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 (28 febbraio 2000 h. 9-11) **1**
- Insiemi e operazioni tra insiemi . . . 1
- Equipotenza di insiemi . . . 3
- Insiemi finiti: il Lemma dei cassetti . . . 3

Lezione 2 (29 febbraio 2000 h. 11-13) **5**
- Insiemi infiniti: l'assioma della scelta . . . 5
- Insiemi numerabili . . . 6

Lezione 3 (6 marzo 2000 h. 9-11) **8**
- Confronto di cardinalità: il Teorema di Cantor-Bernstein . . . 8
- La tricotomia dei cardinali . . . 9
- Il procedimento diagonale di Cantor . . . 9
- Operazioni tra cardinalità . . . 10

Lezione 4 (7 marzo 2000 h. 11-13) **11**
- I numeri naturali: gli assiomi di Peano . . . 11
- Il principio di induzione (prima forma) . . . 12
- L'assioma di buon ordinamento . . . 12
- Il principio di induzione (seconda forma) . . . 13
- La divisione euclidea . . . 13
- Scommettiamo che due di voi hanno lo stesso compleanno? . . . 14

Lezione 5 (13 marzo 2000 h. 9-11) **15**
- Scrittura in base arbitraria dei naturali. . . . 15
- Divisibilità e sue prime proprietà . . . 15
- Il massimo comun divisore: definizione, esistenza e unicità . . . 16
- Il coefficiente binomiale . . . 17
- k-sottinsiemi . . . 17
- Il binomio di Newton . . . 17
- Perché non gioco al Superenalotto! . . . 18

Lezione 6 (14 marzo 2000 h. 11-13) **18**
- L'algoritmo di Euclide per il calcolo del M.C.D. . . . 18
- Proprietà dei numeri coprimi e caratterizzazione dei numeri primi 18
- Il minimo comune multiplo: definizione, esistenza e unicità 19
- Il teorema fondamentale dell'Aritmetica 19
- Esistenza di infiniti numeri primi 20
- Il principio di inclusione ed esclusione 20

Lezione 7 (27 marzo 2000 h. 9-11) **20**
- Definizione di congruenza e prime proprietà 20
- Classi di congruenza 21
- Le classi modulo n sono esattamente n 21
- Successioni di tipo Fibonacci 22

Lezione 8 (28 marzo 2000 h. 11-13) **22**
- Somma e prodotto di classi di congruenza 22
- equazioni lineari modulo n 24
- Il teorema cinese del resto 24

Lezione 9 (31 marzo 2000 h. 9-11) **25**
- Elementi invertibili modulo n 25
- Il piccolo teorema di Fermat 26
- Crittografia RSA 26

Lezione 10 (3 aprile 2000 h. 9-11) **27**
- Quadrati latini 27
- Quadrati latini ortogonali 27

Lezione 11 (4 aprile 2000 h. 11-13) **28**
- Permutazioni di un insieme finito 28
- Decomposizione in cicli disgiunti 28
- Segno di una permutazione 28
- Il gioco del quindici 28

Lezione 12 (10 aprile 2000 h. 9-11) **28**
- Esercizi 28

Lezione 13 (11 aprile 2000 h. 11-13) **28**
- Esercizi 28

Lezione 14 (2 maggio 2000 h. 11-13) **28**
- Definizione di grafo 28
- Grafi notevoli 29
- Isomorfismo di grafi 30
- Una stima del numero di grafi non isomorfi su n vertici 31

Lezione 15 (8 maggio 2000 h. 9-11) **31**
- Sottografi e sottografi indotti 31
- Passeggiate, cammini e cicli 31
- La relazione di essere congiungibili 31
- Componenti connesse di un grafo 31
- La matrice di incidenza di un grafo 31

Lezione 16 (9 maggio 2000 h. 11-13) **31**
- Grado di un vertice . . . 31
- Il lemma delle strette di mano . . . 31
- Score di un grafo . . . 32
- Teorema dello score . . . 32

Lezione 17 (12 maggio 2000 h. 10.30-12.30) **32**
- Definizione di grafo euleriano . . . 32
- Caratterizzazione dei grafi euleriani . . . 32
- Cenni sui multigrafi . . . 32
- Definizione di grafo hamiltoniano . . . 32
- Grafo duale di un grafo dato . . . 32
- G è connesso se e solo se il suo duale lo è . . . 32
- Se G è euleriano allora il suo duale è hamiltoniano . . . 32

Lezione 18 (15 maggio 2000 h. 9-11) **32**
- Alcune costruzioni con i grafi . . . 32
- Definizione di grafo 2-connessi . . . 32
- Prima caratterizzazione dei grafi 2-connessi . . . 32
- Seconda caratterizzazione dei grafi 2-connessi . . . 32

Lezione 19 (16 maggio 2000 h. 11-13) **33**
- Alberi . . . 33
- Il teorema di caratterizzazione degli alberi . . . 33
- Il teorema di caratterizzazione degli alberi finiti . . . 35

Lezione 20 (22 maggio 2000 h. 9-11) **36**
- Alberi radicati . . . 36
- La relazione $\rightarrow$ di "paternità" in un albero radicato . . . 37
- Cenni sui grafi diretti . . . 37
- Composizione di relazioni . . . 38
- Potenza di una relazione . . . 38
- Chiusura transitiva di una relazione . . . 38

Lezione 21 (23 maggio 2000 h. 11-33) **40**
- L'ordinamento degli alberi radicati . . . 40
- Gli alberi radicati sono ben fondati . . . 40
- Induzione sugli alberi radicati . . . 40

Lezione 22 (29 maggio 2000 h. 9-11) **41**
- Il lemma di König . . . 41
- Albero generatore di un grafo . . . 42
- Esistenza di alberi generatori: il caso finito . . . 42

Lezione 23 (30 maggio 2000 h. 11-13) **43**
- Il lemma di Zorn . . . 43
- Esistenza di alberi generatori: il caso infinito . . . 43

Lezione 24 (31 maggio 2000 h. 9-11) **45**
- Esercizi . . . 45

Soluzione di alcuni degli esercizi proposti **46**

Lezione 1 (28 febbraio 2000 h. 9-11)

Insiemi e operazioni tra insiemi

Non intendiamo qui dare un'assiomatica della teoria degli insiemi, per noi un insieme sarà soltanto una collezione di oggetti detti i suoi *elementi*. La proprietà fondamentale che si richied 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 vuota 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*.

L'altra proprietà fondamentale degli insiemi, e che fornisce un criterio per stabilire quando due insiemi sono uguali, è la seguente

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

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

Ricordiamo alcune definizioni.

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 $X \neq Y$.

Se X e Y sono insiemi si costruiscono altri insiemi:

- *intersezione* $X \cap Y = \{x \mid x \in X \text{ e } x \in Y\}$
- *unione* $X \cup Y = \{x \mid x \in X \text{ o } x \in Y\}$
- *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
- *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* $2^X = \{x \mid x \subseteq X\}$
- $X^Y = \{f \subseteq X \times Y \mid f \text{ è una funzione totale } X \to Y\}$

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* $\bigcup_{i \in I} X_i = \{x \mid \exists\, i\ x \in X_i\}$

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

Equipotenza di insiemi

Definizione 1.3. 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 1.4. 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.

Proposizione 1.5. *Valgono le seguenti proprietà:*

1. *X è equipotente a se stesso.*
2. *se X è equipotente a Y allora X 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 1.5. 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 1.6. Si provi che $\left|2^X\right| = |\{0,1\}|^X$.

Esercizio 1.7. Si provi che $|X \times X| = \left|X^{\{0,1\}}\right|$.

Esercizio 1.8. Si provi che se X, Y, Z sono insiemi, allora $\left|(X^Y)^Z\right| = \left|X^{Y \times Z}\right|$.

Esercizio 1.9. Si provi che se X, Y, Z sono insiemi con $Y \cap Z = \varnothing$, allora $\left|X^{Y \cup Z}\right| = \left|X^Y \times X^Z\right|$.

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 1.6. 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 1.7 (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. ❑

Corollario 1.8. *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 $n = m$.

Si osservi che questo corollario fa sì che si possa definire la cardinalità degli insiemi finiti.

Definizione 1.9. Sia X un insieme finito, si dice *cardinalità* di X l'unico numero naturale n tale che $|X| = |I_n|$.

Osservazione 1.10. 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.*

Proposizione 1.11. *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 $f : I_n \to X$ una bigezione e sia, poniamo $x_n = f(n)$ e $X' = X - \{x_n\}$. Chiaramente $|X'| = n$. 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 1.12. *Un insieme finito non è equipotente ad alcun suo sottoinsieme proprio.*

Esempio 1.13. L'insieme $\mathbb{N}$ non è finito, si consideri ad esempio l'applicazione $\mathbb{N} \to \mathbb{N}$ definita da $n \mapsto 2n$, questa è una bigezione tra $\mathbb{N}$ ed il sottinsieme proprio dei numeri pari.

Esercizio 1.10. 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 1.11. 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 1.12. 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 1.13. Siano X e Y insiemi finiti entrambi di cardinalità n. Si provi che ogni funzione iniettiva $X \to Y$ è anche surgettiva.

Esercizio 1.14. Sia X un insieme finito di cardinalità n. Si determini il numero delle applicazioni biunivoche di X in sé.

Lezione 2 (29 febbraio 2000 h. 11-13)

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 2.1 (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 2.2. 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 **non costruttivo** per antonomasia: ci dice che una funzione di scelta esiste, ma non dà alcun modo per trovarla.

Esercizio 2.1. 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 2.2. 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 2.3. *Se X è un insieme infinito, allora contiene un sottinsieme Y con $|Y| = |\mathbb{N}|$.*

Dimostrazione. Sia $\varphi : 2^X - \{\varnothing\} \to X$ una funzione di scelta e, dato un elemento $x_0 \in X$ consideriamo la funzione $\psi : \mathbb{N} \to 2^X$ 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 2.4. In qualche senso il teorema precedente mostra come la cardinalità dei numeri naturali sia, in un senso ancora da specificare (vedi 3.1) la "più piccola" tra le cardinalità infinite.

Proposizione 2.5. *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 (proposizione 1.13) 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 $Y' \subsetneq Y$. 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 1.12, provano la seguente caratterizzazione degli insiemi infiniti.

Teorema 2.6. *Un insieme è infinito se e solo se è equipotente ad un suo sottinsieme proprio.*

Insiemi numerabili

Definizione 2.7. 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 2.8. *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 2.9. *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 2.10. *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 3.4. ❑

Proposizione 2.11. *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 (2.10) e la proposizione 1.11 $Y - X$ è finito o numerabile.

Sia $Z \subseteq X$ un sottinsieme numerabile (teorema 2.3), per le due proposizioni 2.9, 2.8, 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 2.12. *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 2.13. *$\mathbb{N} \times \mathbb{N}$ 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 1.5). ❑

Proposizione 2.14. *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 2.3. Si eseguano nel dettaglio tutte le verifiche necessarie a concludere le dimostrazioni delle proposizioni di questa sezione.

Esercizio 2.4. 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 2.5. 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 2.6. Si provi che $\mathbb{Q}$ è numerabile.

Lezione 3 (6 marzo 2000 h. 9-11)

Confronto di cardinalità: il Teorema di Cantor-Bernstein

Definizione 3.1. 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 3.1. 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 3.2. Si provi che $|X| \leq |Y|$ se e solo se esiste $f : Y \to X$ surgettiva.

Proposizione 3.2. *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 3.3. 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 3.4. *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 $B = \bigcup_n A_n$. 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

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

Proviamo che g è una bigezione. g è iniettiva ❑

Teorema 3.5 (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 (3.4) $|X| = |g(Y)|$. 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 3.6 (tricotomia dei cardinali). *Per ogni coppia di insiemi X, Y si ha che o $|X| \leq |Y|$ oppure $|Y| \leq |X|$.*

Osservazione 3.7. 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 3.8 (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 3.9. 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 1.6)

		0	1	2	3	4	5	6	...
$f(0)$	=	$\boxed{1}$	0	0	1	1	0	0	...
$f(1)$	=	0	$\boxed{0}$	1	1	0	1	1	...
$f(2)$	=	1	0	$\boxed{0}$	0	1	0	1	...
$f(3)$	=	1	1	1	$\boxed{1}$	0	0	0	...
$f(4)$	=	0	0	0	1	$\boxed{1}$	1	1	...
$f(5)$	=	1	1	1	0	0	$\boxed{0}$	0	...
$f(6)$	=	1	0	1	1	1	1	$\boxed{0}$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
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 3.10. 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.

$$\begin{array}{lcllllllll}
f(0) & = & 0. & \boxed{1} & 4 & 9 & 2 & 2 & 0 & 3 & \dots \\
f(1) & = & 0. & 2 & \boxed{3} & 7 & 2 & 7 & 2 & 1 & \dots \\
f(2) & = & 0. & 1 & 3 & \boxed{2} & 1 & 8 & 2 & 5 & \dots \\
f(3) & = & 0. & 8 & 1 & 7 & \boxed{6} & 1 & 7 & 8 & \dots \\
f(4) & = & 0. & 7 & 6 & 8 & 3 & \boxed{8} & 9 & 5 & \dots \\
f(5) & = & 0. & 5 & 7 & 6 & 5 & 7 & \boxed{1} & 3 & \dots \\
f(6) & = & 0. & 4 & 9 & 9 & 4 & 3 & 1 & \boxed{4} & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\
 & & & & & & & & & & \\
r & = & 0. & 2 & 2 & 1 & 1 & 1 & 2 & 1 & \dots
\end{array}$$

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 3.3). Si può in realtà dimostrare che $|\mathbb{R}| = 2^{\aleph_0}$ (cfr. esercizio 3.6).

Esercizio 3.3. Si provi che $|(0,1)| = |\mathbb{R}|$.

Esercizio 3.4. Siano $Y \subseteq X$. Si provi che se $|X| > |Y| = \aleph_0$ allora $|X - Y| = |X|$.

Esercizio 3.5. Siano $F = \{A \in 2^{\mathbb{N}} \mid A \text{ è finito}\}$. Si provi che $|F| = \aleph_0$

Esercizio 3.6. 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 $|\mathbb{R}| = \left|2^{\mathbb{N}}\right|$.

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 1.9)), con una serie di esercizi, vediamo come si possano ugualmente definire delle operazioni tra cardinalità.

Esercizio 3.7. 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 3.11. 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 3.8. Si provi che le operazioni appena definite, nel caso di insiemi finiti, coincidono con le usuali operazioni tra numeri naturali.

Esercizio 3.9. 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 3.10. 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. $\left(|X|^{|Y|}\right)^{|Z|} = |X|^{|Y|\,|Z|}$

Lezione 4 (7 marzo 2000 h. 11-13)

I numeri naturali: gli assiomi di Peano

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

Assioma 4.1. $0 \in \mathbb{N}$

Assioma 4.2. $\mathrm{succ} : \mathbb{N} \to \mathbb{N}$ è una funzione iniettiva

Assioma 4.3. $\forall n \in \mathbb{N} \quad \mathrm{succ}(n) \neq 0$

Assioma 4.4 (di induzione). se $A \subseteq \mathbb{N}$ è un sottinsieme tale che

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

allora $A = \mathbb{N}$.

Proposizione 4.5. *Sia $n \in \mathbb{N}$, $n \neq 0$ allora esiste un unico $m \in \mathbb{N}$ tale che* $\mathrm{succ}(m) = n$. *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 $\mathrm{succ}(n) \neq m$ 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. ❑

A partire dagli assiomi si possono definire ricorsivamente la somma, il prodotto di numeri naturali e il loro ordinamento.

Definizione 4.6. Si definisce la somma di due naturali:

$$\begin{array}{rcll} n+0 & = & n & \forall n \in \mathbb{N} \\ n+\mathrm{succ}(m) & = & \mathrm{succ}(n+m) & \forall n,m \in \mathbb{N} \end{array}$$

Avendo la somma si definisce induttivamente il prodotto:

$$\begin{array}{rcll} n \cdot 0 & = & 0 & \forall n \in \mathbb{N} \\ n \cdot (m+1) & = & (n \cdot m) + n & \forall n,m \in \mathbb{N} \end{array}$$

Dalla somma si ricava anche la definizione delll'ordinamento:

$$n \leq m \iff \exists k \in \mathbb{N} : n+k = m$$

Esercizio 4.1. Si dimostrino le proprietà associativa, commutativa della somma e del prodotto, la proprietà distributiva del prodotto rispetto alla somma

Esercizio 4.2. Si provi che $\leq$ è un ordinamento totale su $\mathbb{N}$ e che verifica le seguenti proprietà:

$$\begin{array}{lrcl} \forall n,m,k \in \mathbb{N} & n \leq m & \Rightarrow & n+k \leq m+k \\ \forall n,m,k \in \mathbb{N} & n \leq m & \Rightarrow & nk \leq mk \\ \forall n,m,k \in \mathbb{N} & n < m \text{e } k \neq 0 & \Rightarrow & nk < mk \end{array}$$

Il principio di induzione (prima forma)

Una conseguenza immediata dell'assioma di induzione (4.4) è il seguente

Teorema 4.7 (prima 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 $n \in \mathbb{N}$ $P(n) \Rightarrow P(n+1)$*

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 $n \in A$ anche $n+1 \in A$, quindi per l'assioma di induzione (4.4) $A = \mathbb{N}$. ❑

L'assioma di buon ordinamento

Definizione 4.8. Un ordinamento totale su un insieme X si dice un *buon ordinamento*, e in tal caso l'insieme ordinatoo $(X, \leq)$ si dice *ben ordinato* se ogni sottinsieme non vuoto di X ha minimo.

Teorema 4.9 (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 4.10 (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 (4.9) 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 4.11. 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 4.12. *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 4.10) 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 $r = r'$. ∎

Scommettiamo che due di voi hanno lo stesso compleanno?

Storiella. Il professore di Matematica Discreta entra nell'aula, davanti ai suoi 60 studenti esclama: —Scommettiamo che due di voi hanno lo stesso compleanno?— e aggiunge —se io perdo pago la cena a tutti, se vinco voi pagete una cena a me.—

Gli studenti accettano entusiasti la scommessa: —Male che vada ci rimettiamo 1000 lire ciascuno, ma in ogni caso— pensano —è praticamente impossibile che il prof. vinca, siamo troppo pochi.—

Una rapida verifica e quindi la delusione: il professore, come ogni anno, si è *guadagnato* una cena.

Perché il prof. ha vinto? È soltanto una fortuna sfacciata, che gli consente di vincere ogni anno, o è qualcos'altro?

Formalizziamo la situazione. Associare ad ogni studente il proprio giorno di nascita è una funzione da un insieme X con 60 elementi (l'insieme degli studenti) in un insieme Y con 365 elementi (l'insieme dei possibili giorni di nascita, escludendo il caso degli anni bisestili). Il professore perde se tale funzione è iniettiva, vince altrimenti. Si tratta allora di contare il numero di funzioni iniettive, e dividerlo per il numero di funzioni, questo darà la probabilità di perdere la scommessa da parte del professore.

Esercizio 4.3. Siano X e Y insiemi finiti di cardinalità rispettivamente k e n, con $k \leq n$. Si provi che l'insieme delle applicazioni iniettive $X \to Y$ ha cardinalità pari a $n!/(n-k)!$.

Questo, assieme al risultato dell'esercizio 1.12 (punto 2), ci dice che:
Se $|X| = k$ e $|Y| = n$ la probabilità che una funzione $f : X \to Y$ sia iniettiva è pari a

$$\frac{n!}{(n-k)!n^k}$$

Questa formula applicata al caso $n = 365$ e $k = 60$ produce: 0.005877. Ciò spiega perché il professore si fa una cena gratis ogni anno (vedi figura 1).

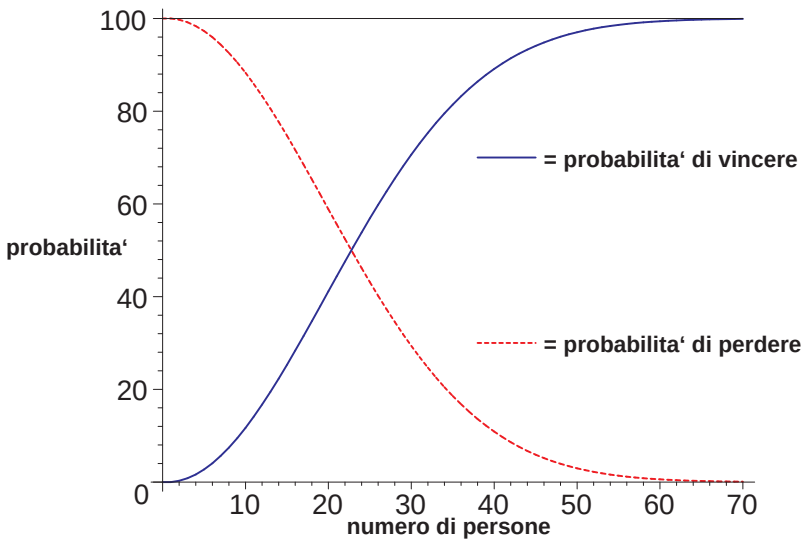

Figura 1: Grafico della probabilità di successo o di insuccesso in funzione del numero di persone. Già con 60 persone si ha la ragionevole certezza di vincere la scommessa: la probabilità di successe è attorno al 99%

Lezione 5 (13 marzo 2000 h. 9-11)

Scrittura in base arbitraria dei naturali.

Teorema 5.1 (scrittura dei naturali in base arbitraria). *Sia $b \geq 2$ un intero. Allora per ogni $n \in \mathbb{N}$ 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. *$n = \sum_{i=0}^{\infty} \varepsilon_i b^i$.*

Tale successione è unica, ovvero se $\{\varepsilon_i\}_{i\in\mathbb{N}}$ e $\{\varepsilon'_i\}_{i\in\mathbb{N}}$ verificano la 1, 2, 3 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 nonnegativo, 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 4.12) 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 $i \geq 1$. ∎

Divisibilità e sue prime proprietà

Definizione 5.2. 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 5.3. $n \mid 0$ 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 5.4.

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 5.5. 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 5.6. 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 5.7. *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 5.4 si ha che $d' = \pm d$. ❑

Definizione 5.8. 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 5.9. *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 5.10. 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 5.11. $n, m \in \mathbb{Z}$ non entrambi nulli si dicono *coprimi* se $(n, m) = 1$.

Osservazione 5.12. $(n, m) = 1$ 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 5.13. *Sia* $d = (n, m)$, *allora* $(\frac{n}{d}, \frac{m}{d}) = 1$.

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

Il coefficiente binomiale

Definizione 5.14. Siano n, $k \in \mathbb{N}$ con $k \leq n$ si pone

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

Esercizio 5.1. Provare che

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

k-sottinsiemi

Definizione 5.15. 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 5.16. *Se X è finito, allora*

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

Dimostrazione. ❑

Definizione 5.17. Una *k-combinazione con ripetizione* di un insieme X è la scelta di k elementi di X, che possono essere anche ripetuti, indipendentemente dall'ordine.

Esempio 5.18. In altri termini una k combinazione di X è il risultato di k scelte indipendenti di elementi di X.

Se $X = \{a, b, c, d\}$ le seguenti sono delle 3-combinazioni: *aaa*, *abb*, *abc*. Si osservi che *aab* e *aba* danno la stessa combinazione, dato che non ci interessa l'ordine in cui viene effettuata la scelta, ma soltanto il risultato complessivo.

Esercizio 5.2. Si elenchino tutte le 3 combinazioni dell'insieme $X = \{a, b, c, d\}$.

Proposizione 5.19. *Se $|X| = n$ allora il numero di k-combinazioni con ripetizione di X è dato da:*

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

Esercizio 5.3. Provare che

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

Il binomio di Newton

Proposizione 5.20. *Siano a, b numeri reali, allora*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Dimostrazione. ❑

Esercizio 5.4. Si provi che

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

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 5.16 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 6 (14 marzo 2000 h. 11-13)

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

Proposizione 6.1 (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.

Proprietà dei numeri coprimi e caratterizzazione dei numeri primi

Proposizione 6.2.

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 6.3. *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 5.4 si ha che $d = \pm p$ e $h = \pm 1$ oppure $p \mid h$ e quindi $h = \pm p$ e $d = \pm 1$. ❑

Esercizio 6.1. 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 6.4. 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 6.5 (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 6.2 si ha che $n'm' \mid c'$ e quindi che $M = n'm'(n, m) \mid c'(n, m) = c$. ❑

Esercizio 6.2. 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 6.3. 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 6.6 (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 $n = p_1 \dots p_k = q_1 \dots q_h$ con p_i e q_j primi positivi e $k \leq h$. Procediamo per induzione su k. Se $k = 1$ allora $n = p_1 = q_1 \dots q_h$, 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 $n = q_1 \dots q_h \geq q_1 q_2 = p_1^2 > p_1 = n$ e questo è assurdo, e quindi $h = 1$ e $q_1 = p_1$.

Sia $k > 1$, allora $p_k \mid n = q_1 \dots q_h$, quindi per l'esercizio 6.1 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 $p_1 \dots p_{k-1} = q_1 \dots q_{j-1} q_{j+1} \dots q_h$, 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 $\delta : \{1, \dots, j-1, j+1, \dots, k\} \to \{1, \dots, k-1\}$ tale che $q_i = p_{\delta(i)}$ per ogni i. Definendo allora $\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$

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

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

Esistenza di infiniti numeri primi

Corollario 6.7. *I numeri primi sono infiniti.*

Dimostrazione. Per assurdo supponiamo che $p_1, p_2, \dots, p_n$ siano tutti iprimi. Si consideri $n = p_1 p_2 \dots p_n + 1$. 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 (6.6). ❑

Esercizio 6.4. [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 $[n, m] = \prod_{i=1}^{s} p_i^{k_i \vee h_i}$.

Il principio di inclusione ed esclusione

Lezione 7 (27 marzo 2000 h. 9-11)

Definizione di congruenza e prime proprietà

Definizione 7.1. 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 7.2. *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 7.3. Una relazione $\mathcal{R}$ su X si dice *d'equivalenza* se

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

Osservazione 7.4. La proposizione precedente può essere allora rienunciato dicendo che *la relazione di congruenza modulo n è una relazione d'equivalenza su $\mathbb{Z}$.*

Classi di congruenza

Definizione 7.5. 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 7.6. $x \equiv a \mod n$ se e solo se $n \mid (x - a)$ se e solo se esiste $k \in \mathbb{Z}$ tale che $x - a = kn$ se e solo se esiste $k \in \mathbb{Z}$ tale che $x = a + kn$ e quindi

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

Proposizione 7.7. *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 $a, b \in \mathbb{Z}$ $[a]_n \cap [b]_n \neq \varnothing \Rightarrow [a]_n = [b]_n$.

Dimostrazione. 1. Segue dalla proprietà riflessiva (1 di 7.2).

2. Se $[a]_n = [b]_n$ in particolare $b \in [b]_n = [a]_n$ e quindi $a \equiv b \mod n$. Viceversa sia $a \equiv b \mod n$. Se $x \in [a]_n$ allora $x \equiv a \mod n$; per la proprietà transitiva (3 di 7.2) $x \equiv b \mod n$ ossia $x \in [b]_n$. Analogamente se $x \in [b]_n$ allora $x \in [a]_n$ e quindi le due classi coincidono.

3. Se $x \in [a]_n \cap [b]_n$ allora $x \equiv a \mod n$ e $x \equiv b \mod n$, usando le proprietà simmetrica e transitiva si ha allora che $a \equiv b \mod n$ e quindi, per la (2), appena dimostrata, $[a]_n = [b]_n$. ❑

In generale data una relazione d'equivalenza su un insieme

Le classi modulo n sono esattamente n

Proposizione 7.8. *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 7.9. *Se $n > 0$ allora $\mathbb{Z}/_{n\mathbb{Z}}$ ha esattamente n elementi.*

Dimostrazione. Da 7.8 e dalla 2 di 7.7 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 $n \not| (k - h)$ e quindi (sempre per la 2 di 7.7) $[h]_n \neq [k]_m$. ❑

Successioni di tipo Fibonacci

La *successione di Fibonacci* è la successione $\{F_n\}$ così definita

$$\begin{cases} F_0 &= 0 \\ F_1 &= 1 \\ F_{n+2} &= F_{n+1} + F_n \qquad \text{se } n \geq 0 \end{cases}$$

Esercizio 7.1. Si provi che $(F_{n+1}, F_n) = 1$ per ogni $n \geq 0$.

Esercizio 7.2. Si provi che

$$F_n = \frac{1}{\sqrt{5}}\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \frac{1}{\sqrt{5}}\Big(\frac{1-\sqrt{5}}{2}\Big)^n$$

Esercizio 7.3. Si provi che dette α e β le radici del polinomio $x^2 - 3x + 2$, allora le successioni $A\alpha^n + B\beta^n$ al variare di A e B sono tutte e sole le successioni tali che

$$x_{n+2} = 3x_{n+1} - 2$$

Esercizio 7.4. Si determini la successione tale che

$$\begin{cases} x_{n+2} &= 4x_{n+1} - 3 \\ x_0 &= 0 \\ x_1 &= 1 \end{cases}$$

In effetti si può dimostrare il seguente

Teorema 7.10. *Siano $a_0, \ldots, a_{k-1} \in \mathbb{R}$ (o anche $\mathbb{C}$), tali che il polinomio $P(t) = t^k - \sum_{i=0} a_i t^i$ ammette k radici distinte $\alpha_1, \ldots, \alpha_k$, allora le successioni del tipo*

$$x_n = A_1\alpha_1^n + \wedge_2\alpha_2^n + \ldots + A_k\alpha_k^n \qquad A_i \in \mathbb{R}\ (\mathbb{C})$$

sono tutte e sole le successioni tali che

$$x_{n+k} = \sum_{i=0} a_i x_{n+i} \qquad \forall\, n \in \mathbb{N}.$$

In più, dati numeri $b_0, \ldots, b_{k-1} \in \mathbb{R}$ ($\mathbb{C}$) esiste un'unica di tali successioni tale che

$$x_0 = b_0,\ x_1 = b_1, \ldots, x_{k-1} = b_{k-1}.$$

Lezione 8 (28 marzo 2000 h. 11-13)

Somma e prodotto di classi di congruenza

Proposizione 8.1. *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 8.2. 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 7.7 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 7.7 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 8.1. 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 8.3. 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
$$\underbrace{1 + 1 + \ldots + 1}_{n-\text{volte}} = 0 \text{ in } \mathbb{Z}/n\mathbb{Z}$$

equazioni lineari modulo n

Proposizione 8.4. *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 5.10), 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 8.5. 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 8.2. Si provi che quando ha soluzione, la congruenza $ax \equiv b \mod n$ è equivalente alla congruenza

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

essendo $a' = a/(a, n)$, $b' = b/(a, n)$, $n' = n/(a, n)$.

Il teorema cinese del resto

Teorema 8.6 (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 5.10, 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

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

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 8.1) 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 8.3. 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 8.4. 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. $11 \mid n \iff 11 \mid (\varepsilon_0 - \varepsilon_1 + \ldots + (-1)^k \varepsilon_k)$

Lezione 9 (31 marzo 2000 h. 9-11)

Elementi invertibili modulo n

Definizione 9.1. Sia $a \in \mathbb{Z}/n\mathbb{Z}$ diremo che a è *invertibile* se esiste $y \in \mathbb{Z}/n\mathbb{Z}$ tale che $ax = 1$ (in $\mathbb{Z}/n\mathbb{Z}$). L'insieme degli elementi invertibili di $\mathbb{Z}/n\mathbb{Z}$ si indica con $\mathbb{Z}/n\mathbb{Z}^*$.

Proposizione 9.2. *a è invertibile in $\mathbb{Z}/n\mathbb{Z}$ se e solo se $(a, n) = 1$.*

Dimostrazione. Segue immediatamente da proposizione 8.4, osservando che $(n, a) \mid 1$ se e solo se $(n, a) = 1$. ❑

Corollario 9.3. *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. ❑

Osservazione 9.4. 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 9.3), 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 9.5. *Siano x, y due inversi di a in $\mathbb{Z}/n\mathbb{Z}$, allora $x = y$ (in $\mathbb{Z}/n\mathbb{Z}$).*

Dimostrazione. Dal fatto che $ax = 1$, moltiplicando entrambi i membri per y, ed usando le proprietà associativa, commutativa e dell'1 (esercizio 8.1) si ottiene

$$y = 1y = (ax)y = (xa)y = x(ay) = x1 = x.$$

❑

La proposizione precedente garantisce che se $a \in \mathbb{Z}/_{n\mathbb{Z}}$ è invertibile, allora c'è un solo $x \in \mathbb{Z}/_{n\mathbb{Z}}$ tale che $ax = 1$. Tale x viene chiamato *l'inverso* di a e viene denotato con a^{-1}.

Proposizione 9.6. *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 9.7. 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 9.4) 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.

Il piccolo teorema di Fermat

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 9.2 e di proposizione 7.8.

Proposizione 9.8. *Per ogni $n > 0$, si ha che $\left|\mathbb{Z}/_{n\mathbb{Z}}{}^*\right| = \Phi(n)$.*

Teorema 9.9. *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 9.7), 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 9.6), ne segue (per quanto osservato in 9.4) che $u^k = 1$. ❑

Corollario 9.10 (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 9.1. 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 9.11. *Sia c coprimo con $\Phi(n)$, allora l'applicazione $C : \mathbb{Z}/_{n\mathbb{Z}}{}^* \to \mathbb{Z}/_{n\mathbb{Z}}{}^8$ 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 (9.9), 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 9.2) $\Phi(m) = (p-1)(q-1)$ e per i quali, determinare $\Phi(m)$ a partire da m è equivalente (esercizio 9.3) a determinare la fattorizzazione di m.

Esercizio 9.2. Provare che se p, q sono primi allora $\Phi(pq) = (p-1)(q-1)$

Esercizio 9.3. 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 9.4. 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 10 (3 aprile 2000 h. 9-11)

Quadrati latini

Definizione 10.1.

Quadrati latini ortogonali

Esercizio 10.1. Determinare tre quadrati latini 5×5 a due a due ortogonali.

Lezione 11 (4 aprile 2000 h. 11-13)

Permutazioni di un insieme finito

Decomposizione in cicli disgiunti

Segno di una permutazione

Il gioco del quindici

Lezione 12 (10 aprile 2000 h. 9-11)

Esercizi

Lezione 13 (11 aprile 2000 h. 11-13)

Esercizi

Lezione 14 (2 maggio 2000 h. 11-13)

Definizione di grafo

Definizione 14.1. Un grafo G è una coppia ordinata $G = (V, E)$ dove V è un insieme 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.

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 14.1).

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 2 sono rappresentati i grafi G e G'definiti da

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

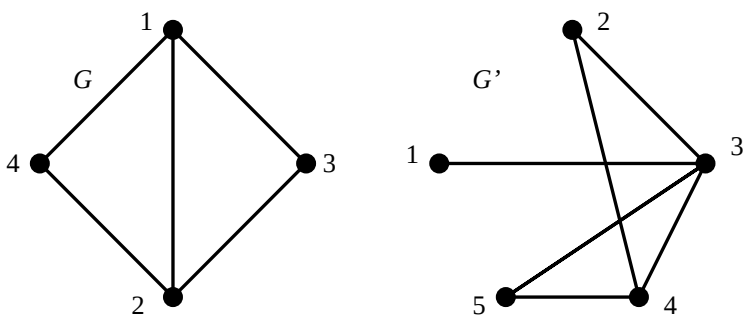

Figura 2: Esempi di grafi

Esercizio 14.1. Sia (V, E) un grafo e si definisca la relazione $\mathcal{R}(E)$ su V ponendo

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

Si provi che:

1. $\mathcal{R}(E)$ è simmetrica (i.e. $v_1\ \mathcal{R}(E)\ v_2 \Rightarrow v_2\ \mathcal{R}(E)\ v_1$)
2. $\mathcal{R}(E)$ è antiriflessiva (i.e. $\forall v \quad \neg\, v\ \mathcal{R}(E)\ v$)

La relazione $\mathcal{R}(E)$ è a volte detta relazione di *adiacenza*.

Esercizio 14.2. Sia V un insieme, e sia $\sim$ una relazione antiriflessiva su V. Si definisca $\mathcal{E}(() \sim) = \{\{v_1, v_2\} \mid v_1 \sim v_2\}$. Si provi che $(V, \mathcal{E}(\sim))$ è un grafo.

Esercizio 14.3. Con riferimento ai due esercizi precedenti, si provi 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 $\mathcal{R}(\mathcal{E}(\sim))=\sim$.

Osservazione 14.2. Gli esercizi precedenti provano che dare un grafo i cui vertici sono l'insieme V è equivalente a dare una relazione simmetrica e antiriflessiva su V.

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

$$\begin{aligned} V(P_n) &= \{0, 1, 2, \ldots, n\} \\ E(P_n) &= \big\{\{i, i+1\} \,\big|\, i = 0, 1, \ldots, n-1\big\} \end{aligned}$$

P_n è detto il *cammino* di lunghezza n (i.e. ha n 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

$$\begin{aligned} V(K_n) &= \{u_1, u_2, \ldots, u_n\} \cup \{v_1, v_2, \ldots, v_m\} \\ E(K_n) &= \big\{\{u_i, v_j\} \,\big|\, i = 1, \ldots, n, j = 1, \ldots, m\big\} \end{aligned}$$

K_n 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).

Isomorfismo di grafi

Definizione 14.3. Due grafi $G = (V, E)$ e $G' = (V', E')$ si dicono *isomorfi*, e si denoterà con $G \cong G'$, se e siste una bigezione $f : V \to V'$ tale che $e \in E \iff f(e) \in E'$, dove se $e = \{x, y\}$ si è denotato $f(e) = \{f(x), f(y)\}$. Una tale applicazione f sarà detta un *isomorfismo* tra G e G'.

Esercizio 14.4. 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 14.5. Si provi che i due grafi rappresentati in figura 3 sono tra loro isomorfi.

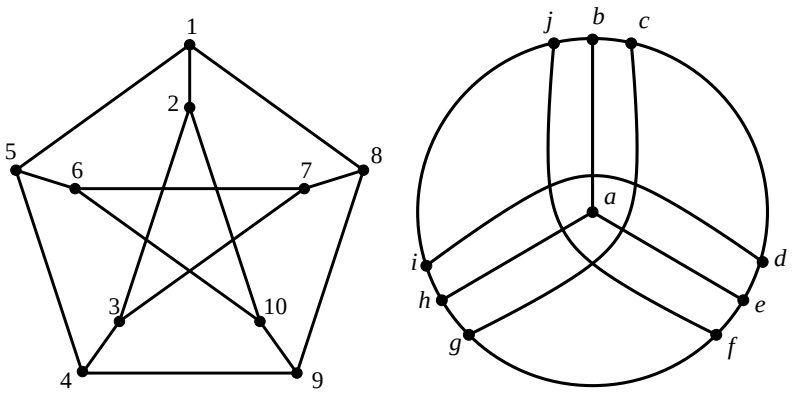

Figura 3: I grafi di esercizio 14.5

Esercizio 14.6. Dire se i due grafi in figura 4 sono isomorfi oppure no.

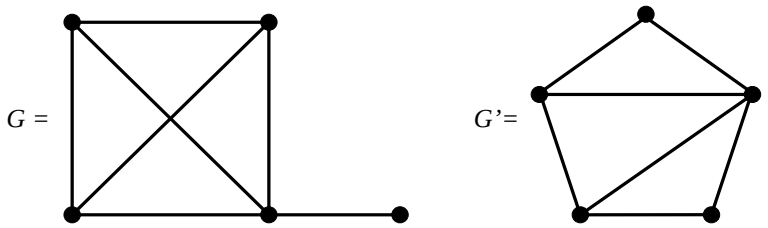

Figura 4: I grafi dell'esercizio 14.6

Esercizio 14.7. Provare che i due grafi in figura 5 non sono isomorfi.

Esercizio 14.8. 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 $G \cong G'$.

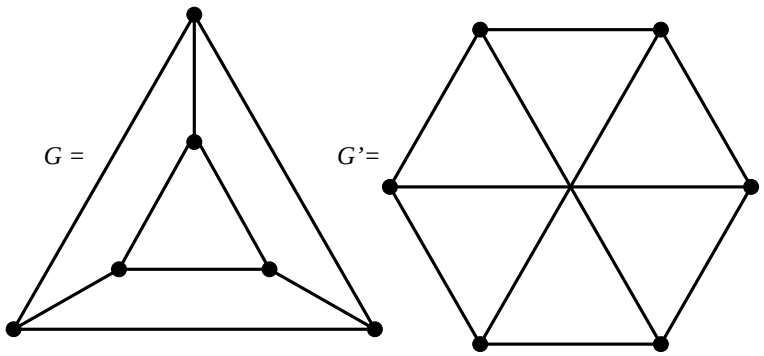

Figura 5: I grafi dell'esercizio 14.7

Una stima del numero di grafi non isomorfi su n vertici

Lezione 15 (8 maggio 2000 h. 9-11)

Sottografi e sottografi indotti

Passeggiate, cammini e cicli

La relazione di essere congiungibili

Proposizione 15.1. *Le relazione di essere congiungibli da un cammino è una relazione d'equivalenza.*

Componenti connesse di un grafo

La matrice di incidenza di un grafo

Definizione 15.2.

Lezione 16 (9 maggio 2000 h. 11-13)

Grado di un vertice

Definizione 16.1. 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 16.2. *Se $G = (V, E)$ è un grafo finito, allora*

$$\sum_{v \in V} \deg(v) = 2\,|E| \tag{1}$$

Il lemma delle strette di mano

Proposizione 16.3. *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 16.4. 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 16.5. *Se G e G' sono grafi isomorfi, allora* $\text{score}(G) = \text{score}(G')$.

Osservazione 16.6. Non è vero il viceversa del precedente teorema.

Teorema dello score

Lezione 17 (12 maggio 2000 h. 10.30-12.30)

Definizione di grafo euleriano

Caratterizzazione dei grafi euleriani

Cenni sui multigrafi

Definizione di grafo hamiltoniano

Grafo duale di un grafo dato

G è connesso se e solo se il suo duale lo è

Se G è euleriano allora il suo duale è hamiltoniano

Lezione 18 (15 maggio 2000 h. 9-11)

Alcune costruzioni con i grafi

Definizione di grafo 2-connessi

Prima caratterizzazione dei grafi 2-connessi

Seconda caratterizzazione dei grafi 2-connessi

Esercizio 18.1. 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 18.2. Si provi che se G e G' sono 2-connessi e $|V \cap V'| \geq 2$ allora $G \cup G'$ è 2-connesso.

Esercizio 18.3. 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 18.4. Si determinino condizioni sufficienti affinché l'unione di due grafi k-connessi sia ancora k-connesso.

Esercizio 18.5. 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 18.6. 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 18.7. 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 19 (16 maggio 2000 h. 11-13)

Alberi

Definizione 19.1. Si dice *albero* un grafo connesso e senza cicli. Si dice una *foresta* un grafo senza cicli.

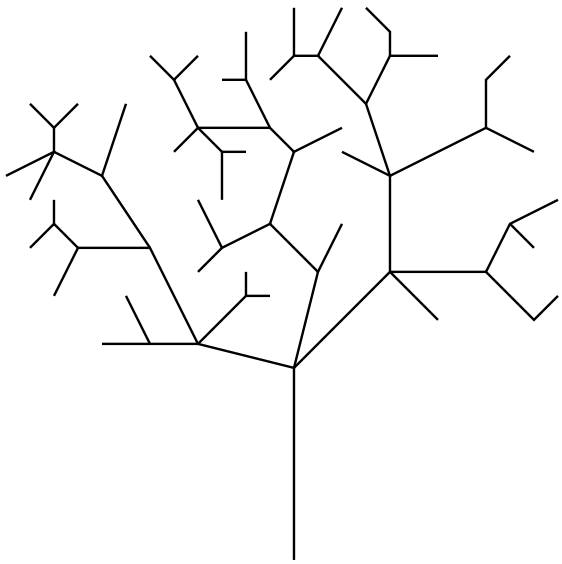

Figura 6: Un albero

Esercizio 19.1. 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 19.2. *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.*

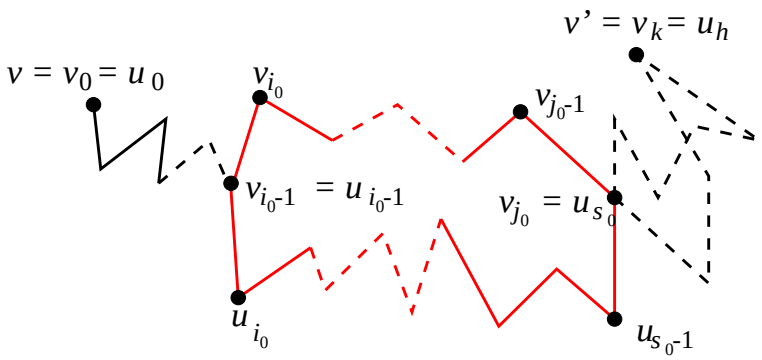

Figura 7: La costruzione del ciclo nella dimostrazione di (1) $\Rightarrow$ (2)

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 $v' = v_k = u_h$ 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).

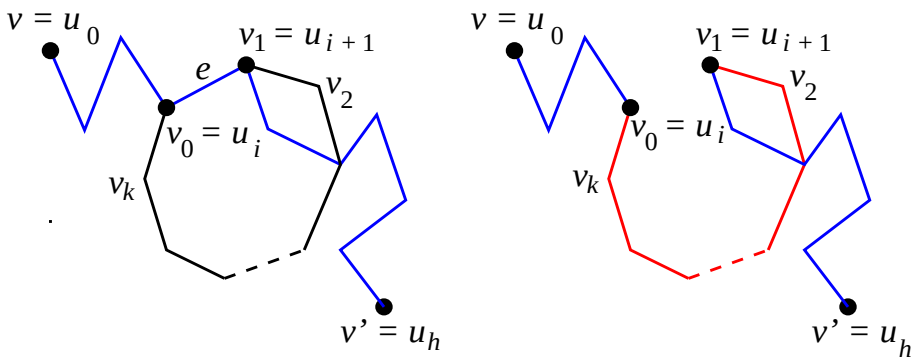

Figura 8: La costruzione della passeggiata nella dimostrazione di (3) $\Rightarrow$ (4)

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

Esercizio 19.2. Si determinino le foglie dell'albero in figura 6

Lemma 19.4. *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 19.5. 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 19.3. 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 19.4. Si provi che se T è un albero con almeno due vertici e v è una sua foglia, allora $T - v$ è un albero.

Esercizio 19.5. Quante foglie può avere al massimo un grafo connesso con n vertici? Si determini un grafo con il massimo numero di foglie possibili.

Teorema 19.6. *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 (19.4), ora $T - e$ è un albero (esercizio 19.4) 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 (1), 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 19.6. Se $F = (V, E)$ è una foresta allora $|V| - |E| = k$, essendo k il numero di componenti connesse di F.

Esercizio 19.7. Si provi che ogni grafo connesso finito G, ha un sottografo che è un albero e contiene tutti i vertici di G.

Un tale albero si chiama *un albero generatore* di G.

Esercizio 19.8. Si provi che se $G = (V, E)$ è un grafo connesso finito, allora $|E| \geq |V| - 1$.

Lezione 20 (22 maggio 2000 h. 9-11)

Alberi radicati

Definizione 20.1. 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 20.1. Si considerino i grafi in figura 9. Si provi che $T \cong T'$ ma $(T, r) \ncong (T', r')$.

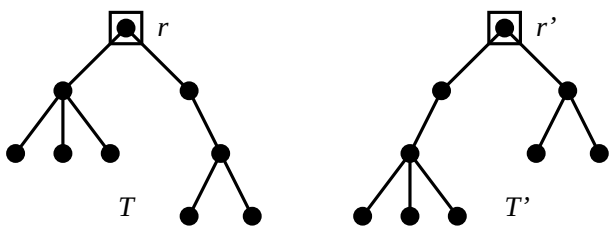

Figura 9: Gli alberi radicati dell'esercizio 20.1

La relazione $\to$ 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 19.2 punto 2) che congiunge r con v.

Proposizione 20.2. *Sia (T, r) un albero radicato e sia $\{v, w\} \in E(T)$, allora vale una e una sola delle seguenti:*

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 19.2 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 20.3. 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 20.4. *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 $\to$. ❑

Cenni sui grafi diretti

Definizione 20.5. Un *grafo diretto* è una coppia (V, E) dove V è un insieme e $E \subset V \times V$. Gli elementi di E vengono ancora chiamati lati e dati $v, w \in V(T)$ scriveremo $v \to_E w$, o più semplicemente $v \to w$ per dire che $(v, w) \in E$.

Osservazione 20.6. Intuitivamente un grafo diretto può essere pensato come un grafo, in cui sono specificati dei "versi di percorrenza" degli archi che congiungono due punti. Un po' come la mappa di una città in cui si tenga conto dei sensi unici.

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 10).

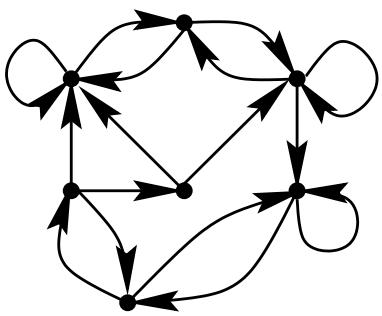

Figura 10: Un grafo diretto

Si noti però che l'osservazione 14.2 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).

Osservazione 20.7. La proposizione 20.4 può essere interpretata dicendo che ogni albero radicato può essere dotato in modo naturale di una struttura di grafo diretto, in modo che ad ogni lato dell'albero corrisponda uno ed un solo lato del grafo diretto.

Esercizio 20.2. Si diano le definizioni di passeggiata diretta, cammino diretto, ciclo diretto in un grafo diretto e si provi che due vertici sono congiungibili da una passeggiata diretta se e solo se sono congiungibili da un cammino diretto. Si usi questo fatto per provare che la relazione "essere congiungibili da un cammino diretto" è una relazione transitiva e riflessiva sull'insieme dei vertici di un grafo diretto. È vero che è una relazione d'equivalenza?

Composizione di relazioni

Ricordiamo la definizione di relazione tra insiemi:

Definizione 20.8. Se X e Y sono insiemi, una *relazione tra* X e Y è un sottinsieme $\mathcal{R} \subseteq X \times Y$, si usa la notazione $x\mathcal{R}y$ per dire che $(x, y) \in \mathcal{R}$.

Definizione 20.9. Siano $\mathcal{R} \subset X \times Y$ e $\mathcal{S} \subset Y \times Z$ si definisce la *composizione* di $\mathcal{R}$ con $\mathcal{S}$ la relazione $\mathcal{R} \circ \mathcal{S} \subseteq x \times Z$ definita da

$$\mathcal{R} \circ \mathcal{S} = \{(x, z) \mid \exists y \in Y : x\mathcal{R}y \text{ e } y\mathcal{S}z\}$$

Esercizio 20.3. Si provi che se $\mathcal{R} \subseteq X \times Y$, $\mathcal{S} \subseteq Y \times Z$ e $\mathcal{T} \subseteq Z \times W$ allora

$$\mathcal{R} \circ (\mathcal{S} \circ \mathcal{T}) = (\mathcal{R} \circ \mathcal{S}) \circ \mathcal{T}.$$

Definizione 20.10. Dato un insieme X si indica con I_X la relazione *identica* su X, ovvero $I_X = \{(x, x) \mid x \in X\}$.

Esercizio 20.4. Si provi che se $\mathcal{R}$ è una relazione tra X e Y, allora si ha che $\mathcal{R} \circ I_Y = I_X \circ \mathcal{R} = \mathcal{R}$.

Esercizio 20.5. Siano $\mathcal{R}_1, \mathcal{R}_2$ delle relazioni tra X e Y e sia $\mathcal{S}$ una relazione tra Y e Z. Si provi che $(\mathcal{R}_1 \cup \mathcal{R}_2) \circ \mathcal{S} = ((\mathcal{R}_1 \circ \mathcal{S}) \cup (\mathcal{R}_2 \circ \mathcal{S})$.

Potenza di una relazione

Definizione 20.11. Data una relazione $\mathcal{R}$ su un insieme X, per ogni $n \in \mathbb{N}$, indicheremo con $\mathcal{R}^n$ la relazione su X definita ricorsivamente da:

$$\begin{cases} \mathcal{R}^0 = I \\ \mathcal{R}^{n+1} = \mathcal{R}^n \circ \mathcal{R} \quad \forall n \in \mathbb{N} \end{cases}$$

$\mathcal{R}^n$ è detta la potenza n-esima di $\mathcal{R}$.

Chiusura transitiva di una relazione

Definizione 20.12. Sia $\mathcal{R}$ una relazione su X, diremo che una relazione $\mathcal{T}$ è una *chiusura transitiva* di $\mathcal{R}$ se

1. $\mathcal{T}$ è transitiva
2. $\mathcal{T} \supseteq \mathcal{R}$
3. per ogni relazione transitiva su X che estende $\mathcal{R}$ si ha $\mathcal{S} \supseteq \mathcal{T}$.

Teorema 20.13. *Sia X un insieme e $\mathcal{R}$ una relazione su X, allora esiste una unica chiusura transitiva di $\mathcal{R}$, che è data da:*

$$\mathcal{R}^+ = \bigcup_{n=1}^{\infty} \mathcal{R}^n.$$

Definizione 20.14. Sia $\mathcal{R}$ una relazione su X, diremo che una relazione $\mathcal{T}$ è una *chiusura transitiva e riflessiva* di $\mathcal{R}$ se

1. $\mathcal{T}$ è transitiva e riflessiva
2. $\mathcal{T} \supseteq \mathcal{R}$
3. per ogni relazione transitiva e riflessiva su X che estende $\mathcal{R}$ si ha $\mathcal{S} \supseteq \mathcal{T}$.

Teorema 20.15. *Sia X un insieme e $\mathcal{R}$ una relazione su X, allora esiste una unica chiusura transitiva e riflessiva di $\mathcal{R}$, che è data da:*

$$\mathcal{R}^* = \bigcup_{n=0}^{\infty} \mathcal{R}^n = I \cup \mathcal{R}^+.$$

Osservazione 20.16. I due teoremi precedenti (20.13 e 20.15) permettono di sostituiore l'articolo indeterminativo nelle definizioni 20.12 e 20.14 con l'articolo determinativo. Si parlerà quindi del*la chiusura transitiva* e del*la chiusura transitiva e riflessiva* di una relazione $\mathcal{R}$, che saranno denotate rispettivamente con $\mathcal{R}^+$ e $\mathcal{R}^*$. I teoremi già citati danno anche un modo costruttivo per trovare $\mathcal{R}^+$ e $\mathcal{R}^*$.

Esercizio 20.6. Sia $\mathcal{R}$ una relazione su X e sia $\mathcal{S}_n$ la successione di relazioni definite ricorsivamente da:

$$\begin{cases} \mathcal{S}_1 = I \cup \mathcal{R} \\ \mathcal{S}_{n+1} = \mathcal{S}_n \circ \mathcal{R} \quad \forall n \geq 1 \end{cases}$$

Si provi che $\mathcal{R}^* = \bigcup_{n=1}^{\infty} \mathcal{S}_n$.

Esercizio 20.7. Si provi che $x\mathcal{R}^n y$ se e solo se esistono $x_0, x_1, \ldots, x_n \in X$ tali che $x_i \mathcal{R} x_{i+1}$ per ogni $i = 0, \ldots, n-1$ e $x_0 = x$, $x_n = y$.

Esercizio 20.8. Si provi che se $\{\mathcal{R}_j\}_{j \in J}$ è un insieme di relazioni transitive su X allora $\bigcap_{i \in I} \mathcal{R}_i$ è ancora una relazione transitiva su X.

Si usi questo fatto per mostrare che

$$\mathcal{R}^+ = \bigcap_{\mathcal{S} \in S} \mathcal{S}$$

essendo $S = \{\mathcal{S} \subseteq X \times X \mid \mathcal{S} \supseteq \mathcal{R} \text{ e } \mathcal{S} \text{ è transitiva}\}$.

Esercizio 20.9. Si provi che se $\{\mathcal{R}_j\}_{j \in J}$ è un insieme di relazioni riflessive su X allora $\bigcap_{i \in I} \mathcal{R}_i$ è ancora una relazione riflessiva su X.

Si usi questo fatto per mostrare che

$$\mathcal{R}^* = \bigcap_{\mathcal{S} \in S} \mathcal{S}$$

essendo $S = \{\mathcal{S} \subseteq X \times X \mid \mathcal{S} \supseteq \mathcal{R} \text{ e } \mathcal{S} \text{ è transitiva e riflessiva}\}$.

Lezione 21 (23 maggio 2000 h. 11-33)

L'ordinamento degli alberi radicati

Sia (T, r) un albero radicato, sull'insieme dei vertici sono allora definite le due relazioni $\rightarrow^+$ e $\rightarrow^*$, ovvero la chiusura transitive e la chiusura transitiva e riflessiva della relazione $\rightarrow$ di paternità (definizione 20.3).

Ricordiamo la seguente

Definizione 21.1. Un *ordinamento parziale* su un insieme X è una relazione $\preccurlyeq$ che sia

1. riflessiva (i. e. $\forall x \in X \; x \preccurlyeq x$)
2. antisimmetrica (i.e. $\forall x_1, x_2 \in X \; x_1 \preccurlyeq x_2$ e $x_2 \preccurlyeq x_1 \Rightarrow x_1 = x_2$)
3. transitiva (i.e. $\forall x_1, x_2, x_3 \in X \; x_1 \preccurlyeq x_2$ e $x_2 \preccurlyeq x_3 \Rightarrow x_1 \preccurlyeq x_3$)

un ordinamento partziale $\preccurlyeq$ su X si dice un *ordinamento totale* se in più

4 per ogni $x_1, x_2 \in X \; x_1 \preccurlyeq x_2$ oppure $x_2 \preccurlyeq x_1$.

Proposizione 21.2. *La relazione $\rightarrow^*$ è un ordinamento parziale. E la relazione $\rightarrow^+$ è l'ordinamento stretto associato a $\rightarrow^*$ ossia $v \rightarrow^+ w$ se e solo se $v \rightarrow^* w$ e $v \neq w$.*

Dimostrazione. ❑

Gli alberi radicati sono ben fondati

Definizione 21.3. 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 $x_n = x_{\overline{n}}$)).

Lemma 21.4. *In un albero radicato l'insieme dei predecessori di un vertice è finito. Formalmente, se (T, r) è un albero radicato, allora per ogni $v \in V(T)$ si ha che l'insieme $\{v \in V(T) \mid w \rightarrow^* v\}$ è finito.*

Dimostrazione. ❑

Teorema 21.5. *L'ordinamento $\rightarrow^*$ è ben fondato.*

Dimostrazione. ❑

Induzione sugli alberi radicati

Teorema 21.6 (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 $(\forall w \rightarrow^+ wP(w)) \Rightarrow P(v)$. Allora $P(v)$ è vera per ogni $v \in V(T)$.*

Dimostrazione. ❑

Osservazione 21.7. 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 sull'insieme dei vertici, e che tale insieme possedesse un minimo rispetto a tale ordinamento. La stessa dimostrazione può quindi essere usata per dimostrare il seguente teorema

Teorema 21.8 (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 $x \in X$.

Lezione 22 (29 maggio 2000 h. 9-11)

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 22.1).

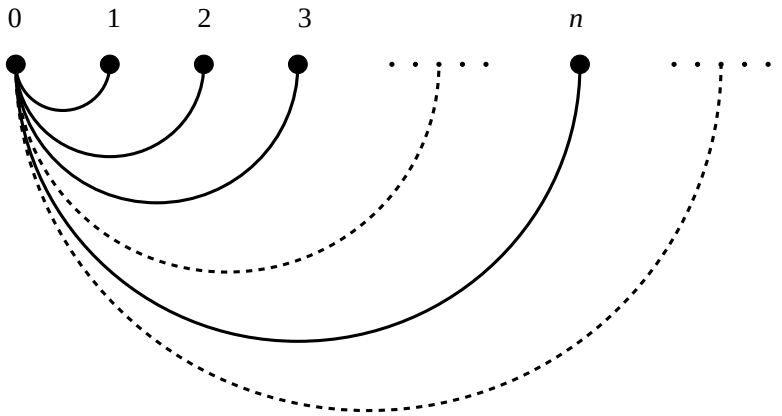

Figura 11: Un contresempio al Lemma di König, senza l'ipotesi dei gradi finiti

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 19.2).

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:

Teorema 22.1 (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. ❑

Albero generatore di un grafo

Definizione 22.2. Sia G un grafo, diremo che un albero T è un *albero generatore* (in inglese *spanning tree* se T è un sottografo di G e $V(T) = V(G)$.

Osservazione 22.3. Si osservi che se G possiede un albero generatore T, allora necessariamente è connesso, in quanto T è connesso.

Esistenza di alberi generatori: il caso finito

Teorema 22.4. *Sia G un grafo finito connesso, allora G possiede un albero generatore.*

Dimostrazione. Procediamo per induzione su $|EG|$. Se $|EG| = 0$ allora $|V(G)| = 1$ (l'unico grafo connesso che non ha lati ha un solo vertice) e quindi $G \cong (\{0\}, \varnothing)$ è un albero.

Supponiamo che $|EG| > 0$, allora o G è un albero e quindi lui stesso è un albero generatore di se stesso, oppure per la terza delle proprietà che caratterizzano gli alberi (teorema 19.2) esiste un lato $e \in E(G)$ tale che $G - e$ è ancora connesso. Ma allora $|E(G-e)| = |E(G)| - 1$, quindi, per ipotesi di induzione, esiste un albero T che è un sottografo di $G-e$ e tale che $V(T) = V(G-e)$. Dato che $V(G-e) = V(G)$, T è un albero generatore anche per G. ❑

Osservazione 22.5. Si osservi che la dimostrazione del teorema precedente, fornisce un algoritmo ricorsivo per la costruzione di un albero generatore di un grafo connesso finito. Un algoritmo più efficiente è dato nel seguenteesercizio.

Esercizio 22.1. Sia G un grafo connesso, finito e siano $e_1, \ldots, e_n$ i suoi lati. Si ponga

$$\begin{aligned} T_0 &= \left(\{V(G)\}, \varnothing\right) \\ T_{i+1} &= \begin{cases} T_i & \text{se } T_i + e_{i+1} \text{ ha cicli} \\ T_i + e_{i+1} & \text{altrimenti} \end{cases} \end{aligned}$$

Si provi che T_n è un albero generatore per G.

Lezione 23 (30 maggio 2000 h. 11-13)

Il lemma di Zorn

Definizione 23.1. Sia X un insieme e sia $\preccurlyeq$ un ordinamento parziale (definizione 21.1) su X. Diremo che $x_0 \in X$ è un *maggiorante* di $Y \subseteq X$ se e solo se $y \preccurlyeq x_0$ per ogni $y \in Y$.

Diremo che $Y \subseteq X$ è una *catena* se è totalmente ordinato da $\preccurlyeq$, ossia se

$$\forall y_1, y_2 \in Y \quad y_1 \preccurlyeq y_2 \text{ o } y_2 \preccurlyeq y_1$$

Un elemento $x_0 \in X$ sarà detto *massimale* se

$$\forall x \in X \quad x_0 \preccurlyeq x \Rightarrow x = x_0$$

ossia non esiste in X niente di strettamente più grande di x_0.

Osservazione 23.2. Si osservi che essere massimale **non** implica *massimo*, (x_0 è *massimo* se $x \preccurlyeq x_0$ per ogni $x \in X$). Potrebbero infatti esserci elementi massimali diversi ma non confrontabili tra loro. Si consideri ad esempio l'ordinamento $\rightarrow^*$ sui vertici dell'albero radicato (T, r) essendo $V(T) = \{r, a, b\}$ e $E(T) = \{\{r, a\}, \{r, b\}\}$ (vedi figura 12). Evidentemente a e b sono entrambi massimali, ma non $a \not\rightarrow^* b$ e $b \not\rightarrow^* a$.

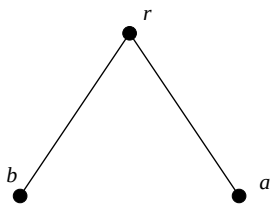

Figura 12: L'albero dell'esempio 23.2

Enunciamo ora un teorema di cui omettiamo la dimostrazione, ma che è uno degli strumenti più potenti per dimostrare l'esistenza di "oggetti" che sono in qualche senso più grandi possibili. Daremo subito nel seguito un'applicazione di tale teorema.

Teorema 23.3 (Lemma di Zorn). *Sia X un insieme non vuoto e sia $\preccurlyeq$ un ordinamento parziale su X. Se ogni catena di X ammetta un maggiorante, allora X ha elementi massimali (se per ogni catena $Y \subseteq X$ esiste $x \in X$ maggiorante di Y, allora esiste $x_0 \in X$ massimale).*

L'unica osservazione che facciamo sulla dimostrazione di questo teorema, è che essa usa im modo sostanziale l'assioma della scelta (2.1), anzi si può dimostrare che il lemma di Zorn è equivalente all'assioma della scelta. Si osservi che come l'assioma della scelta anche il lemma di Zorn ha una natura non costruttiva: garantisce l'esistenza di elementi massimali, ma non dà alcuna "ricetta" per individuarli.

Esistenza di alberi generatori: il caso infinito

Teorema 23.4. *Sia G un grafo connesso non vuoto. Allora G ha un albero generatore.*

Dimostrazione. Consideriamo l'insieme

$$\mathcal{T} = \{T \mid T \text{ è un albero sottografo di } G\}$$

Chiaramente $\mathcal{T} \neq \varnothing$, dato che se v è un vertice di G, allora il grafo $(\{v\}, \varnothing) \in \mathcal{T}$.

Definiamo la relazione $\preccurlyeq$ su $\mathcal{T}$, ponendo per ogni $T_1, T_2 \in \mathcal{T}$

$$T_1 \preccurlyeq T_2 \iff T_1 \text{ è sottografo di } T_2$$

ovvero

$$T_1 \preccurlyeq T_2 \iff V(T_1) \subseteq V(T_2) \text{ e } E(T_1) \subseteq E(T_2)$$

Chiaramente $\preccurlyeq$ è un ordinamento parziale su $\mathcal{T}$.

Proviamo che tale ordinamento verifica le ipotesi del lemma di Zorn (teorema 23.3). Sia $\mathcal{S} \subset \mathcal{T}$ una catena e proviamo che ha un maggiorante. Poniamo

$$\overline{S} = \Big(\bigcup_{T \in \mathcal{S}} V(T), \bigcup_{T \in \mathcal{S}} E(T) \Big)$$

Chiaramente, se $\overline{S} \in \mathcal{T}$ allora è un maggiorante, dato che se $S \in \mathcal{S}$, allora

$$\begin{aligned} V(S) &\subseteq \bigcup_{T \in \mathcal{S}} V(T) = V(\overline{S}) \\ E(S) &\subseteq \bigcup_{T \in \mathcal{S}} E(T) = E(\overline{S}) \end{aligned}$$

ossia $S \preccurlyeq \overline{S}$.

Proviamo nell'ordine che $\overline{S}$ è un grafo, che è un sottografo di G, che è connesso e che non ha cicli.

$\overline{S}$ è un grafo. Se $e \in E(\overline{S})$ allora esiste $S \in \mathcal{S}$ tale che $e \in E(S)$. Dato che S è un grafo allora $E(S) \subseteq \binom{V(S)}{2}$, e dato che $V(S) \subseteq V(\overline{S})$ allora $\binom{V(S)}{2} \subseteq \binom{V(\overline{S})}{2}$. Quindi $e \in \binom{V(\overline{S})}{2}$, e per l'arbitrarietà di $e \in E(\overline{S})$ si ha che $E(\overline{S}) \subseteq \binom{V(\overline{S})}{2}$.

$\overline{S}$ è un sottografo di G. Dato che ogni S è sottografo di G, si ha che per ogni $T \in \mathcal{S}$ si ha che $V(T) \subseteq V(G)$ e $E(T) \subseteq E(G)$, da cui segue immediatamente che $V(\overline{S}) = \bigcup_{T \in \mathcal{S}} V(T) \subseteq V(G)$ $E(\overline{S}) = \bigcup_{T \in \mathcal{S}} E(T) \subseteq E(G)$.

$\overline{S}$ è connesso. Siano $v, w \in V(\overline{S})$, allora esistono $T_1, T_2 \in \mathcal{S}$ tali che $u \in V(T_1)$ e $w \in V(T_2)$. Dato che $\mathcal{S}$ è totalmente ordinato da $\preccurlyeq$ uno tra T_1 e T_2 è più grande dell'altro. Supponiamo che sia $T_1 \preccurlyeq T_2$. Aallora $V(T_1) \subseteq V(T_2)$ e quindi $v, w \in V(T_2)$. Dato che T_2 è un albero, esiste un cammino in T_2 che congiunge v a w, sia questo $(v = v_0, v_1, \ldots, v_k = w)$. Tale cammino è un cammino anche in $\overline{S}$ dato che per ogni i si ha che $v_i \in V(T_2) \subseteq V(\overline{S})$ e $\{v_i, v_{i+1}\} \in E(T_2) \subseteq E(\overline{S})$.

$\overline{S}$ non ha cicli. Supponiamo per assurdo che $\overline{S}$ abbia un ciclo $(v_0, v_1, \ldots, v_k = v_0)$. Per ogni i $v_i \in V(\overline{S}$, quindi esiste un $T_i \in \mathcal{S}$ tale che $v_i \in V(T_i)$. Usando iterativamente il fatto che a due a due i T_i sono uno più grande dell'altro, se ne trova uno che è più grande di tutti gli altri, ossia esiste j tale che $T_i \preccurlyeq T_j$ per ogni i. In modo analogo per ogni lato $\{v_i, v_{i+1}\} \in E(\overline{S})$ e quindi per ogni i esiste un $S_i \in \mathcal{S}$ tale che $\{v_i, v_{i+1}\} \in E(S_i)$. In modo analogo a quanto fatto sopra si trova un h tale che $S_i \preccurlyeq S_h$ per ogni i. Detto infine U il più grande tra S_h e T_j si ha che per ogni i si ha che

$$\begin{aligned} T_i \preccurlyeq U &\Rightarrow V(T_i) \subseteq V(U) \Rightarrow v_i \in V(U) \\ S_i \preccurlyeq U &\Rightarrow V(S_i) \subseteq V(U) \Rightarrow \{v_i, v_{i+1}\} \in E(U) \end{aligned}$$

Ma allora $(v_0, v_1, \ldots, v_k = v_0)$ sarebbe un ciclo in U, ma ciò è assurdo dato che U è un albero.

Siamo allora nelle ipotesi per applicare il lemma di Zorn (teorema 23.3). Sia allora $T \in \mathcal{T}$ un elemento massimale. Quindi T è un albero che è un sottografo di G, massimale rispetto all'ordinamento $\preccurlyeq$. Proviamo che $V(T) = V(G)$. Per assurdo, sia $v \in V(G)$ ma $v \notin V(T)$. Dato che G è connesso (è qui che si usa la connessione di G), preso $w \in V(T)$ esiste un cammino $(v = v_0, \ldots, v_k = w)$, sia allora i tale che $v_i \notin V(T)$ e $v_{i+1} \in V(T)$. Allora il grafo $T' = \Big(V(T) \cup \{v_{i+1}\}, E \cup \big\{\{V_i, v_{i+1}\}\big\}\Big)$ sarebbe ancora un elemento di $\mathcal{T}$, sarebbe diverso da T e $T \preccurlyeq T'$, che è contro la massimalità di T. ❑

Esercizio 23.1. Sia $\{G_i\}_{i \in I}$ un insieme di grafi, e si ponga

$$\begin{aligned} \bigcup_{i \in I} G_i &= \Big(\bigcup_{i \in I} V(G_i), \bigcup_{i \in I} E(G_i)\Big) \\ \bigcap_{i \in I} G_i &= \Big(\bigcap_{i \in I} V(G_i), \bigcap_{i \in I} E(G_i)\Big) \end{aligned}$$

Si provi che $\bigcup_{i \in I} G_i$ e $\bigcap_{i \in I} G_i$ sono grafi.

Si provi inoltre che se i G_i sono tutti connessi e $V(G_i) \cap V_(G_j) \neq \varnothing$ per ogni $i, j \in I$ allora $\bigcup_{i \in I} G_i$ è connesso.

Resta vero l'enunciato precedente se si sostituisce la parola connesso con 2-connesso? In caso di risposta negativa si determini l'ipotesi giusta affinché lo sia.

Lezione 24 (31 maggio 2000 h. 9-11)

Esercizi

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 1.10 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 1.11 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 1.10), 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 1.12
❑

Soluzione dell'esercizio 1.13
❑

Soluzione dell'esercizio 1.14
❑

Soluzione dell'esercizio 2.1 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 (2.1), 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 2.2 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 2.3
❑

Soluzione dell'esercizio 2.4 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 2.10) A è finito o numerabile. Nel primo caso A è finito (esercizio 1.11), nel secondo caso è numerabile (proposizione 2.12). ❑

Soluzione dell'esercizio 2.5 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 2.10) 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 2.6
❑

Soluzione dell'esercizio 3.1
❑

Soluzione dell'esercizio 3.2
❑

Soluzione dell'esercizio 3.3 La funzione $f : (0,1) \to \mathbb{R}$ definita da $f(t) = \tan(\pi t - \pi/2)$ è una bigezione. ❑

Soluzione dell'esercizio 3.4 Osserviamo che $X - Y$ non può essere né finito né numerabile, altrimenti $X = (X-Y)\cup Y$ sarebbe numerabile (cfr. proposizione 2.11). Ma allora $X - Y$ contiene (teorema 2.3) un sottinsieme, Y', numerabile. Dato che Y e Y' sono entrambi numerabili, la loro unione è numerabile (proposizione 2.11), 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 3.5 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 2.5). ❑

Soluzione dell'esercizio 3.6
❑

Soluzione dell'esercizio 3.7
❑

Soluzione dell'esercizio 3.8
❑

Soluzione dell'esercizio 3.9
❑

Soluzione dell'esercizio 3.10
❑

Soluzione dell'esercizio 4.1
❑

Soluzione dell'esercizio 4.2
❑

Soluzione dell'esercizio 4.3
❑

Soluzione dell'esercizio 5.1
❑

Soluzione dell'esercizio 5.2
❑

Soluzione dell'esercizio 5.3 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

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

❑

Soluzione dell'esercizio 5.4
❑

Soluzione dell'esercizio 6.1 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 6.3, 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 6.2
❑

Soluzione dell'esercizio 6.3
❑

Soluzione dell'esercizio 6.4 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 7.1
❑

Soluzione dell'esercizio 7.2
❑

Soluzione dell'esercizio 7.3
❑

Soluzione dell'esercizio 7.4
❑

Soluzione dell'esercizio 8.1
❑

Soluzione dell'esercizio 8.2
❑

Soluzione dell'esercizio 8.3
❑

Soluzione dell'esercizio 8.4
❑

Soluzione dell'esercizio 9.1
❑

Soluzione dell'esercizio 9.2 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, $2p, \ldots, qp$, quelli che sono divisibili per q sono invece q, $2q, \ldots, pq$ 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 9.3 $\Phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$ 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 9.4
❑

Soluzione dell'esercizio 10.1
❑

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 La colorazione dei lati data in figura 13 suggerisce

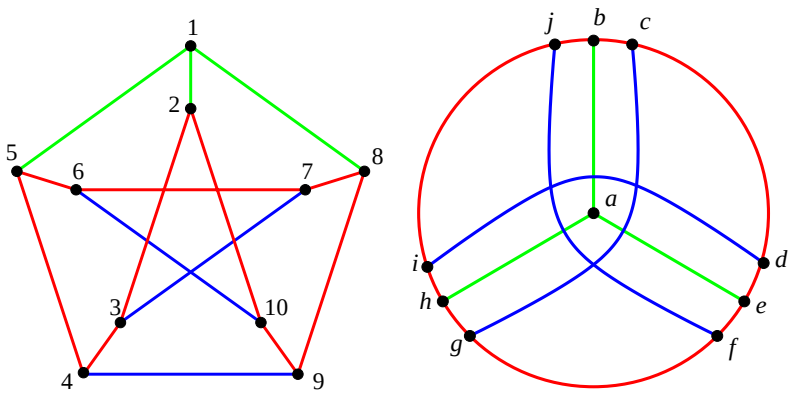

Figura 13: Soluzione grafica dell'esercizio 14.5

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 14.6
❑

Soluzione dell'esercizio 14.7
❑

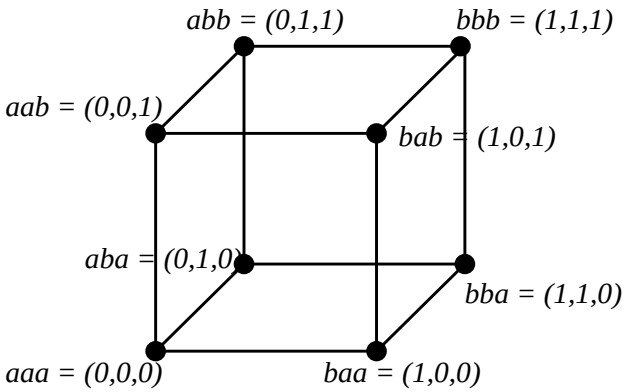

Figura 14: L'isomorfismo tra i grafi dell'esercizio 14.8

Soluzione dell'esercizio 14.8 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 18.1
❑

Soluzione dell'esercizio 18.2
❑

Soluzione dell'esercizio 18.3
❑

Soluzione dell'esercizio 18.4
❑

Soluzione dell'esercizio 18.5
❑

Soluzione dell'esercizio 18.6
❑

Soluzione dell'esercizio 18.7
❑

Soluzione dell'esercizio 19.1
❑

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 Procediamo per induzione sul numero dei lati. Se $|E(G)| = 0$ il grafo ha un solo vertice e quindi è lui stesso un albero.

Supponiamo che $|E(G)| \geq 1$, allora s. Se per ogni $e \in E$, $G - e$ è sconnesso, allora per la terza delle proprietà che caratterizzano gli alberi (teorema 19.2), si ha che G è un albero. Se invece esiste un e tale che $G - e$ è connesso, allora, avendo un lato in meno di G, per ipotesi di induzione $G - e$ ha un per sottografo un albero che contiene tutti i suoi vertici (e quindi tutti i vertici di G). Chiaramente questo sottografo è sottografo anche di G. ❑

Soluzione dell'esercizio 19.8 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 19.6), si ha

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

❑

Soluzione dell'esercizio 20.1
❑

Soluzione dell'esercizio 20.2 Si definisce passeggiata diretta una successione finita di vertici $(v_0, v_1, \ldots, v_n)$ tali che $v_i \to v_{i+1}$ per ogni i. Una passeggiata diretta si dirà un cammino diretto se e solo se i vertici v_1 sono a due a due distinti, una passeggiata diretta si dirà un ciclo diretto se e solo se i vertici sono a due a due distinti a parte il primo e l'ultimo che coincidono.

Proviamo che se due vertici sono congiungibili da una passeggiata diretta, allora sono congiungibili da un cammino diretto. Siano v, $w \in V(G)$ e sia $P = (v_0, v_1, \ldots, v_n)$ una passeggiata diretta di lunghezza minima che congiunge v e w e proviamo che P è un cammino diretto. Infatti se per assurdo $v_i = v_j$ con $i < j$ allora $(v_1, \ldots v_i, v_{j+1}, \ldots, v_n$ sarebbe ancora una passeggiata diretta tra v e w, ma ciò è in contraddizione con il fatto che P sia di lunghezza minima.

La riflessività è ovvia (basta prendere cammini di lunghezza 0, e la transitività, come nel caso dei grafi (proposizione 15.1), si prova congiungendo due passeggiate.

L'essere congiungibili da un cammino diretto non è una relazione d'equivalenza. Basta considerare il seguente esempio: $V = \{0, 1\}$ e $E = \{(0, 1)\}$. 0 è congiungibile a 1 ma non il viceversa. ❑

Soluzione dell'esercizio 20.3 $x\mathcal{R} \circ (\mathcal{S} \circ \mathcal{T})w$ se e solo se esiste $y \in Y$ tale che $x\mathcal{R}y$ e $y\mathcal{S} \circ \mathcal{T}w$ e quest'ultima è vera se e solo se esiste $z \in Z$ tale che $y\mathcal{S}z$ e $z\mathcal{T}w$. In definitiva

$$x\mathcal{R} \circ (\mathcal{S} \circ \mathcal{T})w \iff \exists y \in Y \ \exists z \in Z : x\mathcal{R}y \text{ e } y\mathcal{S}z \text{ e } z\mathcal{T}w.$$

In modo analogo si ha che $x(\mathcal{R} \circ \mathcal{S}) \circ \mathcal{T}$ se e solo se esiste $z \in Z$ tale che $x\mathcal{R} \circ \mathcal{S}z$ e $z\mathcal{T}w$, e la prima equivale a dire che esiste $y \in Y$ tale che $x\mathcal{R}y$ e $y\mathcal{S}z$, e quindi:

$$x(\mathcal{R} \circ \mathcal{S}) \circ \mathcal{T}w \iff \exists z \in Z\ \exists y \in Y : x\mathcal{R}y \text{ e } y\mathcal{S}z \text{ e } z\mathcal{T}w.$$

Evidentemente le due cose coincidono. ❑

Soluzione dell'esercizio 20.4
❑

Soluzione dell'esercizio 20.5
❑

Soluzione dell'esercizio 20.6
❑

Soluzione dell'esercizio 20.7
❑

Soluzione dell'esercizio 20.8
❑

Soluzione dell'esercizio 20.9
❑

Soluzione dell'esercizio 22.1
❑

Soluzione dell'esercizio 23.1
❑