Matematica Discreta (II modulo)

Domenico Luminati

a.a. 1999/2000

Questo è il diario "in tempo reale" del corso, corredato da brevi note delle lezioni. Alla fine del corso servirà come programma d'esame. Non vuole sostitutire i libri di testo, che restano quelli indicati nel programma del corso, ma soltanto una traccia da seguire per la preparazione dell'esame.

Programma svolto a lezione

Lezione 1 (26 febbraio 2001 h. 9.30-10.30) **1**
- Insiemi e operazioni tra insiemi . . . 1
- Relazioni, funzioni parziali e funzioni totali . . . 3

Lezione 2 (28 febbraio 2001 h. 10.30-11.30) **5**
- Equipotenza di insiemi . . . 5
- I numeri naturali: gli assiomi di Peano . . . 6
- Il principio di induzione (prima forma) . . . 6
- Il teorema di ricorsione . . . 6

Lezione 3 (5 marzo 2001 h. 9.30-10.30) **7**
- Le operazioni sui naturali . . . 7
- L'ordinamento dei naturali . . . 8
- Insiemi ordinati . . . 8
- L'ordinamento dei naturali e le operazioni . . . 9
- Insiemi finiti: il Lemma dei cassetti . . . 9

Lezione 4 (7 marzo 2001 h. 10.30-11.30) **10**
- Cardinalità degli insiemi finiti . . . 10
- Sottinsiemi di un insieme finito . . . 10

Lezione 5 (12 marzo 2001 h. 9.30-10.30) **11**
- Insiemi infiniti: l'assioma della scelta . . . 11

Lezione 6 (14 marzo 2001 h. 10.30-11.30) **13**
- Insiemi numerabili . . . 13
- Confronto di cardinalità: il Teorema di Cantor-Bernstein . . . 14
- La tricotomia dei cardinali . . . 15
- Il procedimento diagonale di Cantor . . . 16

Lezione 7 (19 marzo 2001 h. 9.30-10.30 **17**
- Operazioni tra cardinalità . . . 17
- L'assioma di buon ordinamento . . . 18
- Il principio di induzione (seconda forma) . . . 18
- La divisione euclidea . . . 18

Lezione 8 (21 marzo 2001 h. 10.30-11.30) **19**
- Scrittura in base arbitraria dei naturali. . . . 19
- Il coefficiente binomiale . . . 20
- k-sottinsiemi . . . 20
- Perché non gioco al Superenalotto! . . . 21

Lezione 9 (26 marzo 2001 h. 9.30-10.30) **21**
- Divisibilità e sue prime proprietà . . . 21
- Il massimo comun divisore: definizione, esistenza e unicità . . . 22
- L'algoritmo di Euclide per il calcolo del M.C.D. . . . 23

Lezione 10 (28 marzo 2001 h. 10.30-11.30) **23**
- Proprietà dei numeri coprimi e caratterizzazione dei numeri primi . . . 23
- Il minimo comune multiplo: definizione, esistenza e unicità . . . 24
- Il teorema fondamentale dell'Aritmetica . . . 24
- Esistenza di infiniti numeri primi . . . 25

Lezione 11 (29 marzo 2001 h. 10.30-11.30) **25**
- Definizione di congruenza e prime proprietà . . . 25
- Classi d'equivalenza . . . 26
- Classi di congruenza . . . 26
- Le classi modulo n sono esattamente n . . . 27
- Somma e prodotto di classi di congruenza . . . 27

Lezione 12 (2 aprile 2001 h. 9.30-10.30) **28**
- Il teorema cinese del resto . . . 28
- Elementi invertibili modulo n . . . 29

Lezione 13 (3 aprile 2001 h. 16.30-17.30) **30**
- Equazioni lineari modulo n . . . 30
- Il piccolo teorema di Fermat . . . 31
- Crittografia RSA . . . 31

Lezione 14 (2 maggio 2001 h. 10.30-12.30) **32**
- Definizione di grafo . . . 32
- Alcuni grafi notevoli . . . 34
- Sottografi e sottografi indotti . . . 35
- Morfismi ed isomorfismo di grafi . . . 35

Lezione 15 (7 maggio 2001 h. 9.30-10.30) **37**
- Una stima del numero di grafi non isomorfi su n vertici . . . 37
- Passeggiate, cammini e cicli . . . 37
- La relazione di essere congiungibili . . . 38

Lezione 16 (9 maggio 2001 h. 10.30-11.30) **38**
- Componenti connesse di un grafo . . . 38
- Le componenti connesse sono invarianti per isomorfismo . . . 38
- Grafi connessi . . . 39
- La matrice di incidenza di un grafo finito . . . 39

Lezione 17 (14 maggio 2001 h. 9.30-10.30) **39**
- Grado di un vertice . . . 39
- Il lemma delle strette di mano . . . 39
- Score di un grafo . . . 40
- Teorema dello score . . . 40

Lezione 18 (16 maggio 2001 h. 10.30-11.30) **40**
- Definizione di grafo euleriano . . . 40
- Caratterizzazione dei grafi euleriani . . . 40
- Definizione di grafo hamiltoniano . . . 40
- Grafo duale di un grafo dato . . . 40
- G è connesso allora anche il suo duale lo è . . . 40
- Se G è euleriano allora il suo duale è hamiltoniano . . . 40

Lezione 19 (21 maggio 2001 h. 9.30-10.30) **40**
- Alcune costruzioni con i grafi . . . 40
- Definizione di grafo 2-connessi . . . 40
- Prima caratterizzazione dei grafi 2-connessi . . . 40
- Seconda caratterizzazione dei grafi 2-connessi . . . 40

Lezione 20 (23 maggio 2001 h. 10.30-11.30) **41**
- Alberi . . . 41
- Il teorema di caratterizzazione degli alberi . . . 41
- Il teorema di caratterizzazione degli alberi finiti . . . 43

Lezione 21 (28 maggio 2001 h. 9.30-10.30) **44**
- Albero di copertura . . . 44
- Alberi radicati . . . 44
- La relazione $\rightarrow$ di "paternità" in un albero radicato . . . 44

Lezione 22 (30 maggio 2001 h. 10.30-11.30) **45**
- L'ordinamento degli alberi radicati . . . 45
- Induzione sugli alberi radicati . . . 46
- Il lemma di König . . . 46

Soluzione di alcuni degli esercizi proposti **48**

Lezione 1 (26 febbraio 2001 h. 9.30-10.30)

Insiemi e operazioni tra insiemi

Non intendiamo qui dare un'assiomatica della teoria degli insiemi (cosa che esula dalle finalità di questo corso e demandata ad altri eventuali corsi successivi), ma soltanto elencare alcune delle proprietà e delle costruzioni che permettono di confrontare insiemi e costruire nuovi insiemi a partire da altri, facendo eventualmente notare la necessità di assiomatizzare tali cosatruzioni.

Per noi un insieme sarà soltanto una collezione di oggetti detti i suoi *elementi*. La proprietà fondamentale che si richiede affinché un oggetto sia un insieme è che si possa sempre stabilire senza ambiguità se qualche cosa è un suo elemento oppure no. In simboli, se A è un insieme allora per ogni x si ha che $x \in A$ (x *appartiene* ad A) oppure $x \notin A$ (x *non appartiene* ad A). Questa che può sembrare una richiesta ovvia in realtà non lo è. Si consideri l'oggetto definito da:

$$A = \{x \mid x \notin x\}$$

e si provi a stabilire se $A \in A$ oppure no.

1. Se $A \in A$, allora, dalla definizione di A segue che $A \notin A$
2. Se $A \notin A$ allora, per definizione di A, $A \in A$

Quindi A non può essere un insieme, in quanto non possiamo decidere se $A \in A$ oppure no. Questo esempio è noto come il *paradosso di Russel*.

Il criterio per stabilire quando due insiemi sono uguali, è fornito dal seguente

Assioma 1.1 (estensionalità). Due insiemi sono uguali se e solo se hanno gli stessi elementi. In simboli

$$A = B \iff (\forall x\, x \in A \iff x \in B)$$

Definizione 1.2. Siano X e Y due insiemi, si dice che X è *contenuto* in Y (o anche X è *sottinsieme* di Y), e si denota con $X \subseteq Y$ se ogni elemento di X è elemento di Y, in simboli, $\forall x\, (x \in X \Rightarrow x \in Y)$.

Si dice che X è *contenuto strettamente* in Y (o anche che è un *sottinsieme proprio* di Y) e si denota con $X \subsetneq Y$, se $X \subseteq Y$ e $X \neq Y$.

Un modo di definire degli insiemi è quello di usare una "proprietà" che ne caratterizzi gli elementi. Ossia se P è una, *formula della teoria degli insiemi*, per intenderci una proprietà esprimibile in termini del simbolo di appartenenza e di uguaglianza, dei quantificatori e dei connettivi logici, (e, o, $\Rightarrow$, non) allora con $\{x \mid P(x)\}$, si intende la collezzione di tutti gli x che soddisfano la proprietà P. Il paradosso di Russel mostra che in generale un tale oggetto può non essere un insieme. Si dà però il seguente

Assioma 1.3 (separazione). Se X è un insieme e P è una proprietà esprimibile in termini del linguaggio della teoria degli insiemi, allora la collezione

$$\{x \mid x \in X \text{ e } P(x)\}$$

è un insieme. Si userà spesso anche la notazione $\{x \in X \mid P(x)\}$, per indicare questo insieme.

Definizione 1.4. Se X e Y sono insiemi si costruiscono altri insiemi:

- *intersezione* $X \cap Y = \{x \mid x \in X \text{ e } x \in Y\}$

- *differenza* $X - Y = \{x \mid x \in X \text{ e } x \notin Y\}$.

  Quando $Y \subseteq X$ la differenza $X - Y$ viene chiamata il *complemento* di Y in X e viene denotata anche con $\complement_X Y$ o semplicemente con $\complement Y$ o con Y' quando non ci sia ambiguità

- *unione* $X \cup Y = \{x \mid x \in X \text{ o } x \in Y\}$
- *differenza simmetrica* $X \triangle Y = (X - Y) \cup (Y - X)$
- *prodotto* $X \times Y = \{(x, y) \mid x \in X \text{ e } y \in Y\}$
- *potenza* $2^X = \{x \mid x \subseteq X\}$

Se I è un insieme e per ogni $i \in I$ è dato un insieme X_i, si definiscono

- *intersezione* $\bigcap_{i \in I} X_i = \{x \mid \forall\, i\ x \in X_i\}$
- *unione* $\bigcup_{i \in I} X_i = \{x \mid \exists\, i\ x \in X_i\}$

Osservazione 1.5. Quelle che abbiamo appena dato come definizioni, sono solo in parte tali. Se infatti gli insiemi intersezione, differenza e complemento sono effettivamente definibili a usando l'assioma di separazione (1.3), per gli altri tale assioma non è più sufficiente (non si separano degli elementi da un insieme, ma si costruiscono, insiemi "più grandi") e quindi tali costruzioni devono essere opportunamente assiomatizzate, cosa che però noi non facciamo.

Esercizio 1.1. Si provi che valgono le seguenti:

1. $\forall X\ X \subseteq X$
2. $\forall X, Y, Z\ X \subseteq Y$ e $Y \subseteq Z$ allora $X \subseteq Z$.
3. $\forall X, Y\ X \subseteq Y$ e $Y \subseteq X$ se e solo se $X = Y$

Esercizio 1.2. Siano X e Y insiemi, si provi che $X \subseteq Y \iff X \cap Y = X \iff X \cup Y = Y$.

Esercizio 1.3. Siano X, Y, Z insiemi, si provino le seguenti:

1. proprietà associativa dell'intersezione e dell'unione

$$\begin{aligned} X \cap (Y \cap Z) &= (X \cap Y) \cap Z \\ X \cup (Y \cup Z) &= (X \cup Y) \cup Z \end{aligned}$$

2. proprietà commutativa

$$\begin{aligned} X \cap Y &= Y \cap X \\ X \cup Y &= Y \cup X \end{aligned}$$

3. proprietà di assorbimento

$$\begin{aligned} X \cup (X \cap Y) &= X \\ X \cap (X \cup Y) &= X \end{aligned}$$

4. proprietà distributiva dell'intersezione rispetto all'unione e dell'unione rispetto all'intersezione

$$\begin{aligned} X \cap (Y \cup Z) &= (X \cap Y) \cup (X \cap Z) \\ X \cup (Y \cap Z) &= (X \cup Y) \cap (X \cup Z) \end{aligned}$$

5. leggi di de Morgan

$$\begin{aligned} X - (Y \cup Z) &= (X - Y) \cap (X - Z) \\ X - (Y \cap Z) &= (X - Y) \cup (X - Z) \end{aligned}$$

6. $X - (X - Y) = X \cap Y$
7. se $Y \subseteq X$ allora $\complement_X \complement_X Y = Y$.

Esercizio 1.4. Siano X, Y, Z insiemi, si provino le seguenti:

1. $X \triangle (Y \triangle Z) = (X \triangle Y) \triangle Z$
2. $X \cap (Y \triangle Z) = (X \cap Y) \triangle (X \cap Z)$

Relazioni, funzioni parziali e funzioni totali

Definizione 1.6. Siano X e Y insiemi si dice *relazione* tra X e Y, un sottinsieme $\mathcal{R} \subseteq \mathcal{X} \times \mathcal{Y}$. Se $\mathcal{R}$ è una relazione si scriverà anche $x\mathcal{R}\dagger$ come sinonimo di $(x, y) \in \mathcal{R}$.

Una relazione tra X e se stesso, si dirà anche una *relazione binaria su* X.

Definizione 1.7. Una relazione $f \subseteq X \times Y$ si dice una *funzione parziale* se per ogni $x \in X$ esiste al più un $y \in Y$ tale che $(x, y) \in f$. In simboli:

$$\forall x \in X((x, y) \in f \text{ e } (x, y') \in f) \Rightarrow y = y'$$

Si scriverà $f : X \rightharpoonup Y$ per dire che f è una funzione parziale da X a Y e in tal caso si scriverà anche $y = f(x)$ come sinonimo di $(x, y) \in f$.

L'insieme $\{x \in X \mid \exists y \in Y : y = f(x)\}$ è detto il *dominio* di f e si denota con $\mathrm{dom}(f)$.

L'insieme $\{y \in Y \mid \exists x \in \mathrm{dom}(f) : y = f(x)\}$ è detto l'*immagine* di f e si denota con $\mathrm{im}(f)$.

Una funzione parziale $f : X \rightharpoonup Y$ si dice *funzione totale* o semplicemente funzione se $\mathrm{dom}(f) = X$, in tal caso si scrive $f : X \to Y$.

Si denota Y^X l'insieme di tutte le funzioni (totali) da X a Y, ossia $X^Y\{f : X \to Y\}$.

Osservazione 1.8. Una funzione parziale può essere pensata come "una legge" che ad ogni elemento $x \in \mathrm{dom}(f)$ associa l'unico elemento $y \in Y$ tale che $(x, y) \in f$, questo elemento si denota con $f(x)$. Con questa interpretazione, dà senso proprio all'uguale contenuto nella scrittura $y = f(x)$. In questa accezione (legge che associa ad un elemento un altro elemento) verranno generalmente usate le funzioni.

Esempio 1.9. Se X è un insieme $\mathrm{id}_X = \{(x_1, x_2) \in X \times X \mid x_1 = x_2\}$ è una funzione, che viene chiamata l'*identità* di X. In altri termini $\mathrm{id}_X(x) = x$ per ogni $x \in X$.

Definizione 1.10. Siano $f : X \rightharpoonup Y$ e $g : Y \rightharpoonup Z$ si chiama *composizione* di f e g la relazione tra X e Z definita da

$$g \circ f = \{(x, z) \mid \exists y \in Y : y = f(x) \text{ e } z = g(y)\}$$

Proposizione 1.11. *Se $f : X \rightharpoonup Y$ e $g : Y \rightharpoonup Z$ allora $g \circ f : X \rightharpoonup Z$. Se $f : X \to Y$ e $g : y \to Z$ allora $g \circ f : X \to Z$.*

Dimostrazione. Per provare il primo punto, dobbiamo mostrare che se $(x, z), (x, z') \in g \circ f$ allora $z = z'$. Per definizione di $g \circ f$ esiste $y \in Y$ tale che $y = f(x)$ e $z = g(y)$ ed esiste un $y' \in Y$ tale che $y' = f(x)$ e $z = g(y')$. Ma allora, dato che f è una funzione parziali, $y = y'$, e quindi, dato che anche g è una funzione parziale $z = z'$).

Se f e g sono funzioni totali, sono in particolare delle funzioni parziali e quindi, per quanto appena mostrato, $g \circ f$ è una funzione parziale. Dobbiamo provare che per ogni $x \in X$ esiste uno $z \in Z$ tale che $z = g \circ f(x)$. Sia $x \in X$, dato che f 'e una funzione totale, esiste $y \in Y$ tale che $y = f(x)$, dato che anche g è totale esiste allora $z \in Z$ tale che $z = g(y)$, ma questo significa che $(x, z) \in g \circ f$, ovvero $z = g \circ f(x)$. ❑

Osservazione 1.12. Con l'interpretazione data nell'osservazione 1.8 si ha allora che $g \circ f(x) = g(f(x))$.

Definizione 1.13. Sia $f : X \to Y$ ed $A \subseteq Y$, si chiamo *immagine inversa* di A tramite f l'insieme:

$$f^{-1}(A) = \{x \in X \mid f(x) \in A\}.$$

Definizione 1.14. Una funzione $f : X \to Y$ si dice:

- *iniettiva* se per ogni $x_1, x_2 \in X$ $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$
- *surgettiva* se per ogni $y \in Y$ esiste $x \in X$ tale che $f(x) = y$
- *bigettiva* se è iniettiva e bigettiva

Proposizione 1.15. *Sia $f : X \to Y$ una bigezione, allora esiste una unica funzione $g : Y \to X$ tale che $f \circ g = \mathrm{id}_Y$ e $g \circ f = \mathrm{id}_X$. Tale funzione si chiama* inversa *di f e si denota con f^{-1}.*

Dimostrazione. Dato $y \in Y$ esiste un unico $x \in X$ tale che $f(x) = y$ (esiste perché f è surgettiva, è unico perché è iniettiva); chiamiamo $g(y)$ tale elemento. È allora evidente che $f(g(y)) = y$ per ogni $y \in Y$. D'altra parte $f(g(f(x))) = f(x)$ per ogni $x \in X$ (applico la relazione precedente con $x = f(x)$), e quindi per l'iniettività di f si ha che $g(f(x)) = x$. È chiaro che tale funzione è l'unica possibile con le proprietà richieste. ❑

Osservazione 1.16. Si osservi che rispetto alla notazione insiemistica di funzione (1.7) si ha che $f^{-1} = \{(y, x) \in Y \times X \mid (x, y) \in f\}$.

Il seguente esercizio inverte il risultato della proposizione precedente.

Esercizio 1.5. Sia $f : X \to Y$ e si supponga che esista una funzione $g : Y \to X$ tale che $g \circ f = \mathrm{id}_X$ e $f \circ g = \mathrm{id}_Y$. Si provi che allora f è bigettiva.

Esercizio 1.6. Perché se X e Y sono insiemi allora anche Y^X è un insieme?

Esercizio 1.7. Siano $f : X \rightharpoonup Y$ e $g : Y \rightharpoonup Z$, si determini $\mathrm{dom}(g \circ f)$.

Esercizio 1.8. Siano $f : X \to Y$ e $g : Y \to Z$ si provi che:

- se f e g sono iniettive allora $g \circ f$ è iniettiva
- se f e g sono surgettive allora $g \circ f$ è surgettiva
- se f e g sono bigettive allora $g \circ f$ è bigettiva

Esercizio 1.9. Siano X, Y, I insiemi, $f : X \to Y$ e $A_i \subseteq Y$ per ogni $i \in I$. Si provi che

$$f^{-1}(\bigcap_{i\in I} A_i) = \bigcap_{i\in I} f^{-1}(A_i) \qquad f^{-1}(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f^{-1}(A_i)$$

Lezione 2 (28 febbraio 2001 h. 10.30-11.30)

Equipotenza di insiemi

Definizione 2.1. Siano X e Y due insiemi, diremo che X e Y sono *equipotenti* se esiste una bigezione $f : X \to Y$. Denoteremo questo fatto con $|X| = |Y|$, che leggeremo anche X e Y *hanno la stessa cardinalità*.

Osservazione 2.2. Si osservi che non stiamo dando alcun significato al simbolo $|X|$, ossia non stiamo definendo cosa sia la *cardinalità* di un insieme. In effetti ciò può essere fatto (e sarà fatto in corsi successivi), ossia si possono definire una classe di particolari insiemi detti *cardinali* che godono della seguente proprietà:

ogni insieme è equipotente ad uno ed un solo cardinale.

Quando questo sarà fatto, quello che per noi è una definizione, ossia $|X| = |Y|$ se e solo se esiste una bigezione tra X e Y, sarà un teorema.

Questa costruzione generale esula dalle finalità di questo corso, ci limiteremo a farla soltanto per una particolare classe di insiemi: gli insiemi finiti (cfr. 3.5 e 4.1

Proposizione 2.3. *Valgono le seguenti proprietà:*

1. *X è equipotente a se stesso.*
2. *se X è equipotente a Y allora Y è equipotente a X*
3. *se X è equipotente a Y e Y è equipotente a Z, allora X è equipotente a Z.*

Dimostrazione. L'identità è una bigezione; se f è una bigezione, allora f^{-1} è una bigezione; composizione di bigezioni è una bigezione. ❑

Esercizio 2.1. Siano X, Y, X', Y' insiemi e siano $f : X \to X'$ e $g : Y \to Y'$ due applicazioni. Si definisca $f \times g : X \times Y \to X' \times Y'$ ponendo

$$f \times g(x, y) = (f(x), g(y)).$$

Si provi che

1. $f \times g$ è surgettiva se e solo se f e g sono entrambe surgettive.
2. $f \times g$ è iniettiva se e solo se f e g sono entrambe iniettive.

Esercizio 2.2. Si provi che $\left|2^X\right| = \left|\{0,1\}^X\right|$.

Esercizio 2.3. Si provi che $|X \times X| = \left|X^{\{0,1\}}\right|$.

Esercizio 2.4. Si provi che se X, Y, Z sono insiemi, allora $\left|(X^Y)^Z\right| = \left|X^{Y\times Z}\right|$.

Esercizio 2.5. Si provi che se X, Y, Z sono insiemi con $Y \cap Z = \varnothing$, allora $\left|X^{Y\cup Z}\right| = \left|X^Y \times X^Z\right|$.

I numeri naturali: gli assiomi di Peano

Ricordiamo gli assiomi (dovuti a Peano) che descrivono la struttura dei numeri naturali.

Assioma 2.4. $0 \in \mathbb{N}$

Assioma 2.5. $\text{succ} : \mathbb{N} \to \mathbb{N}$ è una funzione iniettiva

Assioma 2.6. $\forall n \in \mathbb{N} \quad \text{succ}(n) \neq 0$

Assioma 2.7 (di induzione). se $A \subseteq \mathbb{N}$ è un sottinsieme tale che

1. $0 \in A$
2. $\forall n \in \mathbb{N} \quad (n \in A \Rightarrow \text{succ}(n) \in A)$

allora $A = \mathbb{N}$.

Proposizione 2.8. *Sia $n \in \mathbb{N}$, $n \neq 0$ allora esiste un unico $m \in \mathbb{N}$ tale che* $\text{succ}(m) = n$. *Tale m viene chiamato il* predecessore *di m.*

Dimostrazione. Avendo l'esistenza, l'unicità segue immediatamente dall'iniettività di succ.

Supponiamo per assurdo che esista un $m \neq 0$ tale che $\text{succ}(n) \neq m$ per ogni n, allora sia $A = \mathbb{N} - \{m\}$. Chiaramente $0 \in A$, in quanto $m \neq 0$. Se $n \in A$, allora $succ(n) \neq m$ e quindi $succ(n) \in A$. Ma allora $A = \mathbb{N}$, e questa è una contraddizione. ❑

L'assioma di induzione fornisce una potente tecnica di dimostrazione di proposizioni indicizzate sui naturali.

Il principio di induzione (prima forma)

Una conseguenza immediata dell'assioma di induzione (2.7) è il seguente

Teorema 2.9 (prima forma dell'induzione). *Sia $P(n)$ una famiglia di proposizioni indicizzate su $\mathbb{N}$ e si supponga che*

1. *$P(0)$ sia vera*
2. *per ogni $n \in \mathbb{N}$ $P(n) \Rightarrow P(succ(n))$*

allora $P(n)$ è vera per ogni $n \in \mathbb{N}$

Dimostrazione. Sia $A = \{n \mid P(n) \text{ è vera}\}$, allora $0 \in A$ e se $n \in A$ allora vale $P(n)$, quindi vale $P(\text{succ}(n))$ ossia anche $succ(n) \in A$, quindi per l'assioma di induzione (2.7) $A = \mathbb{N}$. ❑

Il teorema di ricorsione

Al momento i naturali sembrano essere una struttura molto povera, non vi è definita né la somma né il prodotto e nemmeno la relazione d'ordine (poter dire quando due numeri sono uno più grande dell'altro). Per poter dare queste definizioni è necessario dimostrare il seguente

Teorema 2.10 (di ricorsione). *Sia X un insieme, $h : \mathbb{N} \times X \to X$ una funzione e $c \in X$. Esiste una unica funzione $f : \mathbb{N} \to X$ tale che:*

$$f(0) = c \tag{1}$$

$$f(\text{succ}(n)) = h(n, f(n)) \quad \forall n \in \mathbb{N} \tag{2}$$

Dimostrazione. Cominciamo con il provare l'unicità di una tale f. Supponiamo che f e g verifichino le due proprietà e proviamo per induzione che $f(n) = g(n)$ per ogni n. Usiamo l'induzione. Per $n = 0$ la proposizione è vera, infatti dato che sia f che g verificano 1, si ha che $f(0) = c = g(0)$.

Supponiamo che $f(n) = g(n)$. Dalla 2 per f si ha che $f(\mathrm{succ}(n)) = h(n, f(n))$ e la stessa applicata a g dà che $g(\mathrm{succ}(n)) = h(n, g(n))$, dato che $f(n) = g(n)$, allora

$$f(\mathrm{succ}(n)) = h(n, f(n)) = h(n, g(n) = g(\mathrm{succ}(n)).$$

Proviamo ora l'esistenza. Per definizione di funzione (1.7) quello che si cerca è un insieme $f \subseteq \mathbb{N} \times X$ tale che:

$$\forall n \in \mathbb{N} \quad \exists \text{ unico } x \in X : (n, x) \in f \tag{3}$$

e, traducendo in termini di appartenenza le richieste (1) e (2)

$$(0, c) \in f \tag{4}$$

$$\forall n \in \mathbb{N} \quad (x, n) \in f \Rightarrow (\mathrm{succ}(n), h(n, x)) \in f \tag{5}$$

Sia $\Omega = \{Z \subseteq \mathbb{N} \times X \mid Z \text{ verifica (1) e (2)}\}$, quello che dobbiamo trovare è un elemento di Ω che sia una funzione.

Sia $f = \bigcap_{Z \in \Omega} Z$. Dato che f è l'intersezione di tutti gli elementi di Ω, necessariamente

$$\forall Z \in \Omega \quad f \subseteq Z \tag{6}$$

Provaiamo che $f \in \Omega$. Infatti $(0, c) \in Z$ per ogni $Z \in \Omega$, quindi $(0, c) \in f$. Se $(n, x) \in f$ allora $(n, x) \in Z$ per ogni $Z \in \Omega$, ma allora dato che ogni $Z \in \Omega$ verifica la (5), $(\mathrm{succ}(n), h(x, n) \in Z$ per ogni $Z \in \Omega$ e quindi $(\mathrm{succ}(n), h(x, n) \in f$.

Per concludere resta da provare che f verifica la (3). Procediamo per induzione su n. Se $n = 0$. Abbiamo già visto che $(0, c) \in f$. Supponiamo per assurdo che esista $(0, d) \in f$ con $d \neq c$, e sia $f' = f - \{(0, d)\}$. Chiaramente $(0, c) \in f'$ e se $(n, x) \in f' \subseteq f$ allora $(\mathrm{succ}(n), h(n, x) \in f$, ma allora, per il terzo assioma di Peano (2.6), $\mathrm{succ}(n) \neq 0$ per ogni $n \in \mathbb{N}$ e quindi $(\mathrm{succ}(n), h(n, x) \neq (0, d)$, pertanto $(\mathrm{succ}(n), h(n, x) \in f'$. Quindi $f' \in \Omega$, ma ciò contraddice la (6) perché $f \not\subseteq f'$.

Supponiamo la tesi vera per n. Sia x l'unico elemento tale che $(n, x) \in f$, dato che f verifica la (5), allora $(\mathrm{succ}(n), h(n, x)) \in f$. Supponiamo per assurdo che anche $(\mathrm{succ}(n), e) \in f$ e si ponga $f' = f - \{(\mathrm{succ}(n), e)\}$. Proviamo che anche in questo caso $f' \in \Omega$ e si avrà, come prima, un assurdo. Dal terzo assioma di Peano segue che $(0, c) \in f'$. Se $(i, z) \in f' \subseteq f$ allora $(\mathrm{succ}(i), h(i, z)) \in f$. Se $i \neq n$ allora, per l'iniettività di succ (assioma 2.5) si ha che $(\mathrm{succ}(i), h(i, z)) \neq (\mathrm{succ}(n), e)$ e quindi $(\mathrm{succ}(i), h(i, z)) \in f'$. Se invece $i = n$ allora $(n, z) \in f$ implica, per l'unicità di x, che $z = x$ e quindi, dato che $h(n, z) \neq e$, $(\mathrm{succ}(i), h(i, z)) = (\mathrm{succ}(n), h(n, x)) \in f'$. Questo conclude la dimostrazione. ❑

Lezione 3 (5 marzo 2001 h. 9.30-10.30)

Le operazioni sui naturali

Il teorema di ricorsione permette di definire la somma il prodotto di numeri naturali.

Definizione 3.1. Dato $n \in \mathbb{N}$ si definisce ;la funzione $m \mapsto n + m$ ricorsivamente nel seguente modo:

$$\begin{aligned} n + 0 &= n \\ n + \mathrm{succ}\, m &= \mathrm{succ}\, n + m \end{aligned}$$

ed analogamente si definisce il prodotto $m \mapsto nm$:

$$\begin{aligned} n0 &= 0 \\ n(m+1) &= nm + n \end{aligned}$$

Osservazione 3.2. Se si chiamo $1 = succ(0)$, allora per ogni $n \in \mathbb{N}$ si ha che $\text{succ}(n) = n + 1$, infatti dalla definizione di $+$ si ha che

$$n + 1 = n + \text{succ}(0) = \text{succ}(n + 0) = \text{succ}(n)$$

D'ora in poi non scriveremo più $\text{succ}(n)$ ma $n + 1$.

Esercizio 3.1. Si provi che per ogni $n \in \mathbb{N}$ si ha $0 + n = n$ e $1 + n = n + 1$ ossia $1 + n = \text{succ}(n)$.

Esercizio 3.2. Si provino le usuali proprietà (i.e. associativa, commutativa, distributiva) della somma e del prodotto di numeri naturali.

L'ordinamento dei naturali

Con la somma si può definire la nozione di ordinamento dei numeri naturali.

Definizione 3.3. Siano $n, m \in \mathbb{N}$ diremo che $n \leq m$ se esiste $k \in \mathbb{N}$ tale che $m = n + k$.

Osservazione 3.4. Si può vedere $\leq$ come un sottinsieme di $\mathbb{N} \times \mathbb{N}$ e precisamente $\leq = \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid \exists k \in \mathbb{N} : n + k = m\}$. E quindi $\leq$ è una relazione (definizione 1.6) sui naturali e quello che abbiamo definito come significato di $n \leq m$ è effettivamente lo stesso che dire $(n, m) \in \leq$.

Si può dimostrare la seguente

Proposizione 3.5. *Valgono le seguenti proprietà:*

1. $\forall n \in \mathbb{N} \quad n \leq n$.
2. $\forall n, m \in \mathbb{N} \quad (n \leq m \text{ e } m \leq n \Rightarrow n = m$
3. $\forall n, m, k \in \mathbb{N} \quad (n \leq m \text{ e } m \leq k \Rightarrow n \leq k$
4. $\forall n, m \in \mathbb{N} \quad n \leq m \text{ o } m \leq n$.

Dimostrazione. La dimostrazione è lasciata per esercizio agli studenti volonterosi. I punti che richiedono maggiore attenzione sono il secondo e il quarto. ∎

Insiemi ordinati

Definizione 3.6. Sia X un insieme e $\mathcal{R}$ una relazione binaria su X, $\mathcal{R}$ si dice un *ordinamento parziale* o anche una *relazione d'ordine parziale* se valgono le seguenti proprietà:

1. *proprietà riflessiva*: $\forall x \in X \quad x\mathcal{R}x$.
2. *proprietà antisimmetrica:* $\forall x, y \in X \quad (x\mathcal{R}y \text{ e } y\mathcal{R}x) \Rightarrow x = y$
3. *proprietà transitiva*: $\forall x, y, z \in X \quad (x\mathcal{R}y \text{ e } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$

Un ordinamento parziale si dice un *ordinamento totale* se in più vale la

4. *tricotomia*: $\forall x, y \in X \quad x\mathcal{R}y \text{ o } y\mathcal{R}x$.

Una coppia $(X, \mathcal{R})$ in cui $\mathcal{R}$ è un ordinamento (parziale o totale) si dice un *insieme (parzialmente o totalmente) ordinato.*

Osservazione 3.7. In genere le relazioni d'ordine si indicano con simboli del tipo $\leq$ o $\preceq$, in tal caso quando si scriverà $x \succeq y$ si intenderà $y \preceq x$, e quando si scriverà $x \prec y$ si intenderà il cosiddetto ordinamento stretto ovvero $x \preceq y$ e $x \neq y$. In termini dell'ordinamento stretto la proprietà di tricotomia per l'ordinamento $\preceq$si può rioenunciare dicendo:

- $\forall x, y \in X$ vale una e una sola delle tre seguenti: $X \prec y$, $x = y$, $y \prec x$.

Osservazione 3.8. In termini di questo nuovo linguaggio $(\mathbb{N}, \leq)$ risulta quindi essere un insieme totalmente ordinato.

L'ordinamento dei naturali e le operazioni

Si possono dimostrare anche le ulteriori proprietèche legano l'ordinamento con le operazioni:

Proposizione 3.9. *Se n, m, k sono numeri naturali:*

1. $n \leq m \Rightarrow n + k \leq m + k$
2. $n \leq m$ e $k \geq 1 \Rightarrow nk \leq mk$

Dimostrazione. Esercizio per lo studente volenteroso. ❑

Esercizio 3.3. A partire dalle proprietà enunciate nella proposizione precedente (3.9) si provi che se $n, m, k, h \in \mathbb{N}$ allora

1. $n \leq m$ e $k \leq h \Rightarrow n + k \leq m + h$
2. $n \leq m$ e $k \leq h \Rightarrow nk \leq mh$

Insiemi finiti: il Lemma dei cassetti

Dato un numero naturale $n \in \mathbb{N}$ denotiamo con I_n l'insieme $I_n = \{0, 1, \ldots, n-1\}$.

Definizione 3.10. Diremo che un insieme è *finito* se esiste $n \in \mathbb{N}$ tale che $|X| = |I_n|$. Un insieme è detto *infinito* se non è finito

Teorema 3.11 (Lemma dei cassetti). *Siano X e Y due insiemi aventi rispettivamente $|X| = |I_n|$ e $|Y| = |I_m|$ con $n < m$ allora ogni applicazione $f : Y \to X$ non è iniettiva.*

Dimostrazione. Procediamo per induzione su n. Se $n = 0$ allora $X = \varnothing$ e $Y \neq \varnothing$, quindi l'insieme X^Y delle applicazioni $Y \to X$ è vuoto, e quindi non c'è nulla da dimostrare (dal falso segue ogni cosa).

Supponiamo che la tesi sia vera per n e proviamola per $n+1$. Sia $|X| = |I_{n+1}|$ e sia, $|Y| = |I_m|$ con $m > n + 1$ e supponiamo per assurdo che l'applicazione $f : Y \to X$ sia iniettiva. Per definizione esiste una bigezione $g : I_{n+1} \to X$; poniamo $x_n = g(n)$ e $X' = X - \{x_n\}$. Chiaramente X' è in bigezione con I_n. Si hanno due casi:

1. $f^{-1}(x_n) = \varnothing$ (i.e.$\forall y \in Y f(y) \neq x_n$)
2. $f^{-1}(x_n) \neq \varnothing$ (i.e.$\exists y \in Y : f(y) = x_n$)

Nel primo caso, $f(Y) \subseteq X'$ e quindi $f : Y \to X'$ sarebbe un'applicazione iniettiva da un insieme equipotente a I_m in un insieme equipotente a I_n; dato che $m > n+1 > n$ questo è assurdo per ipotesi di induzione.

Nel secondo caso, sia $y \in Y$ tale che $f(y) = x_n$ e sia $Y' = Y - \{y\}$. Dato che f è iniettiva, $f(Y') \subseteq X'$ e quindi, $f|_{Y'} : Y' \to X'$ è una applicazione iniettiva. Dato che $|Y'| = |I_{m-1}|$, $|X'| = |I_n|$ e $m-1 > n$, ciò è assurdo per ipotesi di induzione. ❑

Osservazione 3.12. Il nome lemma dei cassetti deriva dal seguente modo *naif* di enunciare il teorema precedente: *se ho un certo numero di oggetti da sistemare in dei cassetti, e il numero di oggetti è superiore a quello dei cassetti, almeno un cassetto conterrà più di un oggetto.*

Lezione 4 (7 marzo 2001 h. 10.30-11.30)

Cardinalità degli insiemi finiti

Una prima immediata conseguenza del lemma dei cassetti (3.11) è il seguente corollario:

Corollario 4.1. *Se $n, m \in \mathbb{N}$ sono due naturali diversi X e Y sono insiemi finiti con $|X| = |I_n|$ e $|Y| = |I_m|$, allora X e Y non sono equipotenti.*

In particolare, se $|X| = |I_n|$ e $|X| = |I_m|$ allora $n = m$.

Questo corollario fa sì che si possa definire la cardinalità degli insiemi finiti.

Definizione 4.2. Sia X un insieme finito, si dice *cardinalità* di X l'unico numero naturale n tale che $|X| = |I_n|$. Tale numero si denota allora con $|X|$.

È facile provare la seguente

Proposizione 4.3. *Due insiemi finiti sono equipotenti se e solo se $|X| = |Y|$.*

Dimostrazione. Se $|X| = |Y|$, allora esiste $n \in \mathbb{N}$ tale che X è equipotente a I_n e Y è equipotente a I_n, ma allora X e Y sono tra loro equipotenti (proposizione 2.3. Viceversa se sono equipotenti il corollario precedente mostra che hanno la stessa cardinalità. ❑

Sottinsiemi di un insieme finito

Proposizione 4.4. *Sia X un insieme finito e $Y \subseteq X$ allora anche Y è finito e $|Y| \leq |X|$. Se Y è un sottoinsieme proprio di X allora $|Y| < |X|$.*

Dimostrazione. Procediamo per induzione su $n = |X|$. Se $n = 0$ allora $X = \varnothing$ e quindi anche $Y = \varnothing$, da cui si conclude. Supponiamo la tesi vera per n e sia dato X con $|X| = n + 1$. Sia $f : I_{n+1} \to X$ una bigezione e poniamo $x_n = f(n)$ e $X' = X - \{x_n\}$. Chiaramente $f|_{I_n} : I_n \to X'$ è una bigezione, quindi $|X'| = n$. Si hanno due casi $x_n \notin Y$ e $x_n \in Y$. Nel primo caso $Y \subseteq X'$, quindi, per ipotesi di induzione, $|Y| \leq |X'| = n < n + 1 = |X|$. Nel secondo caso, detto $Y' = Y - \{x_n\}$ si ha che $Y' \subseteq X'$ e quindi $|Y'| \leq |X'|$ e quindi $|Y| = |Y'| + 1 \leq |X'| + 1 = |X|$. Si osservi che in quest'ultimo caso, se $Y \neq X$ allora anche $Y' \neq X'$ e quindi, per ipotesi di induzione si ha che $|Y'| < |X'|$ da cui $|Y| < |X|$. ❑

Come conseguenza si ha il seguente

Corollario 4.5. *Un insieme finito non è equipotente ad alcun suo sottinsieme proprio.*

Esempio 4.6. L'insieme $\mathbb{N}$ è infinito, si consideri ad esempio l'applicazione $\mathbb{N} \to \mathbb{N}$ definita da $n \mapsto \text{succ}(n)$, questa è una bigezione tra $\mathbb{N}$ ed il sottinsieme proprio $\mathbb{N} - \{0\}$.

Esercizio 4.1. Si determinino altri sottinsiemi propri di $\mathbb{N}$ equipotenti a $\mathbb{N}$

Esercizio 4.2. Siano X e Y insiemi finiti. Si provi che

1. se $X \cap Y = \varnothing$ allora $|X \cup Y| = |X| + |Y|$.
2. in generale $|X \cup Y| = |X| + |Y| - |X \cap Y|$

Esercizio 4.3. Siano $X_1, \ldots, X_n$ insiemi finiti a due a due disgiunti si provi che $\bigcup_{i=1}^{n} X_i$ è finito e che

$$\left| \bigcup_{i=1}^{n} X_i \right| = \sum_{i+1}^{n} |X_i| .$$

Esercizio 4.4. Se X e Y sono insiemi finiti, si provi che

1. $|X \times Y| = |X||Y|$.
2. $\left|X^Y\right| = |X|^{|Y|}$
3. $\left|2^X\right| = 2^{|X|}$.

Esercizio 4.5. Siano X e Y insiemi finiti entrambi di cardinalità n. Si provi che ogni funzione iniettiva $X \to Y$ è anche surgettiva.

Esercizio 4.6. Sia X un insieme finito di cardinalità n. Si determini il numero delle applicazioni biunivoche di X in sé.

Lezione 5 (12 marzo 2001 h. 9.30-10.30)

Insiemi infiniti: l'assioma della scelta

Uno degli strumenti più potenti di cui si ha spesso bisogno quando si deve trattare con insiemi infiniti, è il seguente:

Assioma 5.1 (della scelta). Sia I un insieme e per ogni $i \in I$ sia dato un insieme $A_i \neq \varnothing$. Allora esiste una funzione, detta *funzione di scelta*,

$$\varphi : I \longrightarrow \bigcup_{i \in I} A_i$$

tale che

$$\forall i \in I \quad \varphi(i) \in A_i$$

Osservazione 5.2. Questo assioma dice essenzialmente che quando si ha un insieme di insiemi non vuotiè possibile scegliere, **in un colpo solo**, un elemento da ciascuno di essi. Si osservi che questo assioma è fortemente **non costruttivo**: ci dice che una funzione di scelta esiste, ma non dà alcun modo per trovarla.

Osservazione 5.3. Una delle situazioni in cui più spesso si adopera l'assioma della scelta (e che anzi ne è una formulazione equivalente) è la seguente: sia X un insieme, prendiamo come insieme di indici l'insieme $2^X - \{\varnothing\}$ e per ogni $i \in I$ (ossia per ogni $i \subseteq X$ diverso da $\varnothing$ poniamo $A_i = i$. L'assioma di scelta ci dice allora che esiste una funzione $\varphi : 2^X - \{\varnothing\} \to X = \bigcup_{i \in 2^X - \{\varnothing\}} i$ tale che $\varphi(i) \in i$ per ogni $i \in 2^X - \{\varnothing\}$.

Esercizio 5.1. Si provi che una funzione $f : X \to Y$ è surgettiva se e solo se esiste $g : Y \to X$ tale che $f \circ g = \mathrm{id}_Y$. Una tale g si chiama una *inversa destra* di f.

Esercizio 5.2. Si provi che una funzione $f : X \to Y$ è iniettiva se e solo se esiste $g : Y \to X$ tale che $g \circ f = \mathrm{id}_X$. Una tale g si chiama una *inversa sinistra* di f.

Teorema 5.4. *Se X è un insieme infinito, allora contiene un sottinsieme Y equipotente a $\mathbb{N}$.*

Dimostrazione. Sia $\varphi : 2^X - \{\varnothing\} \to X$ una funzione di scelta e denotiamo con 2^X_F l'insieme delle *parti finite* di X, ovvero $2^X_F = \{Z \subset X \mid Z \text{è finito}\}$. Dato un elemento $x_0 \in X$, (che esiste essendo X infinito e quindi non vuoto) consideriamo la funzione $\psi : \mathbb{N} \to 2^X_F$ definita ricorsivamente da:

$$\begin{aligned} \psi(0) &= \{x_0\} \\ \psi(n+1) &= \psi(n) \cup \{\varphi(X - \psi(n))\} \end{aligned}$$

e quindi definiamo la funzione $f : \mathbb{N} \to Y$ ponendo $f(0) = x_0$ e per ogni $n > 0$, $f(n) = \varphi(X - \psi(n-1))$. Osserviamo che, dalla definizione di ψ segue che per ogni $n \in \mathbb{N}$ si ha $f(n) \in \psi(n)$ e $\psi(n) \subseteq \psi(n+1)$, da cui segue che se $n \leq m$ allora $\psi(n) \subseteq \psi(m)$ e quindi $f(n) \in \psi(m)$. Ma allora se $n < m$, $f(n) \in \psi(m-1)$, mentre $f(m) = \varphi(X - \psi(m-1)) \in X - \psi(m-1)$ e quindi $f(n) \neq f(m)$, pertanto f è iniettiva. L'insieme $f(\mathbb{N})$ è allora l'insieme cercato. ❑

Osservazione 5.5. Nella dimostrazione del teorema precedente si definisce ricorsivamente una funzione $\psi : \mathbb{N} \to 2^X_F$. La funzione $h : \mathbb{N} \times 2^X_F \to 2^X_F$ che si in questa definizione ricorsiva è la funzione data da $h(n, Z) = Z \cup X - Z$. Si osservi che dato che X è infinito, se Z è finito, allora $X - Z \neq \varnothing$ e quindi ha senso prendere $\varphi(X - Z)$ e il risultato dell'applicare *psi*, $\psi(Z)$ è ancora un insieme finito. È esattamente in questo punto che si usa l'ipotesi di infinitezza dell'insieme X.

Osservazione 5.6. In qualche senso il teorema precedente mostra come la cardinalità dei numeri naturali sia, in un senso ancora da specificare (vedi 6.2) la "più piccola" tra le cardinalità infinite.

Proposizione 5.7. *Ogni insieme infinito è equipotente ad un suo sottinsieme proprio.*

Dimostrazione. Sia X un insieme infinito e sia $Y \subseteq X$ un sottinsieme equipotente a $\mathbb{N}$. Abbiamo già visto (esempio 4.6) che $\mathbb{N}$ è equipotente ad un suo sottinsieme proprio, quindi se $|Y| = |\mathbb{N}|$, Y è equipotente ad un suo sottinsieme proprio, in parrtcolare esiste una bigezione $f : Y \to Y'$ essendo $Y' \subsetneq Y$ (si provi questa affermazione, cfr. esercizio 5.3). Ma allora la funzione $g : X \to X$ definita da

$$g(x) = \begin{cases} x & \text{se } x \in X - Y \\ f(x) & \text{se } x \in Y \end{cases}$$

dà una bigezione tra X ed il sottinsieme $(X - Y) \cup Y' \subsetneq X$. ❑

La proposizione precedente ed il corollario 4.5, provano la seguente caratterizzazione degli insiemi infiniti.

Teorema 5.8. *Un insieme è infinito se e solo se è equipotente ad un suo sottinsieme proprio.*

Esercizio 5.3. Si provi quanto affermato nella dimostrazione della proposizione 5.7, ossia che se Y è equipotente a $\mathbb{N}$ allora esiste una bigezione di Y con un suo sottinsieme proprio.

Lezione 6 (14 marzo 2001 h. 10.30-11.30)

Insiemi numerabili

Definizione 6.1. Un insieme X si dice *numerabile* se $|X| = |\mathbb{N}|$. La cardinalità di $\mathbb{N}$ viene spesso indicata con $\aleph_0$ (si legge aleph con zero). Quindi per dire che X è numerabile si scriverà anche $|X| = \aleph_0$.

Il simbolo $\aleph$ è la prima lettera dell'alfabeto ebraico.

Diamo ora alcune proprietà degli insiemi numerabili.

Proposizione 6.2. *Se X e Y sono insiemi numerabili disgiunti, allora $X \cup Y$ è numerabile.*

Dimostrazione. Siano $f : X \to \mathbb{N}$ e $g : Y \to \mathbb{N}$ due bigezioni, allora si definisca $h : X \cup Y \to \mathbb{N}$ ponendo

$$h(x) = \begin{cases} 2f(x) & \text{se } x \in X \\ 2g(x) + 1 & \text{se } x \in Y \end{cases}$$

Si verifica facilmente che h è una bigezione. ❑

Proposizione 6.3. *Se X e Y sono disgiunti, X numerabile e Y è finito, allora $X \cup Y$ è numerabile.*

Siano $f : X \to \mathbb{N}$ e $g : Y \to I_n$ due bigezioni, allora si definisca $h : X \cup Y \to \mathbb{N}$ ponendo

$$h(x) = \begin{cases} g(x) & \text{se } x \in Y \\ f(x) + n & \text{se } x \in X \end{cases}$$

Si verifica facilmente che h è una bigezione. ❑

Proposizione 6.4. *Se X è numerabile e $Y \subseteq X$ allora Y è finito o numerabile.*

Dimostrazione. Se Y non è finito, allora contiene un sottinsieme numerabile Z, ma allora la tesi segue dal lemma 6.12. ❑

Proposizione 6.5. *Se X è un insieme infinito ed Y è un insieme finito o numerabile allora $|X \cup Y| = |X|$.*

Dimostrazione. Possiamo supporre che Y sia disgiunto da X, in quanto $X \cup Y = X \cup (Y - X)$ e per la proposizione precedente (6.4) e la proposizione 4.4 $Y - X$ è finito o numerabile.

Sia $Z \subseteq X$ un sottinsieme numerabile (teorema 5.4), per le due proposizioni 6.3, 6.2, esiste una bigezione $f : Z \to Z \cup Y$. Si definisca allora $g : X \to X \cup Y$ ponendo

$$g(x) = \begin{cases} f(x) & \text{se } x \in Z \\ x & \text{se } x \in X - Z \end{cases}$$

Proviamo che g è iniettiva. Siano $x_1, x_2 \in X$ diversi, chiaramente, dato che f è iniettiva, se $x_1, x_2 \in Z$ allora $f(x_1) \neq f(x_2)$ e quindi $g(x_1) \neq g(x_2)$. Se $x_1, x_2 \in X - Z$, evidentemente $g(x_1) \neq g(x_2)$. Se $x_1 \in Z$ e $x_2 \in X - Z$ allora $g(x_1) = f(x_1) \in Z \cup Y$ e, dato che Y è disgiunto da X, $(Z \cup Y) \cap (X - Z) = \varnothing$, e quindi $f(x_1) \notin X - Z$, mentre $g(x_2) = x_2 \in X - Z$.

Proviamo che g è surgettiva. Sia $w \in X \cup Y$, allora si hanno due casi: $w \in X - Z$ oppure $W \in Z \cup Y$. Nel primo caso, preso $x = w$, si ha che $g(x) = w$. Nel secondo caso, dato che f è surgettiva, esiste $z \in Z$ tale che $f(z) = w$, e quindi $g(z) = w$. ❑

Proposizione 6.6. *Se $\{X_n \mid n \in \mathbb{N}\}$ è una famiglia numerabile di insiemi finiti e a due a due disgiunti, allora $\bigcup_n X_n$ è numerabile.*

Dimostrazione. Sia $m_n = |X_n|$ e per ogni n sia $f_n : I_{m_n} \to X_n$ una bigezione. Si considerino i numeri $M_n = \sum_{i=0}^{n} m_i$, $M_{-1} = 0$, e si definisca $f : \mathbb{N} \to \bigcup_n X_n$ ponendo

$$f(k) = f_n(k - M_{n-1}) \quad \text{se } M_{n-1} \leq k < M_n$$

Una semplice verifica mostra che f è ben definita ed è una bigezione. ❑

Proposizione 6.7. *$\mathbb{N} \times \mathbb{N}$ è numerabile, e quindi il prodotto di due insiemi numerabili è numerabile.*

Dimostrazione. Per ogni $m \in \mathbb{N}$ si consideri $X_m = \{(n_1, n_2) \in \mathbb{N} \times \mathbb{N} \mid n_1 + n_2 = m\}$. Chiaramente $|X_m| = m + 1$ per ogni m, $X_m \cap X_k = \varnothing$ se $m \neq k$ e infine $\bigcup_m X_m = \mathbb{N} \times \mathbb{N}$ (si osservi che $(n_1, n_2) \in X_{n_1+n_2}$). Ma allora la tesi segue dalla proposizione precedente.

Per quanto riguarda la seconda parte dell'enunciato, si osservi che se X e Y sono numerabili, e $f : X \to \mathbb{N}$ e $g : Y \to \mathbb{N}$ sono bigezioni, allora l'applicazione prodotto $f \times g : X \times Y \to \mathbb{N} \times \mathbb{N}$ è bigettiva (Esercizio 2.1). ❑

Proposizione 6.8. *Se $\{X_n \mid n \in \mathbb{N}\}$ è una famiglia numerabile di insiemi numerabili e a due a due disgiunti, allora $\bigcup_n X_n$ è numerabile.*

Dimostrazione. Per ogni $n \in \mathbb{N}$ sia $f_n : \mathbb{N} \to X_n$ una bigezione, definiamo $f : \mathbb{N} \times \mathbb{N} \to \bigcup_n X_n$ ponendo $f(n, m) = f_n(m)$. Si conclude verificando che f è una bigezione. ❑

Esercizio 6.1. Si eseguano nel dettaglio tutte le verifiche necessarie a concludere le dimostrazioni delle proposizioni di questa sezione.

Esercizio 6.2. Si provi che se $\{X_m \mid m \in \mathbb{N}\}$ è una famiglia numerabile di insiemi finiti, allora la loro unione è finita o numerabile.

Esercizio 6.3. Si provi che se $\{X_m \mid m \in \mathbb{N}\}$ è una famiglia numerabile di insiemi numerabili, allora la loro unione è numerabile.

Esercizio 6.4. Si provi che $\mathbb{Q}$ è numerabile.

Confronto di cardinalità: il Teorema di Cantor-Bernstein

Definizione 6.9. Dati due insiemi, X e Y diremo che la cardinalità di X è *minore o uguale* alla cardinalità di Y, e lo scriveremo $|X| \leq |Y|$, se esiste una funzione iniettiva, $f : X \to Y$.

Diremo che la cardinalità di X è *strettamente minore* di quella di Y, e lo denoteremo con $|X| < |Y|$, se $|X| \leq |Y|$ e $|X| \neq |Y|$.

È immediato verificare che $|X| \leq |Y|$ se e solo se Y contiene un sottinsieme equipotente a X.

Esercizio 6.5. Si provi che nel caso di insiemi finiti, la nozione di ordinamento appena introdotta tra le cardinalità, coincide con l'usuale ordinamento dei numeri naturali.

Esercizio 6.6. Si provi che $|X| \leq |Y|$ se e solo se esiste $f : Y \to X$ surgettiva.

Proposizione 6.10. *Valgono le seguenti proprietà:*

1. *Per ogni X, $|X| \leq |X|$*
2. *per ogni X, Y, Z, se $|X| \leq |Y|$ e $|Y| \leq |Z|$ allora $|X| \leq |Z|$*

Dimostrazione. Basta osservare che l'identità è iniettiva e che composizione di funzioni inettive è una funzione iniettiva. ❑

Osservazione 6.11. La proposizione precedente mostra che la relazione di *avere cardinalità minore o uguale* gode delle proprietà *riflessiva* e *transitiva*. Vedremo tra poco che gode anche della proprietà *antisimmetrica*.

Lemma 6.12. *Supponiamo che $X \subseteq Y \subseteq Z$ e che $|X| = |Z|$, allora $|Y| = |Z|$.*

Dimostrazione. Sia $f : Z \to X$ una bigezione. Poniamo $A_0 = Z - Y$ e $A_{n+1} = f(A_n)$, e si ponga $A = \bigcup_n A_n$. Osserviamo che $f(A) \subseteq A \cap Y$, e che f è una bigezione tra A e la sua immagine. Definiamo allora $g : Z \to Y$ ponendo

$$g(z) = \begin{cases} f(z) & \text{se } z \in A \\ z & \text{se } z \in Z - A \end{cases}$$

e proviamo che è una bigezione.
g è iniettiva, siano infatti $z_1, z_2 \in Z$, $z_1 \neq z_2$. Si hanno tre casi:

1. $z_1, z_2 \in A$. In questo caso, dato che f è iniettiva, $g(z_1) = f(z_1) \neq f(z_2) = g(z_2)$.
2. $z_1, z_2 \in Z - A$. In questo caso $g(z_1) = z_1 \neq z_2 = g(z_2)$.
3. $z_1 \in A$ e $z_2 \in Z - A$. In tal caso $g(z_1) = f(z_1) \in A$, mentre $g(z_2) = z_2 \in Z - A$ quindi $g(z_1) \neq g(z_2)$.

g è surgettiva. Sia $y \in Y$, allora o $y \in Y - A$ e allora $g(y) = y$, oppure $y \in A$. In questo caso esiste $i \in \mathbb{N}$ tale che $y \in A_i$, inoltre dato che $y \in Y$ e $A_0 = Z - Y$, sicuramente $i > 0$. Ma allora $A_i = f(A_{i-1})$, quindi esiste $z \in A_{i-1}$ tale che $f(z) = y$. Dato che $z \in A$ allora $g(z) = f(z) = y$. ❑

Teorema 6.13 (Cantor-Bernstein). *Siano X e Y due insiemi e supponiamo che $f : X \to Y$ e $g : Y \to X$ siano due funzioni iniettive. Allora esiste una funzione bigettiva $h : X \to Y$.*

Dimostrazione. Si osservi che $|X| = |f(X)|$ e che $|g(f(X))| = |f(X)|$ e quindi $|X| = |g(f(X))|$. D'altra parte, $g(f(x)) \subseteq g(Y) \subseteq X$, quindi per il lemma precedente (6.12) $|X| = |g(Y)|$. Dato che $|g(Y)| = |Y|$ segue la tesi. ❑

La tricotomia dei cardinali

Enunciamo senza dimostrare un importante teorema, la cuidimostrazione richiede tecniche che esulano dalle finalità del corso, ma che è comunque importante conoscere:

Teorema 6.14 (tricotomia dei cardinali). *Per ogni coppia di insiemi X, Y si ha che o $|X| \leq |Y|$ oppure $|Y| \leq |X|$.*

Osservazione 6.15. Come era naturale aspettarsi, la relazione di *avere cardinalità minore o uguale* gode di tutte le proprietà di un ordinamento totale.

che mostra come la relazione di *avere cardinalità minore o uguale* goda di tutte le proprietà di un ordinamento totale

Il procedimento diagonale di Cantor

Le cardinalità finite e numerabile **non** esauriscono tutte le possibili cardinalità, il seguente teorema dimostra che esistonoo insiemi di cardinalità arbitrariamente elevata.

Teorema 6.16 (Cantor). *Per ogni X si ha che $|X| < \left|2^X\right|$.*

Dimostrazione. La funzione $f : X \to 2^X$ definita da $f(x) = \{x\}$ è iniettiva. Se $f : X \to 2^X$ è una qualsiasi funzione allora non è surgettiva, infatti l'insieme $\{x \in X \mid x \notin f(x)\}$ non appartiene all'immagine di f. ❑

Osservazione 6.17. La tecnica di dimostrazione usata in questo teorema è nota come procedimento diagonale. Il perché di tale nome appare chiaro se consideriamo la dimostrazione nel caso particolare di $\mathbb{N}$. Supponiamo di avere una numerazione di sottinsiemi di $\mathbb{N}$, rappresentiamo ogni sottinsieme di $\mathbb{N}$ con una successione di 0 e 1 (mettiamo un 1 in corrispondenza degli elementi che appartengono al sottinsieme e uno 0 altrimenti, cfr. esercizio 2.2)

		0	1	2	3	4	5	6	...
$f(0)$	=	**1**	0	0	1	1	0	0	...
$f(1)$	=	0	**0**	1	1	0	1	1	...
$f(2)$	=	1	0	**0**	0	1	0	1	...
$f(3)$	=	1	1	1	**1**	0	0	0	...
$f(4)$	=	0	0	0	1	**1**	1	1	...
$f(5)$	=	1	1	1	0	0	**0**	0	...
$f(6)$	=	1	0	1	1	1	1	**0**	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
A	=	0	1	1	0	0	1	1	...

Costruiamo una nuova successione di 0 e 1 ponendo all'n-esimo posto uno 0 se all'n-esimo posto di $f(n)$ c'è un 1, e 1 altrimenti. Chiaramente tale successione è diversa da ciascuna delle $f(n)$. La successione così costruita rappresenta proprio l'insieme $\{n \in \mathbb{N} \mid n \notin f(n)\}$.

Esempio 6.18. La stessa tecnica diagonale può essere usata per provare che l'insieme dei numeri reali è più che numerabile. Si supponga di avere un'applicazione $f : \mathbb{N} \to (0, 1)$, e per ogni n sia ε_n la n-esima cifra dello sviluppo decimale infinito di $f(n)$. Si ponga

$$\delta_n = \begin{cases} 1 & \text{se } \varepsilon_n \text{ è pari} \\ 2 & \text{se } \varepsilon_n \text{ è dispari} \end{cases}$$

Si costruisca quindi il numero reale r che ha δ_n come n-esima cifra del suo sviluppo decimale.

$f(0)$	=	0.	**1**	4	9	2	2	0	3	...
$f(1)$	=	0.	2	**3**	7	2	7	2	1	...
$f(2)$	=	0.	1	3	**2**	1	8	2	5	...
$f(3)$	=	0.	8	1	7	**6**	1	7	8	...
$f(4)$	=	0.	7	6	8	3	**8**	9	5	...
$f(5)$	=	0.	5	7	6	5	7	**1**	3	...
$f(6)$	=	0.	4	9	9	4	3	1	**4**	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
r	=	0.	2	2	1	1	1	2	1	...

Chiaramente, questo numero sta nell'intervallo $(0,1)$ ma è diverso da tutti gli $f(n)$. in quanto differisce da $f(n)$ nella n-esima cifra decimale. Per concludere, si osserva che $|(0,1)| = |\mathbb{R}|$ (cfr. esercizio 6.7). Si può in realtà dimostrare che $|\mathbb{R}| = 2^{\aleph_0}$ (cfr. esercizio 6.10).

Esercizio 6.7. Si provi che $|(0,1)| = |\mathbb{R}|$.

Esercizio 6.8. Siano $Y \subseteq X$. Si provi che se $|X| > |Y| = \aleph_0$ allora $|X - Y| = |X|$.

Esercizio 6.9. Siano $F = \{A \in 2^{\mathbb{N}} \mid A \text{ è finito}\}$. Si provi che $|F| = \aleph_0$

Esercizio 6.10. Si identifichi ogni numero reale in $(0,1)$ con la successione di 1 e 0 data del suo sviluppo binario, scegliendo quello infinito nei casi di ambiguità (i.e. $0.11 = 0.10111\ldots$) e si usino i due esercizi precedenti per provare che $|\mathbb{R}| = \left|2^{\mathbb{N}}\right|$.

Lezione 7 (19 marzo 2001 h. 9.30-10.30

Operazioni tra cardinalità

Sebbene non abbiamo dato la definizione di cardinalità di un insieme, (abbiamo dato significato al simbolo $|X|$ solo nel caso finito (definizione 4.2)), con una serie di esercizi, vediamo come si possano ugualmente definire delle operazioni tra cardinalità.

Esercizio 7.1. Supponiamo che $|X| = |X'|$ e che $|Y| = |Y'|$ allora

1. $|X \times Y| = |X' \times Y'|$
2. $\left|X^Y\right| = \left|{X'}^{Y'}\right|$
3. $|(X \times \{0\}) \cup (Y \times \{1\})| = |(X' \times \{0\}) \cup (Y' \times \{1\})|$

L'esercizio precedente permette di dare la seguente

Definizione 7.1. Se X e Y sono insiemi, si definiscono

1. $|X| + |Y| = |(X \times \{0\}) \cup (Y \times \{1\})|$
2. $|X|\,|Y| = |X \times Y|$
3. $|X|^{|Y|} = \left|X^Y\right|$

Esercizio 7.2. Si provi che le operazioni appena definite, nel caso di insiemi finiti, coincidono con le usuali operazioni tra numeri naturali.

Esercizio 7.3. Si provi che $2^{|X|} = \left|2^X\right|$.

Lasciamo come esercizio la dimostrazione del fatto che queste operazioni verificano tutte le propruietà delle usuali operazioni tra numeri naturali.

Esercizio 7.4. Si provino le seguenti:

1. $|X| + |Y| = |Y| + |X|$
2. $|X|\,|Y| = |Y|\,|X|$
3. $(|X| + |Y|) + |Z| = |X| + (|Y| + |Z|)$
4. $(|X|\,|Y|)\,|Z| = |X|\,(|Y|\,|Z|)$
5. $|X|\,(|Y| + |Z|) = (|X|\,|Y|) + (|X|\,|Z|)$
6. $|X|^{|Y|+|Z|} = |X|^{|Y|}\,|X|^{|Z|}$
7. $\left(|X|^{|Y|}\right)^{|Z|} = |X|^{|Y|\,|Z|}$

L'assioma di buon ordinamento

Definizione 7.2. Sia X un insieme e sia $\leq$ un ordinamento su X. Sia $A \subseteq X$, diremo che $z \in A$ è un *minimo* di A (in simboli $z = \min A$ se per ogni $x \in A$ si ha che $z \leq x$.

Definizione 7.3. Un ordinamento totale su un insieme X si dice un *buon ordinamento*, e in tal caso l'insieme ordinato $(X, \leq)$ si dice *ben ordinato* se ogni sottinsieme non vuoto di X ha minimo.

Teorema 7.4 (buon ordinamento). *L'ordinamento dei numeri naturali è un buon ordinamento.*

Dimostrazione. Supponiamo che l'insieme $A \subseteq \mathbb{N}$ non abbia minimo e proviamo che allora $A = \varnothing$. Chiamiamo B il suo complementare ($B = \mathbb{N} - A$) e dimostriamo per induzione che

$$\forall n \in \mathbb{N} \quad \{0, 1, \ldots, n\} \subseteq B$$

$0 \notin A$, altrimenti ne sarebbe il minimo, quindi $0 \in B$ e pertanto $\{0\} \subseteq B$.

Supponiamo che $\{0, 1, \ldots, n\} \subseteq B$, allora $0, 1, \ldots, n \notin A$ e quindi $n + 1 \notin A$, altrimenti ne sarebbe il minimo, ma allora $n+1 \in B$ e pertanto $\{0, 1, \ldots, n, n+1\} \subseteq B$.

Ma allora $B = \mathbb{N}$ e quindi $A = \varnothing$. ❑

Il principio di induzione (seconda forma)

Teorema 7.5 (seconda forma dell'induzione). *Sia $P(n)$ una famiglia di proposizioni indiciate su $\mathbb{N}$ e si supponga che*

1. *$P(0)$ sia vera*
2. *per ogni $n > 0$ ($P(k)$ vera $\forall k < n$) $\Rightarrow P(n+1)$*

allora $P(n)$ è vera per ogni $n \in \mathbb{N}$

Dimostrazione. Sia $A = \{n \in \mathbb{N} \mid P(n) \text{ non è vera}\}$, e supponiamo per assurdo che $A \neq \varnothing$. Allora per la proprietà di buon ordinamento (7.4) A ha minimo n. Chiaramente $n \neq 0$ in quanto $P(0)$ è vera. Inoltre se $k < n$ allora $k \notin A$ in quanto $n = \min A$, ma allora dalla (2) segue che $P(n)$ è vera e quindi $n \notin A$, contraddicendo il fatto che $n \in A$. ❑

Osservazione 7.6. Si osservi che sia l'enunciato che la dimostrazione precedenti non usano il fatto che si stia parlando di numeri naturali, ma soltanto che si sta lavorando in un insieme bene ordinato. Quindi il principio di induzione in questa forma è applicabile ad ogni insieme bene ordinato.

La divisione euclidea

Nel seguito denoteremo con $\mathbb{Z}$ l'insieme dei *numeri interi*. Supporremo nota la sua definizione e la definizione delle operazioni tra i suoi elementi. Ci limitiamo a dire che gli interi e le operazioni tra interi possono essere definiti a partire dai naturali e dalle operazioni tra naturali.

Teorema 7.7. *Siano $n, m \in \mathbb{Z}$ con $m \neq 0$, allora esistono unici $q, r \in \mathbb{Z}$ tai che*

$$\begin{aligned} n &= mq + r \\ 0 &\leq r < |m| \end{aligned}$$

Dimostrazione. Esistenza. Supponiamo dapprima che $n, m \in \mathbb{N}$, ed usiamo il principio di induzione nella seconda forma (teorema 7.5) su n. Se $n = 0$ basta prendere $q = 0$ e $r = 0$. Supponiamo $n > 0$ e che la tesi sia vera per ogni $k < n$. Se $n < m$ basta prendere $q = 0$ e $r = n$, altrimenti sia $k = n - m$, dato che $m \neq 0$ $0 \leq k < n$, quindi per ipotesi di induzione esistono $q, r \in \mathbb{N}$ tali che

$$\begin{aligned} k &= mq + r \\ 0 &\leq r < m \end{aligned}$$

ma allora $n = k + m = mq + r + m = (q + 1)m + r$.

Supponiamo ora $n < 0$ e $m > 0$. Allora $-n > 0$ e quindi per il caso precedente si ha che esistono $q, r \in \mathbb{Z}$ tali che $-n = mq + r$ e $0 \leq r < m = |m|$. E quindi $n = m(-q) - r$. Se $r = 0$ abbiamo finito, se invece $0 < r < m$ allora $0 < m - r < m = |m|$ e $n = m(-q) - r = m(-q) - m + m - r = m(-1 - q) + (m - r)$.

Sia infine $m < 0$ allora $-m > 0$, quindi per i due casi precedenti esistono $q, r \in \mathbb{Z}$ tali che $n = (-m)q + = m(-q) + r$ con $0 \leq r < -m = |m|$.

Unicità. Supponiamo che $n = mq + r$ e $n = mq' + r'$ con $0 \leq r, r' < m$. Supponiamo che $r' \geq r$, allora $m(q - q') = r' - r$ e quindi passando ai moduli si ha $|m|\,|q - q'| = |r' - r| = r' - r < |m|$,da cui $0 \leq |q - q'| < 1$ e quindi $|q - q'| = 0$ ovvero $q = q'$. Ma allora da $mq + r = mq' + r'$ segue che anche $r = r'$. ❑

Lezione 8 (21 marzo 2001 h. 10.30-11.30)

Scrittura in base arbitraria dei naturali.

Definizione 8.1. Sia $b\mathbb{N}$. Diremo che $n \in \mathbb{N}$ è *rappresentabile in base* b se esistono numeri $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_k \in \{0, 1, \ldots, b - 1\}$ tali che $n = \varepsilon_0 + \varepsilon_1 b + \varepsilon_2 b^2 + \ldots \varepsilon_k b^k$.

Osservazione 8.2. La rappresentabilità in base b può essere espressa anche nel seguente modo: esiste una successione $\{\varepsilon_i\}_{i \in \mathbb{N}}$ di interi tali che:

1. $\{\varepsilon_i\}$ è definitivamente nulla (i.e. esiste $i_0 \in \mathbb{N}$ tale che $\varepsilon_i = 0$ per ogni $i > i_0$);
2. $0 \leq \varepsilon_i < b$ per ogni $i \in \mathbb{N}$;
3. $n = \sum_{i=0}^{\infty} \varepsilon_i b^i$.

Questo perché la condizione (1) implica che la somma in (3) ha un numero finito di addendi non nulli.

Osservazione 8.3. Si osservi che l'unico numero rappresentabile in base 1 è lo 0. In questo caso infatti la condizione (2) implica che ogni $\varepsilon_i = 0$.

Teorema 8.4 (scrittura dei naturali in base arbitraria). *Sia $b\mathbb{N}$. Allora ogni $n \in \mathbb{N}$ è rappresentabile in modo unico in base b. Ossia esiste esiste una successione $\{\varepsilon_i\}_{i \in \mathbb{N}}$ come nell'osservazione precedente (8.2) e se $\{\varepsilon'_i\}_{i \in \mathbb{N}}$ è un'altra tale successione, allora $\varepsilon_i = \varepsilon'_i$ per ogni $i \in \mathbb{N}$.*

Dimostrazione. Dimostriamo l'esistenza per induzione su n. Se $n = 0$ basta prendere $\varepsilon_i = 0$ per ogni $i \in \mathbb{N}$. Supponiamo ora $n > 0$ e che la tesi sia vera per ogni $k < n$. Siano q, r tali che $n = bq + r$ con $0 \leq r < b$. Dato che $b \geq 2$ si ha che $0 \leq q < bq \leq bq + r = n$ e quindi per ipotesi di induzione esiste una successione definitivamente nulla $\{\delta_i\}$, costituita di interi tali che $0 \leq \delta_i < b$ per ogni i e tale che $q = \sum_{i=0}^{\infty} \delta_i b^i$. Ma allora

$$n = bq + r = b \sum_{i=0}^{\infty} \delta_i b^i + r = \sum_{i=0}^{\infty} \delta_i b^{i+1} + r = \sum_{i=1}^{\infty} \delta_{i-1} b^i + r = \sum_{i=0}^{\infty} \varepsilon_i b^i$$

dove si è posto $\varepsilon_0 = r$ e $\varepsilon_i = \delta_{i-1}$ per ogni $i > 0$. La successione $\{\varepsilon_i\}$ è definitivamente nulla, dato che lo è $\{\delta_i\}$ ed inoltre $0 \leq \varepsilon_i = \delta_{i-1} < b$ per ogni $i > 0$ e $0 \leq \varepsilon_0 = r < b$.

Dimostriamo ora l'unicità. Procediamo per induzione su n. Se $n = 0 = \sum_i \varepsilon_i b^i$ allora ogni addendo della somma essendo non negativo, deve essere nullo e quindi $\varepsilon_i = 0$ per ogni i.

Supponiamo ora $n > 0$ e che l'espressione in base b sia unica per tutti i numeri $k < n$. Sia n tale che $n = \sum_{i=0}^{\infty} \varepsilon_i b^i = \sum_{i=0}^{\infty} \varepsilon'_i b^i$. Allora possiamo scrivere

$$n = b \sum_{i=1}^{\infty} \varepsilon_i b^{i-1} + \varepsilon_0 = b \sum_{i=1}^{\infty} \varepsilon'_i b^{i-1} + \varepsilon'_0$$

ma per l'unicità della divisione euclidea (teorema 7.7) si ha che $\varepsilon_0 = \varepsilon'_0$ e $q = \sum_{i=1}^{\infty} \varepsilon_i b^{i-1} = \sum_{i=1}^{\infty} \varepsilon'_i b^{i-1}$. Come prima $q < n$ e quindi per ipotesi di induzione si ha anche che $\varepsilon_i = \varepsilon'_i$ per ogni $i \geq 1$. ∎

Il coefficiente binomiale

Definizione 8.5. Siano $n, k \in \mathbb{N}$ con $k \leq n$ si pone

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

Osservazione 8.6. È immediato verificare che $\binom{n}{k} = \binom{n}{n-k}$.

Esercizio 8.1. Provare che

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

k-sottinsiemi

Definizione 8.7. Sia X un insieme e $k \in \mathbb{N}$, un sottinsieme $A \subseteq X$ sarà detto un *k-sottinsieme* se $|A| = k$. Denoteremo con $\binom{X}{k}$ l'insieme dei k-sottinsiemi di X. I k-sottinsiemi sono anche chiamati *k-combinazioni semplici*.

Proposizione 8.8. *Se X è finito e $k \leq |X|$, allora*

$$\left|\binom{X}{k}\right| = \binom{|X|}{k}.$$

Dimostrazione. Procediamo per induzione su $|X|$. Se $|X| = 0$ allora $k = 0$ e $X = \varnothing$. Ma allora

$$\left|\binom{\varnothing}{0}\right| = |\{\varnothing\}| = 1 = \binom{0}{0} = \binom{|\varnothing|}{0}.$$

Supponiamo ora che $|X| > 0$. Se $k = |X|$, allora $\binom{X}{k} = \{X\}$ e quindi $\left|\binom{X}{k}\right| = 1$. D'altra parte anche $\binom{|X|}{k} = 1$. ANche il caso $k = 0$ è facile. Supponiamo allora $0 < k < |X|$. Fissiamo $x_0 \in X$ un elemento e poniamo

$$\begin{aligned} \mathcal{A}_1 &= \{A \subset X \mid |A| = k \text{ e } x_0 \in A\} \\ \mathcal{A}_2 &= \{A \subset X \mid |A| = k \text{ e } x_0 \notin A\} \end{aligned}$$

chiaramente si ha

$$\binom{X}{k} = \mathcal{A}_1 \cup \mathcal{A}_2, \qquad \mathcal{A}_1 \cap \mathcal{A}_2 = \varnothing$$

da cui $\left|\binom{X}{k}\right| = |\mathcal{A}_1| + |\mathcal{A}_2|$)cfr esercizio4.2). Posto $X' = X - \{x_0\}$ si ha che

$$\mathcal{A}_2 = \binom{X'}{k}. \tag{7}$$

inoltre la funzione $F : \binom{X'}{k-1} \to \mathcal{A}_1$ definita da $F(A) = A \cup \{x_0\}$ è una bigezione e quindi, dato che $|X'| = |X| - 1$, per ipotesi di induzione si ha

$$\begin{aligned} |\mathcal{A}_1| &= * \left|\binom{X'}{k-1}\right| = \binom{|X'|}{k-1} \\ |\mathcal{A}_2| &= * \left|\binom{X'}{k}\right| = \binom{|X'|}{k} \end{aligned}$$

Ma allora, usando il risultato dell'esercizio 8.1

$$\left|\binom{X}{k}\right| = \binom{|X'|}{k-1} + \binom{|X'|}{k} = \binom{|X'|+1}{k} = \binom{|X|}{k}.$$

□

Esercizio 8.2. Provare che

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

Perché non gioco al Superenalotto!

Una sestina al Superenalotto, è un sottinsieme di 6 elementi dell'insieme dei numeri naturali da 1 a 90, quindi, per la proposizione 8.8 il numero di sestine possibili è dato da:

$$\binom{90}{6} = 622614630$$

Pertanto, la probabilità di vincere giocando una sestina è pari a $1/622614630 = 0.000000161$ % di vincere giocando una sestina. Se quindi il gioco fosse equo, la puntata su una giocata dovrebbe essere pagata 622614630 volte la posta. Dato che la puntata su una sestina costa 800 L., mi aspetterei, in caso di successo, un premio di $800 \cdot 622614630 = 498091704000$ L.

Un montepremi così alto non si è ancora visto!

Lezione 9 (26 marzo 2001 h. 9.30-10.30)

Divisibilità e sue prime proprietà

Definizione 9.1. Dati due interi n, m si dice che n è un *divisore* di m (o che m è un *multiplo* di n) se esiste un $k \in \mathbb{Z}$ tale che $m = nk$. Si indica con $n \mid m$ (si legge *n divide m*).

Esempio 9.2. $n \mid 0$ per ogni n mentre se $n \neq 0$ allora $0 \not| n$, si ha inoltre che $\pm 1 \mid n$ e $\pm n \mid n$ per ogni n.

Proposizione 9.3.

1. *Se $n \mid m$ e $m \mid q$ allora $n \mid q$.*
2. *Se $n \mid m$ e $m \mid n$ allora $n = \pm m$.*

Dimostrazione. 1. Se $m = kn$ e $q = hm$ allora $q = hkm = (hk)m$ ossia $n \mid q$.

2. Se $n = mk$ e $m = nh$ allora $m = hkm$ e quindi $m(1 - hk) = 0$ e quindi o $m = 0$ e quindi anche $n = 0$, oppure $1 - hk = 0$ ma allora o $h = k = 1$ e quindi $n = m$ oppure $n = m = -1$ e quindi $n = -m$. ❑

Definizione 9.4. Il numero n si dice *primo* se i suoi unici divisori sono $\pm 1, \pm n$.

Il massimo comun divisore: definizione, esistenza e unicità

Definizione 9.5. Dati due interi n, m non entrambi nulli, si dice che d è *un massimo comun divisore*tra n e m se:

1. $d \mid n$ e $d \mid m$;
2. Se $c \mid n$ e $c \mid m$ allora $c \mid d$.

Proposizione 9.6. *Se d e d' sono due massimi comun divisori tra n e m allora $d' = \pm d$.*

Dimostrazione. d è un divisore comune di n e m, quindi poiché d' è un massimo comun divisore si ha che $d \mid d'$. Scambiando i ruoli di d e d' si ha allora che anche $d' \mid d$ e quindi per 9.3 si ha che $d' = \pm d$. ❑

Definizione 9.7. Diremo che d è *il massimo comun divisore* di n e m se è un massimo comun divisore positivo. La proposizione precedente garantisce che se esiste il massimo comun divisore è unico. Esso verrà indicato con (n, m).

Teorema 9.8. *Dati due numeri $n, m \in \mathbb{Z}$ non entrambi nulli esiste il massimo comun divisore di n ed m.*

Dimostrazione. Si consideri l'insieme $S = \{s \in \mathbb{Z} \mid s > 0, \exists\, x, x \in \mathbb{Z} : s = nx+my\}$. $S \neq \varnothing$ dato che $nn + mm > 0$ (dato che n e m non sono entrambi nulli). Sia $d = nx + my = \min S$, dimostriamo che d è il massimo comun divisore. Se $c \mid n$ e $c \mid m$ allora $n = ck$ e $m = ch$, quindi $d = nx + my = ckx + chy = c(kx + hy)$ ossia $c \mid d$. Dimostriamo ora che $d \mid n$. Consideriamo la divisione euclidea tra n e d ossia $n = dq + r$ con $0 \leq r < d$, se $r > 0$ allora $r = n - dq = n - (nx + my)q = n(1 - qx) + (-m)y$ è un elemento di S. Ciò è assurdo perché $r < d$ e $d = \min S$. Quindi $r = 0$ ossia $d \mid n$. In modo analogo si prova che $d \mid m$. ❑

Osservazione 9.9. Dalla dimostrazione precedente segue che dati $n, m \in \mathbb{Z}$ esistono $x, y \in \mathbb{Z}$ tali che $(n, m) = nx + my$ e che gli interi della forma $nx + my$ con $x, y \in \mathbb{Z}$ sono tutti e soli i multipli di (n, m).

Definizione 9.10. $n, m \in \mathbb{Z}$ non entrambi nulli si dicono *coprimi* se $(n, m) = 1$.

Osservazione 9.11. $(n, m) = 1$ se e solo se esistono $x, y \in \mathbb{Z}$ tali che $nx + my = 1$. Ad esempio $(n, n + 1) = 1$ per ogni n. Infatti $1 = (n + 1)1 + n(-1)$.

Proposizione 9.12. *Sia $d = (n, m)$, allora $(\frac{n}{d}, \frac{m}{d}) = 1$.*

Dimostrazione. $d = nx + my$ e quindi $1 = \frac{n}{d}x + \frac{m}{d}y$. ❑

L'algoritmo di Euclide per il calcolo del M.C.D.

Proposizione 9.13 (algoritmo di Euclide). *Siano $n, m \in \mathbb{Z}$, $m \neq 0$. Sia $n = mq + r$ la divisione euclidea di n per m allora $\{c \in \mathbb{Z} \mid c \mid n \text{ e } c \mid m\} = \{c \in \mathbb{Z} \mid c \mid m \text{ e } c \mid r\}$, in particolare quindi $(n, m) = (m, r)$.*

Dimostrazione. Se $c \mid n$ e $c \mid m$ allora $n = ch$ e $m = ck$ e quindi $r = n - mq = ch - ckq = c(h - kq)$ ossia $c \mid r$ e $c \mid m$. Viceversa se $c \mid r$ e $c \mid m$ allora $m = ch$ e $r = ck$ e quindi $n = mq + r = chq + ck = c(hq + r)$ ossia $c \mid n$ e $c \mid m$. ❑

La proposizione precedente assieme all'osservazione che $(n, 0) = n$ per ogni $n \neq 0$ permette di costruire un algoritmo (*algoritmo di Euclide*) per il calcolo del M.C.D.

ALGORITMO DI EUCLIDE
- INPUT: n, $m \in \mathbb{Z}$.
- $n = 0 \Rightarrow$ OUTPUT: m
- $m = 0 \Rightarrow$ OUTPUT: n
- $n \neq 0$ e $m \neq 0$ esegui la divisione euclidea $n = mq + r$ e applica l'algoritmo di Euclide a m, r.

Lezione 10 (28 marzo 2001 h. 10.30-11.30)

Proprietà dei numeri coprimi e caratterizzazione dei numeri primi

Proposizione 10.1.

1. *se $(n, m) = 1$ e $n \mid mq$ allora $n \mid q$.*
2. *se $(n, m) = 1$ e $n \mid q$ e $m \mid q$ allora $nm \mid q$.*

Dimostrazione. 1. Se $(n, m) = 1$ allora esistono $x, y \in \mathbb{Z}$ tali che $1 = nx + my$ e quindi $q = nqx + mqy$. Ma allora se $n \mid mq$ esiste h tale che $mq = nh$ e quindi $q = nqx + nhy = n(qx + hy)$.

2. $n \mid q$ quindi $q = nh$, dato che $m \mid q = nh$ e $(n, m) = 1$ allora per la 1 si ha che $m \mid h$ ossia $h = km$ e quindi $q = nh = nmk$, ovvero $nm \mid q$. ❑

Corollario 10.2. *p è primo se e solo se per ogni $n, m \in \mathbb{Z}$ si ha che $p \mid nm \Rightarrow p \mid n$ oppure $p \mid m$.*

Dimostrazione. Supponiamo che $p \mid nm$, dato che p è primo, se $p \not| n$ allora $(p, n) = 1$, per lo proposizione precedente si ha allora che $p \mid m$.

Viceversa supponiamo che per ogni $n, m \in \mathbb{Z}$ si ha che $p \mid nm \Rightarrow p \mid n$ oppure $p \mid m$, allora se $p = dh$ allora $p \mid dh$ e quindi $p \mid d$, e quindi per 9.3 si ha che $d = \pm p$ e $h = \pm 1$ oppure $p \mid h$ e quindi $h = \pm p$ e $d = \pm 1$. ❑

Esercizio 10.1. Siano $n_1, \ldots, n_k \in \mathbb{Z}$ e sia p un primo tale che $p \mid n_1 n_2 \ldots n_k$. Si provi che allora esiste i tale che $p \mid n_i$.

Il minimo comune multiplo: definizione, esistenza e unicità

Definizione 10.3. Dati due interi $n, m \in \mathbb{Z}$ si dice che M è un minimo comune multiplo di n e m se

1. $n \mid M$ e $m \mid M$;
2. se $n \mid c$ e $m \mid c$ allora $M \mid c$.

Come nel caso del massimo comun divisore si dimostra che due minimi comuni multipli sono uguali a meno del segno e quindi si chiama *il minimo comune multiplo* quello positivo e sarà indicato con $[n, m]$.

Teorema 10.4 (esistenza del m.c.m.). *Siano $n, m \in \mathbb{Z}$ non entrambi nulli allora esiste il minimo comune multiplo tra n e m.*

Dimostrazione. Sia $M = \frac{nm}{(n,m)} = n'm'(n,m)$ dove si è posto $n = n'(n,m)$ e $m = m'(n,m)$. Chiaramente allora $M = nm' = n'm$ e quindi $n \mid M$ e $m \mid M$.

Se $n \mid c$ e $m \mid c$ allora $(n,m) \mid c$ e quindi posto $c = c'(n,m)$ si ha che $n' \mid c'$ e $m' \mid c'$. Dato che $(n', m') = 1$, per 10.1 si ha che $n'm' \mid c'$ e quindi che $M = n'm'(n,m) \mid c'(n,m) = c$. ❑

Esercizio 10.2. Si generalizzino al caso di più di due interi le definizioni di MCD e mcm tra due interi, e se ne dimostrino esistenza e unicità.

Esercizio 10.3. Denotando con $(n_1, n_2, \ldots, n_k)$ e con $[n_1, n_2, \ldots, n_k]$ rispettivamente il massimo comun divisore ed il minimo comune multiplo tra gli interi $n_1, n_2, \ldots, n_k$ (cfr. esercizio precedente), si provi che:

1. $(n_1, \ldots, n_k, n_{k+1}) = ((n_1, \ldots, n_k), n_{k+1})$
2. $[n_1, \ldots, n_k, n_{k+1}] = [[n_1, \ldots, n_k], n_{k+1}]$

Il teorema fondamentale dell'Aritmetica

Teorema 10.5 (Teorema fondamentale dell'aritmetica). *Per ogni $n \in \mathbb{Z}, n \geq 2$ esistono numeri primi $p_1, p_2, \ldots, p_k > 0$ tali che $n = p_1 p_2 \ldots p_k$. Se anche $q_1, \ldots, q_h$ sono primi positivi tali che $n = q_1 q_2 \ldots q_h$, esiste una bigezione $\sigma : \{1, 2, \ldots, h\} \to \{1, 2, \ldots, k\}$ tale che $q_i = p_{\sigma(i)}$.*

In altre parole, ogni intero maqggiore di 1 si scrive in modo unico, a meno dell'ordine, come prodotto di numeri primi positivi.

Dimostrazione. Procediamo per induzione su n. Se $n = 2$ non c'è nulla da dimostrare in quanto 2 è primo. Supponiamo $n > 2$ e che la tesi sia vera per ogni $k < n$. Se n è primo non c'è nulla da dimostrare, se n non è primo allora esistono due numeri $d_1 d_2$ con $1 < d_1, d_2 < n$ tali che $n = d_1 d_2$. Per ipotesi di induzione esistono dei primi positivi p_i e q_j tali che $d_1 = p_1 \ldots p_{k_1}$ e $d_2 = q_1 \ldots q_{k_2}$, ma allora $n = p_1 \ldots p_{k_1} q_1 \ldots q_{k_2}$ è prodotto di primi positivi.

Unicità. Sia $n = p_1 \ldots p_k = q_1 \ldots q_h$ con p_i e q_j primi positivi e $k \leq h$. Procediamo per induzione su k. Se $k = 1$ allora $n = p_1 = q_1 \ldots q_h$, quindi $q_j \mid p_1$ per ogni j, e dato che p_1 è primo ogni $q_j = 1$ oppure $q_j = p_1$. Poiché per ipotesi ogni $q_j > 1$ allora $q_j = p_1$ per ogni j. Se ora fosse $h > 1$ si avrebbe $n = q_1 \ldots q_h \geq q_1 q_2 = p_1^2 > p_1 = n$ e questo è assurdo, e quindi $h = 1$ e $q_1 = p_1$.

Sia $k > 1$, allora $p_k \mid n = q_1 \ldots q_h$, quindi per l'esercizio 10.1 esiste un j tale che $p_k \mid q_j$. Dato che sia p_k che q_j sono primi positivi, allora $p_k = q_j$. Ma allora $p_1 \ldots p_{k-1} = q_1 \ldots q_{j-1} q_{j+1} \ldots q_h$, per ipotesi di induzione possiamo allora dire che le due fattorizzazioni hanno lo stesso numero di elementi, ossia $k - 1 = h - 1$, e che

esiste una bigezione $\delta : \{1, \ldots, j-1, j+1, \ldots, k\} \to \{1, \ldots, k-1\}$ tale che $q_i = p_{\delta(i)}$ per ogni i. Definendo allora $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$

$$\sigma(i) = \begin{cases} k & \text{se } i = j \\ \delta(i) & \text{se } i \neq j \end{cases}$$

si ottiene una bigezione tale che $q_i = p_{\sigma(i)}$ per ogni i. ❑

Esistenza di infiniti numeri primi

Corollario 10.6. *I numeri primi sono infiniti.*

Dimostrazione. Per assurdo supponiamo che $p_1, p_2, \ldots, p_n$ siano tutti iprimi. Si consideri $n = p_1 p_2 \ldots p_n + 1$. Chiaramente $n > 1$ e non è divisibile per nessun p_i e quindi n sarebbe un numero maggiore di 1 che non è divisibile per nessun primo e ciò contraddice il teorema fondamentale dell'aritmetica (10.5). ❑

Esercizio 10.4. [Calcolo del M.C.D. e del m.c.m. usando la fattorizzazione in primi] Se $a, b \in \mathbb{N}$ denotiamo con $a \vee b = \max\{a, b\}$ e con $a \wedge b = \min\{a, b\}$.

Siano $n = \prod_{i=1}^{s} p_i^{k_i}$, $m = \prod_{i=1}^{s} p_i^{h_i}$ con p_i numeri primi, allora $(n, m) = \prod_{i=1}^{s} p_i^{k_i \wedge h_i}$ e $[n, m] = \prod_{i=1}^{s} p_i^{k_i \vee h_i}$.

Lezione 11 (29 marzo 2001 h. 10.30-11.30)

Definizione di congruenza e prime proprietà

Definizione 11.1. Siano $a, b \in \mathbb{Z}$, si dice che a è congruo a b modulo n (in simboli $a \equiv b \mod n$) se $n \mid a - b$.

Proposizione 11.2. *Valgono le seguenti proprietà:*

1. *(proprietà riflessiva)* $a \equiv a \mod n$ *per ogni* $a, n \in \mathbb{Z}$*;*
2. *(proprietà simmetrica)* $a \equiv b \mod n \Rightarrow b \equiv a \mod n$ *per ogni* $a, b, n \in \mathbb{Z}$*;*
3. *(proprietà transitiva)* $a \equiv b \mod n$ *e* $b \equiv c \mod n \Rightarrow a \equiv c \mod n$ *per ogni* $a, b, c, n \in \mathbb{Z}$*.*

Dimostrazione. 1. $n \mid 0 = a - a$ per ogni $n \in \mathbb{Z}$.

2. Se $n \mid a - b$ allora $a - b = kn$ e quindi $b - a = (-k)n$ e quindi $n \mid b - a$ ossia $b \equiv a \mod n$.

3. Se $a \equiv b \mod n$ e $b \equiv c \mod n$ allora $a - b = kn$ e $b - c = hn$ e quindi $a - c = a - b + b - c = kn + hn = (k + h)n$ e quindi $a \equiv c \mod n$. ❑

Ricordiamo la definizione di relazione d'equivalenza su un insieme.

Definizione 11.3. Una relazione $\mathcal{R}$ su X si dice *d'equivalenza* se

1. è *riflessiva*, ossia $\forall x \in X \; x \mathcal{R} x$;
2. è *simmetrica*, ossia $\forall x, y \in X \; x \mathcal{R} Y \Rightarrow y \mathcal{R} \S$
3. è *transitiva*, ossia $\forall x, y, z \in X \; (x \mathcal{R} y \text{ e } y \mathcal{R} z) \Rightarrow x \mathcal{R} z$.

Osservazione 11.4. È prassi comune denotare le relazioni d'equivalenza con simboli del tipo $\sim$, $\equiv$, $\approx$ e simili.

Osservazione 11.5. La proposizione precedente (11.2) può essere allora rienunciato dicendo che *la relazione di congruenza modulo n è una relazione d'equivalenza su $\mathbb{Z}$.*

Classi d'equivalenza

Definizione 11.6. Siano X un insieme, $\sim$ una relazione d'equivalenza su X e $x \in X$. Si chiame *classe d'equivalenza* di x in X rispetto a $\sim$, l'insieme:

$$[x]_{\sim} = \{y \in x \mid y \sim x\}.$$

Quando non ci sarà ambiguità, si scriverà semplicemente $[x]$ invece che $[x]_{\sim}$.

L'isieme costituito da tutte le classi d'equivalenza si chiama *insieme quoziente di X modulo $\sim$* e si denota con il simbolo $X/\sim$, quindi:

$$X/\sim = \{[x]_{\sim} \mid x \in X\}.$$

Proposizione 11.7. Proposizione 11.8. *Sia X un insieme e sia $\sim$ una relazione d'equivalenza su X, allora*

1. *per ogni $x \in X$ $x \in [x]$*
2. *per ogni $x, y \in X$ $[x] = [y]$ se e solo se $x \sim y$.*
3. *per ogni $x, y \in X$ $[x] \cap [y] \neq \varnothing \Rightarrow [x] = [y]$.*

Dimostrazione. 1. Segue dalla proprietà riflessiva (1 di 11.3).

2. Se $[x] = [y]$ in particolare $y \in [y] = [x]$ e quindi $x \sim y$. Viceversa sia $x \sim y$. Se $z \in [x]$ allora $z \sim x$; per la proprietà transitiva (3 di 11.3) $z \equiv y$ ossia $z \in [y]$, ossia $[x] \subseteq [y]$. Scambiando i ruoli di x e y si ha anche l'inclusione opposta e quindi l'uguaglianza.

3. Se $z \in [x] \cap [y]$ allora $z \sim x$ e $z \sim y$, usando le proprietà simmetrica e transitiva si ha allora che $x \sim y$ e quindi, per la (2), appena dimostrata, $[x] = [y]$. ❑

Classi di congruenza

Definizione 11.9. Siano $a, n \in \mathbb{Z}$, si chiama classe di congruenza di a modulo n l'insieme

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a \mod n\}.$$

Indicheremo $\mathbb{Z}/_{n\mathbb{Z}} = \{\, [a]_n \mid a \in \mathbb{Z} \,\}$

Osservazione 11.10. Osserviamo che

$$x \equiv a \mod n \iff n \mid (x-a) \iff \exists\, k \in \mathbb{Z} : x - a = kn \iff \exists\, k \in \mathbb{Z} : x = a + kn$$

e quindi

$$[a]_n = \{a + kn \mid k \in \mathbb{Z}\}.$$

Osservazione 11.11. La classe di congruenza di a modulo n non è altro che la classe d'equivalenza di a rispetto alla relazione d'equivalenza (cfr. proposizione11.2) $\equiv \mod n$ e $\mathbb{Z}/_{n\mathbb{Z}}$ quindi è l'insieme quoziente di $\mathbb{Z}$ rispetto a tale relazione d'equivalenza.

In virtù di questa osservazione e della proposizione 11.8 si ha la seguente:

Proposizione 11.12. 1. *per ogni $a \in \mathbb{Z}$ $a \in [a]_n$*

2. *per ogni $a, b \in \mathbb{Z}$ $[a]_n = [b]_n$ se e solo se $a \equiv b \mod n$.*

3. *per ogni $a, b \in \mathbb{Z}$ $[a]_n \cap [b]_n \neq \varnothing \Rightarrow [a]_n = [b]_n$.*

Le classi modulo n sono esattamente n

Proposizione 11.13. *Se $n > 0$ e r è il resto della divisione euclidea di a per n allora $a \equiv r \mod n$.*

Dimostrazione. $a = nq + r$ quindi $n \mid nq = a - r$. ❑

Corollario 11.14. *Se $n > 0$ allora $\mathbb{Z}/n\mathbb{Z}$ ha esattamente n elementi.*

Dimostrazione. Da 11.13 e dalla 2 di 11.12 segue immediatamente che l'insieme in questione ha al più n elementi e precisamente $[0]_n, [1]_n, \ldots, [n-1]_n$. D'altra parte se $0 \leq h < k < n$ allora $0 < k - h < n$ e quindi $n \nmid (k - h)$ e quindi (sempre per la 2 di 11.12) $[h]_n \neq [k]_m$. ❑

Osservazione 11.15. La proposizione precedente spiega come mai le classi di congruenza modulo n vengono anche chiamate *classi di resto* modulo n.

Somma e prodotto di classi di congruenza

Proposizione 11.16. *Siano $a, b, a', b', n \in \mathbb{Z}$ e si supponga che $a \equiv a' \mod n$ e $b \equiv b' \mod n$. Allora*

1. *$a + b \equiv a' + b' \mod n$;*
2. *$ab \equiv a'b' \mod n$.*

Dimostrazione. (1). Se $n \mid (a - a')$ e $n \mid (b - b')$ allora $n \mid ((a - a') + (b - b')) = ((a + b) - (a' + b'))$.

(2). Esistono $k, h \in \mathbb{Z}$ tali che $a = a' + kn$ e $b = b' + hn$, ma allora, moltiplicando membro a membro si ottiene $ab = a'b' + a'hn + b'kn + hkn^2 = a'b' + n(a'h + b'k + hkn)$ e quindi la tesi. ❑

Osservazione 11.17. La proposizione precedente permette di definire le operazioni di somma e prodotto tra classi modulo n. Ponendo

$$\begin{aligned} [a]_n + [b]_n &= [a + b]_n \\ [a]_n [b]_n &= [ab]_n \end{aligned}$$

si ottengono delle buone definizioni. Infatti se $[a]_n = [a']_n$ e $[b]_n = [b']_n$ allora per la 2 di 11.12 si ha che $a \equiv a' \mod n$ e $b \equiv b' \mod n$ e quindi per la proposizione precedente si ha che $a + a' \equiv b + b' \mod n$ e $aa' \equiv bb' \mod n$ e quindi di nuovo per la 2 di 11.12 si ha che $[a + b]_n = [a' + b']_n$ e $[ab]_n = [a'b']_n$.

Nel seguito, quando parleremo di classi di congruenza e di operazioni tra esse, potrà succedere che, nella notazione, confonderemo la classe con uno dei suoi rappresentanti. Sarà chiaro dal contesto a cosa ci si starà riferendo. Ad esempio useremo indifferentemente una delle tre espressioni

$$\begin{gathered} 3 + 3 \equiv 0 \mod 6 \\ [3]_6 + [3]_6 = [0]_6 \\ 3 + 3 = 0 \text{ in } \mathbb{Z}/6\mathbb{Z} \end{gathered}$$

per indicare lo stesso concetto.

Esercizio 11.1. Si provino le seguenti proprietà delle operazioni tra classi di congruenza:

1. $([a] + [b]) + [c] = [a] + ([b] + [c])$

2. $([a]\,[b])\,[c] = [a]\,([b]\,[c])$
3. $[a] + [b] = [b] + [a]$
4. $[a]\,[b] = [b]\,[a]$
5. $[a] + [0] = [a]$
6. $[a]\,[-a] = [0]$
7. $[a]\,[1] = [a]$
8. $[a]\,([b] + [c]) = ([a]\,[b]) + ([a]\,[c])$

Osservazione 11.18. L'esercizio precedente, mostra che le operazioni tra classi di congruenza godono delle stesse proprietà di cui godono le operazioni tra interi. Attenzione però a due importanti differenze:

1. Ci possono essere classi diverse da 0 che moltiplicate tra loro danno 0, ad esempio
$$2 \cdot 3 = 0 \text{ in } \mathbb{Z}/6\mathbb{Z}$$
2. Se $n > 0$ allora
$$\underbrace{1 + 1 + \ldots + 1}_{n-\text{volte}} = 0 \text{ in } \mathbb{Z}/n\mathbb{Z}$$

Lezione 12 (2 aprile 2001 h. 9.30-10.30)

Il teorema cinese del resto

Teorema 12.1 (Cinese del resto). *Il sistema di congruenze*

$$\begin{cases} x & \equiv & a & \mod n \\ x & \equiv & b & \mod m \end{cases}$$

ha soluzione se e solo se $(n, m) \mid b - a$.

Se c è una soluzione del sistema, allora gli elementi di $[c]_{[n,m]}$ sono tutte e sole le soluzioni del sistema (i.e. le soluzioni sono tutte e sole della forma $c + k[n, m]$ al variare di $k \in \mathbb{Z}$).

Dimostrazione. Sia c una soluzione del sistema allora esistono $h, k \in \mathbb{Z}$ tali che $c = a + hn = b + km$ e quindi $a - b = km - hn$. Ma allora dal fatto che $(n, m) \mid n$ e $(n, m) \mid m$ si ha che $(n, m) \mid a - b$. Viceversa, supponiamo che $(n, m) \mid a - b$, allora, per quanto osservato in 9.9, esistono $h, k \in \mathbb{Z}$ tali che $a - b = hn + km$. Ma allora $a - hn = b + kn$, detto quindi $c = a - hn = b + kn$, si ha evidentemente che c risolve entrambe le congruenze.

Sia $S = \{x \in \mathbb{Z} \mid x \text{ risolve il sistema}\}$. Dobbiamo provare che se c è una soluzione allora $S = [c]_{[n,m]}$.

$S \subseteq [c]_{[n,m]}$. Sia c' un'altra soluzione, allora $c = a + hn = b + km$ e $c' = a + h'n = b + k'm$ e quindi sottraendo si ha

$$\begin{array}{rcll} c - c' & = & a + hn - a' - h'n = (h - h')n & \Rightarrow \quad n \mid (c - c') \\ c - c' & = & b + km - b' - k'm = (k - k')m & \Rightarrow \quad m \mid (c - c') \end{array}$$

Ma allora $[n, m] \mid c - c'$ ossia $c' \equiv c \mod [n, m]$ ovvero $c' \in [c]_{[n,m]}$.

$[c]_{[n,m]} \subseteq S$. Sia $c' \in [c]_{[n,m]}$, ovvero $c' = c + h[n, m]$. Dal fatto che $c \equiv a \mod n$ e che $h[n, m] \equiv 0 \mod n$ segue (per proposizione 11.16) che $c' = c + h[n, m] \equiv a \mod n$. In modo analogo si ha che $c' \equiv b \mod m$ e quindi che $c' \in S$. ∎

Esercizio 12.1. Siano $n_1, \ldots, n_k$ interi a due a due primi tra loro. Si provi che il sistema di congruenze

$$\begin{cases} x & \equiv & a_1 & \mod n_1 \\ x & \equiv & a_2 & \mod n_2 \\ & \vdots & & \\ x & \equiv & a_k & \mod n_k \end{cases}$$

ammette soluzione e che se c è una soluzione, tutte le altre sono del tipo $c + kn_1 \cdot \ldots \cdot n_k]$.

Esercizio 12.2. Siano $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_k$ le cifre della espressione decimale del numero n. Si provi che

1. $3 \mid n \iff 3 \mid (\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_k)$
2. $9 \mid n \iff 9 \mid (\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_k)$
3. $11 \mid n \iff 11 \mid (\varepsilon_0 - \varepsilon_1 + \ldots + (-1)^k \varepsilon_k)$

Elementi invertibili modulo n

Definizione 12.2. Sia $a \in \mathbb{Z}$ diremo che a è *invertibile modulo* n se esiste $x \in \mathbb{Z}$ tale che $ax \equiv 1 \mod n$ (in $\mathbb{Z}/n\mathbb{Z}$). Un tale x si dice un *inverso di* a *modulo* n.

Proposizione 12.3. *a è invertibile modulo n se e solo se $(a, n) = 1$.*

Dimostrazione. Se a è invertibile e x è un suo inverso, allora $n \mid (ax - 1)$, quindi esiste k tale che $nk = ax - 1$ e quindi $1 = nk - ax$, da cui (osservazione 9.11) $1 = (a, n)$.

Viceversa, se $1 = (a, n)$ allora esistono (osservazione 9.9) $\alpha, \beta \in \mathbb{Z}$ tali che $1 = a\alpha + n\beta$, ma allora $a\alpha \equiv 1 \mod n$. ❑

Proposizione 12.4. *Siano x, y due inversi di a modulo n, allora $x = y$ (in $\mathbb{Z}/n\mathbb{Z}$).*

Dimostrazione. Dal fatto che $ax = 1$ in $\mathbb{Z}/n\mathbb{Z}$, moltiplicando entrambi i membri per y, ed usando le proprietà associativa, commutativa e dell'1 (esercizio 11.1) si ottiene

$$[y]_n = [1]_n [y]_n = ([a]_n [x]_n) [y]_n = ([x]_n [a]_n) [y]_n = [x]_n ([a]_n [y]_n) = [x]_n [1]_n = [x]_n$$

❑

Proposizione 12.5. *Sia a invertibile modulo n e sia $a' = a$ in $\mathbb{Z}/n\mathbb{Z}$ allora anche a' è invertibile e a e a' hanno gli stessi inversi.*

Dimostrazione. Se $ax = i$ in $\mathbb{Z}/n\mathbb{Z}$ allora $n \mid (ax - 1)$, se $a' = a$ in $\mathbb{Z}/n\mathbb{Z}$ allora esiste k tale che $a' = a + kn$. Ma allora $a'x - 1 = ax - 1 + knx$ è divisibile per n e quindi $a'x = 1$ in $\mathbb{Z}/n\mathbb{Z}$. ❑

Osservazione 12.6. Osserviamo che le due proposizioni precedenti permettono di definire l'invertibilità e l'inverso di una classe di congruenza. Diremo che $[a]_n$ è invertibile se e solo se a è invertibile modulo n (la seconda delle proposizioni (12.5) assicura che tale definizione dipende solo dalla classe e non dal rappresentante) e permette di d. Se $[a]$ è invertibile, l'insieme degli inversi di a (che dipende solo dalla classe e non dal rappresentante) formano una classe di congruenza (12.4), che viene chiamata l'*inverso* di $[a]_n$ e denotata con $[a]_n^{-1}$.

La proposizione 12.3 può allora essere rienunciata

Proposizione 12.7. *$[a]_n$ è invertibile se e solo se $(a, n) = 1$.*

Corollario 12.8. *Se p è primo, ogni elemento non nullo di $\mathbb{Z}/p\mathbb{Z}$ è invertibile.*

Dimostrazione. Se $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ allora $p \not| a$ e quindi, dato che p è primo, $(p, a) = 1$, da cui la tesi. ❑

Lezione 13 (3 aprile 2001 h. 16.30-17.30)

Equazioni lineari modulo n

Osservazione 13.1. Si osservi che se a è invertibile in $\mathbb{Z}/n\mathbb{Z}$, allora se $c, d \in \mathbb{Z}/n\mathbb{Z}$ sono tali che $ac = ad$ (in $\mathbb{Z}/n\mathbb{Z}$) allora necessariamente $c = d$ (in $\mathbb{Z}/n\mathbb{Z}$). In quanto se x è tale che $ax = 1$, allora

$$ac = ad \Rightarrow xac = xad \Rightarrow 1c = 1d \Rightarrow c = d.$$

In particolare se a è invertibile, allora da $ab =$ si deduce che $b = 0$. In generale tale conclusione non si può inferire se a non è invertibile, ad esempio $2 \cdot 3 = 2 \cdot 0$ in $\mathbb{Z}/6\mathbb{Z}$, ma $3 \neq 0$ in $\mathbb{Z}/6\mathbb{Z}$.

Se p è primo tutti gli elementi non nulli sono invertibili (corollario 12.8), e quindi se $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ allora $ac = ad$ in $\mathbb{Z}/p\mathbb{Z}$ implica che $c = d$ (in $\mathbb{Z}/p\mathbb{Z}$), in particolare $ab = 0$ in $\mathbb{Z}/p\mathbb{Z}$ implica che $a = 0$ o $b = 0$.

Proposizione 13.2. *Siano $a, b \in \mathbb{Z}$, allora esiste un intero x tale che*

$$ax \equiv b \mod n$$

se e solo se $(a, n) \mid b$.

Dimostrazione. Se $ax \equiv b \mod n$ allora $n \mid (ax - b)$ quindi esiste k tale che $ax - b = kn$ ossia $b = ax - kn$ e quindi $(a, n) \mid b$.

Viceversa supponiamo che $(a, n) \mid b$. Siano α, β tali che $(a, n) = \alpha a + \beta n$ (osservazione 9.9), e sia k tale che $b = k(a, n)$ allora $b = k(\alpha a + \beta n)$ e quindi $n \mid (a(k\alpha) - b)$, ossia $k\alpha$ è una soluzione della congruenza. ❑

Osservazione 13.3. La dimostrazione precedente dà un metodo operativo per trovare una soluzione della congruenza, basta usare l'algoritmo di Euclide per determinare α e β in modo che $(a, n) = \alpha a + \beta n$.

Esercizio 13.1. Si provi che quando ha soluzione, la congruenza $ax \equiv b \mod n$ è equivalente alla congruenza

$$a'x \equiv b' \mod n'$$

essendo $a' = a/(a, n)$, $b' = b/(a, n)$, $n' = n/(a, n)$. (Con equivalente si intende che hanno le stesse soluzioni).

Proposizione 13.4. *Siano $a, b \in \mathbb{Z}$, e sia $n \in \mathbb{N}$ tale che $(a, n) = 1$ allora l'insieme degli x tali che $ax \equiv b \mod n$ sono una classe di congruenza modulo n.*

Dimostrazione. La congruenza ha soluzioni per quanto visto sopra (proposizione 13.2). Passando alle classi di congruenza, si ha che se x è una soluzione, allora $[a]_n [x]_n = [b]_n$ e dato che a è invertibile, questo implica, moltiplicando entrambi membri per $[a]_n^{-1}$, che $[x]_n = [a]_n^{-1} [b]_n$, da cui la tesi. ❑

Osservazione 13.5. La proposizione 13.4 e l'esercizio 13.1 forniscono un metodo per trovare tutte le soluzioni di un'equazione lineare.

Il piccolo teorema di Fermat

Proposizione 13.6. *Siano $u, v \in \mathbb{Z}/n\mathbb{Z}^*$ allora $uv \in \mathbb{Z}/n\mathbb{Z}^*$.*

Dimostrazione. $uv(v^{-1}u^{-1}) = u(vv^{-1})u^{-1} = u1u^{-1} = uu^{-1} = 1$. ❑

Osservazione 13.7. Una immediata conseguenza della proposizione precedente, è che se si fissa $u \in \mathbb{Z}/n\mathbb{Z}^*$, allora è possibile definire la funzione $L_u : \mathbb{Z}/n\mathbb{Z}^* \to \mathbb{Z}/n\mathbb{Z}^*$ ponendo $L_u(v) = uv$, e t. Per quanto osservato sopra (osservazione 13.1) tale funzione risulta iniettiva, infatti $L_u(v_1) = L_u(v_2)$ vuol dire che $uv_1 = uv_2$, e dato che u è invertibile, $v_1 = v_2$. Dato che l'insieme $\mathbb{Z}/n\mathbb{Z}^*$ è finito, L_u è bigettiva.

Dato un numnero naturale n si indica con $\Phi(n)$ il numero di naturali minori o uguali a n e coprimi con n. La funzione Φ si chiama *funzione Φ di Eulero.* La seguente proposizione è una conseguenza immediata di proposizione 12.3 e di proposizione 11.13.

Proposizione 13.8. *Per ogni $n > 0$, si ha che $\left|\mathbb{Z}/n\mathbb{Z}^*\right| = \Phi(n)$.*

Teorema 13.9. *Sia $u \in \mathbb{Z}/n\mathbb{Z}^*$ allora $u^{\Phi(n)} = 1$ (in $\mathbb{Z}/n\mathbb{Z}$).*

Dimostrazione. Sia $k = \Phi(n)$, e siano $x_1, \ldots, x_k$ tutti gli elementi di $\mathbb{Z}/n\mathbb{Z}^*$, dato che l'applicazione L_u è bigettiva (osservazione 13.7), allora $l_u(x_1), \ldots, L_u(x_k)$ sono ancora tutti gli elementi di $\mathbb{Z}/n\mathbb{Z}^*$, ma allora, per la commutatività del prodotto, $x_1x_2 \ldots x_k = L_u(x_1)L_u(x_2) \ldots L_u(x_k)$ e quindi

$$x_1x_2 \ldots x_k = ux_u1x_2 \ldots ux_k = u^k x_1x_2 \ldots x_k$$

Da, questa uguaglianza, osservando che $x_1x_2 \ldots x_k$ è invertibile (proposizione 13.6), ne segue (per quanto osservato in 13.1) che $u^k = 1$. ❑

Corollario 13.10 (Piccolo teorema di Fermat). *Se p è un primo allora per ogni $x \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ si ha che $x^{p-1} = 1$ in $\mathbb{Z}/p\mathbb{Z}$.*

Dimostrazione. Segue immediatamente dal teorema precedente, osservando che se p è primo, allora tutti i numeri più piccoli di p sono coprimi con p, e quindi $\Phi(p) = p - 1$. ❑

Esercizio 13.2. Si provi che se p è un primo allora per ogni intero x si ha che $x^p \equiv x \mod p$.

Crittografia RSA

Proposizione 13.11. *Sia c coprimo con $\Phi(n)$, allora l'applicazione $C : \mathbb{Z}/n\mathbb{Z}^* \to \mathbb{Z}/n\mathbb{Z}^*$ definita da $x \mapsto x^c$ è invertibile e la sua inversa è data da $D(x) = x^d$ essendo $cd \equiv 1 \mod \Phi(n)$.*

Dimostrazione. Se c è coprimo con $\Phi(n)$ allora esiste un d come nell'enunciato, ossia tale che $cd \equiv 1 \mod \Phi(n)$, ma allora $cd = k\Phi(n) + 1$ e quindi, usando la proposizione dimostrata precedentemente (13.9), per ogni $x \in \mathbb{Z}/n\mathbb{Z}$ si ha

$$D(C(x)) = (x^c)^d = x^{cd} = x^{\Phi(n)+1} = x(x^{\Phi}(n))^k = x1^k = x.$$

Del tutto analoga è la prova che anche $C(D(x)) = x$ per ogni x, da cui la tesi. ❑

La proposizione appena dimostrarta è alla base del metodo RSA di *crittografia a chiave pubblica*. Supponiamo cha A debba trasmettere un messaggio riservato a B, allora B rende noti due numeri m e c (detti rispettivamente il modulo e la chiave di codifica), che hanno la proprietà $(c, \Phi(m)) = 1$. L'alfabeto della trasmissione sarà allora costituito da $\mathbb{Z}/m\mathbb{Z}^*$ e la codifica sarà costituita da sostituire la lettera x con x^c (modulo m).

Il fatto che $(c, \Phi(m)) = 1$, garantisce che si può determinare un numero d tale che $cd \equiv 1 \mod \Phi(m)$, ossia tale che $cd = k\Phi(m) + 1$. Per decodificare il messagio è allora sufficiente elevare alla potenza d, in quanto

$$(x^c)^d = x^{cd} = x^{k\Phi(m)=1} = (x^{\Phi(m)})^k x = 1^k x = x \quad \text{in } \mathbb{Z}/m\mathbb{Z}$$

Chiaramente chiunque conosca c e $\Phi(m)$ è in grado di determinare la chiave di decodifica d. Ma determinare $\Phi(m)$ è molto facile se si conosce la fattorizzazione in primi di m, e fattorizzare un intero è un problema computazionalmente molto complesso. Quindi soltanto chi ha costruito m e c è in grado di determinare d facilmente. I numeri che vengono usati sono in realtà del tipo $m = pq$ con p, q primi, per i quali siha (esercizio 13.3) $\Phi(m) = (p-1)(q-1)$ e per i quali, determinare $\Phi(m)$ a partire da m è equivalente (esercizio 13.4) a determinare la fattorizzazione di m.

Esercizio 13.3. Provare che se p, q sono primi allora $\Phi(pq) = (p-1)(q-1)$

Esercizio 13.4. Supponiamo che $n = pq$ sia con p e q primi. Si provi che se si conoscono n e $\Phi(n)$ si possono determinare pe q.

Esercizio 13.5. Si risolvano, se possibile, le seguenti congruenze:

1. $x^7 \equiv 3 \mod 11$
2. $x^14 \equiv 2 \mod 45$
3. $x^6 \equiv 2 \mod 13$
4. $x^2 + 3x \equiv 0 \mod 17$

Lezione 14 (2 maggio 2001 h. 10.30-12.30)

Definizione di grafo

Definizione 14.1. Un grafo G è una coppia ordinata $G = (V, E)$ dove V è un insieme non vuoto detto insieme dei *vertici* del grafo ed $E \subseteq \binom{V}{2}$ è detto l'insieme dei *lati*. Se $e = \{v_1, v_2\} = inE$, si dirà che il lato e *congiunge* i due vertici v_1 e v_2 e si dirà anche che v_1 e v_2 sono gli *estremi* del lato e.

Se G è un grafo, indicheremo con $V(G)$ l'insieme dei suoi vertici e con $E(G)$ l'insieme dei suoi lati, ovvero $G = (V(G), E(G))$.

Se $G = (V, E)$ è un grafo e $v, v' \in V$ si dirà che v e v' sono *adiacenti* o che v' è *vicino* a v se $\{v, v'\} \in E$ (cfr. esercizio 14.2).

Spesso i grafi sono rappresentati graficamente mediante dei punti a rappresentare i vertici e delle linee congiungenti due vertici a rappresentare i lati. Ad esempio in figura 1 sono rappresentati i grafi G e G'definiti da

$$\begin{array}{rclrcl} V(G) & = & \{1,2,3,4\} & E(G) & = & \big\{\{1,2\},\{1,3\},\{2,3\},\{1,4\},\{2,4\}\big\} \\ V(G') & = & \{1,2,3,4,5\} & E(G') & = & \big\{\{1,3\},\{2,3\},\{3,4\},\{3,5\},\{4,5\},\{2,4\}\big\}. \end{array}$$

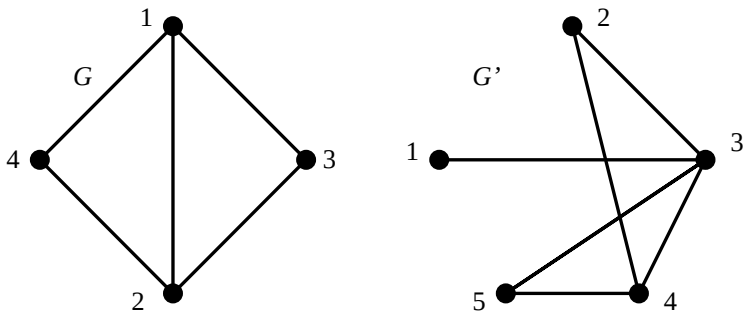

Figura 1: Esempi di grafi

Osservazione 14.2. Se $G = (V, G)$ è un grafo, l'essere adiacenti, definisce una relazione su V detta *relazione d'adiacenza* che denoteremo con $\mathcal{R}(E)$. Ossia:

$$v_1 \, \mathcal{R}(E) \, v_2 \iff \{v_1, v_2\} \in E.$$

Tale relazione risulta essere oviamente

- simmetrica ossia $v_1 \, \mathcal{R}(E) \, v_2 \Rightarrow v_2 \, \mathcal{R}(E) \, v_1$
- *antiriflessiva* ossia $\forall v \quad \neg \, v \, \mathcal{R}(E) \, v$

Viceversa, data una relazione simmetrica e antiriflessiva $\sim$ sull'insieme V, l'insieme $\mathcal{E}(() \sim) = \{\{v_1, v_2\} \mid v_1 \sim v_2\}$ è un sottinsieme di $\binom{V}{2}$, e quindi $(V, \mathcal{E}(() \sim)$ è un grafo.

Proposizione 14.3. *Con le notazioni appena introdotte si ha che*

1. *Se (V, E) è un grafo allora $\mathcal{E}(\mathcal{R}(E)) = E$*
2. *Se $\sim$ è una relazione simmetrica e antiriflessiva su V allora $\mathcal{R}(\mathcal{E}(\sim))=\sim$.*

Dimostrazione. (1). Dalle definizioni si ha immediatamente che

$$\{v_1, v_2\} \in \mathcal{E}(\mathcal{R}(E)) \iff v_1 \, \mathcal{R}(E) \, v_2 \iff \{v_1, v_2\} \in E$$

e quindi $\mathcal{E}(\mathcal{R}(E)) = E$.
(2). $v_1 \, \mathcal{R}(\mathcal{E}(\sim)) \, v_2$ se e solo se $\{v_1, v_2\} \in \mathcal{E}(\sim)$ e per definizione di $\mathcal{E}(() \sim)$ questo è vero se e solo se o $v_1 \sim v_2$ o $v_2 \sim v_1$. Dato che la relazione $\sim$ è simmetrica, ciò equivale a dire $v_1 \sim v_2$. ❑

Osservazione 14.4. La proposizione precedente prova che dare un grafo i cui vertici sono l'insieme V è equivalente a dare una relazione simmetrica e antiriflessiva su V.

Osservazione 14.5. Si osservi che affinchè $\mathcal{E}(() \sim)$ sia l'insieme dei lati di un grafo è necessario soltanto che $\sim$ sia antiriflessiva. La simmetria di $\sim$ è necessaria però per provare la seconda proprietà della proposizione precedente.

Esercizio 14.1. Provare nel dettaglio quanto asserito nell'osservazione 14.2.

Esercizio 14.2. Sia V un insieme, e sia $\sim$ una relazione antiriflessiva su V. Si provi che se $\sim$ non è simmetrica allora $\mathcal{R}(\mathcal{E}(\sim))\neq\sim$.

Si produca anche un esempio di relazione $\sim$ su un insieme tale che $\mathcal{R}(\mathcal{E}(\sim))\neq\sim$.

Definizione 14.6. Un *grafo diretto* è una coppia (V, E) dove $E \subset V \times V$ è una relazione binaria su V.

Osservazione 14.7. Intuitivamente un grafo diretto può essere pensato come un grafo, in cui sono specificati dei "versi di percorrenza" degli archi che congiungono due punti. In questa ottica denoteremo anche con $v \to w$ il fatto che $(v, w) \in E$.

Si osservi che, a differenza dei grafi dove tra due vertici cè soltanto un lato e non ci sono lati che vanno da un vertice a se stesso, tra due vertici v e w di un grafo diretto ci possono essere entrambi i lati $v \to w$ e $w \to v$, e si possono avere anche lati del tipo $v \to v$ (vedi figura 2).

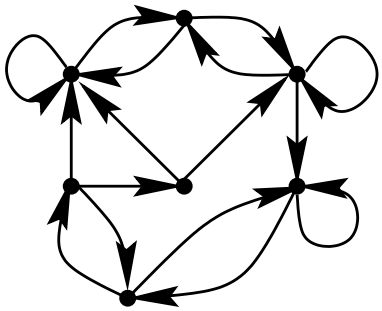

Figura 2: Un grafo diretto

Si noti però che l'osservazione 14.4 mostra che dare un grafo è equivalente a dare un grafo diretto simmetrico (i.e. se $v \to w$ anche $w \to v$) e antiriflessivo (i.e. $v \not\to v$ per ogni v). In altri termini la nozione di grafo diretto è una estensione di quella di grafo.

Alcuni grafi notevoli

Diamo alcuni esempi di grafi notevoli, per i quali esiste anche una notazione standard.

Per ogni $n \in \mathbb{N}$ indicheremo con P_n il grafo tale che

$$\begin{aligned} V(P_n) &= \{1, 2, \ldots, n\} \\ E(P_n) &= \big\{\{i, i+1\} \;\big|\; i = 1, \ldots, n-1\big\} \end{aligned}$$

P_n è detto il *cammino* di lunghezza $n-1$ (i.e. ha $n-1$ lati).

Indicheremo con P_∞ il grafo

$$\begin{aligned} V(P_\infty) &= \mathbb{N} \\ E(P_\infty) &= \big\{\{i, i+1\} \;\big|\; i \in \mathbb{N}\big\} \end{aligned}$$

P_n è detto il *cammino infinito*.

Per ogni $n \in \mathbb{N}$, $n \geq 3$ indicheremo con C_n il grafo tale che

$$\begin{aligned} V(C_n) &= \{1, 2, \ldots, n\} \\ E(C_n) &= \big\{\{i, i+1\} \;\big|\; i = 1, \ldots, n-1\big\} \cup \big\{\{1, n\}\big\} \end{aligned}$$

C_n è detto il *ciclo* di lunghezza n (i.e. ha n lati e n vertici).

Per ogni $n \in \mathbb{N}$, indicheremo con K_n il grafo tale che

$$\begin{aligned} V(K_n) &= \{1, 2, \ldots, n\} \\ E(K_n) &= \binom{V(K_n)}{2} \end{aligned}$$

K_n è detto il *grafo completo* su n vertici (i.e. ha tutti i lati possibili che congiungono i suoi n vertici).

Per ogni $n, m \in \mathbb{N}$, indicheremo con $K_{n,m}$ il grafo tale che

$$\begin{aligned} V(K_{n,m}) &= \{1, 2, \ldots, n\} \cup \{n+1, n+2, \ldots, n+m\} \\ E(K_{n,m}) &= \left\{ \{i, j\} \;\middle|\; i = 1, \ldots, n, j = n+1, \ldots, n+m \right\} \end{aligned}$$

$K_{n,m}$ è detto il *grafo completo bipartito* su n ed m vertici (i.e. ha tutti i lati possibili che congiungono i suoi primi n vertici con gli altri m).

Sottografi e sottografi indotti

Definizione 14.8. Siano $G = (V, E)$ e $G = (V', E')$ due grafi, si dirà che G' è *sottografo* di G se e solo se $V' \subseteq V$ e $E' \subseteq E$.

Definizione 14.9. Sia $G = (V, E)$ un grafo e sia $V' \subseteq V$, chiameremo il *sottografo indotto* da G su V' il grafo $(V', E \cap \binom{V'}{2})$.

Detto in altri termini nel sottografo indotto si mettono tutti i lati del grafo G che congiungono vertici di V'.

Esercizio 14.3. Si provi che P_n è sottografo di C_n per ogni n.

Esercizio 14.4. Sia $m < n$ e sia $V = \{1, \ldots, m\}$. Si determini il sottografo indotto da K_n su V.

Esercizio 14.5. Siano G, G', G'' grafi e si provi che se G è sottografo di G' e G' è sottografo di G'' allora G è sottografo di G''.

Morfismi ed isomorfismo di grafi

Definizione 14.10. Siano $G = (V, E)$ e $G' = (V', E')$ due grafi. Una funzione $f : V \to V'$ è detta un *morfismo* di grafi se

$$\forall v_1, v_2 \in V \quad \{v_1, v_2\} \in E \Rightarrow \{f(v_1), f(v_2)\} \in E'.$$

Osservazione 14.11. Osserviamo che la condizione di essere un morfismo può essere espressa anche dicendo che

$$\forall e \in E \quad f(e) \in E' \quad \text{ovvero} \quad f(E) \subseteq E'$$

dove con $f(e)$ si intende l'immagine mediante f del sottinsieme $e \subseteq V$ e con $f(E) \subseteq 2^V$ l'insieme di tali immagini al variare di $e \in E$. In simboli $f(e) = \{f(v) \mid v \in e\}$ (ovvero se $e = \{v_1, v_2\}$ allora $f(e) = \{f(v_1), f(v_2)\}$), e $f(E) = \{f(e) \mid e \in E\}$.

Per questo motivo un morfismo sarà denotato anche con $f : (V, E) \to (V', E')$.

Osservazione 14.12. Se $\mathcal{R}$ e $\mathcal{R}'$ denotano le relazioni di adiacenza dei grafi G e G', la proprietà di essere un morfismo si rienuncia in termini di $\mathcal{R}$ e $\mathcal{R}'$

$$\forall v_1, v_2 \in V \quad v_1 \mathcal{R} v_2 \Rightarrow f(v_1) \mathcal{R}' f(v_2)$$

ed in questa forma può essere estesa ai grafi diretti.

Definizione 14.13. Un morfismo $f : G \to G'$ si dice un *isomorfismo* se

1. f è bigettiva
2. f^{-1} è a sua volta un morfismo.

In tal caso i due grafi G e G' si direnno *isomorfi*, e si denoterà con $G \cong G'$.

Proposizione 14.14. *Siano $G = (V, E)$ e $G' = (V', E')$ due grafi. Una funzione $f : V \to V'$ è un isomorfismo se e solo se*

1. *f è bigettiva*
2. *$\forall e\ e \in E \iff f(e) \in E'$.*

Dimostrazione. Supponiamo che f sia un isomorfismo, allora per definizione f è bigettiva. Dal fatto che f è un morfismo segue che se $e \in E \Rightarrow f(e) \in E'$, dal fatto che f^{-1} è un morfismo segue allora che se $f(e) \in E'$ allora $f^{-1}(f(e)) \in E$, ma $f^{-1}(f(e)) = e$ e quindi è verificata la (2).

Viceversa dalla (2) segue che se $e \in E$ allora $f(e) \in E'$ e quindi f è un morfismo. Proviamo che f^{-1} è a sua volta un morfismo. Sia $e' \in E$, dato che f è bigettiva allora esiste $e \in \binom{V}{2}$ tale che $e' = f(e)$. Ma allora dalla (2) segue che $e = f^{-1}(e') \in E$ e quindi la tesi. ∎

Esercizio 14.6. Si provi che $K_{n,m} \cong K_{m,n}$ per ogni $n, m \in \mathbb{N}$.

Esercizio 14.7. Siano $G = (V, E)$ e $G' = (V', E')$ due grafi. Si provi che se $f : G \to G'$ è un morfismo tale che f è iniettiva e $f(E) = E'$ allora f è un isomorfismo.

Esercizio 14.8. Si provi che:

1. L'identità è un isomorfismo tra G e se stesso (quindi $G \cong G$).
2. Se f è un isomorfismo tra G e G' allora f^{-1} è un isomorfismo tra G' e G (quindi $G \cong G'$ allora $G' \cong G$).
3. Se f è un isomorfismo tra G e G' e g è un isomorfismo tra G' e G'' allora $G \circ f$ è un isomorfismo tar G e G'' (quindi $G \cong G'$ e $G' \cong G'' \Rightarrow G \cong G''$).

Esercizio 14.9. Si provi che i due grafi rappresentati in figura 3 sono tra loro isomorfi.

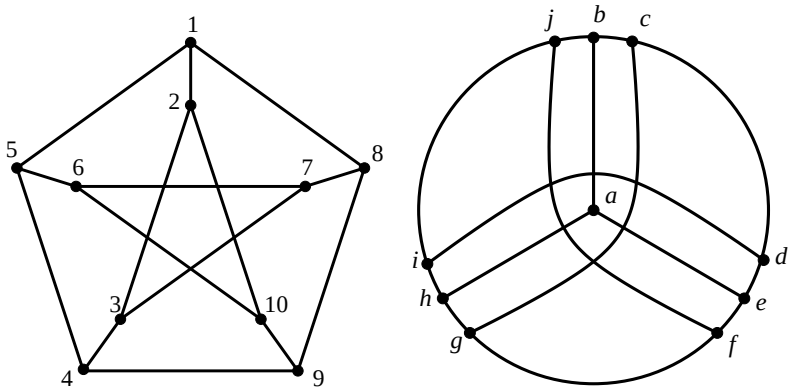

Figura 3: I grafi di esercizio 14.9

Esercizio 14.10. Dire se i due grafi in figura 4 sono isomorfi oppure no.

Esercizio 14.11. Provare che i due grafi in figura 5 non sono isomorfi.

Esercizio 14.12. Sia G il grafo dato dai vertici e dagli spigoli di un cubo e sia G' il grafo tale che $V(G')$ sia l'insieme delle parole di tre lettere nell'alfabeto di due lettere $\{a, b\}$ ed in cui due parole sono congiunte da un lato se e solo se differiscono per una lettera soltanto. Si provi che $G \cong G'$.

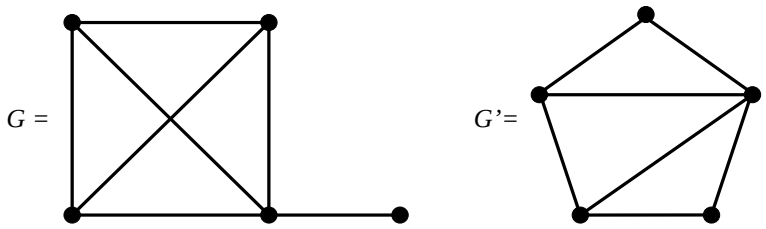

Figura 4: I grafi dell'esercizio 14.10

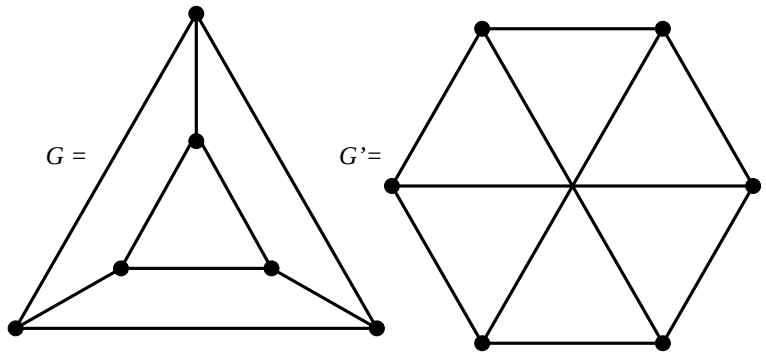

Figura 5: I grafi dell'esercizio 14.11

Lezione 15 (7 maggio 2001 h. 9.30-10.30)

Una stima del numero di grafi non isomorfi su n vertici

Sia $V = \{1, 2, \ldots, n\}$ e indichiamo con $\mathcal{G}_n$ l'insieme dei grafi che hanno V come insieme dei vertici. Dall'esercizio 14.8 segue che $\cong$ è una relazione d'equivalenza su $\mathcal{G}_n$. Indichiamo con $g_n = \left|\mathcal{G}_n / \cong\right|$.

In parolo povere g_n è il massimo numero di grafi di $\mathcal{G}_n$ tra loro non isomorfi. ovvero se si è interessati a sapere quanti sono i grafi essenzialmente diversi con vertici V il numero interessante è g_n.

Proposizione 15.1. *Con le notazioni appena introdotte si ha che*

$$\frac{n^2}{2}\Big(1 - \frac{1}{n} - \frac{2}{n}\log_2(n)\Big) \leq \log_2(g_n) \leq \frac{n^2}{2}\Big(1 - \frac{1}{n}\Big)$$

Dimostrazione. ❑

Passeggiate, cammini e cicli

Definizione 15.2. Sia $G = (V, E)$ un grafo una successione finita di vertici $(v_0, \ldots, v_n)$ sarà detta

- *passeggiata* se $\{v_i, v_{i+1}\} \in E$ per ogni $i = 0, \ldots, n-1$
- *cammino* se è una passeggiata e $v_i \neq v_j$ per ogni $i \neq j$.
- *ciclo* se è una passeggiata e $v_i \neq v_j$ per ogni $i \neq j$ a parte $v_0 = v_n$.

Proposizione 15.3. *Sia G un grafo e sia $(_0, \ldots, v_n)$ un cammino in G allora il grafo G' definito da:*

- $V(G') = \{v_0, \ldots, v_n\}$
- $E(G') = \big\{\{v_i, v_{i+1} \mid i = 0, \ldots, n-1\}$

è un sottografo di G isomorfo a P_n.

Dimostrazione. Esercizio. ❑

Proposizione 15.4. *Sia G un grafo e sia $(v_0, \ldots, v_n)$ un ciclo in G allora il grafo G' definito da:*

- $V(G') = \{v_0, \ldots, v_{n-1}\}$
- $E(G') = \big\{\{v_i, v_{i+1} \mid i = 0, \ldots, n-1\} \cup \big\{\{v_n, v_0\}\big\}$

è un sottografo di G isomorfo a C_n.

Dimostrazione. Esercizio. ❑

Osservazione 15.5. In effetti è facile vedere che dare un cammino o un ciclo in un grafo è equivalente a dare un sottografo isomorfo a P_n o C_n per qualche n.

La relazione di essere congiungibili

Definizione 15.6. Sia $G = (V, E)$ e siano $v, w \in V$. Diremo che v e w sono *congiungibili* con un cammino [risp. una passeggiata] se e siste un cammino [risp. una passeggiata] $(v_0, \ldots, v_n)$ tale che $v_0 = v$ e $v_n = w$.

Proposizione 15.7. *Le relazione di essere congiungibli da un cammino è una passeggiata d'equivalenza.*

Proposizione 15.8. *Due punti sono congiungibili mediante un cammino se e solo se lo sono mediante una passeggiata.*

Dimostrazione. Dato che un cammino è una passeggiata, se due vertici sono congiungibili mediante un cammino lo sono anche mediante una passeggiata.

Viceversa. Sia $\mathcal{P}$ ❑

Lezione 16 (9 maggio 2001 h. 10.30-11.30)

Componenti connesse di un grafo

Le componenti connesse sono invarianti per isomorfismo

Proposizione 16.1. *Sia $f : G \to G'$ un morfismo di grafi e $v, w \in V(G)$. v e w sono congiungibili allora anche $f(v)$ e $f(w)$ lo ¡sono.*

Dimostrazione. Se $(v = v_0, v_1, \ldots, v_n = w)$ è una passeggiata, allora, per definizione di morfismo (definizione 14.10), anche $(f(v) = f(v_0), f(v_1), \ldots, f(v_n) = f(w))$ lo è. ❑

Proposizione 16.2. *Sia $f : G \to G'$ un isomorfismo di grafi e $v, w \in V(G)$. v e w sono congiungibili se e solo se lo sono $f(v)$ e $f(w)$.*

Dimostrazione. Segue immediatamente dalla proposizione precedente applicata ad f e ad f^{-1}. ❑

Teorema 16.3. *Siano G e G' grafi isomorfi, allora hanno componenti connesse isomorfe. Più precisamente, se $\{G_i\}_{i\in I}$ e $\{G'_j\}_{j\in J}$ sono gli insiemi delle componenti connesse di G e G' rispettivamente, allora esiste una bigezione $\varphi : I \to J$ tale che $G_i \cong G'_{\varphi(i)}$.*

Se G è un grafo finito e $G_1, \ldots, G_k$ sono le sue componenti connesse, allora $\sum_{i=1}^{k} |V(G_i)| = |V(G)|$ e $\sum_{i=1}^{k} |E(G_i)| = |E(G)|$.

Esercizio 16.1. Se G è un grafo finito e $G_1, \ldots, G_k$ sono le sue componenti connesse, allora $\sum_{i=1}^{k} |V(G_i)| = |V(G)|$ e $\sum_{i=1}^{k} |E(G_i)| = |E(G)|$.

Grafi connessi

Definizione 16.4. Un grafo si dice *connesso* se ha una sola componente connessa. Un grafo non connesso si dice *sconnesso*.

Osservazione 16.5. Un grafo G è connesso se e solo se per ogni $v, w \in V(G)$ v e w sono congiungibili da un cammino (risp. da una passeggiata).

Osservazione 16.6. Dal teorema 16.3 segue in particolare che se due grafi sono isomorfi, allora o sono entrambi connessi oppure sono entrambi sconnessi.

La matrice di incidenza di un grafo finito

Definizione 16.7. Sia G un grafo finito e siano $v_1, \ldots, v_n$ i sui vertici. Si chiama matrice di incidenza di G la matrice A_G, che al posto i, j ha 1 se $\{v_i, v_j\} \in EG$ e ha 0 altrimenti.

Proposizione 16.8. *Sia A la matrice di incidenza del grafo G, allora l'elemeto di posto i, j della matrice A^k è pari al numero di passeggiate lunghe k dal vertice v_i al vertice v_j.*

Esercizio 16.2. Si provi che un grafo finito G ha 3-cicli se e solo se la matrice A_G^3 ha elementi non nulli sulla diagonale.

Esercizio 16.3. Si provi che il numero di 3[cicli di un grafo finito G è pari a $\mathrm{tr}(A_G^3)/6$.

Lezione 17 (14 maggio 2001 h. 9.30-10.30)

Grado di un vertice

Definizione 17.1. Sia G un grafo e sia $v \in V(G)$, chiameremo *grado* di v il numero (cardinale) $\deg(v) = |\{e \in E(G) \mid v \in e\}|$. Diremo che v ha grado finito se $\deg(v) \in \mathbb{N}$.

Proposizione 17.2. *Se $G = (V, E)$ è un grafo finito, allora*

$$\sum_{v \in V} \deg(v) = 2\,|E| \tag{8}$$

Il lemma delle strette di mano

Proposizione 17.3. *In un grafo il numero di vertici di grado dispari è pari.*

Proposizione 17.4. *Se f è un isomorfismo tra G e G' e $v \in V(G)$ allora* $\deg(v) = \deg(f(v))$.

Score di un grafo

Definizione 17.5. Sia G un grafo finito e sia $V(G) = \{v_1, \ldots, v_n\}$, si chiama *score* di G la successione (finita)n-pla dei gradi dei suoi vertici ovvero $\text{score}(G) = (\deg(v_1), \ldots, \deg(v_n))$.

Per scrivere lo score abbiamo dovuto ordinare i vertici del grafo e, ordinamenti diversi producono n-ple diverse, ma che coincidono a meno di riordinamento. Due score si considereranno quindi uguali se lo sono a meno di riordinarli. Per comodità si ordineranno i vertici in modo che la successione dei gradi sia non decrescente (i.e. $\deg(v_i) \leq \deg(v_{i+1})$ per ogni i).

Teorema 17.6. *Se G e G' sono grafi isomorfi, allora* $\text{score}(G) = \text{score}(G')$.

Osservazione 17.7. Non è vero il viceversa del precedente teorema, si vedano ad esempio i grafi i due grafi di figura 5 dell'esercizio 14.11.

Teorema dello score

Lezione 18 (16 maggio 2001 h. 10.30-11.30)

Definizione di grafo euleriano

Caratterizzazione dei grafi euleriani

Definizione di grafo hamiltoniano

Grafo duale di un grafo dato

G è connesso allora anche il suo duale lo è

Se G è euleriano allora il suo duale è hamiltoniano

Lezione 19 (21 maggio 2001 h. 9.30-10.30)

Alcune costruzioni con i grafi

Definizione di grafo 2-connessi

Prima caratterizzazione dei grafi 2-connessi

Seconda caratterizzazione dei grafi 2-connessi

Esercizio 19.1. Siano $G = (V, E)$ e $G' = (V'.e')$ due grafi. Si denoti con $G \cup G'$ il grafo tale che $V(G \cup G') = V \cup V'$ e $E(G \cup G') = E \cup E'$. Si provi che se G e G' sono connessi e $V \cap V' \neq \varnothing$ allora $G \cup G'$ è connesso.

Esercizio 19.2. Si provi che se G e G' sono 2-connessi e $|V \cap V'| \geq 2$ allora $G \cup G'$ è 2-connesso.

Esercizio 19.3. Sia $k \geq 1$, si dice che un grafo $G = (V, E)$ è *k-connesso* se per ogni $v_1, \ldots, v_{k-1} \in V$ si ha che $G - v_1 - v_2 - \ldots - v_{k-1}$ è connesso. Si osservi che 1-connesso è sinonimo di connesso.

Si provi che G è *$k-$connesso* se e solo se per ogni $v \in V$ $G - v$ è $k-1$-connesso.

Esercizio 19.4. Si determinino condizioni sufficienti affinché l'unione di due grafi k-connessi sia ancora k-connesso.

Esercizio 19.5. Per ogni $n \in \mathbb{N}$ sia $G_n = (V_n, E_n)$ un grafo connesso e si supponga che $V_n \subseteq V_{n+1}$ per ogni n. Si provi che allora $G = \bigcup_{n \in \mathbb{N}} G_n$ è connesso.

Esercizio 19.6. Per ogni $n \in \mathbb{N}$ sia $G_n = (V_n, E_n)$ un grafo connesso e si supponga che $V_n \cap V_{n+1} \neq \varnothing$ per ogni n. Si provi che allora $G = \bigcup_{n\in\mathbb{N}} G_n$ è connesso.

Esercizio 19.7. Per ogni $n \in \mathbb{N}$ sia $G_n = (V_n, E_n)$ un grafo k-connesso e si supponga che $|V_n \cap V_{n+1}| \geq k$ per ogni n. Si provi che allora $G = \bigcup_{n\in\mathbb{N}} G_n$ è k-connesso.

Lezione 20 (23 maggio 2001 h. 10.30-11.30)

Alberi

Definizione 20.1. Si dice *albero* un grafo connesso e senza cicli. Si dice una *foresta* un grafo senza cicli.

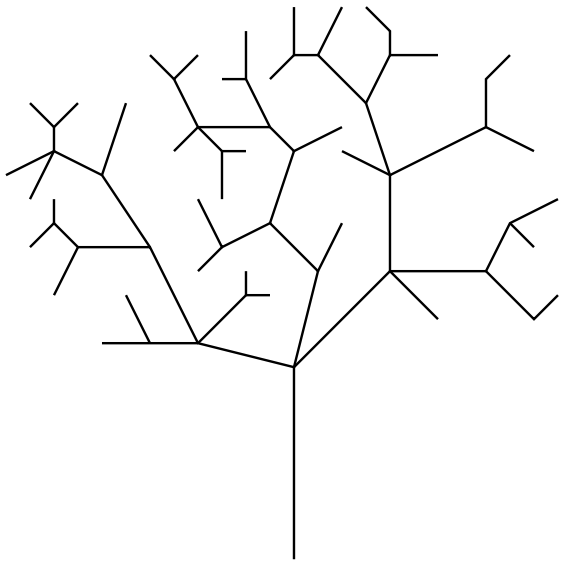

Figura 6: Un albero

Esercizio 20.1. Si provi che un grafo F è una foresta se e solo se ogni sua componente connessa è un albero.

Il teorema di caratterizzazione degli alberi

Teorema 20.2. *Sia $T = (V, E)$ un grafo. Sono equivalenti i seguenti fatti:*

1. *T è un albero*
2. *$\forall v, v' \in V$ esiste un unico cammino che congiunge v a v'*
3. *T è connesso e $\forall e \in E$ il grafo $T - e$ è sconnesso*
4. *T non ha cicli e $\forall e \in \binom{V}{2}$ il grafo $T + e$ ha almeno un ciclo.*

Dimostrazione. Dimostriamo le implicazioni (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1).
(1) $\Rightarrow$ (2). Supponiamo per assurdo che esistano due diversi cammini in T che congiungono v e v'. Siano questi $(v_0, v_1, \ldots, v_k)$, $(u_0, u_1, \ldots, u_h)$ (i.e. $v = v_0 = u_0$ e

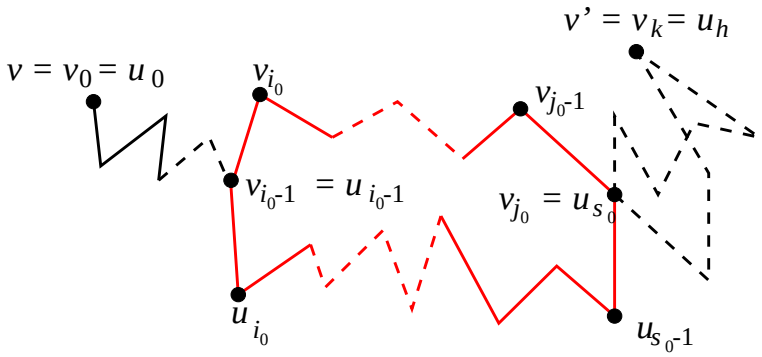

Figura 7: La costruzione del ciclo nella dimostrazione di (1) $\Rightarrow$ (2)

$v' = v_k = u_h$ e per ogni i si ha che $\{v_i, v_{i+1}\}, \{u_i, u_i+1\} \in E$). Dato che i due cammini sono diversi esiste un i tale che $v_i \neq u_i$, sia quindi i_0 il minimo per cui ciò succede. Dato che $v_k = u_h$ esiste un $j > i_0$ tale che $v_j = u_s$ per qualche s, sia j_0 il minimo di tali j ed s_0 tale che $v_{j_0} = u_{s_0}$. Allora $(v_{i_0-1}, v_{i_0}, \ldots, v_{j_0}, u_{s_0-1}, \ldots, u_{i_0+1}, u_{i_0})$ è un ciclo (si veda figera 7).
(2) $\Rightarrow$ (3). Chiaramente T è connesso, dato che dati comunque due suoi vertici esiste (e per giunta è unico) un cammino che li congiunge.

Sia $e = \{v, v'\} \in E$, allora l'unico cammino in T tra v e v' è dato da (v, v'), quindi non esiste alcun cammino tra v e v' che non contenga il lato e, pertanto $T - e$ è sconnesso.
(3) $\Rightarrow$ (4). Proviamo innanzitutto che T non ha cicli. Infatti se $(v_0, v_1, \ldots, v_k, v_0)$ fosse un ciclo in T, allora detto $e = \{v_0, v_1\}$, il grafo $T - e$ risulterebbe connesso. Infatti siano $v, v' \in V$, e sia $P = (u_0, \ldots, u_h)$ un cammino che li congiunge. Allora o nessuno dei lati di tale cammino coincide con il lato e, ed in tal caso P è un cammino anche in $T - e$, oppure un lato è uguale a e. In questa evenienza esiste i tale che $\{u_i, u_{i+1}\} = \{v_0, v_1\}$ e, a meno di riordinare in ordine inverso i vertici del cammino, possiamo supporre cghe $u_i = v_0$ e $u_{i+1} = v_1$. Ma allora $(u_0, \ldots, u_i, v_k, v_{k-1}, \ldots, v_1, u_{i+2}, \ldots, u_h)$ risulta essere una passeggiata in $T - e$ che congiunge v e v' (vedi figura 8).

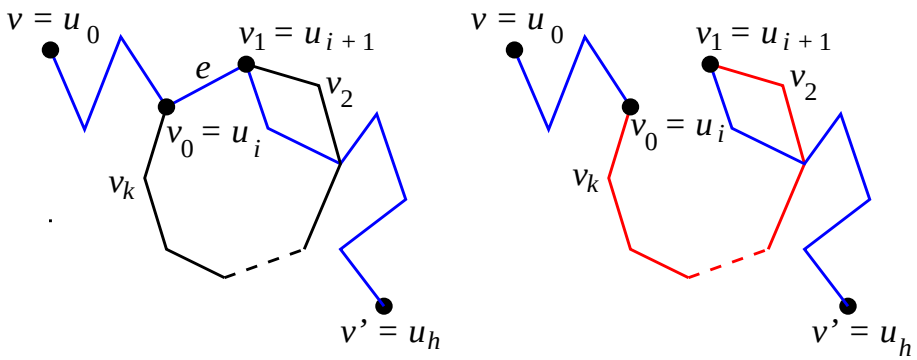

Figura 8: La costruzione della passeggiata nella dimostrazione di (3) $\Rightarrow$ (4)

Proviamo ora che $T+e$ ha dei cicli. Siano $v, v' \in V$ tali che $e = \{v, v'\} \notin E$. Dato che T è connesso, esiste un cammino che congiunge v a v'. Sia questo $(v_0, v_1, \ldots, v_k)$. Evidentemente allora $(v_0, v_1, \ldots, v_k, v_0)$ è un ciclo in $T + e$.
(4) $\Rightarrow$ (1). Dobbiamo provare che T è connesso (sappiamo già che non ha cicli).

Siano $v, v' \in V$. Se $\{v, v'\} \in E$ non c'è nulla da provare, dato che (v, v') è un cammino che congiunge v a v'. Se $e = \{v, v'\} \notin E$, allora sappiamo che il grafo $T+e$ contiene un ciclo, sia questo $C = (v_0, v_1, \ldots, v_k, v_0)$. Chiaramente uno dei lati del ciclo deve essere proprio e, dato che altrimenti il ciclo sarebbe in T (che non ha cicli!). Supponiamo quindi $v_i = v$ e $v_{i+1} = v'$. Il cammino $(v_{i+1}, \ldots, v_k, v_0, v_1, \ldots, v_i)$ è allora un cammino in T che congiunge v' a v. ❑

Il teorema di caratterizzazione degli alberi finiti

Definizione 20.3. Sia G un grafo, un vertice $v \in V(G)$ tale che $\deg(v) = 1$ sarà detto una *foglia*.

Esercizio 20.2. Si determinino le foglie dell'albero in figura 6

Lemma 20.4. *Ogni albero finito ha almeno due foglie*

Dimostrazione. Sia $P = (v_0, v_1, \ldots, v_k)$ un cammino di lunghezza massima, proviamo che v_0 e v_k sono due foglie. Se per assurdo $\deg(v_0) > 1$ allora esisterebbe $v' \in V$ tale che $\{v', v_0\} \in E$ e $v' \neq v_1$. Osserviamo che allora non potrebbe essere $v' = v_i$ per qualche $i > 1$, perché in tal caso, detto i_0 il minimo di tali i si avrebbe che $(v', v_0, \ldots, v_i)$ sarebbe un ciclo, contro l'ipotesi che T sia un albero. Ma allora $(v', v_0, \ldots, v_k)$ sarebbe un cammino di lunghezza maggiore di quella di P, che è assurdo.

In modo analogo si prova che anche v_k è una foglia. (Oppure ci si riconduce al caso precedente, prendendo il cammino $P' = (v_k, \ldots, v_1, v_0)$). ❑

Osservazione 20.5. Si osservi che il lemma precedente è falso se non si assume la finitezza dell'albero. Ad esempio l'albero $(\mathbb{N}, \{\{n.n+1\} \mid n \in \mathbb{N}\}$ ha una sola foglia (il vertice 0), mentre l'albero $(\mathbb{Z}, \{\{n.n+1\} \mid n \in \mathbb{Z}\}$ non ha foglie.

Esercizio 20.3. Si provi che se G è un grafo connesso con almeno due vertici e v è una sua foglia, allora $G - v$ è ancora connesso.

Esercizio 20.4. Si provi che se T è un albero e v è una sua foglia, allora $T - v$ è un albero.

Esercizio 20.5. Quante foglie può avere al massimo un grafo connesso con n vertici? Si determini un grafo con il massimo numero di foglie possibili.

Teorema 20.6. *Sia $T = (V, E)$ un grafo finito. Sono fatti equivalenti:*

1. *T è un albero*

5. *T è connesso e $|V| - 1 = |E|$*

Dimostrazione. (1) $\Rightarrow$ (5). Procediamo per induzione su $|V(T)|$. Se $|V(T)| = 1$ la tesi è vera. Supponiamo che $|V(T)| \geq 2$, e sia $v \in V(T)$ una sua foglia (che esiste per il lemma precedente (20.4), ora $T - e$ è un albero (esercizio 20.4) ed inoltre $|V(T - e)| = |V(T)| - 1$. Per ipotesi di induzione si ha allora che

$$|V(T)| - 1 - 1 = |V(T - e)| - 1 = |E(T - e)|\,.$$

Ma dato che $\deg(v) = 1$, $|E(T - e)| = card E(T) - 1$ e quindi la tesi.
(5) $\Rightarrow$ (1). Dobbiamo provare che T non ha cicli. Procediamo ancora per induzione su $|V(T)|$. Se $|V(T)| = 1$ la tesi è vera. Supponiamo che $|V(T)| \geq 2$. Proviamo innanzitutto che T ha una foglia. Dalla relazione tra numero di vertici e numero di lati, e dalla relazione che lega il numero di lati con i gradi dei vertici (8), si ottiene

$$2\,|V(T)| - 2 = 2\,|E(T)| = \sum_{v \in V(T)} \deg(v)$$

se per ogni v si avesse che $\deg(v) \geq 2$ si otterrebbe subito un assurdo ($2|V(T)|-2 \geq 2|V(T)|$) e quindi almeno un vertice deve avere grado 1. Sia quindi v una foglia di T, e si consideri il grafo $T - v$.

Dato che T è connesso e $\deg(v) = 1$, anche $T - v$ è connesso (un cammino in T che congiunge due vertici diversi da v non può passare per v, in quanto i vertici di un cammino, eccetto al più il primo e l'ultimo, hanno grado almeno 2). Inoltre, poiché $|V(T-v)| = |V(T)| - 1$ e $|E(T-v)| = |E(T)| - 1$, si ha che $|V(T-v)| - 1 = |E(T-v)|$. Per ipotesi di induzione allora $T - v$ è un albero. Ma allora T non ha cicli, in quanto i vertici di un ciclo hanno tutti grado almeno 2 e quindi un ciclo in T non potrebbe passare per v, ossia sarebbe contenuto in $T - v$ e ciò contraddice il fatto che $T - v$ è un albero. ❑

Esercizio 20.6. Se $F = (V, E)$ è una foresta finita allora $|V| - |E| = k$, essendo k il numero di componenti connesse di F.

Esercizio 20.7. Si provi che se $G = (V, E)$ è un grafo connesso finito, allora $|E| \geq |V| - 1$.

Lezione 21 (28 maggio 2001 h. 9.30-10.30)

Albero di copertura

Definizione 21.1. Sia G un grafo, un sottografo T di G si dirà un *albero di copertura* di G se

- T è un albero;
- $V(T) = V(G)$.

Osservazione 21.2. Chiaramente, se G è un grafo che possiede un albero di copertura, allora G è connesso.

Teorema 21.3. *Sia G un grafo connesso finito allora G ha un albero di copertura.*

Osservazione 21.4. Il teorema precedente è vero anche senza l'ipotesi di finitezza, del grafo G, la sua dimostrazione nel caso infinito, richiede però degli strumenti un po' più sofisticati (il lemma di Zorn).

Alberi radicati

Definizione 21.5. Un *albero con radice* è una coppia (T, r) con T un albero e $r \in V(T)$ un vertice fissato che sarà detto *radice*.

Se (T, r) e (T', r') sono due alberi radicati, si dirà che sono isomorfi (come alberi radicati) se esiste un isomorfismo di grafi f tra T e T' tale che $f(r) = r'$, e si scriverà $(T, r) \cong (T'.r')$.

Esercizio 21.1. Si considerino i grafi in figura 9. Si provi che $T \cong T'$ ma $(T, r) \ncong (T', r')$.

La relazione $\rightarrow$ di "paternità" in un albero radicato

Dato un albero radicato, (T, r) per ogni vertice $v \in V(T)$ indichiamo con P_v l'unico cammino (teorema 20.2 punto 2) che congiunge r con v.

Proposizione 21.6. *Sia (T, r) un albero radicato e sia $\{v, w\} \in E(T)$, allora vale una e una sola delle seguenti:*

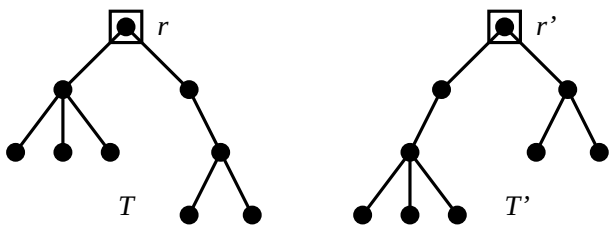

Figura 9: Gli alberi radicati dell'esercizio 21.1

1. *v è un vertice di P_w*

2. *w è un vertice di P_v.*

Dimostrazione. Proviamo che ne vale almeno una. Se non vale la (1), allora $P_w = (v_0, \ldots, v_k)$ con $v_0 = r$, $v_k = w$ e $v_i \neq v$ per ogni i. Ma allora, dato che $\{v, w\} \in E(T)$, $(v_0, \ldots, v_k, v)$ è un cammino che congiunge r a v, per l'unicità di tale cammino (teorema 20.2 punto 2) $P_v = (v_0, \ldots, v_k, v)$, e quindi vale la (2).

Proviamo ora che non possono valere contemporaneamente. Se vale la (1), allora $P_w = (v_0, \ldots, v_k)$ con $v_0 = r$, $v_k = w$ ed esiste un i tale che $v_i = v$. Ma allora $P_v = (v_0, \ldots, v_i)$. Dato che, $\{v, w\} \in E(T)$, $w \neq v$, quindi $i < k$, e dato che P_w è un cammino $w = v_k \neq v_j$ per ogni $j < k$, quindi w non compare in $P_v = (v_0, \ldots, v_i)$. ❑

Definizione 21.7. Sia (T, r) un albero radicato, e siano $v, w \in V(T)$, diremo che v è *padre* di w, o che w è figlio di v, e lo indicheremo con $v \to w$, se $\{v, w\} \in E(T)$ e v è un vertice di P_w.

Proposizione 21.8. *Sia (T, r) un albero radicato, e sia $\{v, w\} \in E(T)$ allora o $v \to w$ o $w \to v$. Inoltre per ogni $v, w \in V(T)$, se $v \to w$ allora $w \not\to v$.*

Dimostrazione. È semplicemente la proposizione precedente tradotta in termini della relazione $\to$. ❑

Osservazione 21.9. La proposizione 21.8 può essere interpretata dicendo che ogni albero radicato può essere dotato in modo naturale di una struttura di grafo diretto (definizione 14.6), in modo che ad ogni lato dell'albero corrisponda uno ed un solo lato del grafo diretto.

Lezione 22 (30 maggio 2001 h. 10.30-11.30)

L'ordinamento degli alberi radicati

Sia (T, r) un albero radicato, sull'insieme dei vertici si definiscono le due relazioni $\to^+$ e $\to^*$, ovvero la chiusura transitive e la chiusura transitiva e riflessiva della relazione $\to$ di paternità (definizione 21.7) ponendo:

$$\begin{aligned} v \to^+ w &\iff \exists v_0, \ldots, v_n \in V : v = v_0 \to v_1 \to \ldots \to v_n = w \\ v \to^* w &\iff v \to^+ w \text{ oppure } v = w \end{aligned}$$

Proposizione 22.1. *La relazione $\to^*$ è un ordinamento parziale. E la relazione $\to^+$ è l'ordinamento stretto associato a $\to^*$ ossia $v \to^+ w$ se e solo se $v \to^* w$ e $v \neq w$.*

Dimostrazione. ❑

Induzione sugli alberi radicati

Teorema 22.2. *Sia (T, r) un albero radicato e per ogni $v \in V(T)$ sia $P(v)$ una proposizione. Si supponga che:*

1. *$P(r)$ sia vera;*
2. *per ogni $v, w \in V(T)$ tali che $v \to w$ si ha che $P(v) \Rightarrow P(w)$*

. Allora $P(v)$ è vera per ogni $v \in V(T)$.

Teorema 22.3 (Induzione sugli alberi). *Sia (T, r) un albero radicato e per ogni $v \in V(T)$ sia $P(v)$ una proposizione. Si supponga che:*

1. *$P(r)$ sia vera;*
2. *per ogni $v \in V(T)$ si ha che $(\forall w \to^+ wP(w)) \Rightarrow P(v)$. Allora $P(v)$ è vera per ogni $v \in V(T)$.*

Dimostrazione. ∎

Osservazione 22.4. Si osservi che nella dimostrazione del teorema precedente non si è mai usato il fatto che si stesse parlando di alberi radicati, ma soltanto che $\to^*$ fosse un *ordinamento ben fondato* ovvero che ogni successione discendente ha minimo, e che tutto l'insieme dei vertici ha un minimo rispetto a tale ordinamento. La stessa dimostrazione può quindi essere usata per dimostrare il seguente teorema di induzione per insiemi ben fondati.

Definizione 22.5. Sia X un insieme e sia $\preccurlyeq$ un ordinamento parziale su X. Diremo che $\preccurlyeq$ è *ben fondato* se ogni successione discendente ha minimo, ossia se per ogni $n \in \mathbb{N}$ $x_n \in X$ sono tali che $x_{n+1} \preccurlyeq x_n$ allora esiste un $\overline{n}$ tale che $x_{\overline{n}} \preccurlyeq x_n$ per ogni $n \in \mathbb{N}$ (in particolare se $n \succcurlyeq \overline{n}$ allora $x_n = x_{\overline{n}}$)).

Teorema 22.6 (Induzione ben fondata). *Sia X un insieme e sia $\preccurlyeq$ un ordinamento ben fondato su X cha ammette minimo x_0 (i.e.esiste $x_0 \in X$ tale che $x_0 \preccurlyeq x$ per ogni $x \in X$). Per ogni $x \in X$ sia $P(x)$ una proposizione. Si supponga che:*

1. *$P(x_0)$ sia vera;*
2. *per ogni $x \in V(T)$ si ha che $(\forall y \prec xP(y)) \Rightarrow P(x)$ (dove $\prec$ è una abbreviazione per $\preccurlyeq$ e $\neq$).*

Allora $P(x)$ è vera per ogni $x \in X$.

Il lemma di König

Domanda. È vero che in un albero infinito esiste un ramo infinito?
Per ramo infinito intendiamo un cammino infinito (i.e. un sottografo isomorfo a P_∞).

In generale la risposta a questa domanda è negativa. Si consideri ad esempio il grafo $G = (\mathbb{N}, \{\{0, i\} \mid i \geq 1\}$ (vedi figura 22.3).

G è un albero. Infatti G è connesso dato che ogni vertice è congiungibile al vertice 0. Inoltre se $e = \{0, i\}$ è un lato, allora $G - e = (\mathbb{N} - \{0, i\}, \varnothing)$ che è sconnesso. Quindi G è un albero per la terza delle proprietà caratterizzanti degli alberi (teorema 20.2).

D'altra parte i cammini più lunghi che si possono trovare sono i cammini del tipo $(i, 0, j)$ con $i \neq j$, che hanno lunghezza 2.

Il problema sta nel fatto che nell'albero dell'esempio c'è un vertice di grado infinito (su 0 arrivano infiniti lati). In effetti vale il seguente teorema:

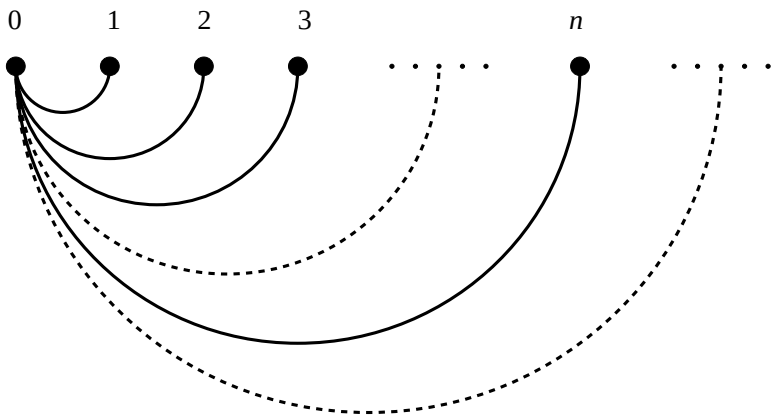

Figura 10: Un contresempio al Lemma di König, senza l'ipotesi dei gradi finiti

Teorema 22.7 (Lemma di König). *Sia T un albero infinito tale che ogni vertice ha grado finito, allora T ha rami infiniti.*

Dimostrazione. Fissiamo una radice r per T e sia $\to$ la relazione di paternità indotta da tale radice. Costruiremo una funzione $f : \mathbb{N} \to V(T)$ con la seguente proprietà:

$$f(n-1) \to f(n) \text{ e } \left\{v \in V(T) \;\middle|\; f(n) \to^* v\right\} \text{ è infinito} \forall n \geq 1$$

Chiaramente, una tale funzione risolve il problema.

Definiamo f ricorsivamente. Poniamo $f(0) = r$. Chiaramente i discendnti di $f(0)$ sono infiniti (tutti i vertici sono discendenti della radice).

Supponiamo di aver definito $f(n)$ (che sia figlio di $f(n-1)$ e che abbia una discendenza infinita). Per ipotesi $\deg(f(n))$ è finito, siano quindi $v_1, \ldots, v_k$ i figli di $f(n)$ (i.e. $f(n) \to v_i$). Per ogni $i = 1, \ldots, k$ sia

$$V_i = \left\{v \in V(T) \;\middle|\; v_i \to^* v\right\}$$

Chiaramente

$$\left\{v \in V(T) \;\middle|\; f(n) \to^* v\right\} = \{f(n)\} \cup V_1 \cup \ldots \cup V_k$$

Pertanto esiste un i tale che V_i è infinito. Basta allora porre $f(n+1) = v_i$. Chiaramente $f(n) \to f(n+1)$ e la discendenza di $f(n+1)$, che è V_i, è infinita. ❑

Soluzione di alcuni degli esercizi proposti

Soluzione dell'esercizio 1.1
❑

Soluzione dell'esercizio 1.2
❑

Soluzione dell'esercizio 1.3
❑

Soluzione dell'esercizio 1.4
❑

Soluzione dell'esercizio 1.5
❑

Soluzione dell'esercizio 1.6
❑

Soluzione dell'esercizio 1.7
❑

Soluzione dell'esercizio 1.8
❑

Soluzione dell'esercizio 1.9
❑

Soluzione dell'esercizio 2.1
❑

Soluzione dell'esercizio 2.2
❑

Soluzione dell'esercizio 2.3
❑

Soluzione dell'esercizio 2.4
❑

Soluzione dell'esercizio 2.5
❑

Soluzione dell'esercizio 3.1
❑

Soluzione dell'esercizio 3.2 Proviamo soltanto l'associatività della somma. Dobbiamo provare che per ogni $n, m, k \in \mathbb{N}$ si ha che $(n+m)+k = n+(m+k)$. Procediamo per induzione su k. Se $k = 0$ dalla definizione si ha $(n+m)+0 = n+m$ e anche $n+(m+0) = n+(m) = n+m$. Supponiamo la tesi vera per k e proviamola per $\mathrm{succ}(k)$.

$$\begin{aligned}(m+n)+\mathrm{succ}(k) &= \mathrm{succ}((m+n)+k) = \mathrm{succ}(m+(n+k)) = \\ &\quad m+\mathrm{succ}(n+k) = m+(n+\mathrm{succ}(k))\end{aligned}$$

❑

Soluzione dell'esercizio 3.3

❑

Soluzione dell'esercizio 4.2 Siano $f : X \to I_n$ e $g : Y \to I_n$ due bigezioni, allora l'applicazione $h : I_{n+m} \to X \cup Y$ definita da

$$h(i) = \begin{cases} f(i) & \text{se } i < n \\ g(i-n) & \text{se } n \leq i < m+n \end{cases}$$

è una bigezione.

Per la seconda parte si osservi innanzitutto che $X = (X-Y) \cup (X \cap Y)$ e che $(X-Y) \cap (X \cap Y) = \varnothing$ e che quindi per l'esercizio precedente,

$$|X| = |X-Y| + |X \cap Y|$$

osserviamo inoltre che $X \cup Y = (X-Y) \cup Y$ con $(X-Y) \cap Y = \varnothing$ e quindi $|X \cup Y| = |X-Y| + |Y|$, da cui

$$|Y| = |X \cup Y| - |X-Y|$$

sommando queste due relazioni si ottiene la tesi. ❑

Soluzione dell'esercizio 4.3 Procediamo per induzione su n. Se $n = 1$ non c'è nulla da dimostrare. Supponiamo la tesi vera per n, usando l'associatività dell'unione si ha

$$\bigcup_{i=1}^{n+1} X_i = (\bigcup_{i=1}^{n} X_i) \cup X_{n+1}$$

e dato che gli X_i sono a due a due disgiunti, anche $(\bigcup_{i=1}^{n} X_i) \cap X_{n+1} = \varnothing$, ma allora per l'esercizio precedente (esercizio 4.2), e l'ipotesi di induzione, si ha che

$$\left|\bigcup_{i=1}^{n+1} X_i\right| = \left|\bigcup_{i=1}^{n} X_i\right| + |X_{n+1}| = \sum_{i+1}^{n} |X_i| + |X_{n+1}| = \sum_{i+1}^{n+1} |X_i|$$

❑

Soluzione dell'esercizio 4.4

❑

Soluzione dell'esercizio 4.5

❑

Soluzione dell'esercizio 4.6
❑

Soluzione dell'esercizio 5.1 Se una tale g esiste, f è surgettiva, dato che per ogni $y \in Y$ si ha che $f(g(y)) = y$.

Viceversa, supponiamo che f sia surgettiva, allora $f^{-1}(y) \neq \varnothing$ per ogni $y \in Y$, per l'assioma di scelta (5.1), esiste una funzione di scelta, $g : Y \to \bigcup_{y \in Y} f^{-1}(y)$, tale che $g(y) \in f^{-1}(y)$ per ogni $y \in Y$, ma ciò significa che $f(g(y)) = y$ per ogni $y \in Y$, ossia che g è una inversa destra di f. ❑

Soluzione dell'esercizio 5.2 Se una tale g esiste allora f deve necessariamente essere iniettiva, infatti se $f(x_1) = f(x_2)$ allora $x_1 = g(f(x_1)) = g(f(x_2))x_2$.

Viceversa, supponiamo che f sia iniettiva. Allora per ogni $y \in f(X)$ esiste un unico $x_y \in X$ tale che $f(x_y) = y$. Preso un arbitrario $\overline{x} \in X$ definiamo $g : Y \to X$ ponendo

$$g(y) = \begin{cases} x_y & \text{se } y \in f(X) \\ \overline{x} & \text{se } y \notin f(X) \end{cases}$$

Dato che per ogni $x \in X$ l'unico elemento avente $f(x)$ come immagine è x stesso, si ha che $g(f(x)) = x$. ❑

Soluzione dell'esercizio 5.3
❑

Soluzione dell'esercizio 6.1
❑

Soluzione dell'esercizio 6.2 A partire dagli X_m costruiamo dei nuovi insiemi, ponendo

$$\begin{aligned} Y_0 &= X_0 \\ Y_{n+1} &= X_{n+1} - \bigcup_{m=0}^{n} X_m \qquad \forall n \geq 0 \end{aligned}$$

Gli insiemi in questione sono a due a due disgiunti, e $\bigcup_n Y_n = \bigcup_n X_n$. Si consideri l'insieme $A = \{n \in \mathbb{N} \mid Y_n \neq \varnothing\}$, allora $Y = \bigcup_{n \in A} Y_n$. Per quanto visto in precedenza (proposizione 6.4) A è finito o numerabile. Nel primo caso A è finito (esercizio 4.3), nel secondo caso è numerabile (proposizione 6.6). ❑

Soluzione dell'esercizio 6.3 Come nell'esercizio precedente, poniamo

$$\begin{aligned} Y_0 &= X_0 \\ Y_{n+1} &= X_{n+1} - \bigcup_{m=0}^{n} X_m \qquad \forall n \geq 0 \end{aligned}$$

Gli insiemi in questione sono a due a due disgiunti, e $\bigcup_n Y_n = \bigcup_n X_n$. Si consideri l'insieme $A = \{n \in \mathbb{N} \mid |Y_n| = \aleph_0\}$, $B = \{n \in \mathbb{N} \mid Y_n \neq \varnothing \text{ ed è finito}\}$, allora $Y = \bigcup_{n \in A} Y_n \cup \bigcup_{n \in B} Y_n$. Per quanto visto in precedenza (proposizione 6.4) A, e B sono finiti o numerabili. Dato che Y_0 è numerabile, $A \neq \varnothing$ e quindi $\bigcup_{n \in A} Y_n$ è numerabile. D'altra parte $\bigcup_{n \in B} Y_n$ è finito o numerabile e quindi la loro unione è numerabile. ❑

Soluzione dell'esercizio 6.4
❑

Soluzione dell'esercizio 6.5
❑

Soluzione dell'esercizio 6.6
❑

Soluzione dell'esercizio 6.7 La funzione $f : (0,1) \to \mathbb{R}$ definita da $f(t) = \tan(\pi t - \pi/2)$ è una bigezione. ❑

Soluzione dell'esercizio 6.8 Osserviamo che $X - Y$ non può essere né finito né numerabile, altrimenti $X = (X-Y) \cup Y$ sarebbe numerabile (cfr. proposizione 6.5). Ma allora $X - Y$ contiene (teorema 5.4) un sottinsieme, Y', numerabile. Dato che Y e Y' sono entrambi numerabili, la loro unione è numerabile (proposizione 6.5), sia quindi $f : Y' \to Y \cup Y'$ una bigezione e si definisca $g : X - Y \to X$ ponendo:

$$g(x) = \begin{cases} f(x) & \text{se } x \in Y' \\ x & \text{se } x \in X - (Y \cup Y') \end{cases}$$

g è chiaramente una bigezione. ❑

Soluzione dell'esercizio 6.9 Per ogni $k \in \mathbb{N}$ sia $F_k = \{A \in 2^{\mathbb{N}} \mid |A| = k\}$. Chiaramente $F = \bigcup_{k \in \mathbb{N}} F_k$. Proviamo che $|F_k| = \aleph_0$ per ogni $k \geq 1$. Procediamo per induzione su k. Se $k = 1$ allora l'applicazione $n \to \{n\}$ è una bigezione $\mathbb{N} \to F_1$. Supponiamo che F_k sia numerabile, allora per ogni $A \in F_k$ sia $F_{k+1}(A) = \{B \in F_{k+1} \mid B \supseteq A\}$. per ogni A l'insieme $F_{k+1}(A)$ è numerabile, in quanto in bigezione con $\mathbb{N} - A$, inoltre $F_{k+1} - \bigcup_{A \in F_k} F_{k+1}(A)$ è numerabile in quanto unione di una famiglia numerabile di insiemi numerabili (esercizio 6.3). ❑

Soluzione dell'esercizio 6.10
❑

Soluzione dell'esercizio 7.1
❑

Soluzione dell'esercizio 7.2
❑

Soluzione dell'esercizio 7.3
❑

Soluzione dell'esercizio 7.4
❑

Soluzione dell'esercizio 8.1 Dalla definizione del coefficiente binomiale (8.5) si ha

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

❑

Soluzione dell'esercizio 8.2 Si osservi che se X è un insieme con n elementi, allora

$$2^X = \bigcup_{i=0}^{n} \binom{X}{k}$$

e che questi insiemi sono a due a due disgiunti. Quindi

$$2^n = 2^{|X|} = \left|2^X\right| = \sum_{i=0}^{n} \left|\binom{X}{k}\right| = \sum_{i=0}^{n} \binom{|X|}{k} = \sum_{i=0}^{n} \binom{n}{k}$$

❑

Soluzione dell'esercizio 10.1 Procediamo per induzione su k. Se $k = 1$ non c'è nulla da dimostrare. Supponiamo che la tesi sia vera per k e supponiamo che $p \mid n_1 n_2 \dots n_{k+1}$, ossia $p \mid (n_1 n_2 \dots n_k) n_{k+1}$. Per il corollario 10.2, si ha che $p \mid n_1 n_2 \dots n_k$ oppure $p \mid n_{k+1}$. Se si verifica la seconda eventualità abbiamo finito, altrimenti, per ipotesi di induzione esiste $i \in \{1, \dots, k\}$ tale che $p \mid n_i$, e quindi si conclude. ❑

Soluzione dell'esercizio 10.2
❑

Soluzione dell'esercizio 10.3
❑

Soluzione dell'esercizio 10.4 Chiaramente $\prod_{i=1}^{s} p_i^{k_i \wedge h_i}$ è un divisore comune a n e m. Inoltre se c è un divisore comune non può avere fattori primi diversi dai p_i, quindi $c = \prod_{i=1}^{s} p_i^{l_i}$. Dal fatto che $c \mid n$ segue allora che $l_i \leq k_i$ e dal fatto che $c \mid m$ segue che $l_i \leq h_i$ per ogni i, e quindi $l_i \leq k_i \wedge h_i$.

La formula per il m.c.m. segue allora dal fatto che $[n, m] = |nm| / (n, m)$, e che per ogni coppia di numeri reali si ha che $h + k - h \wedge k = h \vee k$. ❑

Soluzione dell'esercizio 11.1
❑

Soluzione dell'esercizio 12.1
❑

Soluzione dell'esercizio 12.2
❑

Soluzione dell'esercizio 13.1
❑

Soluzione dell'esercizio 13.2
❑

Soluzione dell'esercizio 13.3 Osserviamo che $(a, pq) \neq 1$ se e solo se $p \mid a$ o $p \mid a$, ma i numeri più piccoli di pq che sono divisibili per p sono p, $2p, \dots, qp$, quelli che sono divisibili per q sono invece q, $2q, \dots, pq$ e quindi i numeri più piccoli di pq e non coprimi con pq sono $p + q - 1$. Quindi $\Phi(pq) = pq - (p + q - 1) = (p - 1)(q - 1)$.
❑

Soluzione dell'esercizio 13.4 $\Phi(n) = (p-1)(q-1) = pq-p-q+1 = n-p-q+1$ da cui $p+q = n+1-\Phi(n)$. Quindi p e q sono determinati dal sistema di equazioni

$$\begin{cases} p+q = n+1-\Phi(n) \\ pq = n \end{cases}$$

Una semplice sostituzione mostra che allora p e q devono essere le due radici dell'equazione $x^2 - (n+1-\Phi(n)) + n = 0$. ❑

Soluzione dell'esercizio 13.5
❑

Soluzione dell'esercizio 14.1
❑

Soluzione dell'esercizio 14.2
❑

Soluzione dell'esercizio 14.3
❑

Soluzione dell'esercizio 14.4
❑

Soluzione dell'esercizio 14.5
❑

Soluzione dell'esercizio 14.6
❑

Soluzione dell'esercizio 14.7
❑

Soluzione dell'esercizio 14.8
❑

Soluzione dell'esercizio 14.9 La colorazione dei lati data in figura 11 suggerisce come definire l'isomorfismo. Precismante se si definisce la funzione $f : \{1,2,\ldots,10\} \to \{a,b,\ldots,j\}$ ponendo

$$\begin{array}{lllllllllllllll} f(1) & = & a & f(2) & = & b & f(3) & = & c & f(4) & = & d & f(5) & = & e \\ f(6) & = & f & f(7) & = & g & f(8) & = & h & f(9) & = & i & f(10) & = & j \end{array}$$

una semplice verifica mostra che f è un isomorfismo. ❑

Soluzione dell'esercizio 14.10
❑

Soluzione dell'esercizio 14.11
❑

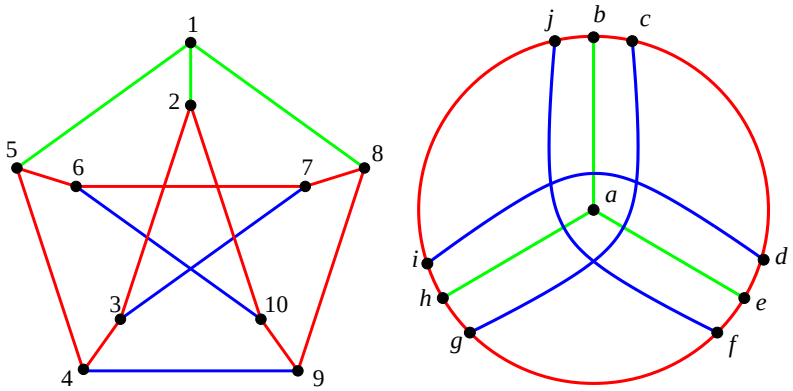

Figura 11: Soluzione grafica dell'esercizio 14.9

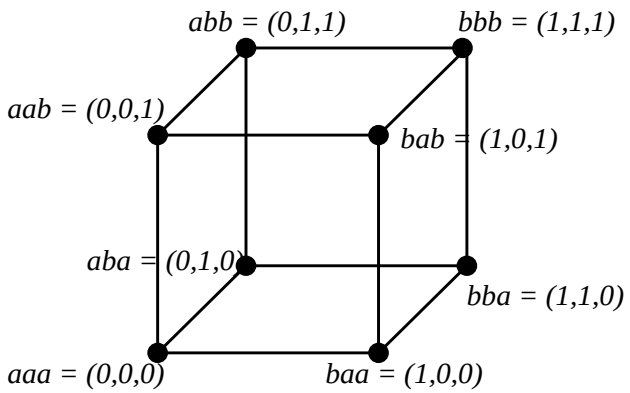

Figura 12: L'isomorfismo tra i grafi dell'esercizio 14.12

Soluzione dell'esercizio 14.12 Se identifichiamo la lettera a con il numero 0 e la b con l'1, si ottiene una identificazione delle parole con le coordinate dei vertici del cubo di $\mathbb{R}^3$ dato da $[0,1] \times [0,1] \times [0,1]$. Inoltre due vertici di tale cubo sono congiunti da uno spigolo se solo se differiscono esattamente per una coordinata. L'identificazione data è quindi un isomorfismo di grafi tra G e G'. ❑

Soluzione dell'esercizio 16.1 La prima segue dal fatto che i vertici delle componenti connesse sono le classi d'equivalenza di una relazione d'equivalenza. La seconda, segue dal fatto che ogni lato di G deve essere lato di una qualche classe d'equivalenza, dato che i suoi estremi sono congiungibili e pertanto appartengono alla stessa classe d'equivalenza. ❑

Soluzione dell'esercizio 19.1
❑

Soluzione dell'esercizio 19.2
❑

Soluzione dell'esercizio 19.3
❑

Soluzione dell'esercizio 19.4
❑

Soluzione dell'esercizio 19.5
❑

Soluzione dell'esercizio 19.6
❑

Soluzione dell'esercizio 19.7
❑

Soluzione dell'esercizio 20.1
❑

Soluzione dell'esercizio 20.3
❑

Soluzione dell'esercizio 20.4
❑

Soluzione dell'esercizio 20.5
❑

Soluzione dell'esercizio 20.6 Siano $T_1, \ldots, T_k$ le componenti connesse di F, allora ogni T_i è un albero, ma allora per ogni i si ha $|(|\,V(T_i)) = |(|\,E(T_i)) + 1$. Dal fatto che $\sum_{i=1}^{k} |(|\,V(T_i) = |(|\,V)$ e $\sum_{i=1}^{k} |(|\,E(T_i) = |(|\,E)$ segue immediatamente la tesi. ❑

Soluzione dell'esercizio 20.7 Sia T un albero generatore di G. Chiaramente $|V(T)| = |V(G)|$ e dato che T è un sottografo di G allora $|E(T)| \leq |E(G)|$ e quindi, usando la formula che lega il numero di lati con il numero dei vertici di un grafo (teorema 20.6), si ha

$$|E(G)| \geq |E(T)| = |V(T)| - 1 = |V(G)| - 1.$$

❑

Soluzione dell'esercizio 21.1
❑