è un reticolo limitato.*

Esercizio 6.12 *Si dia un esempio di un reticolo che ha un sottoinsieme ordinato che non è un reticolo.*

SVOLGIMENTO. Consideriamo l'insieme Y di tutti i divisori di 15, ordinato per divisibilità: $Y = \{1, 3, 5, 15\}$ e $a \preceq b$ se e solo se $a|b$. $(Y, |)$ è un reticolo e non è totalmente ordinato perché $3 \not| 5$ e $5 \not| 3$. Il sottoinsieme parzialmente ordinato $X = \{3, 5\}$ non è un reticolo perché $3 \vee 5 = 15$ non esiste in X. $\square$

Esercizio 6.13 *Dimostrare che*
i) la relazione $a \preceq b$ in $\mathbb{C}$ definita da

$$a \preceq b \text{ se e solo se } Im\, a \leq Im\, b$$

è una relazione di preordine.
ii) la relazione $a \preceq_r b$ in $\mathbb{C}$ definita da

$$a \preceq_r b \text{ se e solo se } Re\, a \leq Re\, b$$

è una relazione di preordine.

È utile rappresentare un insieme finito ordinato sul piano di Gauss-Argand, nel modo seguente. Sia $(X, \leq)$ un insieme dotato di preordine. Se $a, b \in X$ vengono rappresentati da α e β sul piano di Gauss-Argand, allora $a < b$ se e solo se $\alpha \prec \beta$, ove $\prec$ è la relazione d'ordine definita sui complessi come nel punto (c) dell'esempio 6.13. Se uniamo con una linea i punti tra loro confrontabili, otteniamo un digramma nel piano, noto come il *diagramma di Hasse*. Osserviamo inoltre che, per rendere meno pesante il diagramma, ogni qualvolta si ha $a < b < c$ e la relazione è transitiva, si omette di disegnare la linea che collega a con c.
Ad esempio, se consideriamo l'insieme $X = \{a, b, c\}$ e la relazione d'ordine definita su $\mathcal{P}(X)$ come nel punto (a) dell'esempio 2.37, otteniamo il seguente diagramma:

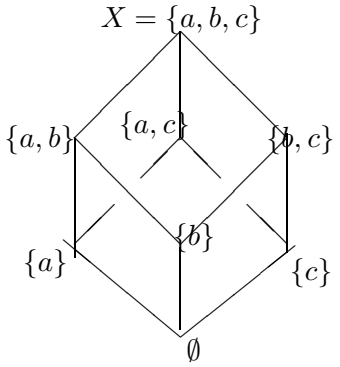
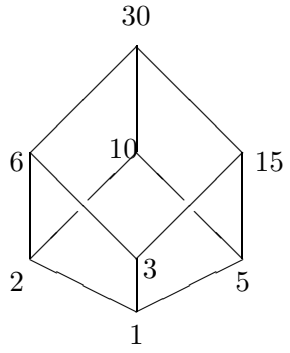


Diagramma di Hasse di $P(\{a, b, c\})$

Esercizio 6.14 *Dimostrare che ogni ordine buono è anche totale.*

Esercizio 6.15 *Si determinino gli elementi massimali e minimali nell'insieme parzialmente ordinato per divisibilità dei divisori propri di 30, 56 e 120.*

SVOLGIMENTO. Tra i divisori propri di 30 gli elementi minimali sono 2, 3, 5 e gli elementi massimali sono 6, 10 e 15.
Tra i divisori propri di 56 gli elementi minimali sono 2 e 7 e gli elementi massimali sono 8 e 28.
Tra i divisori propri di 120 gli elementi minimali sono 2, 3, 5 e gli elementi massimali sono 60, 40 e 24. □



L'insieme ordinato dei divisori di 30

6.3 Esercizi sui prodotti cartesiani

Esercizio 6.16 *Sia $A \neq \emptyset$. Trovare una biiezione tra $A^{\{1,2,\ldots,n\}}$ ed il prodotto cartesiano $\underbrace{A \times A \times \ldots \times A}_{n \ \ volte}$.*

SUGGERIMENTI. Si procede come nel Lemma 5.5, mettendo in corrispondenza all'applicazione

$$f : \{1, 2, \ldots, n\} \to A$$

la n-upla ordinata $(f(1), f(2), \ldots, f(n))$. Nel verso opposto, alla n-upla ordinata $(a_1, a_2, \ldots, a_n)$ si associ l'applicazione $f : \{1, 2, \ldots, n\} \to A$ definita da $f(1) = a_1, f(2) = a_2, \ldots, f(n) = a_n$. □

Esercizio 6.17 *Dimostrare che $\varphi : \mathcal{P}(X) \to 2^X$ definita da $\varphi(A) = \chi_A$ è una biiezione.*

SVOLGIMENTO. Per ogni funzione $f : X \to \{0, 1\}$ si ha $f = \varphi(\{x \in X : f(x) = 1\})$, pertanto φ è suriettiva. D'altra parte, se $\chi_A = \chi_B$, allora $A = B$. Infatti, se $a \in A$, allora $\chi_B(a) = \chi_A(a) = 1$, perciò $a \in B$ e pertanto $A \subseteq B$. Analogamente si vede che $B \subseteq A$, e quindi $A = B$. Questo dimostra che φ è anche iniettiva. □

Esercizio 6.18 *Sia $n > 1$ e siano A_1, A_2, …, A_n insiemi non vuoti. Denotiamo con X l'insieme delle applicazioni $f : \{1, 2, \ldots, n\} \to A_1 \cup A_2 \cup \ldots \cup A_n$ con la proprietà $f(1) \in A_1$, $f(2) \in A_2$, …, $f(n) \in A_n$. Trovare una biiezione tra X ed il prodotto cartesiano $A_1 \times A_2 \times \ldots \times A_n$.*

SUGGERIMENTI. All'applicazione $f \in X$ mettere in corrispondenza la n-upla ordinata $(f(1), f(2), \ldots, f(n))$ di $A_1 \times A_2 \times \ldots \times A_n$. Questo definisce un'applicazione $\varphi : X \to A_1 \times A_2 \times \ldots \times$

A_n. Provare che φ è invertibile, avente come inversa l'applicazione $\psi : A_1 \times A_2 \times \ldots \times A_n \to X$ che alla n-upla $(a_1, a_2, \ldots, a_n)$ associa l'applicazione $f : \{1, 2, \ldots, n\} \to A_1 \cup A_2 \cup \ldots \cup A_n$ definita da $f(1) = a_1$, $f(2) = a_2$, ..., $f(n) = a_n$. □

Esercizio 6.19 *Sia $n > 1$ e siano A_1, $A_2, \ldots, A_n$ insiemi non vuoti.*

(a) Dimostrare che la proiezione p_i ($i = 1, 2, \ldots, n$) è suriettiva, ma non necessariamente iniettiva.

(b) Siano B_1, $B_2, \ldots, B_n$ insiemi non vuoti e siano $f_i : A_i \to B_i$ applicazioni ($i = 1, 2, \ldots, n$). Si definisca l'applicazione

$$f_1 \times f_2 \times \ldots \times f_n : A_1 \times A_2 \times \ldots \times A_n \to B_1 \times B_2 \times \ldots \times B_n$$

con $(f_1 \times f_2 \times \ldots \times f_n)(a_1, a_2, \ldots, a_n) = (f_1(a_1), f_2(a_2), \ldots, f_n(a_n))$. Dimostrare che:

- *$p_i \circ (f_1 \times f_2 \times \ldots \times f_n) = f_i$ per $i = 1, 2, \ldots, n$;*
- *$f_1 \times f_2 \times \ldots \times f_n$ è iniettiva (risp. suriettiva) se e solo se tutte le applicazioni f_i sono iniettive (risp. suriettive).*

Esercizio 6.20 *Sia $n > 1$ e siano A_1, $A_2, \ldots, A_n$ insiemi non vuoti.*
(a) Trovare una biiezione tra i prodotti $(A_1 \times A_2 \times \ldots \times A_{n-1}) \times A_n$ e $A_1 \times A_2 \times \ldots \times A_n$.
(b) In caso di insiemi finiti dimostrare che $|A_1 \times A_2 \times \ldots \times A_n| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_n|$.

SUGGERIMENTI. (a) Considerare la corrispondenza $((a_1, a_2, \ldots a_{n-1}), a_n) \mapsto (a_1, a_2, \ldots, a_n)$. (b) Daremo una dimostrazione per induzione su n. Sia $A(n)$ l'affermazione che la formula è vera per tutte le n-uple di insiemi finiti A_1, $A_2, \ldots, A_n$. Ovviamente, $A(1)$ è vera. Supponiamo ora che siano vere tutte le $A(k)$ con $k < n$. Poniamo $B = A_1 \times A_2 \times \ldots \times A_{n-1}$. Allora $|A_1 \times A_2 \times \ldots \times A_{n-1} \times A_n| = |B \times A_n|$. Per l'ipotesi induttiva $|B \times A_n| = |B| \cdot |A_n|$ e $|B| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_{n-1}|$. Ora la tesi segue immediatamente. □

Esercizio 6.21 *Trovare l'errore nella dimostrazione al punto b) dell'Esercizio precedente e dare una dimostrazione corretta.*

SUGGERIMENTI. Cercare di trovare l'errore da soli. □

Esercizio 6.22 *Siano $\{A_i\}_{i \in I}$ e $\{B_j\}_{j \in J}$ due famiglie di insiemi non vuoti con $I \neq \emptyset \neq J$. Se esiste una biiezione $\varphi : I \to J$ e per ogni $i \in I$ una biiezione $\psi_i : A_i \to B_{\varphi(i)}$, allora esiste anche una biiezione $\prod_{i \in I} A_i \to \prod_{j \in J} B_j$.*

Esercizio 6.23 *Sia $\{A_i\}_{i \in I}$ è una famiglia di insiemi non vuoti con $\emptyset \neq J \subset I$. Dimostrare che esiste una biiezione $\prod_{i \in I} A_i \to \prod_{j \in J} A_j \times \prod_{i \in I \setminus J} A_i$.*

6.4 Esercizi sugli insiemi ordinati e i prodotti cartesiani

Siano $(A, \leq)$ e $(B, \leq')$ due insiemi parzialmente ordinati. Allora sul prodotto cartesiano $A \times B$ consideriamo le relazioni binarie $\prec$ e $\lhd$ definite come segue

$$(a, b) \prec (a_1, b_1) \text{ se } a < a_1 \text{ oppure } a = a_1 \text{ e } b \leq' b_1, \tag{1}$$

$$(a, b) \lhd (a_1, b_1) \text{ se } a \leq a_1 \text{ e } b \leq' b_1. \tag{2}$$

Esercizio 6.24 *Dimostrare che $\prec$ e $\lhd$ sono ordini parziali (chiamati, rispettivamente, ordine lessicografico e prodotto cartesiano di $\leq$ e $\leq'$).*

Esercizio 6.25 *Dimostrare che $\prec$ è totale se $\leq$ e $\leq'$ sono totali, mentre $\lhd$ non è totale se $|A| > 1$ e $|B| > 1$.*

L'*altezza* di un insieme parzialmente ordinato finito L è il massimo tra le lunghezze delle catene di L e sarà denotata con $h(L)$, dal termine inglese *height* - altezza.

Esercizio 6.26 *Siano $A = \{1, 2, \ldots, n\}$ e $B = \{1, 2, \ldots, m\}$ con l'ordine usuale e $X = A \times B$ munito dell'ordine $\lhd$. Dimostrare che $h(X) = m + n - 1$.*

SUGGERIMENTI. Supponiamo $n \leq m$, allora una catena di lunghezza $m + n - 1$ è

$$\{(1,1), (2,1), (3,1), \ldots, (n,1), (n,2), (n,3), \ldots, (n,m)\}.$$

Ora dimostrare che ogni catena in X ha lunghezza $\leq m + n - 1$. □

Esercizio 6.27 *Siano A e B insiemi parzialmente ordinati finiti e $X = A \times B$ munito dell'ordine $\lhd$. Dimostrare che $h(X) = h(A) + h(B) - 1$.*

SUGGERIMENTI. Applicare l'Esercizio 6.26. □

Sia $(A, \leq)$ un insieme parzialmente ordinato. Un sottoinsieme B di A si dice una *anticatena*, se $(B, \leq)$ ha l'ordine discreto (cioè, se $x, y \in B$ con $x \neq y$ allora $x \not\leq y$ e $y \not\leq x$). La *larghezza* dell'anticatena B è il numero cardinale $|B|$. Se A è finito, la *larghezza* di A è il massimo tra le larghezze delle anticatene di A e sarà denotata con $w(A)$, dal termine inglese *width* - larghezza.

Esercizio 6.28 *Dimostrare che L è totalmente ordinato se e solo se $w(L) = 1$.*

Esercizio 6.29 *Individuare tutte le anticatene di larghezza 2 nell'insieme ordinato $P(\{1, 2, 3\})$.*

Esercizio 6.30 *Siano $A = \{1, 2, \ldots, n\}$ e $B = \{1, 2, \ldots, m\}$ con l'ordine usuale e $X = A \times B$ munito dell'ordine $\lhd$. Dimostrare che $w(X) = min\{m, n\}$.*

Esercizio 6.31 *Siano A e B insiemi parzialmente ordinati finiti e $X = A \times B$ munito dell'ordine $\lhd$. Dimostrare che $w(X) \geq \min\{h(A), h(B)\}$. Se A e B sono totalmente ordinati, si ha l'uguaglianza. Trovare esempi dove vale la disuguaglianza stretta.*

Esercizio 6.32 *Sia $(L, \leq)$ un reticolo, allora sull'insieme L^X definiamo un ordine parziale nel modo seguente:*

$$f, g \in L^X \quad f \prec g \quad \Longleftrightarrow \quad f(x) \leq g(x) \quad \textit{per ogni} \quad x \in X.$$

Si dimostri che $(L^X, \prec)$ è un reticolo.

SVOLGIMENTO. Dimostriamo che dati due elementi f, g di L^X, questi ammettono massimo e minimo. Definiamo la funzione $h(x) = f(x) \vee g(x)$: è ben definita perché L è un reticolo e $f(x), g(x)$ sono due elementi del reticolo. Allora $h = f \vee g$. Analogamente per l'estremo inferiore. □

Esercizio 6.33 *Sia $(S, \leq)$ un insieme ordinato e nell'insieme S^S delle applicazioni di S in sè si consideri la relazione binaria $\mathcal{R}$, definita ponendo $f\mathcal{R}g$ se e solo se $f(x) \leq g(x)$ per ogni $x \in S$. Provare che $\mathcal{R}$ è una relazione d'ordine e che $\mathcal{R}$ risulta totale se e solo se S è costituito da un solo elemento.*

SUGGERIMENTI. La dimostrazione che $\mathcal{R}$ sia una relazione d'ordine deriva dal fatto che $\leq$ è una relazione d'ordine in S. Vediamo per esempio la dimostrazione della proprietà antisimmetrica: $f\mathcal{R}g$ e $g\mathcal{R}f$ implicano che $f(x) \leq g(x)$ e $g(x) \leq f(x)$ per ogni $x \in S$. Per la proprietà antisimmetrica di $\leq$, si ha $f(x) = g(x)$ per ogni $x \in S$, cioè $f = g$.
Supponiamo che $\mathcal{R}$ sia di ordine totale e supponiamo che esistano due elementi distinti x ed y in S. Consideriamo la funzione $f : S \to S$ tale che $f(x) = y$, $f(y) = x$ e $f(z) = z$ per ogni altro z in S, $z \neq x$, $z \neq y$. Allora f ed id sono due elementi di S^S, pertanto devono essere confrontabili rispetto alla relazione $\mathcal{R}$. Allora si avrà o $f\mathcal{R}id$ oppure $id\mathcal{R}f$. Nel primo caso si ha $f(x) = y \leq id(x) = x$ e $f(y) = x \leq id(y) = y$, da cui si ricava $x = y$. Si conclude allo stesso modo nel secondo caso.
Se S contiene solo un elemento, allora anche S^S contiene solo un elemento e l'ordine è totale. □

6.5 Esercizi sui numeri cardinali

Esercizio 6.34 *Se un insieme X non è infinito, allora esiste una biiezione $X \to \{1, 2, \ldots, n\}$.*

SUGGERIMENTI. Ragioniamo per assurdo, supponendo che non esista alcuna biiezione dall'insieme $\{1, 2, \ldots, n\}$ all'insieme X per alcun n e quindi, non esista una suriezione $\{1, 2, \ldots, n\} \to X$ per alcun n. Pertanto, esistono almeno $n + 1$ elementi distinti di X. Possiamo costruire così una iniezione $\mathbb{N} \to X$ nel modo seguente. Scegliamo un elemento arbitrario $x_0 \in X$ e poniamo $f(0) = x_0$. Supponiamo di aver già definito $f(0), \ldots, f(n-1)$. Poichè X ha un elemento x_n diverso da $f(0), \ldots, f(n-1)$, possiamo porre $f(n) = x_n$ ecc. □

Esercizio 6.35 *Se un insieme X ammette una suriezione $X \to X$ che non è iniettiva, allora esiste anche una iniezione $X \to X$ che non è suriettiva.*

Esercizio 6.36 *Dimostrare che vale $|A| \leq |B|$ per due insiemi A, B se e solo se esiste un'applicazione suriettiva $B \to A$.*

SVOLGIMENTO. Da $|A| \leq |B|$ concludiamo che esiste un'iniezione $f : A \to B$. Per definire un'applicazione suriettiva $g : B \to A$ scegliamo un elemento arbitrario $a_0 \in A$ e poniamo $g(b) = a$ se risulta $b = f(a)$ per qualche $a \in A$ (che è necessariamente unico). Se $b \in B \setminus f(A)$ poniamo $g(b) = a_0$. Se esiste un'applicazione suriettiva $B \to A$, allora il Teorema 5.3 implica che esiste un'applicazione iniettiva $A \to B$, e quindi vale $|A| \leq |B|$. □

Esercizio 6.37 *Per ogni insieme X si ha $|X| < |\mathcal{P}(X)|$.*

DIMOSTRAZIONE. Notiamo che $|X| \leq |\mathcal{P}(X)|$ in quanto esiste l'applicazione $j_X : X \to \mathcal{P}(X)$ che manda ogni elemento $x \in X$ nel singoletto $\{x\}$ e tale applicazione è iniettiva. Per dimostrare che non vale $|X| \geq |\mathcal{P}(X)|$ basta applicare il Teorema di Cantor. □

Esercizio 6.38 *Sia $f : X \to X$ un'applicazione iniettiva, ma non suriettiva. Allora per ogni $x \in X \setminus f(X)$ esiste un'applicazione iniettiva $h : \mathbb{N} \to X$ con $h(0) = x$.*

SVOLGIMENTO. Scegliamo $x \in X \setminus f(X)$ e definiamo un'applicazione iniettiva $h : \mathbb{N} \to X$ con $h(0) = x$. Cominciamo ponendo $h(0) = x$. Supponendo di aver definito $h(n)$ per qualche $n \in \mathbb{N}$, poniamo $h(n+1) = f(h(n))$. Allora l'insieme A di tutti gli $n \in \mathbb{N}$ per i quali $h(n)$ è definito contiene 0 e se $n \in A$, allora anche $n+1 \in A$. Quindi $A = \mathbb{N}$ per il principio di induzione. In questo modo $h : \mathbb{N} \to X$ è stata definita. Supponiamo per assurdo che h non sia iniettiva. Allora esistono $n < m$ in $\mathbb{N}$ con $h(n) = h(m)$. Scegliamo n minimo con questo proprietà (questo è possibile per il principio del minimo applicato all'insieme $B = \{n \in \mathbb{N} : h(n) = h(m) \text{ per qualche } m > n\}$). Vediamo che questa scelta implica $n = 0$. Infatti, supponiamo per assurdo $n > 0$. Allora $f(h(n-1)) = h(n) = h(m) = f(h(m-1))$. Per l'iniettività di f concludiamo che $h(n-1) = h(m-1)$ e quindi $n-1 \in A$ contrariamente alla scelta di n come elemento minimale di A. Questo dimostra che la nostra ipotesi per assurdo implica $h(0) = h(m)$ per qualche $m > 0$. Ora $x = h(0) = h(m) = f(h(m-1))$ contraddice la scelta di x con $x \in X \setminus f(X)$. L'assurdo dimostra che h è iniettiva. □

Esercizio 6.39 *Sia X un insieme non vuoto e sia $\mathcal{A} = \{A_i : i \in I\}$ una famiglia di sottoinsiemi di X tali che*
a) $X = \bigcup_{i \in I} A_i$,
b) $\mathcal{A}$ è chiusa per intersezioni.
Allora la relazione $\sim$ su X definita da $x \sim y$ se e solo se per ogni $i \in I$ si ha $x \in A_i$ se e solo se $y \in A_i$, è una relazione di equivalenza.

Esercizio 6.40 *Sia $X = \bigcup_{i \in I} C_i$ una partizione e sia Y un sottoinsieme di X. Se per ogni $i \in I$ $h_i : C_i \to C_i \cap Y$ è un applicazione iniettiva, allora l'applicazione $h : X \to Y$ definita da $h(x) := h_i(x)$ per $x \in C_i$ è iniettiva. Inoltre, h è biiettiva se e solo se ogni h_i è biiettiva. In particolare, se per ogni $i \in I$ esiste una biiezione $h_i : C_i \to C_i \cap Y$, allora esiste anche una biiezione $h : X \to Y$.*

Esercizio 6.41 *Sia X un insieme infinito. Dimostrare che:*
a) per ogni elemento $x \in X$ esiste una biiezione fra X e $X \setminus \{x\}$;
b) per ogni insieme finito $F \subseteq X$ esiste una biiezione fra X e $X \setminus F$.

Esercizio 6.42 *Dimostrare che esiste una biiezione fra l'intervallo chiuso $[0, 1]$ e l'insieme $\mathbb{R}$ dei numeri reali. Costruire esplicitamente una tale biiezione.*

Esercizio 6.43 *Dimostrare che:*
(a) i seguenti insiemi sono numerabili: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$;
(b) se $A_1, A_2, \ldots, A_n, \ldots$ sono insiemi numerabili, allora anche gli insiemi $\bigcup_{n=1}^{\infty} A_n$ e $A_1 \times A_2 \times \ldots \times A_k$ sono numerabili per ogni k.

SUGGERIMENTI. (a) Per vedere che $\mathbb{Z}$ è numerabile applicheremo il Teorema di Cantor–Bernstein. Poiché esiste una iniezione di $\mathbb{N}$ in $\mathbb{Z}$ (l'inclusione), basta vedere che esiste anche una iniezione $h : \mathbb{Z} \hookrightarrow \mathbb{N}$. Definiamo $h(0) = 0$ e $h(n) = 2n$ se $n > 0$, altrimenti $h(n) = 1 - 2n$. Non è difficile verificare che h è iniettiva (addirittura biiettiva). Questo dimostra che $\mathbb{Z}$ è numerabile e implica anche che $\mathbb{Z} \times \mathbb{Z}$ è numerabile per il Lemma 5.10.
Poiché ogni numero razionale r si può scrivere almeno in un modo come $r = a/b$, con $a, b \in \mathbb{Z}$ (e $b \neq 0$), esiste una suriezione $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$. Poiché $\mathbb{Z} \times \mathbb{Z}$ è numerabile, allora anche $\mathbb{Q}$ risulta numerabile.
(b) Per vedere che $\bigcup_{n=1}^{\infty} A_n$ è numerabile basta trovare una suriezione $f : \mathbb{N} \times \mathbb{N} \to \bigcup_{n=1}^{\infty} A_n$. Sia $f_n : \mathbb{N} \to A_n$ una suriezione che testimonia la numerabilità di A_n. Definiamo f con $f(n, m) = f_n(m)$ per ogni $n, m \in \mathbb{N}$.
Per la seconda parte si usi induzione su k e il Lemma 5.10. □

Esercizio 6.44 *Sia $n > 0$ un numero naturale fissato e sia S l'insieme delle soluzioni delle equazioni*

$$(a_1x^2 + b_1x + c_1)(a_2x^2 + b_2x + c_2) \dots (a_nx^2 + b_nx + c_n) = 0,$$

dove $a_1, b_1, c_1, a_2, b_2, c_2, \dots a_n, b_n, c_n$ variano nell'insieme dei numeri razionali. Si dimostri che S è numerabile.

Esercizio 6.45* *Dimostrare che il Teorema di Zermelo implica l'assioma della scelta.*

SUGGERIMENTI. Si fissi un buon ordine $\leq$ su I e si ponga $I_0 = \{\alpha \in I : \prod_{\beta\leq\alpha} A_\beta \neq \emptyset\}$. Dimostrare che:
a) se $\beta \in I_0$ e $\alpha \leq \beta$ allora anche $\alpha \in I_0$;
b) $\prod_{\beta\in I_0} A_\beta \neq \emptyset$. (Infatti, se $f_\alpha : \{\beta \in I : \beta \leq \alpha\} \to \bigcup_{i\leq\alpha} A_i$ è definita da $f_\alpha(\beta) \in A_\beta$ per $\beta \leq \alpha$, definiamo $f : I_0 \to \bigcup_{i\in I_0} A_i$ ponendo $f(\alpha) = f_\alpha(\alpha)$.)
c) $I_0 = I$. Si ragiona per assurdo, supponendo $I_0 \neq I$. Allora esiste il minimo α_0 dell'insieme non vuoto $I \setminus I_0$. Ora $\prod_{\beta\in I_0\cup\{\alpha_0\}} A_\beta = \prod_{\{\beta\in I:\beta\leq\alpha_0\}} A_\beta \neq \emptyset$ poiché $\prod_{\beta\in I_0\cup\{\alpha_0\}} A_\beta$ è equipotente al prodotto $A_{\alpha_0} \times \prod_{i\in I_0} A_i$ per l'Esercizio 6.23. Quindi, $\alpha_0 \in I_0$ contrariamente all'ipotesi $\alpha_0 \notin I_0$ - assurdo. □

Esercizio 6.46 *Trovare una forma esplicita per l'applicazione $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ nell'Esercizio 5.10.*

Esercizio 6.47 *Siano X ed Y due insiemi che ammettono delle partizioni $X = \bigcup\{X_i : i \in I\}$ e $Y = \bigcup\{Y_i : i \in I\}$ rispettivamente, con $|X_i| = |Y_i|$ per ogni $i \in I$. Allora X ed Y sono equipotenti.*

SUGGERIMENTI. Per ogni $i \in I$ scegliamo una biiezione $h_i : X_i \to Y_i$, che proviene dal fatto che $|X_i| = |Y_i|$. Ora definiamo $h : X \to Y$ ponendo $h(x) = h_i(x)$, se $x \in X_i$. Adesso basta verificare che h è una biiezione. □

Esercizio 6.48* *Sia X un insieme infinito. Allora esiste una partizione $\{X_i : i \in I\}$ di X in insiemi numerabili.*

SVOLGIMENTO. Consideriamo la famiglia $\mathfrak{A}$ di tutte le famiglie $\mathcal{A} = \{X_i : i \in I\}$ di sottoinsiemi numerabili a due a due disgiunti X_i di X. Ordiniamo $\mathfrak{A}$ per inclusione. Allora $(\mathfrak{A}, \subseteq)$ è un insieme ordinato induttivo. Infatti, se $\mathfrak{C}$ è una catena in $\mathfrak{A}$, allora $\bigcup\mathfrak{C} \in \mathfrak{A}$, poiché $A, B \in \bigcup\mathfrak{C}$ implica che A e B appartengono allo stesso membro della catena $\mathfrak{C}$ e quindi sono disgiunti. Inoltre, $\bigcup\mathfrak{C}$ contiene ogni membro di $\mathfrak{C}$ e quindi è un maggiorante di $\mathfrak{C}$ in $(\mathfrak{A}, \subseteq)$. Quindi possiamo applicare il lemma di Zorn ad $(\mathfrak{A}, \subseteq)$ e affermare che esiste una famiglia massimale $\mathcal{M} = \{X_i : i \in I\} \in \mathfrak{A}$. Sia $Y = \bigcup\{X_i : i \in I\}$. Allora $X \setminus Y$ è finito (altrimenti, si prende un insieme infinito $Z \subseteq X \setminus Y$ e la famiglia $\{Z\} \cup \mathcal{M} \in \mathfrak{A}$ e contiene strettamente $\mathcal{M}$, assurdo). Aggiungendo l'insieme finito $X \setminus Y$ a qualche membro X_{i_0} di $\mathcal{M}$ troviamo una famiglia $\mathcal{M}' = \{X_{i_0} \cup (X \setminus Y)\} \cup \{X_i : i \in I, i \neq i_0\} \in \mathfrak{A}$. Inoltre, $\mathcal{M}'$ è una partizione di X e quindi $\mathcal{M}'$ è la partizione desiderata. □

Esercizio 6.49 $|X| = |X \times \{0, 1\}|$ *per ogni insieme infinito.*

SUGGERIMENTI. Sia $\{X_i : i \in I\}$ una partizione di X in insiemi numerabili. Allora $|X_i \times \{0, 1\}| = |X_i|$ per ogni $i \in I$ per il Lemma 5.10. Poiché $\{X_i \times \{0, 1\} : i \in I\}$ è una partizione di $X \times \{0, 1\}$, basta applicare l'Esercizio 6.48. □

Esercizio 6.50 *Se X è un insieme infinito, allora esiste una partizione $X = X_1 \cup X_2$ di X con $|X_1| = |X_2| = |X|$.*

SUGGERIMENTI. Per l'Esercizio 6.49 esiste una biiezione $f : X \to X \times \{0, 1\}$. Ora se poniamo $X_i = f^{-1}(X \times \{i - 1\})$ per $i = 1, 2$ abbiamo la partizione desiderata. □

Esercizio 6.51* $|X| = |X \times \mathbb{N}|$ *per ogni insieme infinito.*

Esercizio 6.52 *Se X è un insieme infinito, allora esiste una partizione $X = \bigcup_{n\in\mathbb{N}} X_n$ di X con $|X_n| = |X|$ per ogni $n \in \mathbb{N}$.*

SUGGERIMENTI. Per l'Esercizio 6.51 esiste una biiezione $f : X \to X \times \mathbb{N}$. Ora se poniamo $X_n = f^{-1}(X \times \{n\})$ per $n \in \mathbb{N}$ abbiamo la partizione desiderata. □

Esercizio 6.53 *Se X è infinito e per ogni $n \in \mathbb{N}$ sia ha $|A_n| \leq |X|$, allora anche $|\bigcup_{n=1}^{\infty} A_n| \leq |X|$.*

SUGGERIMENTI. Per l'Esercizio 6.36 basta trovare un'applicazione suriettiva $X \to A = \bigcup_{n=1}^{\infty} A_n$. Sempre per l'Esercizio 6.36, per ogni $n \in \mathbb{N}$ esiste un'applicazione suriettiva $f_n : X \to A_n$ che testimonia il fatto $|A_n| \leq |X|$. Sia $f : X \times \mathbb{N} \to A$, definita con $f(x, n) = f_n(x)$ per ogni $n \in \mathbb{N}$ e $x \in X$. Allora f è suriettiva. Per l'Esercizio 6.51 esiste un'applicazione suriettiva $h : X \to X \times \mathbb{N}$. Adesso la composizione $f \circ h : X \to A$ è suriettiva. □

Esercizio 6.54* *Dimostrare che $|\mathbb{R}| = \mathfrak{c}$.*

SUGGERIMENTI. Sfruttare il fatto che $|\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}|$ e definire un'iniezione di $\mathcal{P}(\mathbb{N})$ nell'intervallo $[0, 1]$ (e quindi in $\mathbb{R}$) nel modo seguente. Ogni elemento $c \in 2^{\mathbb{N}}$ si può pensare come una successione $c_1, c_2, c_3 \ldots c_n \ldots$, dove $c_n \in \{0, 1\}$. Poniamo $a_n = \sum_{k=1}^{n} c_k \cdot 10^{-k}$ e notiamo che la successione a_n è crescente a soddisfa $0 \leq a_n \leq 1$. Pertanto esiste il limite $a = \lim_n$ e appartiene all'intervallo $[0, 1]$. Poniamo $f(c) = a$. Provare che l'applicazione $f : 2^{\mathbb{N}} \to [0, 1]$ così definita è iniettiva. Questo dimostra che $|\mathbb{R}| \geq \mathfrak{c}$. Nell'altro verso, per vedere che $|\mathbb{R}| \leq \mathfrak{c}$ notiamo che $\mathbb{R}$ è unione numerabile degli intervalli $[n, n + 1]$, al variare di $n \in \mathbb{Z}$. Quindi, per 6.53 basterebbe dimostrare che $[0, 1] \leq \mathfrak{c}$ (essendo $|[n, n + 1]| = |[0, 1]|$ per ogni $n \in \mathbb{N}$). Pertanto basta provare che $[0, 1]$ ammette un'iniezione in $\mathcal{P}(\mathbb{N})$. Poiché ogni numero irrazionale in $[0, 1]$ ammette un'unica rappresentazione binaria $0, c_1c_2c_3 \ldots c_n \ldots$, dove $c_n \in \{0, 1\}$ e poiché i numeri razionali formano un insieme numerabile, possiamo concludere che $[0, 1]$ ammette un'iniezione in $\mathcal{P}(\mathbb{N})$. □

Esercizio 6.55** $|X \times X| = |X|$ *per ogni insieme infinito X.*

SVOLGIMENTO. Sia A_0 un sottoinsieme numerabile di X. Per il Lemma 5.10, esiste una biiezione $i_{A_0} : A_0 \times A_0 \to A_0$. Si consideri la famiglia $\mathcal{A}$ delle coppie (A, i_A), dove $A_0 \subseteq A \subseteq X$ e $i_A : A \times A \to A$ è una biiezione che estende i_{A_0}. Si consideri in $\mathcal{A}$ la relazione $\leq$ definita da $(A, i_A) \leq (B, i_B)$ se e solo se $A \subseteq B$ e $i_B \restriction_A$. Non è difficile provare che $\leq$ è un ordine per il quale $(\mathcal{A}, \leq)$ è un insieme ordinato induttivo. Per il Lemma di Zorn esiste un membro massimale $(M, i_M) \in \mathcal{A}$. Chiaramente $(M, i_M) \in \mathcal{A}$ implica

$$|M \times M| = |M|. \tag{1}$$

Se $|M| = |X|$, allora abbiamo anche $|X \times X| = |M \times M|$ (vedi l'Esercizio 6.22), e quindi l'uguaglianza (2) assieme alla nostra ipotesi implica $|X \times X| = |X|$. Supponiamo per assurdo che $|M| \neq |X|$. Poiché $|M| \leq |X|$, resta la sola possibilità $|M| < |X|$. D'altra parte $X = M \cup (X \setminus M)$, quindi $|X \setminus M| \geq |M|$ per il Teorema 5.11. Quindi possiamo trovare un sottoinsieme $N \subseteq X \setminus M$ con $|N| = |M|$. Ora $M' = M \cup N$ contiene M propriamente, e $M' \times M' = (M \times M) \cup D$, dove $D = (M \times N) \cup (N \times M) \cup (N \times N)$. Ora $|N \times M| = |M \times N| = |N \times N| = |M| = |N|$. Allora esiste una biiezione $D \to N$, che, assieme alla biiezione $i_M : M \times M \to M$ ci da' una biiezione $i_{M'} : M' \times M' \to M'$ che estende i_M. Quindi $(M', i_{M'}) \in \mathcal{A}$ e $(M, i_M) < (M', i_{M'})$, assurdo. Pertanto $|M| = |X|$. □

Esercizio 6.56* *Dimostrare che* $|X| = |X \times \{0,1\}|$ *per ogni insieme infinito senza far ricorso all'Esercizio 6.48.*

SUGGERIMENTI. Ragionare seguendo lo svolgimento del Lemma 5.13. A questo scopo considerare la famiglia $\mathcal{A}$ delle coppie (A, i_A), dove $A \subseteq X$ e $i_A : A \times \{0,1\} \to A$ è una biiezione, ordinando $\mathcal{A}$ nello stesso modo. Applicando il Lemma di Zorn trovare un membro massimale $(M, i_M) \in \mathcal{A}$. Ragionare per assurdo per provare che $|M| = |X|$ e concludere che la tesi vale. Infatti, se $|M| < |X|$ trovare $N \subseteq X$ con $|N| = |M|$. Ora $|N| = |N \times \{0,1\}|$ essendo $|M| = |M \times \{0,1\}|$. Concludere che per $M' = M \cup N$ esiste una biiezione tra $M' \times \{0,1\} = (M \times \{0,1\}) \cup (N \times \{0,1\})$ e $M \cup N = M'$ che estende i_M e contraddice la massimalità di (M, i_M). □

7 Complementi sui numeri primi

In questa sezione daremo informazione su due celebri "generatori" di numeri primi (i numeri di Fermat e i numeri di Mersenne) e sui numeri perfetti ed amicabili, legati in modo del tutto naturale ai numeri primi. Concluderemo con qualche cenno sulla distribuzione dei numeri primi e sul gioco di Conway che permette di generare i numeri primi ragionando solamente sui primi dieci numeri primi $2, 3, 5, 7, 11, 13, 17, 19, 23$ e 29 e quattordici frazioni composte da questi.

7.1 I numeri di Fermat

I numeri $F_n = 2^{2^n} + 1$ $(n = 0, 1, 2, \ldots)$ sono noti come *numeri di Fermat*.
Osserviamo subito che se vogliamo ottenere dei numeri primi aggiungendo 1 a potenze di 2, dobbiamo imporre all'esponente di essere lui stesso una potenza di 2. Infatti:

Esercizio 7.1 *Dimostrare che se* $2^m + 1$ *è primo, allora* $m = 2^n$ *per qualche numero naturale* n.

SUGGERIMENTI. Se $m = q \cdot r$, dove $r > 1$ è un divisore dispari di m, allora $2^{qr} + 1 = (2^q + 1)(2^{q(r-1)} - \cdots + 1)$ e $1 < 2^q + 1 < 2^m + 1$, quindi $2^m + 1$ non può essere primo. Non avendo m dei divisori dispari concludiamo che $m = 2^n$ per qualche numero naturale n. □

Esercizio 7.2 *Dimostrare che* $F_{n+1} = (F_n - 1)^2 + 1$. *Di conseguenza,* F_{n+1} *è primo se non ha divisori primi* p *con* $p < F_n - 1$.

Lemma 7.3 *Dimostrare che:*
(a) se p *è un divisore primo del numero di Fermat* F_n *allora* p *è del tipo* $2^{n+1}m + 1$*;*
(b) i numeri di Fermat sono a due a due coprimi.

DIMOSTRAZIONE. (a) Notare che $p|F_n$ implica $2^{2^n} \equiv_p -1$ e di conseguenza, elevando al quadrato, $2^{2^{n+1}} \equiv_p 1$. Quindi, $o_p(2)$ divide 2^{n+1}. Ora, per il punto (a) dell'Esercizio 3.34, la prima congruenza dimostra che $o_p(2)$ non è un divisore di 2^n. Poiché tutti i divisori di 2^{n+1} sono del tipo 2^k, concludiamo che $o_p(2) = 2^{n+1}$. Per il teorema di Fermat $2^{p-1} \equiv_p 1$. Ora (b) dell'Esercizio 3.34 ci permette di concludere che $2^{n+1}|p-1$. Quindi, $p - 1 = 2^{n+1}m$ per qualche $m \in \mathbb{Z}$.
(b) Se $p|F_n$ e $p|F_m$, con $n > m$, allora $2^{2^{m+1}} \equiv_p 1$ per (a). Poiché $m + 1 \leq n$, 2^{2^n} è potenza di $2^{2^{m+1}}$ e quindi $2^{2^n} \equiv_p 1$. D'altra parte, $p|F_n$ implica anche $2^{2^n} \equiv_p -1$, assurdo. Pertanto nessun numero primo p divide simultaneamente F_n ed F_m, quindi F_n e F_m sono coprimi. □

Ci si può a questo punto chiedere quali di questi numeri di Fermat sono effettivamente dei primi. La risposta per i primi 5 numeri di Fermat è stata data da Eulero nel 1732. Si osservi che, a parte F_0, F_1, F_2, F_3 e F_4 non sono noti altri numeri di Fermat primi.

Proposizione 7.4 (Fermat) *F_0, F_1, F_2, F_3 e F_4 sono primi, mentre $F_5 = 641 \cdot 6700417$ non è primo*

DIMOSTRAZIONE. Per $F_0 = 3$, $F_1 = 5$ e $F_2 = 17$ questo è ovvio. Segue dall'Esercizio 7.2 che per verificare se F_n è primo basta vedere che F_n non ha divisori primi $p < F_{n-1} - 1$. Per $F_3 = 257$ notiamo che i divisori primi di F_3 con $p < 16 = F_2 - 1$ possono essere tra $2, 3, 5, 7, 11$ e 13. Secondo il Lemma 7.3, i divisori primi di F_3 sono del tipo $16k + 1$ e quindi nessuno di questi primi divide F_3.
Per $F_4 = 2^{32} + 1$ notiamo che per il Lemma 7.3 i divisori primi di F_4 sono del tipo $32k + 1$. Ma i numeri primi di questo tipo minori di $F_3 - 1 = 256$ sono 33, 65, 97, 129, 161, 193 e 225. Tra questi solo 97 e 193 sono primi. Che nessuno dei primi 97 e 193 divida F_4 segue dallo svolgimento dell'Esercizio 3.36.
Per F_5 sappiamo dal Lemma 7.3 che i divisori primi di F_5 sono del tipo $64k + 1$. Tra questi 65 e 129 non sono primi. Dal suggerimento all'Esercizio 3.36 segue che nè 193 nè 257 dividono $F_5 = 2^{32} + 1$. Tra i numeri successivi in questa serie 321, 385 e 513 non sono primi, mentre 449 e 577 sono primi ma non dividono F_5. Per 641 si dimostra che divide F_5 osservando che da $641 = 2^4 + 5^4 = 2^7 \cdot 5 + 1$ seguono le congruenze $2^4 \equiv_{641} -5^4$ e $2^7 \cdot 5 \equiv_{641} -1$. Elevando l'ultima congruenza alla quarta e sostituendo 5^4 con -2^4 si ha

$$1 \equiv_{641} 2^{28} \cdot 5^4 \equiv_{641} -2^{28} \cdot 2^4 \equiv_{641} -2^{32},$$

cioè 641 divide F_5. □

Esercizio 7.5 *Rifare l'Esercizio 3.21, usando il piccolo teorema di Fermat per $p = 2$ e $p = 5$.*

7.2 Numeri primi di Mersenne

I numeri del tipo $M_n = 2^n - 1$ sono noti come *numeri di Mersenne*, dovuto al fatto che Mersenne (1588-1648) li ha studiati in modo sistematico nel suo trattato "Cogita physico-matematica". Tuttavia, questi numeri erano noti anche prima (ai greci, vedi il paragrafo 7.3) e al matematico italiano Cataldi che sapeva che M_{17} e M_{19} sono primi.

Esercizio 7.6 *Siano x, n, m numeri naturali maggiori di 0. Dimostrare che:*
(i) $(x^n - 1) = (x - 1)(x^{n-1} + x^{n-2} + \ldots + x + 1)$;
(ii) se m divide n, allora $(x^m - 1)$ divide $(x^n - 1)$;
(ii) se $x^m - 1$ è primo, allora $x = 2$ e m è primo.

SVOLGIMENTO. i) Basta eseguire il prodotto di destra e osservare che si cancellano tutti i termini, eccetto il primo e l'ultimo.
ii) Se $m|n$, allora $n = mq$, pertanto

$$(x^n - 1) = ((x^m)^q - 1) = (x^m - 1)((x^m)^{n-1} + \ldots + x^m + 1)$$

per il punto i). Da questo si vede che $(x^m - 1)$ divide $(x^n - 1)$.
iii) Se $x > 2$, allora $x^m - 1 = (x - 1)(x^{r-1} + \cdots + x + 1)$ per il punto (i), e quindi è divisibile per $x - 1$. Se d divide m allora $x^d - 1$ divide $x^m - 1$ per il punto (ii). □

Abbiamo visto che M_n è primo solo se n è primo (Esercizio 7.6), tuttavia M_{11} non è primo: si verifica che è divisibile per 23, elevando al quadrato la congruenza $2^6 \equiv_{23} -5$. Il seguente Esercizio chiarisce perché si verifica con 23 il fatto che M_{11} non è primo (è il più piccolo numero primo che ha resto 1 modulo 11).

Esercizio 7.7 *Se un primo p divide un numero di Mersenne M_n, allora $p \equiv_n 1$ se n è primo.*

SUGGERIMENTI. Poiché $2^{p-1} \equiv_p 1$ per il piccolo teorema di Fermat e $2^n \equiv_p 1$ per ipotesi, abbiamo $n|p - 1$ poiché n è primo. □

Gran parte dei numeri di Mersenne sono composti (per esempio, tutti gli M_n con $2300 \leq n \leq 3300$). Tuttavia, per lungo tempo, i più grandi numeri primi noti sono stati i numeri primi di Mersenne. Il motivo di questo è il seguente teorema (criterio) scoperto da Lucas che fa uso dei seguenti numeri L_n, detti *numeri di Lucas* definiti da $L_1 = 4$ e $L_n = L_{n-1}^2 - 2$ per $n > 1$.

Teorema 7.8 *Per $n > 2$ il numero M_n è primo se e solo se M_n divide il numero L_{n-1}.*

Facciamo alcune verifiche. Si vede facilmente che $M_3 = 7$ divide $L_2 = 14$, $M_5 = 31$ divide $L_4 = L_3^2 - 2 = 194^2 - 2 = 37954$ (infatti, $194 \equiv_{31} 8$, e quindi $L_4 \equiv_{31} 8^2 - 2 = 62 \equiv_{31} 0$). Per $n = 7$ si ha $M_7 = 127$, mentre $L_5 = 1416317954 \equiv_{128} 42^2 - 2$, poiché $L_4 \equiv_{128} 67^2 - 2 \equiv_{128} 67 + 66 \cdot 67 - 2 = 65 + 33 \cdot 134 \equiv_{128} 65 + 33 \cdot 7 = 65 + 231 \equiv_{128} 42$.
Ora $L_5 \equiv_{128} 126 \cdot 14 - 2 \equiv_{128} -14 - 2 = -16$, quindi $L_6 \equiv_{128} 16^2 - 2 = 2 \cdot 8 \cdot 16 - 2 = 2(8 \cdot 16 - 1) = 2 \cdot 127 \equiv_{128} 0$. Lasciamo al lettore la verifica del fatto che M_{11} non divide L_{10}, non essendo M_{11} un numero primo. D'altra parte, M_{13} divide L_{12}, essendo M_{13} un numero primo:

Esercizio 7.9 *Dimostrare che $M_{13} = 2^{13} - 1$ è un numero primo.*

SUGGERIMENTI. Per l'Esercizio 7.7 ogni divisore primo p di M_{13} è del tipo $p = 13k + 1$. In più essendo p dispari, si avrà anche $p = 26k + 1$ (in altre parole k può essere solo pari). D'altra parte, $M_{13} < 91^2$, quindi $p \leq 89$ e quindi $k = 1, 2, 3$ sono gli unici possibili valori di k. Per $k = 1$ risulta $p = 27$ non primo. Resta da verificare che 53 e 79 non dividono M_{13}. □

Usando questo criterio, Lucas ha provato nel 1875 che il numero M_{127} è primo e questo risultato rimase insuperato per 75 anni, data la grandezza di

$$M_{127} = 2^{127} = 170141183460469231731687303715884105727.$$

Solo nel 1951, con l'uso dei calcolatori, fu trovato un primo più grande, il numero $\frac{2^{148}+1}{17}$ (con 44 cifre, mentre M_{127} ne ha *solo* 39). I numeri M_{23209} e M_{44497} sono primi, ed erano i più grandi numeri primi verso l'inizio degli anni ottanta del secolo scorso. L'importanza dei numeri primi di Mersenne diviene più chiara nel paragrafo successivo.

7.3 Numeri perfetti e numeri amicabili

Si denoti con $\sigma(n)$ la somma dei divisori di n. Chiaramente la somma $\sigma(n) - n$ di tutti i divisori di n *minori* di n misura, in un certo senso, la quantità di divisori di n. I numeri n con pochi divisori, cioè $\sigma(n) - n < n$ si dicono *scarsi*, mentre quelli con molti divisori, cioè $\sigma(n) - n > n$ si dicono *abbondanti*. Per esempio, 10 è scarso, tutti i numeri primi sono scarsi, mentre 12 e 60 sono abbondanti. Per questo motivo i matematici antichi preferivano i sistemi di numerazione a base 12 o 60 (per esempio in Babilonia). Da questo punto di vista si capisce perché la scelta del termine numero perfetto nella seguente

Definizione 7.10 Un numero naturale n dicesi *perfetto* se $\sigma(n) = 2n$.

Esercizio 7.11 *Dimostrare che 6, 28 e 496 sono perfetti.*

I numeri perfetti erano ben noti nell'antica Grecia. Prima di descrivere tutti i numeri perfetti pari vedremo alcune proprietà utili della funzione σ.

Esercizio 7.12 *Dimostrare che :*
(a) se p è primo, allora $\sigma(p^k) = \frac{p^{k+1}-1}{p-1}$;
(b) se $n = n_1 n_2$ con $(n_1, n_2) = 1$ allora $\sigma(n) = \sigma(n_1)\sigma(n_2)$.
(c) se $n = p_1^{k_1} \dots p_s^{k_s}$ allora $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \dots \frac{p_1^{k_s+1}-1}{p_s-1}$.

SVOLGIMENTO. (a) Tutti i divisori di p^k sono del tipo p^s per $0 \le s \le k$.
(b) Se d divide $n_1 n_2$, allora raccogliendo i primi che compaiono nella fattorizzazione di n_1 e quelli che appaiono nella fattorizzazione di n_2 troviamo una fattorizzazione $d = d_1 d_2$, con $d_1 | n_1$ e $d_2 | n_2$. Quindi

$$\sigma(n_1 n_2) = \sum_{d | n_1 n_2} d = \sum_{d_1 | n_1, d_2 | n_2} d_1 d_2 = \left(\sum_{d_1 | n_1} d_1 \right) \left(\sum_{d_2 | n_2} d_2 \right) = \sigma(n_1)\sigma(n_2).$$

(c) Segue da (a) e (b). □

Il punto (a) del seguente teorema era noto dal famoso trattato di Euclide. Il punto (b) è stato dimostrato da Eulero.

Teorema 7.13 *(a) Sia $p = 2^n - 1$ un numero primo. Allora $\frac{1}{2}p(p+1) = 2^{n-1}(2^n - 1)$ è perfetto.*

(b) Dimostrare che ogni numero perfetto pari è di questo tipo.

SUGGERIMENTI. (a) è ovvio perché con $2^n - 1$ primo $\sigma(2^{n-1}(2^n - 1)) = (2^n - 1)\sigma(2^n - 1) = 2^n(2^n - 1)$.
(b) Sia $n = 2^s n_1$ un numero perfetto, con n_1 dispari. Allora l'ipotesi $\sigma(n) = 2n$ ci dà $(2^{s+1} - 1)\sigma(n_1) = 2^{s+1} n_1$ che implica $2^{s+1} - 1 | n_1$. Sia $n_1 = (2^{s+1} - 1)k$. Allora $\sigma(n_1) = 2^{s+1}k$. Allora $k = 1$, perché altrimenti $\sigma(n_1) \ge n_1 + k + (2^{s+1} - 1) + 1 = 2^{s+1}k + 2^{s+1} > 2^{s+1}k$. Ora $\sigma(n_1) = n_1 + 1$ implica che $n_1 = 2^{s+1} - 1$ è primo. □

Il teorema dice in sostanza, che i numeri perfetti pari sono del tipo $2^{n-1}M_n$, dove M_n è un primo di Mersenne. Non è ancora noto se esistono numeri perfetti dispari.
Nell'antichità conoscevano anche i cosiddetti numeri *amicabili*, cioè coppie di numeri naturali a e b, tali che ognuno sia uguale alla somma dei divisori dell'altro. In termini precisi, $\sigma(a) - a = b$

e $\sigma(b) - b = a$. Quindi, $\sigma(a) = a + b = \sigma(b)$. La prima coppia di numeri amicabili proviene da Pitagora: 220 e 284. Si racconta addirittura che, alla domanda "Che cos'è un amico?", il grande Pitagora abbia risposto: "Uno che sia l'altro 'Io', come 220 e 284".
Il seguente teorema del matematico arabo Thabit (836–901) ci dà altre coppie di numeri amicabili.

Teorema 7.14 *Se i numeri* $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$ *e* $r = 9 \cdot 2^{2n-1} - 1$ *sono primi, allora i numeri* $A = 2^n \cdot p \cdot q$ *e* $B = 2^n \cdot r$ *sono amicabili.*

La dimostrazione segue facilmente dall'Esercizio 7.12. Con $n = 2$ troviamo la coppia 220 e 284 di Pitagora. Non è noto se Thabit conoscesse altri casi oltre a questo. Altre coppie si trovano con $n = 4$ ($A = 17296$, $B = 18416$ scoperta da P. Fermat[7]) e $n = 7$ (scoperta da Cartesio). Entrambi sono arrivati in modo autonomo al teorema di Thabit che nel frattempo è stato completamente dimenticato. Eulero scoprì 59 coppie di numeri amicabili. Il suo record è stato superato solo nel 1929 dal matematico belga Paule Poulet (nel 1929 comparve il suo libro "La caccia ai numeri" con 62 nuove coppie di numeri amicabili, in totale Poulet ne ha scoperte 108). Un fatto curioso è che Fermat è arrivato al suo teorema (il piccolo Teorema di Fermat) proprio nei tentativi di trovare numeri amicabili. Infatti per questo scopo bisogna fattorizzare in prodotto di primi le somme dei divisori di numeri del tipo p^n. Essendo tale somma uguale a $\frac{p^n-1}{p-1}$ Fermat si è domandato se $p^n - 1$ sia divisibile per $n + 1$ quando $n + 1$ è primo.

7.4 Distribuzione dei numeri primi

La domanda "Quanti primi ci sono?" è del tutto naturale, ma posta così ha l'ovvia risposta (infiniti !) dovuta al teorema di Euclide. Cerchiamo allora di togliere la possibilità di "specularе" con l'infinito, chiedendo: quanti primi ci sono $\leq n$, dove n è un dato numero naturale $n > 1$. Denotiamo la quantità di questi primi con $\pi(n)$. Si ha ovviamente

$$\pi(2) = 1, \pi(3) = \pi(4) = 2, \pi(5) = \pi(6) = 3, \pi(7) = \pi(8) = \pi(9) = \pi(10) = 4,$$

$$\pi(11) = \pi(12) = 5, \pi(14) = \pi(15) = \pi(16) = \pi(17) = 6, \pi(18) = \pi(19) = 7,$$

$$\pi(20) = \pi(21) = \pi(22) = 8, \pi(23) = \pi(24) = \pi(25) = \pi(26) = \pi(27) = \pi(28) = 9, \ldots.$$

Si vede che questa distribuzione è molto caotica, lunghi intervalli senza numeri primi si alternano a brevissimi intervalli tra due primi consecutivi a distanza 2 (coppie di primi gemelli). Tuttavia, ci sono certe regole come ci mostra il seguente

Postulato di Bertrand. *Per ogni* $n \in \mathbb{N}_+$ *l'intervallo* $[n, 2n]$ *contiene almeno un numero primo.*

Infatti, per ogni $n \in \mathbb{N}$ maggiore di 3 l'intervallo $[n, 2n-2]$ contiene almeno un numero primo. Mentre da un teorema più preciso di Chebishev segue che esistono almeno due numeri primi p nell'intervallo $[n, 2n]$ per ogni $n \in \mathbb{N}$ maggiore di 1. Questo ci permette di dimostrare facilmente per induzione che se $p_1, p_2, \ldots, p_n, \ldots$ sono tutti i numeri primi in ordine crescente, allora $p_n < 2^n$:

Esercizio 7.15 *Sia* $n > 3$ *un numero naturale. Dimostrare che ci sono almeno* $\log_2 n$ *numeri primi nell'intervallo* $[2, n]$.

[7]ma nota molto prima anche a Ibn Al Banna del Marocco (1256-1321).

Il rapporto $\pi(n)/n$ che permette di parlare della densità dei numeri primi è stato dimostrato essere circa $1/\log n$ (qui il logaritmo è a base $e = \lim_n(1+1/n)^n$). In altre parole, con la crescita di n i primi diventano più "rari". D'altra parte, è noto che per ogni n la somma di tutti valori reciproci $1/p$, dove $p \leq n$ è primo, è $> \log\log n - 1$ (che dà un'ulteriore dimostrazione del teorema di Euclide dell'infinità dei numeri primi).
Per il postulato di Bertrand ogni intervallo del tipo $[n, 2n-2]$ contiene almeno un numero primo. Vediamo adesso che ci sono intervalli arbitrariamente lunghi di numeri naturali consecutivi che non contengono numeri primi.

Esercizio 7.16 *Sia $n > 1$ un intero, allora nessuno degli $n-1$ numeri consecutivi $n!+2, n!+3, \ldots, n!+n$ è primo.*

Si può osservare la distribuzione dei numeri primi limitandosi a specifiche progressioni aritmetiche. Abbiamo visto (vedi gli Esercizi 3.17 e 3.18) che ciascuna delle progressioni aritmetiche $3k+2$, $4k+3$ e $6k+5$ contiene infiniti numeri primi.

Esercizio 7.17 *Si dimostri che ci sono infiniti numeri primi del tipo $4k+1$ e infiniti numeri primi del tipo $8k+1$.*

Svolgimento. Supponiamo per assurdo che ci sia un numero finito di numeri primi del tipo $4k+1$ e li elenchiamo: $p_1, p_2, \ldots, p_n$. Sia adesso $N = 4(p_1 p_2 \ldots p_n)^2 + 1$. Per la nostra ipotesi N non può essere primo essendo maggiore di tutti i p_k. Sia p un divisore primo di N. Allora, per l'Esercizio 8.5, p deve essere della forma $4k+1$ e coincidere con qualche p_k, assurdo perché nessun p_k divide N. Similmente per i primi del tipo $8k+1$. □

Ragionando allo stesso modo si dimostra

Esercizio 7.18 *Sia $s > 1$ un intero. Si dimostri che ci sono infiniti numeri primi del tipo $2^s k + 1$.*

Per quanto riguarda le progressioni aritmetiche in generale, vale il seguente risultato.

Teorema 7.19 (**Teorema di Dirichlet**) *Siano a e b due numeri naturali relativamente primi. Allora esistono infiniti numeri primi della forma $ak+b$.*

Ovviamente, $ak+b$ non può essere primo se a e b non sono relativamente primi.
La seguente congettura è rimasta tuttora aperta, dopo più di duecento anni!.

Congettura 7.20 (Goldbach) *Ogni numero pari maggiore di 3 è somma di due numeri primi.*

Non è risolta nemmeno la forma più debole della congettura: *ogni numero dispari maggiore di 5 è somma di tre numeri primi.*

7.5 Il gioco di Conway

Questo gioco permette di ottenere consecutivamente i numeri primi a partire da 2. Come base serve la seguente successione di 14 numeri razionali

$$\frac{17}{91}, \frac{78}{85}, \frac{19}{51}, \frac{23}{38}, \frac{29}{33}, \frac{77}{29}, \frac{95}{23}, \frac{77}{19}, \frac{1}{17}, \frac{11}{13}, \frac{13}{11}, \frac{15}{14}, \frac{15}{2}, 55. \qquad (*)$$

Si comincia con $N = 2$ e si rimpiazza ad ogni passo N con aN, dove a è il primo tra i numeri della successione (*) per il quale aN sia un numeri intero. Così si ricava la successione

$$2, 15, 825, 725, 1825, 2275, \ldots \qquad (**)$$

Infatti, il primo a tale che $2a \in \mathbb{Z}$ è $\frac{15}{2}$, perciò il secondo membro di (**) è 15. Ora il primo a tale che $15a \in \mathbb{Z}$ è 55, perciò il terzo membro è $825 = 15 \cdot 55$. È utile tenere presente anche la fattorizzazione in primi $825 = 3 \cdot 5^2 \cdot 11$ e di tenere conto della fattorizzazione dei denominatori $91 = 7 \cdot 13$, $85 = 5 \cdot 17$, $51 = 3 \cdot 17$, $38 = 2 \cdot 19$, $33 = 3 \cdot 11$, $14 = 2 \cdot 7$ e dei nominatori $78 = 2 \cdot 3 \cdot 13$, $77 = 7 \cdot 11$, $95 = 5 \cdot 19$, $15 = 3 \cdot 5$. Questo permette di vedere più facilmente che al passo successivo $825a \in \mathbb{Z}$ accade per prima volta con $\frac{29}{33}$ e così ricaviamo $725 = 5^2 \cdot 29$. Adesso $725a \in \mathbb{Z}$ accade per prima volta con $\frac{77}{29}$, così ricaviamo $1825 = 5^2 \cdot 7 \cdot 11$ ecc. Consigliamo il lettore di verificare che dopo un certo numero di passi si ricava $4 = 2^2$, poi da 4, dopo un'altra successione di passi, si ricava $8 = 2^3$ e dopo altri passi si trova $32 = 2^5$. Proseguendo in questo modo, si vede che le potenze di 2 che compaiono in questa successione sono proprio quelle del tipo 2^p, dove p è il numero primo di turno, cioè (**) ha la forma

$$2, 15, \ldots, 2^2, 30, \ldots, 2^3, 60, \ldots, 2^5, 240, \ldots, 2^7, \ldots, 2^{11}, \ldots, 2^{13}, \ldots, 2^{17}, \ldots$$

8 Esercizi di Aritmetica

Esercizio 8.1 *Siano a e b due numeri naturali coprimi. Dimostrare che se il prodotto è un quadrato perfetto*[8]*, lo sono anche entrambi i fattori a e b.*

Esercizio 8.2 *Fattorizzare in prodotto di numeri primi i seguenti numeri 120=5!, 6!, 7!, 8!.*

Esercizio 8.3 *Determinare con quanti zeri terminano i numeri 10! e 20!*

Esercizio 8.4 *(a) Sia $a = \overline{a_3a_2a_1a_0}$ un numero naturale con quattro cifre decimali. Allora a è divisibile per 1001 precisamente quando $a_2 = a_1 = 0$ e $a_3 = a_0$. In tal caso a è divisibile anche per 7, 11 e 13. In particolare,*

(1) 2002 è divisibile per 7, 11 e 13.

(2) l'anno futuro più vicino con questa proprietà è 3003.

(b) Sia $a = \overline{a_4a_3a_2a_1a_0}$ un numero naturale con cinque cifre decimali. Allora a è divisibile per 1001 precisamente quando $a_2 = 0$, $a_4 = a_1$ e $a_3 = a_0$. In tal caso a è divisibile anche per 7, 11 e 13.

(c) Sia $a = \overline{a_5a_4a_3a_2a_1a_0}$ un numero naturale con sei cifre decimali. Allora a è divisibile per 1001 precisamente quando $\overline{a_5a_4a_3} = \overline{a_2a_1a_0}$. In tal caso a è divisibile anche per 7, 11 e 13.

Esercizio 8.5 *Sia $p > 2$ un numero primo. Dimostrare che:*
(a) se p divide $a^2 + 1$ per qualche numero intero a, allora p è del tipo $4k + 1$.
(b) se p divide $a^4 + 1$ per qualche numero intero a, allora p è del tipo $8k + 1$.

Svolgimento. (a) Essendo p dispari, per $t = \frac{p-1}{2}$ abbiamo $1 \equiv_p a^{p-1} = (a^2)^t \equiv_p (-1)^t$, quindi $(-1)^t = 1$ e di conseguenza $t = 2k$ è pari. Questo dimostra $p = 4k + 1$.
(b) Dal punto (a) applicato ad a^2 concludiamo che $p = 4t + 1$ per qualche $t \in \mathbb{Z}$. Sia $t = \frac{p-1}{2}$. Allora $1 \equiv_p a^{p-1} = (a^4)^t \equiv_p (-1)^t$, quindi $(-1)^t = 1$ e di conseguenza $t = 2k$. Questo dimostra $p = 8k + 1$. □

[8] cioè coincide con il quadrato di un altro numero naturale

Esercizio 8.6 *Si dimostri che ogni numero naturale $n > 0$ si può scrivere in modo unico nella forma $\Sigma_{i=1}^{n} c_i \cdot i!$, con $0 \leq c_i \leq i$.*

SVOLGIMENTO. Lo dimostriamo usando il principio di induzione nella seconda forma. Se $n = 1$ allora basterà prendere $c_n = 0$ per ogni $n \geq 1$ e $c_1 = 1$. Sia ora n un numero naturale e sia m il massimo dei naturali tali che $m! \leq n$, allora $(m+1)! > n$. Grazie alla divisione euclidea di n per $m!$, esistono $q, r \in \mathbb{N}$, con $0 \leq r < m!$ tali che $n = q \cdot m! + r$. Applichiamo ora a $r < m! \leq n$ l'ipotesi induttiva. Otteniamo $r = \Sigma_{i=1}^{r} c_i \cdot i!$, con $0 \leq c_i \leq i$. Poiché $r < m!$, la sommatoria precedente si arresta ad $m-1$, cioè $r = \Sigma_{i=1}^{m-1} c_i \cdot i!$, con $0 \leq c_i \leq i$. Pertanto

$$n = q \cdot m! + r = q \cdot m! + \Sigma_{i=1}^{m-1} c_i \cdot i! = \Sigma_{i=1}^{m} c_i \cdot i!$$

ponendo $q = c_m$ ed osservando che $0 \leq q = c_m \leq m$, cioè $q < m+1$. Infatti $(m+1)m! = (m+1)! > n = q \cdot m! + r \geq q \cdot m!$, da cui dividendo per $m!$, si ottiene $q < m+1$. □

Esercizio 8.7 *Sia $b_0 = 1, b_1, b_2, \ldots b_n, \ldots$ una successione di numeri naturali con $b_n > 1$ per $n > 0$ e sia $M_k = b_0 \ldots b_k$ per ogni $k \in \mathbb{N}$. Dimostrare che ogni numero naturale $n > 0$ si può scrivere in modo unico nella forma $\Sigma_{i=0}^{\infty} c_i \cdot M_i$, con $0 \leq c_i < b_{i+1}$.*

Definiamo ora il seguente polinomio: $f_b(x) = x^2 - x + b$, con $b \in \mathbb{N}$ e $b > 1$. Allora $f_b(x)$ si dice un *polinomio di Eulero* se per ogni $x \in \mathbb{N}$, $x < b$ si ha che $f_b(x)$ è un numero primo. Poiché $f_b(-x+1) = f_b(x)$, anche tutti i valori $f_b(x)$ con $-b+1 < x < 0$, x intero, saranno primi.

Esercizio 8.8 *Dimostrare che*

(i) se $f_b(x) = x^2 - x + b$ è un polinomio di Eulero, allora b è primo;

(ii) per $b = 2, 3, 5, 11, 17, 41$ $f_b(x)$ è un polinomio di Eulero;

(iii) per $b \leq 1000$, questi sono gli unici polinomi di Eulero.

SUGGERIMENTI. (i) Se esiste $d \in \mathbb{N}$ con $1 < d < b$ e $d|b$, allora $d < b$ è un divisore proprio di $f_b(d)$, che pertanto non può essere un primo.
(ii) Le prime verifiche sono immediate, per $b = 17$ si utilizzi l'Esercizio 3.3 e per $b = 41$ si facciano le opportune verifiche.
(iii) Supponiamo $b \geq 7$. Notiamo che per $x = 2, 3, 4, 5, 6$, si ha $x(x-1) = 2, 6, 12, 20, 30$ rispettivamente. Se $f_b(x) = x^2 - x + b = x(x-1) + b$ è un polinomio di Eulero, allora per il punto i), b è un primo. Inoltre da quanto appena osservato e dalla definizione si ha che anche $b+2$, $b+6$, $b+12$, $b+20$ e $b+30$ devono essere dei primi. Quindi in particolare b deve essere il più piccolo di una coppia di *primi gemelli* (due primi p e q si dicono primi gemelli se $q - p = 2$). Osserviamo che, poiché b è un primo, $b \equiv_6 1$ o 5. Ma se fosse $b \equiv_6 1$, allora $b + 2 \equiv_6 3$ e quindi $b+2$ sarebbe divisibile per 3 e non potrebbe essere un primo.
Vediamo quale può essere l'ultima cifra di b. Se fosse $b \equiv_{10} 5$, b sarebbe divisibile per 5 e quindi non potrebbe essere un primo. Se fosse $b \equiv_{10} 3$, $b+2$ sarebbe divisibile per 5 e infine $b \equiv_{10} 9$, $b+6$ sarebbe divisibile per 5, in contraddizione con quanto richiesto.
Concludendo abbiamo $b \equiv_6 5$ e $b \equiv_{10} 1$ oppure 7. Questo ci permette di concludere allora che b deve essere del tipo $b = 11 + 30k$ oppure $b = 17 + 30k$. Gli unici possibili primi che dobbiamo indagare sono: $b = 11, 17, 41, 47, 71, 77$ se vogliamo fermarci a 100. Ma 77 non è un primo, e 47 non è un primo gemello (infatti 49 non è primo). Per quel che riguarda 71, osserviamo che 71+2= 73 è un primo, ma 71+6=77 non lo è già più. Se vogliamo continuare fino a 1000, è facile scrivere tutti i numeri del tipo descritto e poi basta avere sottomano una lista dei primi

minori di 1000 per controllare che gli unici primi della forma $b = 11 + 30k$ oppure $b = 17 + 30k$ con $b + 2$ primo sono b =101, 107, 137, 191, 197, 227, 281, 347, 431, 461, 491, 521, 617, 641, 821, 827, 857, 88 1. Per questi, un facile controllo mostra che almeno uno dei $b + 6$, $b + 12$, $b + 20$, $b + 30$, $b + 42$ o $b + 72$ non è un primo. □

Si può dimostrare che non esiste alcun polinomio $f(x)$ con coefficienti interi, tale che tutti i valori $f(x)$ per $x \geq x_0$, intero, siano primi. Tuttavia esistono delle funzioni più complesse che danno come valori soli numeri primi (per esempio, è noto che esiste una costante positiva A tale che per ogni numero naturale x il valore $[A^{3^x}]$ è un numero primo). È molto più facile trovare invece dei polinomi che danno come valori solamente numeri composti, come per esempio $n^4 + 4$. Infatti, $n^4 + 4$ è composto per ogni $n \in \mathbb{Z}$ essendo $n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$ (il così detto Teorema di Sophie Germain).

Esercizio 8.9 *Dimostrare che per ogni numero $n \in \mathbb{N}_+$ i numeri $2^{2^{10n+1}} + 19$ e $2^{2^{4n+1}} + 7$ sono composti.*

Esercizio 8.10 *Dimostrare che ci sono infiniti numeri composti del tipo:*
(a) $10^n + 3$*;*
(b) $(2^{2n} + 1)^2 + 2$.

Esercizio 8.11 *Dimostrare che nessuna potenza 3^k finisce con ...11.*

Esercizio 8.12 *Dimostrare che $2^{13} - 1$ è un primo.*

Esercizio 8.13 *Risolvere le equazioni congruenziali:*
a) $102x \equiv_{21} 14$*;*
b) $15x \equiv_{87} 122$*;*
c) $402x \equiv_{57} 45$*;*
d) $37x \equiv_{16} 14$*;*
e) $82x \equiv_{13} 174$.

Esercizio 8.14 *Risolvere le seguenti equazioni congruenziali:*
a) $4x \equiv_{17} -3$*;* *b)* $29x + 3 \equiv_{12} 0$*;* *c)* $3x - 8 \equiv_{13} 0$*;* *d)* $7x \equiv_{19} 4$*;* *e)* $37x \equiv_{117} 25$*;*
f)$13x \equiv_{153} 178$*;* *g)*$18x \equiv_{51} 5$

Esercizio 8.15 *Trovare i numeri interi x che soddisfano le equazioni congruenziali:*

$$x \equiv 2(mod\ 3),\ \ x \equiv 1(mod\ 4)\ \text{ e }\ x \equiv 3(mod\ 5).$$

Esercizio 8.16 *Dimostrare che :*
a) per k dispari 7 divide $13^{k+1} - 1$;
b) per k pari 5 non divide $3^{k+1} - 1$;
c) per k pari 5 non divide $3^{k+1} + 1$;
d) per k pari 5 non divide $13^{k+1} - 1$;
e) per k pari 5 non divide $13^{k+1} + 1$;

Esercizio 8.17 *Trovare il massimo comun divisore $d = (2^{44} - 1, 2^{26} - 1)$.*

Esercizio 8.18 *Trovare il massimo comun divisore $d = (2^{52} - 1, 2^{39} - 1)$.*

Esercizio 8.19 *Trovare il massimo comun divisore $d = (2^{63} - 1, 2^{36} - 1)$.*

Esercizio 8.20 *Siano x, n, m numeri naturali maggiori di 0. Dimostrare che:* $(x^m - 1, x^n - 1) = x^{(m,n)} - 1$.

SVOLGIMENTO. Sia $d = (x^m - 1, x^n - 1)$ e sia $c = (m, n)$. Poiché c divide sia m che n, avremo che $x^c - 1$ divide sia $(x^m - 1)$ che $(x^n - 1)$ per il punto ii) dell'Esercizio 7.6. Pertanto $x^c - 1$ divide anche d.
Poiché $c = (m, n)$, esistono $u, v \in \mathbb{N}$ tali che $c = mu - nv$. Allora d divide $x^m - 1$ e quindi per ii) divide anche $x^{mu} - 1$ e analogamente d divide $x^{nv} - 1$. Allora d divide anche la loro differenza, cioè d divide $(x^{mu} - 1) - (x^{nv} - 1) = x^{mu} - x^{nv} = x^{nv}(x^{mu-nv} - 1)$. Poiché $x^m - 1$ e x sono due numeri naturali coprimi, e d divide $x^m - 1$, si avrà che d è coprimo con x^{nv} e quindi divide $(x^{mu-nv} - 1) = x^c - 1$. □

Esercizio 8.21 *Dimostrare che 59 divide* $2^{29} + 1$.

Esercizio 8.22 *Dimostrare che:*

(a) *13 divide* $2^{70} + 3^{70}$*;*

(b) $11 \cdot 31 \cdot 61$ *divide* $20^{15} - 1$.

Esercizio 8.23 *Sia $a > 1$ un numero naturale. Trovare il resto di a^{100} modulo 125.*

Esercizio 8.24 *Sia $a > 1$ un numero naturale. Dimostrare che il numero $\frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ non è mai intero.*

Esercizio 8.25 *Sia n un numero naturale dispari. Dimostrare che n divide $a^{n!} - 1$ se a è coprimo con n.*

Esercizio 8.26 *Sia $n > 0$ un numero naturale. Dimostrare che il numero $\frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n+1}$ non è mai intero.*

Esercizio 8.27 *Sia n un numero naturale dispari. Dimostrare che n divide $2^{n!} - 1$.*

SUGGERIMENTI. Notare che $\varphi(n)$ divide $n!$. □

Esercizio 8.28 *Trovare le ultime due cifre di*

(a) 2^{999}*;*

(b) a^2*, dove a è un numero pari;*

(c) $(\ldots(((7^7)^7)^7)^7\ldots)^7$ *(7 compare n volte).*

(d) $7^{7^{\cdot^{\cdot^{7}}}}$ *(7 compare n volte).*

Esercizio 8.29 *Sia p un numero primo. Dimostrare che*

(a) *p divide il coefficiente binomiale C_k^p per ogni $0 < k < p$.*

(b) $(x + y)^{p^s} \equiv_p x^{p^s} + y^{p^s}$ *per ogni $x, y \in \mathbb{Z}$ e $s \in \mathbb{N}$.*

(c) la massima potenza p^m con la quale p divide $n!$ è data da

$$m = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^k}\right] + \ldots . \qquad (*)$$

SUGGERIMENTI. (a) Sfruttare la formula $C_k^p = \frac{p!}{k!(p-k)!}$ e il fatto che p divide il nominatore ed è coprimo con il numeratore.
(b) Segue da (a) per induzione su s.
(c) $\left[\frac{n}{p}\right]$ coincide con il numero dei multipli di p nel prodotto che definisce $n!$. Di questi $\left[\frac{n}{p^2}\right]$ sono multipli di p^2 (e contribuiscono ciascuno con un altro fattore p), $\left[\frac{n}{p^3}\right]$ ecc. □

Esercizio 8.30 *Trovare con quanti zeri termina* 2000!.

Esercizio 8.31 *Dimostrare che il numero* ((3!)!)! *ha più di mille cifre decimali e trovare con quanti zeri termina questo numero.*

Esercizio 8.32 *Se $n \in \mathbb{N}_+$, allora $(n!)^{(n-1)!}$ divide $(n!)!$.*

Esercizio 8.33 *Se $n \in \mathbb{N}$ è maggiore di 2, allora 2^n non divide $n!$.*

Esercizio 8.34 *Determinare i numeri $n \in \mathbb{N}_+$ tali che n non divide $(n-1)!$.*

Esercizio 8.35 *Sia $p > 2$ un numero primo. Dimostrare che:*
(a) se $x \equiv_p y$ per $x, y \in \mathbb{Z}$, allora $x^p \equiv_{p^2} y^p$.
(b) se $x^p + y^p \equiv_p 0$ per $x, y \in \mathbb{Z}$, allora $x^p + y^p \equiv_{p^2} 0$.

Adesso vediamo che una "piccola" modifica nel piccolo teorema di Fermat cambia completamente la situazione.

Esercizio 8.36 *Sia p un numero primo e sia $a \in \mathbb{Z}$. Se $a^p \equiv_p 1$, allora $a^p \equiv_{p^2} 1$.*

Esercizio 8.37 *Sia p un numero primo. Dimostrare che $C_k^{p-1} \equiv_p (-1)^k$ per ogni $0 < k < p$.*