APPUNTI DEL CORSO DI MATEMATICA DISCRETA
per il corso di Laurea in Informatica [1]

ELEMENTI DI TEORIA DEGLI INSIEMI

1. Insiemi e sottoisiemi

In questa parte richiamiamo alcune nozioni di base sul linguaggio degli insiemi. Non tenteremo definizioni formali, ne' ci addentreremo nella teoria assiomatica degli insiemi, introdurremo solo un linguaggio che sara' utile nel seguito.

Sono noti i concetti di **insieme** e di **elemento** di un insieme.
L'affermazione "a e' un elemento dell'insieme A" si scrivera' sinteticamente

$$a \in A.$$

Dati due insiemi A e B, diremo che A è **sottoinsieme** di B se ogni elemento di A è anche elemento di B (scriveremo $A \subseteq B$).

Se $A \subseteq B$ e $B \subseteq A$ i due insiemi si dicono uguali e si scrive $A = B$. Quindi per verificare che due insiemi sono uguali dobbiamo provare che ogni elemento di A e' anche elemento di B e che ogni elemento di B e' anche elemento di A.

Se $A \subseteq B$, ma $A \neq B$, diremo che A è un sottoinsieme **proprio** di B e scriveremo $A \subset B$. .

1. Un sottoinsieme puo' essere definito elencando semplicemente i suoi elementi:

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

si legge l'insieme costituito dagli elementi $a_1, \ldots, a_n$.

2. Un sottoinsieme puo' essere definito indicando una proprieta' P che deve essere soddisfatta dai suoi elementi:

$$B = \{a \in A : a \text{ soddisfa } P\}$$

L'insieme privo di elementi si dice insieme **vuoto** e si indica con il simbolo $\emptyset$. L'insieme vuoto e' sottoinsieme di ogni insieme. E' facile quindi verificarne l'unicita'.

[1] Con tali appunti si vuole fornire un sussidio didattico per lo studente. Essi raccolgono i principali argomenti affrontati, non contengono le dimostrazioni e non presentano molti degli esempi ed esercizi svolti a lezione.

Quando introdurremo il concetto di operazione, vedremo le principali operazioni tra insiemi.

Ricordiamo ora brevemente gli insiemi numerici nei quali supponiamo che siano di vostra conoscenza le operazioni elementari.

L'insieme $\mathbb{N}$ dei numeri naturali e' l'insieme infinito costituito dagli interi positivi o nulli:

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$$

In tale insieme, un importante risultato sul quale ritorneremo nel corso, e' il teorema di divisione. Dati m e $n \in \mathbb{N}$ $(n \neq 0)$, esistono unici due numeri naturali q e r tali che $r < n$ e $m = n \cdot q + r$. Se $r = 0$, diremo che m e' divisibile per n.

Denotiamo con $\mathbb{Z}$ l'insieme dei numeri interi:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\}$$

Pertanto $\mathbb{N} \subset \mathbb{Z}$.

L'insieme $\mathbb{Q}$ dei numeri razionali e' l'insieme:

$$\mathbb{Q} = \{ \frac{p}{q} \ \text{(frazioni)} \ : \ p, q \in \mathbb{Z}, \ q \neq 0\}.$$

Ricordiamo che $\frac{p}{q}$ e $\frac{p'}{q'}$ rappresentano lo stesso numero razionale se e soltanto se $p \cdot q' = p' \cdot q$. Si identifica la frazione $\frac{p}{1}$ con il numero intero p. Questo consente di affermare che $\mathbb{Z} \subset \mathbb{Q}$.

L'insieme $\mathbb{R}$ dei numeri reali e' un insieme numerico contenente $\mathbb{Q}$. Per la sua definizione rinviamo al corso di Analisi Matematica, mentre vedremo nel seguito in modo rigoroso la costruzione di $\mathbb{Z}$ e $\mathbb{Q}$.

Definiamo l'insieme **prodotto cartesiano** di due insiemi A e B l'insieme formato da tutte le coppie **ordinate** (a, b) in cui la prima componente a è un elemento di A e b e' un elemento di B e si indica con $A \times B$.

$$A \times B = \{(a, b) \ : a \in A, \ b \in B\}.$$

Ne prodotto cartesiano due coppie ordinate (a, b) e (a', b') sono uguali se e solo se $a = a'$ e $b = b'$.
In generale indichiamo con $A_1 \times A_2 \times \ldots \times A_n$ l'insieme delle n - uple ordinate $(a_1, a_2, \ldots, a_n)$ la cui i - esima componente a_i, è un elemento di A_i. Il prodotto cartesiano di n copie di A cioè $A \times A \ldots \times A$ (n volte) si indica di solito con A^n. Un esempio a voi gia' noto e' il piano cartesiano $\mathbb{R}^2$.

2. Corrispondenze e funzioni

Dati due insiemi A e B, si dice **funzione** (o applicazione) di A in B, e si denota $f\colon A \longrightarrow B$, una legge che *ad ogni* elemento $a \in A$ associa *uno e un solo* elemento $b \in B$. Tale b si dice **valutazione** o **immagine** di a mediante f e si scrive $b = f(a)$. Gli insiemi A e B si dicono rispettivamente dominio e codominio dell'applicazione f.

Una **corrispondenza** tra due insiemi A e B è un sottoinsieme $D \neq \emptyset$ del prodotto cartesiano $A \times B$. Si dice che $a \in A$ e $b \in B$ sono corrispondenti se $(a, b) \in D$.

Allora una corrispondenza $D \subseteq A \times B$ è il grafico di una funzione se per ogni $a \in A$ esiste un unico $b \in B$ tale che $(a, b) \in D$.

Data una funzione $f\colon A \longrightarrow B$ e dati $S \subseteq A, T \subseteq B, b \in B$ si definiscono:

immagine di S l'insieme $f(S) = \{b \in B : \exists\ a \in S \text{ con } b = f(a)\}$ (in particolare $f(A)$ si dice immagine di f e si denota anche Imf);

controimmagine di b l'insieme $f^{-1}(b) = \{a \in A :\ f(a) = b\}$;

controimmagine di T l'insieme $f^{-1}(T) = \{a \in A :\ f(a) \in T\} = \bigcup_{b \in T} f^{-1}(b)$;

In Informatica si usa anche il concetto di *funzione parziale.* Come abbiamo visto, $f\colon A \longrightarrow B$ e' una funzione se soddisfa una *condizione di univocita'* (ad un elemento di A corrisponde al piu' un elemento di B) e una *condizione di totalita'* (ad ogni elemento di A corripsonde almeno un elemento di B).
Diremo che $f\colon A \longrightarrow B$ e' una **funzione parziale** se soddisfa la condizione di univocita'. Una funzione (con univocita' e totalita') si dice anche funzione totale.

Ad esempio $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ definita da $f(x) = \frac{1}{x}$ e' una funzione parziale.

Una funzione $f\colon A \longrightarrow B$ si dice **iniettiva** se

$$\forall a_1, a_2 \in A \quad a_1 \neq a_2 \Longrightarrow f(a_1) \neq f(a_2)$$

o equivalentemente se

$$\forall a_1, a_2 \in A \quad f(a_1) = f(a_2) \Longrightarrow a_1 = a_2$$

o anche se e solo se

$$f^{-1}(b) \text{ e}' \text{ costituita da un solo elemento } \forall \text{ b} \in \text{Imf}.$$

Una funzione $f: A \longrightarrow B$ si dice **surgettiva** se

$$Imf = B$$

o equivalentemente se

$$\forall \ b \in B \ \ \exists \ \ a \in A \ \text{ tale che } \ \text{f(a)} = \text{b}$$

o ancora se e solo se

$$f^{-1}(b) \neq \emptyset \quad \forall \quad b \in B.$$

Una funzione $f: A \longrightarrow B$ si dice **bigettiva** se è iniettiva e surgettiva e in tal caso si chiama anche **corrispondenza biunivoca**.

Esempi.
• $id_A: A \longrightarrow A$ definita dalla legge $f(a) = a \ \forall \ a \in A$ si dice *funzione identica* ed è bigettiva.

• Si dice che $f: A \longrightarrow B$ e' una *funzione costante* di valore $b_0 \in B$ se $f(a) = b_0 \ \ \forall \ \ a \in A$.
Una funzione costante è iniettiva se e solo se $A = \{a\}$; è surgettiva se e solo se $B = \{b_0\}$.

Esercizi.
1. Provare che $f: \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ definita da $f((x, y)) = 2x - 2y$ e' surgettiva, ma non iniettiva.
2. Provare che $f: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ definita da $f((x, y)) = 2x - 2y$ non e' surgettiva e non e' iniettiva.
3. Provare che $f: \mathbb{N} \longrightarrow \mathbb{Z}$ definita da

$$f(n) = \begin{cases} \frac{n}{2,} & \text{se } \ n \ e' \ pari \\ -\frac{n+1}{2} & \text{se } \ n \ e' \ dispari. \end{cases}$$

e' bigettiva.
4. Sia A un insieme finito e $f: A \to A$ una funzione. Provare che
f e' iniettiva $\iff$ f e' surgettiva $\iff$ f e' bigettiva.
5. Costruire una funzione $f: \mathbb{N} \to \mathbb{N}$ che sia iniettiva, ma non surgettiva e una funzione $g: \mathbb{N} \to \mathbb{N}$ che sia surgettiva, ma non iniettiva.

Siano $\varphi: A \to B$ e $\psi: B \to C$ due funzioni, diremo **funzione composta** di φ e ψ e scriveremo $(\psi \circ \varphi)$ l'applicazione definita ponendo

$$(\psi \circ \varphi)(a) = \psi(\varphi(a))$$

Esempio. Siano $\varphi\colon \mathbb{R} \to \mathbb{R}$ definita da $\varphi(x) = x^2$ e $\psi\colon \mathbb{R} \to \mathbb{R}$ definita da $\psi(x) = x + 2$.
Allora $\psi \circ \varphi\colon \mathbb{R} \to \mathbb{R}$ e' definita da $\psi \circ \varphi(x) = \psi(\varphi(x)) = \psi(x^2) = x^2 + 2$.
Inoltre $\varphi \circ \psi\colon \mathbb{R} \to \mathbb{R}$ e' definita da $\varphi \circ \psi(x) = \varphi(\psi(x)) = \varphi(x + 2) = (x + 2)^2$.
Osserviamo che $\psi \circ \varphi \neq \varphi \circ \psi$.

La composizione di funzioni in generale non e' commutativa, ma si prova che la composizione di funzioni e' associativa. Siano infatti $\varphi\colon A \to B$, $\psi\colon B \to C$ e $\gamma\colon C \to D$ funzioni. Allora

$$(\gamma \circ \psi) \circ \varphi = \gamma \circ (\psi \circ \varphi)$$

Il seguente risultato prova che la composizione di funzioni mantiene le buone proprieta' delle singole componenti.

Proposizione. *Siano $\varphi\colon A \to B$ e $\psi\colon B \to C$: due funzioni. Allora*
i) *se φ e ψ sono iniettive, allora $\psi \circ \varphi$ è iniettiva;*
ii) *se φ e ψ sono surgettive, allora $\psi \circ \varphi$ è surgettiva;*
iii) *se φ e ψ sono bigettive, allora $\psi \circ \varphi$ è bigettiva.*

Il viceversa delle asserzioni precedenti non vale, ma dalle proprieta' della composizione possiamo ancora dedurre qualche informazione su almeno una delle componenti.

Proposizione. *Siano $\varphi\colon A \to B$ e $\psi\colon B \to C$: due funzioni. Allora*
i) *se $\psi \circ \varphi$ è iniettiva, allora φ è iniettiva;*
ii) *se $\psi \circ \varphi$ è surgettiva, allora ψ è surgettiva;*
iii) *se $\psi \circ \varphi$ è bigettiva, allora φ è iniettiva e ψ è surgettiva*

Sia $\varphi\colon A \to B$ una funzione, diremo che φ e' **invertibile** se esiste $\psi\colon B \to A$ tale

$$\psi \circ \varphi = id_A \quad \text{e} \quad \varphi \circ \psi = id_B$$

La funzione ψ e' detta **inversa** di φ. Si prova che se una funzione e' invertibile, l'inversa e' unica e viene denotata φ^{-1}.

Si ha la seguente caratterizzazione

Proposizione. *Una funzione $\varphi\colon A \to B$ e' invertibile se e solo se φ e' bigettiva.*

Se $\varphi\colon A \to B$ e' invertibile, allora l'inversa $\psi\colon B \to A$ e' definita da $\psi(b) = a$ dove a e' l'unica controimmagine di b.

3. Operazioni

Diamo ora la definizione di operazione in un insieme A.

Se A e' un insieme, un'*operazione n-aria* su A e' una funzione:

$$*: A^n \to A.$$

L'intero positivo n si dice arieta' dell'operazione. Se $n = 2$, l'operazione si dice binaria.

Su un insieme non vuoto A, definiamo operazione di arieta' zero il fissare un elemento di A.

Esempio. L'addizione tra numeri reali e' un'operazione binaria su $\mathbb{R}$, perche' e' la funzione $+: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ definita da $+(x, y) = x + y$ per ogni $(x, y) \in \mathbb{R}$.
Analogamente la moltiplicazione tra numeri reali e' un'operazione su $\mathbb{R}$ in quanto e' la funzione $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$ definita da $\cdot(x, y) = x \cdot y$.

Osserviamo invece che la divisione nei numeri reali non e' un'operazione in quanto e' definita da una funzione parziale.

Esempio. L'opposto di un intero e' un'operazione di arita' uno su $\mathbb{Z}$ in quanto e' la funzione $-: \mathbb{Z} \to \mathbb{Z}$ definita da $-(x) = -x$ per ogni $x \in \mathbb{Z}$.

Sia A un insieme, ricordiamo che l'*insieme delle parti* di A e' l'insieme i cui elementi sono i sottoinsiemi di A e si indica con $\mathcal{P}(A)$.

Esempio. L'intersezione (risp. l'unione) tra sottoinsiemi di A e' un' operazione su $\mathcal{P}(A)$. Basta infatti considerare la funzione $f: \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A)$ definita da $f((X, Y)) = X \cap Y$ (risp. $f((X, Y)) = X \cup Y$). Inoltre la complementazione di in sottoinsieme X di A, ossia $\mathcal{C}_A(X) = \{a \in A : a \notin X\}$ e' un'operazione di arieta' uno su $\mathcal{P}(A)$.

Esempio. Siano A un insieme e A^A l'insieme di tutte le funzioni da A in A. Date due funzioni $f, g \in A^A$, la funzione composta $f \circ g: A \to A$ e' ancora un elemento di A^A. Questo significa che la composizione di funzioni puo' essere vista come una funzione $\circ: A^A \times A^A \to A^A$ e quindi la composizione di funzioni e' un'operazione su A^A.

Sia $*$ un'operazione binaria su un insieme A. Scriveremo semplicemente $x * y$ invece della notazione funzionale $*(x, y)$. Diremo inoltre che

$*$ e' **commutativa** se $x * y = y * x$ per ogni $x, y \in A$.

$*$ e' **associativa** se $(x * y) * z = x * (y * z)$ per ogni $x, y, z \in A$.

u e' **elemento neutro** rispetto a $*$ se $x * u = u * x = x$ per ogni $x \in A$.

L'elemento neutro, se esiste, e' unico.

y e' l'**inverso** di x se $x * y = y * x = u$. Se esiste l'inverso di un elemento, esso e' unico. L'inverso di x viene usualmente denotato x^{-1}.

Sia A un insieme, osserviamo che la legge $f: A \to A$ definita da $f(x) = x^{-1}$ e' una funzione parziale.

Studieremo nel seguito insiemi dotati di operazioni, ossia *strutture algebriche*. Per il momento ricordiamo solo che la struttura algebrica significativa piu' semplice e' il *semigruppo* che e' un insieme dotato di un'operazione binaria associativa.

Esempio. Sia $A = \{1, 2, 3\}$ e siano $a, b \in A^A$ definiti da $a(1) = 1, a(2) = 3, a(3) = 2$, $b(1) = 2, b(2) = 1, b(3) = 3$. Si provi che nel semigruppo A^A con l'operazione $\circ$, si ha $(a \circ b)^2 \neq a^2 \circ b^2$.

Esempio. Siano $\mathbb{R}^* = \mathbb{R} - \{0\}$ e S il prodotto cartesiano $\mathbb{R}^* \times \mathbb{N}$. Si definisca un'operazione su S ponendo

$$(a, n)(b, m) = (ab^n, nm)$$

per ogni $(a, n), (b, m) \in S$. Si provi che S e' un semigruppo.

4. Connettivi logici e tavole di verità

Consideriamo altri esempi molto semplici di operazioni che realizzano modi con cui legare le frasi del linguaggio. A tale scopo introduciamo i **connettivi logici.**

Sia $\mathbb{B}$ l'insieme $\{T, F\}$: è comodo pensare a questi come ai "valori di verità" vero (*true*) e falso (*false*).

Un connettivo è formalmente un'operazione su $\mathbb{B}$.

Nel seguito, indichiamo con p, q elementi generici di $\mathbb{B}$. I connettivi di uso più frequente sono i seguenti:

• La *congiunzione*, detta anche *and logico*, connettivo binario che indichiamo con $\wedge$. Corrisponde a "p e q" e si scrive $p \wedge q$. La definizione della legge che definisce l'operazione è data mediante una **tavola di verità** (così detta in assonanza con le *tavole pitagoriche*, in uso nei tempi passati per le operazioni numeriche):

$\wedge$	F	T
F	F	F
T	F	T

• La *disgiunzione*, detta anche *or logico*, connettivo binario che indichiamo con $\vee$. Corrisponde a "p o q" e si scrive $p \vee q$. È definita dalla seguente tavola di verità:

$\vee$	F	T
F	F	T
T	T	T

• La *negazione*, detta anche *not logico*, connettivo unario che indichiamo con $\neg$. Corrisponde a " non p" e si scrive $\neg p$. Capita di trovare anche altre notazioni per la negazione, ad esempio il simbolo $\sim$. È definita dalla seguente tavola di verità:

$\neg$	
F	T
T	F

• L'*implicazione*, connettivo binario, che indichiamo con $\Rightarrow$. Corrisponde a "se p allora q" e si scrive $p \Rightarrow q$. Capita di trovare anche altre notazioni per l'implicazione, ad esempio il simbolo $\supset$ (scelta alquanto disgraziata, vista la facile confusione con il segno per le inclusioni!). È definita dalla seguente tavola di verità:

$\Rightarrow$	F	T
F	T	T
T	F	T

• La *doppia implicazione* (o equivalenza), connettivo binario, che indichiamo con $\Leftrightarrow$. Corrisponde a "p se e solo se q", "p esattamente quando q" e si scrive $p \Leftrightarrow q$. È definita dalla seguente tavola di verità:

$\Leftrightarrow$	F	T
F	T	F
T	F	T

Notiamo alcune proprietà delle tavole di verità precedenti:

(1) $p \wedge q$ vale T se e solo se sia p che q valgono T. (Perciò, implicitamente negli altri tre casi vale F.)

(2) $p \vee q$ vale F se e solo se sia p che q valgono F. (Perciò, implicitamente negli altri tre casi vale T.)

(3) $\neg p$ vale T se e solo se p non vale T.

(4) $p \Rightarrow q$ vale F se e solo se p vale T e q vale F. (Perciò, implicitamente negli altri tre casi vale T.)

(5) $p \Leftrightarrow q$ vale T se e solo se $p = q$. (Perciò, vale F se e solo se $p \neq q$.)

Ricordiamo ancora di non incorrere in errore nel valutare il connettivo "implicazione". Nel linguaggio naturale non è evidente quale valore di verità dare ad una frase del tipo "se p, allora q" quando p è falsa, in quanto siamo abituati ad attribuire a "se... allora..." un nesso di causalità. Nessun nesso di causalità va pensato nell'attribuire un valore alla proposizione $p \Rightarrow q$.

Usando i connettivi logici, si possono riscrivere le definizioni di unione e intersezione di sottoinsiemi. Sia A un insieme, X e Y in $\mathcal{P}(\mathcal{A})$

$$X \cap Y = \{a \in A : \ a \in X \wedge a \in Y\} \quad X \cup Y = \{a \in A : \ a \in X \vee a \in Y\}$$

Esercizio. Calcolare il valore di verità dell'espressione $(p \wedge q) \vee p$ al variare dei valori di p e q.

Lo studio dei connettivi ed il loro collegamento con i circuiti (detti appunto *logici*) usati nella costruzione dei calcolatori, verrà approfondito nel corso di Architettura.

Nelle seguenti proprieta' si usera' il simbolo di eguaglianza intendendo "stesso valore di verita' al variare dei valori di p e q."

Proprietà delle operazioni logiche

Commutatività $\quad p \wedge q = q \wedge p \qquad p \vee q = q \vee p$

Associatività $\quad (p \wedge q) \wedge r = p \wedge (q \wedge r) \qquad (p \vee q) \vee r = p \vee (q \vee r)$

Distributività $\quad p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r) \qquad p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$

Idempotenza $\quad p \wedge p = p \qquad p \vee p = p$

Assorbimento $\quad p \wedge (q \vee p) = p \qquad p \vee (q \wedge p) = p$

Leggi di De Morgan $\quad \neg(p \wedge q) = (\neg p) \vee (\neg q) \qquad \neg(p \vee q) = (\neg p) \wedge (\neg q)$

Interdefinibilià $\quad p \Rightarrow q = (\neg p) \vee q \qquad p \Leftrightarrow q = (p \Rightarrow q) \wedge (q \Rightarrow p)$

Passaggio alla contronominale $\quad p \Rightarrow q = (\neg q) \Rightarrow (\neg p)$

Legge del terzo escluso $\quad p \vee (\neg p) = T$

Riduzione ad assurdo $\quad \neg(\neg p) = p$

Osserviamo che l'ultima tautologia (stesso valore di verita') sta alla base delle dimostrazioni *per assurdo*:

> *"Supponiamo che p non sia vera* (cioè $\neg p$ è vera) e proviamo che non è vero che $\neg p$ è vera, in altre parole $\neg(\neg p)$ è vera. Ma $\neg(\neg p) = p$. *Dunque* (magicamente!) *abbiamo dimostrato che p è vera."*

Dalle proprietà precedenti, seguono molte altre uguaglianze. Ne segnaliamo alcune:

$$(p \Rightarrow p) = T \qquad ((p \wedge q) \Rightarrow p) = T \qquad (p \Rightarrow (p \vee q)) = T.$$

Esempio Dalle precedenti proprietà delle operazioni logiche, possiamo dedurre importanti proprietà dell'unione, intersezione e complementazione di sottoinsiemi. Sia A un insieme e siano X, Y, Z sottoinsiemi di A, allora :

a) $X \cup Y = Y \cup X$ e $X \cap Y = Y \cap X$

b) $(X \cap Y) \cap Z = X \cap (Y \cap Z)$,

c) $(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$,

d) $\mathcal{C}_A(X \cup Y) = \mathcal{C}_A(X) \cap \mathcal{C}_A(Y)$

e) $\mathcal{C}_A(X \cap Y) = \mathcal{C}_A(X) \cup \mathcal{C}_A(Y)$

f) $\mathcal{C}_A(\mathcal{C}_A(X)) = X$

5. Cardinalità di insiemi

Se A è un insieme finito, cioè se A contiene un numero finito di elementi, il numero di elementi di A è un numero naturale detto **cardinalità** di A e denotato con $|A|$ oppure con card$A$. In tal caso $|A| = 0$ se e solo se $A = \emptyset$, $|A| = n$ se e solo se A è in corrispondenza biunivoca con $\{1, 2, \ldots, n\}$.
Se A è un insieme finito e $B \subseteq A$, allora $|B| \leq |A|$.

Piu' in generale:

Definizione. Siano A e B insiemi qualunque (non necessariamente finiti), A e B si dicono **equipotenti** o che **hanno la stessa cardinalità** se esiste una funzione bigettiva tra A e B.

La definizione è in linea con il caso degli insiemi finiti precedentemente trattato,

dato che hanno lo stesso numero di elementi, diciamo n, esattamente quando sono ciascuno in bigezione con l'insieme $\{1, \ldots, n\}$.

Vediamo il comportamento della cardinalità nel caso di unione e intersezione di insiemi finiti.

Proposizione. Se A e B sono insiemi finiti e disgiunti ($A \cap B = \emptyset$), si ha

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

Se A e B sono insiemi finiti, dal precedente risultato si possono dedurre i seguenti fatti:

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

Usando tecniche di enumerazione, si prova che:

Proposizione. Se A e B sono insiemi finiti e B^A è l'insieme di tutte le funzioni di A in B, allora

$$|B^A| = |B|^{|A|}$$

Ricordiamo che se $|A| = n$, le funzioni bigettive $f: A \to A$ sono dette *permutazioni* e si prova che sono $n!$

Possiamo dare una semplice prova del seguente fatto

- Se A è un insieme finito, allora $|P(A)| = 2^{|A|}$

Tale eguaglianza puo' essere provata anche usando l'induzione matematica. Rimandiamo questo ad un momento successivo.

Riportiamo invece un'altra prova che si avvale di un fatto piu' generale.

Dato un qualunque insieme A, si costruisce una corrispondenza biunivoca

$$\sigma: P(A) \to \{T, F\}^A.$$

Infatti per ogni sottoinsieme S di A, si consideri la funzione $\chi_S: A \to \{T, F\}$ detta *funzione caratteristica* come segue:

$$\chi_S(a) = \begin{cases} F & \text{se } a \in C_A(S) \\ T & \text{se } a \in S. \end{cases}$$

Definiamo ora $\sigma: P(A) \to \{T,F\}^A$ ponendo $\sigma(S) = \chi_S$ per ogni S in $P(A)$. Si prova che σ e' bigettiva.
Se A e' finito segue quindi che $|P(A)| = |\{T,F\}^A| = 2^{|A|}$.

Vediamo di approfondire il concetto di equipotenza nel caso di insiemi infiniti.

Diremo che un insieme A è **numerabile** se e' finito oppure è equipotente all'insieme $\mathbb{N}$ dei numeri naturali. Scriveremo in tal caso $|A| = \aleph_0$.

Ad esempio $\mathbb{N}$ è numerabile: è sufficiente considerare come funzione bigettiva la funzione identica da $\mathbb{N}$ in $\mathbb{N}$.
Osserviamo anche che $\mathbb{N}^*$ è numerabile (si consideri la funzione $f: \mathbb{N} \to \mathbb{N}^*$ definta da $f(n) = n+1$). Si prova piu' in generale che:

Proposizione Ogni sottoinsieme S di un insieme numerabile A, e' numerabile.

Il caso non banale e' quando S e' infinito. Possiamo inoltre limitarci a provare che ogni sottoinsieme (infinito) di $\mathbb{N}$ e' in corrispondenza biunivoca con $\mathbb{N}$. In tal caso basta considerare la funzione bigettiva:

$$\varphi: \mathbb{N} \to S$$

definita da $\varphi(0) = minS, \quad \varphi(1) = min\{S - \{\varphi(0)\}\}, \quad \ldots, \quad \varphi(n+1) = \\ = min\{S - \{\varphi(0), \ldots \varphi(n)\}\}, \ldots .$

Abbiamo visto inoltre che $f: \mathbb{N} \longrightarrow \mathbb{Z}$ definita da

$$f(n) = \begin{cases} \frac{n}{2}, & \text{se } n \text{ è pari} \\ -\frac{n+1}{2} & \text{se } n \text{ è dispari.} \end{cases}$$

è bigettiva. Segue quindi che anche $\mathbb{Z}$ è numerabile.

Possiamo provare il seguente fatto:

Teorema. L'insieme $\mathbb{Q}$ dei numeri razionali è numerabile.

Teorema. (senza dimostrazione) L'insieme $\mathbb{R}$ dei numeri reali non è numerabile.

6. Ordinamenti

Sia A un insieme, una **relazione** in A e' una corrispondenza di A in A, ossia un qualunque sottoinsieme del prodotto cartesiano $A \times A$. Se $\mathcal{R}$ e' una relazione in A, ossia $\mathcal{R} \subseteq A \times A$ e $a, b \in A$, invece di scrivere $(a, b) \in \mathcal{R}$, scriveremo

$$a \ \mathcal{R} \ b$$

e diremo che a e' in relazione $\mathcal{R}$ con b.

Una relazione $\mathcal{R}$ in un insieme A si dice:

- *riflessiva* se per ogni $a \in A$ si ha $a \ \mathcal{R} \ a$.
- *simmetrica* se per ogni $a, b \in A$ da $a \ \mathcal{R} \ b$ segue $b \ \mathcal{R} \ a$.
- *antisimmetrica* se per ogni $a, b \in A$ da $a \ \mathcal{R} \ b$ e $b \ \mathcal{R} \ a$ segue che $a = b$.
- *transitiva* se per ogni $a, b, c \in A$ da $a \ \mathcal{R} \ b$ e $b \ \mathcal{R} \ c$ segue che $a \ \mathcal{R} \ c$.

Sia A un qualunque insieme, naturalmente la *relazione di eguaglianza* "=" soddisfa tutte le precedenti proprieta'.

Esempi. Consideriamo le seguenti relazioni:

1. In $\mathbb{N}^*$ consideriamo la relazione $\leq$, ossia $a \leq b$ se esiste $c \in \mathbb{N}$ tale $a + c = b$.

2. In $\mathbb{N}^*$ consideriamo la relazione $/$, ossia a/b se esiste $c \in \mathbb{N}$ tale $b = ac$.

3. In $\mathbb{N}$ consideriamo la relazione $\mathcal{R}$ definita da $a \ \mathcal{R} \ b$ se $a = 2b$.

4. Sia n un intero positivo. In $\mathbb{Z}$ consideriamo la relazione $\sim_n$ definita da $a \sim_n b$ se $a - b$ e' un multiplo di n.

Possiamo verificare che 1. e 2. non verificano la proprieta' simmetrica e verificano le altre proprieta', 3. non e' riflessiva, non e' simmetrica, non e' antisimmetrica e non e' transitiva, 4. e' riflessiva, e' simmetrica, non e' antisimmetrica ed e' transitiva.

Una relazione $\mathcal{R}$ su A che sia *riflessiva, antisimmetrica e transitiva*, si dice un **ordinamento parziale** su A.

In $\mathbb{N}^*$ le relazioni degli esempi 1. e 2. sono quindi ordinamenti parziali.

Un insieme A su cui e' definito un ordinamento parziale si dice *insieme parzialmente ordinato*.

Un ordinamento parziale $\mathcal{R}$ su A si dice un **ordinamento totale** se

$$\text{per ogni } a, b \in A, \text{ si ha } a \mathcal{R} b \text{ oppure } b \mathcal{R} a,$$

ossia se ogni coppia di elementi di A e' confrontabile. In tal caso l'insieme A si dice totalmente ordinato.

Osserviamo che nei precedenti esempi, $\mathbb{N}^*$ con $\leq$ e' totalmente ordinato, mentre $\mathbb{N}^*$ con / non e' un insieme totalmente ordinato (ad esempio 2 non divide 3 e 3 non divide 2).

Siano $(A, \mathcal{R})$ e $(B, \sim)$ insiemi parzialmente ordinati. Un *omomorfismo di insiemi ordinati* e' una funzione $f\colon A \to B$ tale che

$$a \mathcal{R} b \text{ implica } f(a) \sim f(b) \text{ per ogni } a, b \in A.$$

Esempio. Per ogni insieme A, l'insieme delle parti $\mathcal{P}(A)$ e' un insieme parzialmente ordinato dalla relazione di inclusione $\subseteq$. Siano ora $A \subseteq B$, se consideriamo la funzione $f\colon \mathcal{P}(B) \to \mathcal{P}(A)$ definita da $f(X) = A \cap X$ per ogni sottoinsieme X si B, si prova che f e' un omomorfismo di insiemi ordinati.

7. **Relazioni di equivalenza**

Sia $\mathcal{R}$ una relazione in A.
$\mathcal{R}$ si dice **relazione di equivalenza** se verifica le proprietà *riflessiva, simmetrica e transitiva.*

Una relazione di equivalenza si indica di solito con $\sim$ oppure $\equiv$.

Sia $\sim$ è una relazione di equivalenza e $x, y \in A$, diremo che x è equivalente a y se $x \sim y$.

Esempi.

1. Sia A un insieme. La relazione definita da $x \sim y$ se $x = y$ e' una relazione di equivalenza detta eguaglianza.
2. In $\mathbb{N}$ la relazione $m \sim n$ se $m + n$ è pari, è una relazione di equivalenza.
3. Fissato un intero positivo n, sia data in $\mathbb{Z}$ la relazione $x \sim_n y$ se $x - y$ è un multiplo intero di n. Si verifica che $\sim_n$ è una relazione di equivalenza.
4. Sia $f\colon A \to B$ una funzione, definiamo su A la seguente relazione:
   $x \sim_f y$ se $f(x) = f(y)$. Si ha che $\sim_f$ è una relazione di equivalenza e si dice *relazione di equivalenza associata a* f.

Sia ora $\sim$ una relazione di equivalenza in un insieme A e sia a un elemento di A. Indichiamo con $\overline{a}$ [1] l'insieme degli elementi di A equivalenti ad a:

$$\overline{a} = \{x \in A \mid x \sim a\}$$

$\overline{a}$ si dice **classe di equivalenza** di a modulo $\sim$.
In particolare $a \in \overline{a}$, quindi $\overline{a} \neq \emptyset$.

Si osservi che $\overline{a}$ è anche la classe di equivalenza individuata da un qualsiasi elemento b equivalente ad a, cioe'

$$\overline{a} = \overline{b} \Longleftrightarrow a \sim b.$$

Si prova inoltre due distinte classi di equivalenza sono sempre disgiunte, ossia

$$\overline{a} \cap \overline{b} \neq \emptyset \Longleftrightarrow \overline{a} = \overline{b}.$$

L'insieme di tutte le classi di equivalenza si dice **insieme quoziente** di A modulo $\sim$ e si indica con $A/\sim$.

Sia $\sim_n$ la relazione di equivalenza definita nell'esempio 3., si verifica che $\overline{x} = \overline{y}$ se il resto della divisione di x per n e' uguale al resto della divisione di y per n. L'insieme $\mathbb{Z}/\sim_n$ e'detto insieme delle classi di resto modulo n e denotato con $\mathbb{Z}_n$. In particolare

$$\mathbb{Z}_n = \{\overline{0}, \ldots, \overline{n-1}\}.$$

La funzione (surgettiva) $\pi\colon A \to A/\sim$ che associa ad ogni elemento di A la sua classe di equivalenza si dice **proiezione canonica**.

Osserviamo che l'insieme quoziente $A/\sim$ è una partizione di A [2], più precisamente la partizione di A nelle classi di equivalenza modulo $\sim$, cioè ad ogni equivalenza $\sim$ è associata, in modo naturale, la partizione $A/\sim = \cup_{a\in A}\overline{a}$.

Viceversa, data una partizione $\mathcal{A}$ di A, si può associare ad $\mathcal{A}$ una equivalenza in A. Sia $\mathcal{A} = \{A_i\}_{i\in I}$ una partizione di A. Associamo ad $\mathcal{A}$ la seguente relazione:

$$x \sim y \Longleftrightarrow \exists\ j \in I \text{ tale che } x, y \in A_j.$$

Usando gli insiemi quoziente possiamo caratterizzare formalmente $\mathbb{Z}$ e $\mathbb{Q}$ a partire da $\mathbb{N}$.

---

[1] la classe di equivalenza di a si indica anche $[a]$ oppure $\overline{\overline{a}}$.

[2] una famiglia $\mathcal{A}$ di sottoinsiemi non vuoti di A si dice partizione di A se i sottoinsiemi sono a due a due disgiunti e se la loro unione è tutto A.

Definiamo nell'insieme $\mathbb{N} \times \mathbb{N}$ la seguente relazione di equivalenza :

$$(m, n) \sim (m', n') \text{ se e solo se } m + n' = n + m'.$$

Si prova che $\mathbb{Z} \simeq \mathbb{N} \times \mathbb{N}/\sim$ considerando $f: \mathbb{N} \times \mathbb{N}/\sim \to \mathbb{Z}$ definita da $f(m, n) = m - n$.

Definiamo ora nell'insieme $\mathbb{Z} \times \mathbb{Z}^*$ la seguente relazione di equivalenza :

$$(m, n) \sim (m', n') \text{ se e solo se } m \cdot n' = n \cdot m'.$$

Si prova che $\mathbb{Q} \simeq \mathbb{Z} \times \mathbb{Z}^*/\sim$ considerando $f: \mathbb{Z} \times \mathbb{Z}^*/\sim \to \mathbb{Q}$ definita da $f(m, n) = m/n$.

GLI INTERI

1. Principio di induzione.

Tale principio che si basa su una delle proprieta' fondamentali dei numeri naturali e fornisce un metodo di dimostrazione per provare che una proprieta' $\mathcal{P}$ e' vera per tutti i numeri naturali $n \in \mathbb{N}$.

Principio di induzione. Sia $P \subseteq \mathbb{N}$ un insieme di numeri naturali. Se valgono le seguenti proprietà:
base: $0 \in P$
passo induttivo: se $m \in P$, allora $m+1 \in P$,
allora $P = \mathbb{N}$.

In altre parole, per ogni numero naturale n si ha che $n \in P$.

La dimostrazione per induzione si basera' sulla seguente formulazione:

Principio di induzione. *Sia $n_0 \in \mathbb{Z}$ e sia $\mathcal{P}$ una affermazione sui numeri interi $n \geq n_0$. Supponiamo siano soddisfatte le seguenti due condizioni:*

i) *$\mathcal{P}$ è vera per il numero n_0;*
ii) *per ogni intero $m \geq n_0$ se $\mathcal{P}$ è vera per il numero m, allora $\mathcal{P}$ è vera per il numero $m+1$.*

Allora $\mathcal{P}$ è vera per ogni numero intero $n \geq n_0$.

Esempi:

1. Proviamo che per ogni numero reale q, $q \neq 1$ la somma delle sue prime n potenze $(n = 0, 1 \ldots)$

$$\sum_{i=0}^{n} q^i = 1 + q + q^2 + \ldots + q^n = \frac{1 - q^{n+1}}{1 - q}$$

L'affermazione è banalmente vera per $n = 0$, supponiamola vera per un qualsiasi intero $m \geq 0$ cioè

$$1 + q + q^2 + \ldots + q^m = \frac{1 - q^{m+1}}{1 - q}$$

e proviamola per $m+1$, ovvero aggiungiamo ai due membri dell'uguaglianza q^{m+1}, avremo che

$$1 + q + q^2 + \ldots + q^m + q^{m+1} = \frac{1 - q^{m+1}}{1 - q} + q^{m+1} = \frac{1 - q^{m+1} + q^{m+1} - q^{m+2}}{1 - q}$$

da cui la tesi.

2. Proviamo che per ogni numero intero $n \geq 2$ si ha

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\ldots\left(1-\frac{1}{n}\right)=\frac{1}{n}$$

L'affermazione è vera per $n = 2$, infatti $1 - \frac{1}{2} = \frac{1}{2}$. Supponiamola vera per un qualsiasi intero $m \geq 2$ cioè

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\ldots\left(1-\frac{1}{m}\right)=\frac{1}{m}$$

Moltiplicando ambo i membri dell'uguaglianza per $1 - \frac{1}{m+1}$ si ottiene la tesi.

3. Denotiamo $0! = 1, n! = 1 \cdot 2 \cdot \cdots \cdot n$ per $n > 0$.

Provare per induzione il **Teorema binomiale**:

Sia n un qualunque intero ≥ 1, si ha:

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \ldots + \binom{n}{r}x^{n-r}y^r + \ldots + \binom{n}{n-1}xy^{n-1} + y^n$$

dove

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

Si puo' provare che il Principio di induzione e' equivalente al Principio del buon ordinamento o del minimo.

Principio del minimo. Sia $\emptyset \neq X \subseteq \mathbb{N}$ un insieme non vuoto di numeri naturali. Esiste il minimo di X, cioè un numero m tale che

- $m \in X$, e
- se $n \in X$, allora $n \geq m$.

2. Algoritmo Euclideo

La proprietà fondamentale di $\mathbb{Z}$ alla base della nostra trattazione è il

Teorema di divisione. *Dati due interi $a > 0$ e $b \geq 0$, sono unicamente determinati due interi $q \geq 0$ e $r, 0 \leq r < a$, tali che $b = qa + r$.*

Dati due interi a e b, diremo che a **divide** b se $b = aq$ per qualche intero q e scriveremo a/b.
Se a e b sono interi, un **divisore comune** di a e b è un intero e che divide sia a che b.

Un intero d è un **massimo comun divisore** (MCD) di due interi a e b se:
i) d/a e d/b;
ii) se p è un divisore comune di a e b allora p divide d.

Osserviamo che se $a, b \in \mathbb{Z}$, se d e' un massimo comun divisore di a e b, allora anche $-d$ e' un massimo comun divisore. Nel seguito quando scriveremo "il massimo comun divisore" indicheremo il valore positivo.

Infine a e b si dicono *coprimi* se il loro MCD è 1. Se non c'e' ambiguita' il massimo comun divisore di a e b si denota con (a, b).

La soluzione del problema di trovare il massimo comun divisore di due numeri è stata data da Euclide (300 a.c. circa).

Enunciamo l' **Algoritmo di Euclide.**

Dati due numeri naturali a, b con $a \neq 0$, si considerino le seguenti divisioni successive:

$$\begin{gathered} b = aq + r_o \text{ (dividendo } b \text{ per } a) \\ a = r_o q_o + r_1 \text{ (dividendo } a \text{ per } r_o) \\ r_o = r_1 q_1 + r_2 \text{ (dividendo } r_o \text{ per } r_1) \\ r_1 = r_2 q_2 + r_3 \\ \cdots \\ \cdots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n \\ r_{n-1} = r_n q_n + 0 \end{gathered}$$

Allora:
a) la successione termina dopo un numero finito di passi (esiste n tale $r_{n+1} = 0$. In particolare $n < a$).
b) r_n (ultimo resto non nullo) è il massimo comun divisore di a e b.

3. Massimo comun divisore.

Abbiamo osservato che l'ultimo resto diverso da 0 nell'algoritmo euclideo applicato ad a e b ne è il massimo comun divisore. Quindi trovare il massimo comun divisore è un processo computazionale effettivo. L'algoritmo euclideo ha inoltre la seguente conseguenza:

Identità di Bezout. *Se d è il massimo comun divisore di a e b, allora $d = ax + by$ per opportuni interi x e y.*

Vediamo per esempio come si procede per determinare x e y nel caso in cui a e b siano 365 e 1876.

E' facile scoprire che $d = 1$ cioè che i due numeri sono coprimi * .

Usiamo l'algoritmo euclideo:

$$1876 = 365 \cdot 5 + 51$$
$$365 = 51 \cdot 7 + 8$$
$$51 = 8 \cdot 6 + 3$$
$$8 = 3 \cdot 2 + 2$$
$$3 = 2 \cdot 1 + 1$$

quindi 1 è il massimo comun divisore.

Ricaviamo i resti dalle equazioni precedenti (cioè rileggiamo da destra verso sinistra le equazioni) e avremo:

$$1 = 3 - 2 \cdot 1$$
$$2 = 8 - 3 \cdot 2$$
$$3 = 51 - 8 \cdot 6$$
$$8 = 365 - 51 \cdot 7$$
$$51 = 1876 - 365 \cdot 5$$

e sostituiamo successivamente i resti nell'equazione $1 = 3 - 2 \cdot 1$ partendo da 2 avremo:

$$1 = 3 - 2 \cdot 1$$
$$1 = 3 - (8 - 3 \cdot 2) = 3 \cdot 3 - 8$$
$$1 = 3(51 - 8 \cdot 6) - 8 = 3 \cdot 51 - 8 \cdot 19$$
$$1 = 3(51 - 19(365 - 51 \cdot 7) = 136 \cdot 51 - 19 \cdot 365$$
$$1 = 136(1876 - 5 \cdot 365) - 19 \cdot 365 = 136 \cdot 1876 - 699 \cdot 365$$

Quindi $x = -699$, $y = 136$.

Possiamo quindi enunciare il seguente :

Teorema. *Se r_n è l'ultimo resto non nullo dell'algoritmo euclideo per a e b, allora r_n è il massimo comun divisore di a e b, e $r_n = ax + by$ per opportuni x e y .*

4. Fattorizzazione degli interi.

Un numero naturale $p > 1$ è **primo** se l'unico divisore di p maggiore di 1 è p stesso ed ogni numero naturale è primo o prodotto di primi.

Il *teorema fondamentale dell'aritmetica* asserisce che la fattorizzazione di un

* $365 = 5 \cdot 73$ e nè 5 nè 73 dividono 1876

numero naturale come prodotto di primi è "essenzialmente" unica .

Sia $a \in \mathbb{N}$, se $a = p_1 \dots p_n = q_1 \dots q_m$ sono fattorizzazioni di a come prodotto di primi, diciamo che le due fattorizzazioni sono uguali se l'insieme dei p_i coincide con l'insieme dei q_j (ripetizioni comprese), cioè $m = n$ ed ogni primo compare lo stesso numero di volte tra i p_i e i q_j.**

Teorema. *Ogni numero naturale $n \geq 2$ si fattorizza in modo unico come prodotto di primi.*

5. Congruenze

Proposizione. *Siano $a, b, c \in \mathbb{Z}$. L'equazione*

$$ax + by = c$$

ha soluzioni intere se e solo se c e' un multiplo di $MCD(a, b)$.

Sia infatti $d = MCD(a, b)$, chiaramente d divide a e divide b, quindi se $ax + by = c$ per qualche $x, y \in \mathbb{Z}$, allora d divde c. Viceversa se $c = kd$ per qualche $k \in \mathbb{Z}$, per l'identita' di Bezout esistono α e $\beta \in \mathbb{Z}$, tali che

$$c = kd = k(a\alpha + b\beta).$$

Quindi $x = k\alpha$ e $y = k\beta$ e' soluzione intera dell'equazione.

Osservazione. Nella proposizione precedente osserviamo che se c e' un multiplo di $d = MCD(a, b)$ (sia $c = kd$), sono soluzioni intere dell'equazione $ax + by = c$ tutte le coppie

$$x = k\alpha + bh \qquad y = k\beta - ah \quad \forall\ h \in \mathbb{Z}.$$

Usando i fatti precedenti possiamo definire un'aritmetica in $\mathbb{Z}_n = \mathbb{Z}/\sim_n$. Ricordiamo che per ogni $a, b \in \mathbb{Z}$, si ha $\overline{a} = \overline{b}$ se e solo se $a \equiv b \pmod{n}$ se e solo se $a - b$ e' un multiplo di n. In particolare $\overline{a} = \overline{0}$ se e solo se n divide a.

Possiamo definire in $\mathbb{Z}_n$ la somma e il prodotto di due classi rispettivamente come la classe della somma e del prodotto e vedremo nel seguito del corso che tali operazioni defiscono su tale insieme una ben definita struttura algebrica. Quindi per ogni $a, b \in \mathbb{Z}$, $+$ e $\cdot$ cosi' definite:

$$\overline{a} + \overline{b} = \overline{a + b}$$

** $2 \cdot 2 \cdot 3 \cdot 5$ è la stessa fattorizzazione di $2 \cdot 5 \cdot 3 \cdot 2$

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

sono operazioni binarie in $\mathbb{Z}_n$ in quanto definiscono delle funzioni da $\mathbb{Z}_n \times \mathbb{Z}_n$ in $\mathbb{Z}_n$.

L'elemento neutro rispetto alla somma e' $\overline{0}$ e l'elemento neutro rispetto al prodotto e' $\overline{1}$. Diremo che $\overline{a}$ e' invertibile in $\mathbb{Z}_n$ se esiste $b \in \mathbb{Z}$ tale $\overline{a} \cdot \overline{b} = \overline{1}$.

Usando la precedente proposizione si prova facilmente:

Corollario. Sia p un numero primo. In $\mathbb{Z}_p$ ogni elemento $\neq \overline{0}$ e' invertibile (rispetto all'operazione $\cdot$).

In generale non e' vero che in $\mathbb{Z}_n$ ogni elemento non nullo e' invertibile.

Esercizio. Determinare gli elementi invertibili di $\mathbb{Z}_{12}$.

In generale si prova che

Teorema. *$\overline{a}$ é un elemento invertibile in $\mathbb{Z}_n$ se e solo se $MCD(a, n) = 1$*

Infatti se $\overline{a}$ é invertibile allora esiste $b \in \mathbb{Z}$ tale che $\overline{a} \cdot \overline{b} = \overline{1}$, quindi in $\mathbb{Z}$ esiste k tale che $a \cdot b = kn + 1$ e di conseguenza $1 = MCD(a, n)$.
Viceversa se $MCD(a, n) = 1$ per l'identitá di Bezout esistono b e k tali che $ab+kn = 1$ e quindi, passando in $\mathbb{Z}_n$ si ha la tesi.

Vediamo una proprietá di $\mathbb{Z}_p$ quando p é un numero primo

Teorema di Fermat: *Sia p un numero primo e sia a un intero non divisibile per p, alllora*

$$a^{p-1} \equiv 1 \pmod{p}$$

(da provare quindi che in $\mathbb{Z}$ esiste un intero k tale che $a^{p-1} = 1 + kp$)

6. Alcune applicazioni dell'algoritmo euclideo

• **Prova del** 9.
Calcolo (a mano) $187 \cdot 21$ e ottengo 3827. Sarà giusto?
Applico la prova del 9:

sommo (ripetutamente) le cifre di 187 e le cifre di 21

$$1+8+7=16 \qquad 1+6=7 \qquad \text{e} \qquad 2+1=3$$

ora moltiplico 7 e 3 (e sommo le cifre) e confronto il risultato con la somma (ripetuta) delle cifre di 3827

$$7\cdot 3=21 \qquad 2+1=3 \qquad \text{e} \qquad 3+8+2+7=20 \qquad 2+0=2$$

Poiche' i risultati sono diversi, allora ho sbagliato! Il risultato giusto è infatti

$$3927 \text{ e } \quad 3+9+2+7=21 \quad 2+1=3$$

Perché questo metodo funziona?
Proviamo a calcolare $187 \cdot 21$ in $\mathbb{Z}_9$:
$\overline{187} = \overline{1\cdot 10^2+8\cdot 10+7} =$ (per la definizione di somma e la sua associatività) $\overline{1\cdot 10\cdot 10}+\overline{8\cdot 10}+\overline{7}=\overline{1}\cdot\overline{10}^2+\overline{8}\cdot\overline{10}+\overline{7}=$ (perché $\overline{10}=\overline{1}$ e $\overline{1}$ è elemento neutro per il prodotto) $\overline{1}+\overline{8}+\overline{7}=\overline{1+8+7}=\overline{16}=\overline{1\cdot 10+6}=$ (per tutte le proprietà che abbiamo usato prima) $\overline{1}+\overline{6}=\overline{7}$.
Analogamente abbiamo che $\overline{21}=\overline{3}$ e $\overline{3927}=3$. Per la definizione di prodotto dobbiamo avere

$$\overline{187}\cdot\overline{21}=\overline{3927}!!!!$$

Come possiamo capire, la prova del 9 non e' un metodo sicuro in quanto permette errori che differiscono dal risultato esatto per multipli di 9.

Esercizio. Descrivere la "prova dell'11" (usando $\mathbb{Z}_{11}$).

• **Divisibilita' per** 11.
Per provare che un numero è divisibile per 11 basta fare la somma a segni alterni delle sue cifre e controlare che il risultato sia divisibile per 11. Ad esempio

$$3927: \qquad 3-9+2-7=-11 \qquad \text{quindi è divisibile per 11}$$

Perchè funziona? Facciamo i conti in $\mathbb{Z}_{11}$:
abbiamo che 3927 è divisibile per 11 se e solo se $\overline{3927}=\overline{0}$.

$$\overline{3}\cdot\overline{(10)^3}+\overline{9}\cdot\overline{(10)^2}+\overline{2}\cdot\overline{10}+\overline{7}=\overline{3}\cdot\overline{(-1)^3}+\overline{9}\cdot\overline{(-1)^2}+\overline{2}\cdot\overline{-1}+\overline{7}=\overline{-3+9-2+7}=\overline{11}=\overline{0}$$

Esercizio. Descrivere i criteri di divisibilità per 3 e 9.

• **Potenze.**
Qual è l'ultima cifra di 7^{126}?

Se abbiamo tempo da perdere o un buon programma di calcolo, possiamo fare

3036358463668595297776148330084231776188483096234283571221425112421198602904695917662770534548 23

Ma possiamo rispondere alla domanda molto più facilmente. L'ultima cifra di un numero è il resto della divisione per 10, quindi è il suo rappresentante canonico in $\mathbb{Z}_{10}$ (cioè quello compreso tra 0 e 9). Quindi calcoliamo il rappresentante canonico di $\overline{7^{126}}$.

$$\overline{7^{126}} = \overline{(7^2)^{63}} = \overline{49)^{63}} = \overline{(-1)^{63}} = \overline{(-1)^{63}} = \overline{(-1)} = \overline{9}$$

L'ultima cifra e' quindi 9.

Esercizio. Quanto vale 7^{122} in $\mathbb{Z}_{12}$? in $\mathbb{Z}_{15}$?

• **Numeri in base** a.
Sia $b = MCCXXXIV$. Lo scriviamo come $b = 1234$ che significa

$$b = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4$$

$(1234)_{10}$ è la rappresentazione di b in base 10.

In generale, se $a \geq 2$ *e* $b = r_n \cdot a^n + r_{n-1} \cdot a^{n-1} + \ldots + r_1 \cdot a + r_0$ *con* $0 \leq r_i < a$ *per ogni* $i = 0, \ldots, n-1$ *e* $0 < r_n < a$*, allora la scrittura*

$$(r_n r_{n-1} \ldots r_0)_a$$

si dice **rappresentazione di** b **in base** a.

Esempio.
i) *Base 2*:
$1234 = 1 \cdot 2^{10} + 0 \cdot 2^9 + 0 \cdot 2^8 + 1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 0 =$
$1024 + 128 + 64 + 16 + 2$. Quindi

$$(1234)_{10} = (10011010010)_2$$

ii) *Base 16* :
$1234 = 4 \cdot 16^2 + 13 \cdot 16 + 2$. In questo caso la scrittura $(4132)_{16}$ è ovviamente ambigua quindi scriviamo $(4, 13, 2)_{16}$ oppure associamo a ogni numero tra 0 e 15 una "cifra"

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

quindi $(1234)_{10} = (4D2)_{16}$. I calcolatori indicano la rappresentazione esadecimale con il prefisso "$0x$", quindi per esempio un indirizzo di memoria verrà scritto $0x4D2$

Dati $a \geq 2$ *e* $b \geq 0$ *esiste la rappresentazione di* b *in base* a*?* E' unica? (Se esiste) Come si calcola?

Usando la divisione euclidea, si dimostra per induzione il seguente risultato.

Teorema. *Fissato $a \geq 2$, possiamo rappresentare ogni intero positivo b in base a, cioè possiamo scrivere b in maniera unica come*

$$(r_n r_{n-1} \dots r_0)_a$$

dove $b = r_n \cdot a^n + r_{n-1} \cdot a^{n-1} + \ldots + r_1 \cdot a + r_0$ con $0 \leq r_i < a$ per ogni $i = 0, \dots, n-1$ e $0 < r_n < a$.

Per induzione su b:

1) Se $0 \leq b < a$ allora la rappresentazione è $(b)_a$.

2) Sia $b \geq a$ e sia vero per ogni $r \in \mathbb{N}$, $r < b$. Mostriamo che è vero anche per b: per il teorema di divisione possiamo sempre scrivere $b = q \cdot a + r$ con $q \in \mathbb{N}$ e $0 \leq r < a$, univocamente determinati.
Notiamo che $q < b$, altrimenti, se $q \geq b$, avremmo $qa + r \geq 2q + r > b$ (assurdo).
Allora, per l'ipotesi induttiva, il teorema vale per q (che è positivo perché $b \geq a$), cioè possiamo scrivere

$$q = r_n \cdot a^n + r_{n-1} \cdot a^{n-1} + \ldots + r_1 \cdot a + r_0$$

con $0 \leq r_i < a$ per ogni $i = 0, \dots, n-1$ e $0 < r_n < a$.

Mettiamo insieme le due formule e otteniamo

$$\begin{aligned} b &= (r_n \cdot a^n + r_{n-1} \cdot a^{n-1} + \ldots + r_1 \cdot a + r_0)a + r \\ &= r_n \cdot a^{n+1} + r_{n-1} \cdot a^n + \ldots + r_1 \cdot a^2 + r_0 \cdot a + r \end{aligned}$$

con $0 \leq r < a$, $0 \leq r_i < a$ per ogni $i = 0, \dots, n-1$ e $0 < r_n < a$.

Oltre a dimostrare l'esistenza e unicità della rappresentazione in base a, abbiamo anche mostrato un algoritmo per calcolarla:

$$\begin{aligned} b &= a \cdot q_0 + r_0 \text{ con } q_0 \in \mathbb{N} \text{ e } 0 \leq r_0 < a \\ q_0 &= a \cdot q_1 + r_1 \text{ con } q_1 \in \mathbb{N} \text{ e } 0 \leq r_1 < a \\ q_1 &= a \cdot q_2 + r_2 \text{ con } q_2 \in \mathbb{N} \text{ e } 0 \leq r_2 < a \\ \dots &= \dots \end{aligned}$$

fino a quando $q_{n-1} < a$. Quindi definiamo $r_n := q_{n-1}$ e scriviamo

$$b = (r_n r_{n-1} \dots r_1 r_0)$$

Esempio. Scrivere 1234 in base 8

$$1234 = 8 \cdot 154 + 2$$

$$154 = 8 \cdot 19 + 2$$

$$19 = 8 \cdot 2 + 3$$

$$2 = 8 \cdot 0 + 2.$$

Allora $(1234)_{10} = (2322)_8$ (i calcolatori indicano i numeri ottali preceduti da "0", cioè 02322).

- **Espansione decimale di una frazione.**

Ad esempio l'espansione decimale di 1/7 in base 10 non e' finita : $0.142\ldots$ ed e' data dall'usuale divisione.

Analizziamo le operazioni: ogni volta che vogliamo calcolare una nuova cifra decimale, moltiplichiamo il resto precedente per 10 (la nostra base). In generale, per calcolare l'espansione di b/c in base a:

$$b = c \cdot q_0 + r_0 \text{ dove } q_0 \in \mathbb{N} \text{ è la "parte intera"}$$

$$r_0 a = c \cdot q_1 + r_1 \text{ con } 0 \leq q_1 < a \text{ e } 0 \leq r_1 < c$$

$$r_1 a = c \cdot q_2 + r_2 \text{ con } 0 \leq q_2 < a \text{ e } 0 \leq r_2 < c$$

$$r_2 a = \ldots$$

per un numero di passi pari al numero di cifre che desidero dopo la virgola. Osserviamo che

$$b/c = q_0 + r_0/c$$

$$r_0/c = \tfrac{c \cdot q_1 + r_1}{ac} = q_1/a + r_1/(ac)$$

$$r_1/(ac) = \tfrac{c \cdot q_2 + r_2}{a^2 c} = q_2/a^2 + r_2/(a^2 c)$$

$\ldots\ldots$

Quindi

$$b/c = q_0 + q_1/a + q_2/a^2 + \ldots$$

e scriviamo

$$b = q + (.q_1 q_2 \ldots)_a$$

Esercizio. Scrivere $1/31$ in base 2.

$1 = 31 \cdot 0 + 1$
$1 \cdot 2 = 31 \cdot 0 + 2$
$2 \cdot 2 = 31 \cdot 0 + 4$
$4 \cdot 2 = 31 \cdot 0 + 8$
$8 \cdot 2 = 31 \cdot 0 + 16$
$16 \cdot 2 = 31 \cdot 1 + 1$
$1 \cdot 2 = 31 \cdot 0 + 2$
$2 \cdot 2 = \ldots$ si ripete la sequenza all'infinito

Quindi scriviamo

$$1/31 = (0.000010000100001 \ldots)_a$$

Si puo' dimostrate (per induzione) che, in qualunque base, una frazione ha una espansione finita o periodica.