Matematica Discreta (II modulo)

Domenico Luminati

a.a. 2003/2004

Questo breve dispensa raccoglie gli argomenti trattati nei corsi di Matematica Discreta da me tenuti in vari anni accademici dal 1999 al 2004.

Essa, non vuole sostitutire i libri di testo, che restano quelli indicati nel programma del corso ed ai quali in alcune parti si rimanda esplicitamente, ma si pone soltanto l'obiettivo di dare allo studente una traccia da seguire per la preparazione dell'esame.

Indice degli argomenti

Lezione 1

Insiemi e operazioni tra insiemi

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

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

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

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

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

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

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

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

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

Definizione 1.2 (vuoto). Si denota con $\varnothing$ l'*insieme vuoto*, ovvero l'insieme caratterizzato dalla proprietà di non avere elementi, in altri termini l'insieme tale che per ogni x $x \notin \varnothing$.

Osservazione 1.3. L'assioma di estensionalità garantisce evidentemente che se l'insieme vuoto esiste esso è anche unico. In effetti la sua esistenza va presa come assioma.

Osservazione 1.4. Se $P(x)$ è una qualsiasi proprietà attribuibile a x, (ad esempio x ha gli occhi azzurri) allora l'asserzione

$$\forall x \quad x \in \varnothing \implies P(x)$$

è vera. Ricordiamo infatti che un'implicazione $Q \implies P$ altro non è che un modo diverso per scrivere

$$P \text{ o } (\text{non } Q)$$

ossia o vale la tesi o non vale l'ipotesi. Quindi se l'ipotesi Q è sempre falsa, l'implicazione risulta vero (gli antichi dicevano *ex falso quodlibet*, dal falso segue qualsiasi cosa).

Nel nostro caso, per definizione di vuoto, la premessa $x \in \varnothing$ è sempre falsa, per qualsiasi x, quindi l'implicazione è vera. Possiamo pertanto asserire che gli elementi dell'insieme vuoto hanno gli occhi azzurri.

Definizione 1.5. 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, $\forall x\,(x \in X \implies x \in Y)$.

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

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

Assioma 1.6 (separazione). Se X è un insieme e P è una proprietà esprimibile in termini del linguaggio della teoria degli insiemi, allora la collezione

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

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

Definizione 1.7. Se X e Y sono insiemi si costruiscono altri insiemi:

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

  Quando $Y \subseteq X$ la differenza $X \setminus Y$ viene chiamata il *complemento* di Y in X e viene denotata anche con $\complement_X Y$ o semplicemente con $\complement Y$ o con Y' quando non ci sia ambiguità
- *unione* $X \cup Y = \{x \mid x \in X \text{ o } x \in Y\}$
- *differenza simmetrica* $X \triangle Y = (X \setminus Y) \cup (Y \setminus X)$
- *prodotto* $X \times Y = \{(x, y) \mid x \in X \text{ e } y \in Y\}$
- *potenza* $2^X = \{x \mid x \subseteq X\}$

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

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

Osservazione 1.8. Quelle che abbiamo appena dato come definizioni, sono solo in parte tali. Se infatti gli insiemi intersezione, differenza e complemento sono effettivamente definibili a usando l'assioma di separazione (1.6), per gli altri tale assioma non è più sufficiente (non si separano degli elementi da un insieme, ma si costruiscono, insiemi "più grandi") e quindi tali costruzioni devono essere opportunamente assiomatizzate, cosa che però noi non facciamo.

Esercizio 1.1. Si provi che valgono le seguenti:

1. $\forall X \quad \varnothing \subseteq X$
2. $\forall X \quad X \subseteq X$

3. $\forall X, Y, Z \quad X \subseteq Y$ e $Y \subseteq Z$ allora $X \subseteq Z$.
4. $\forall X, Y \quad X \subseteq Y$ 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
$$\begin{aligned} X \setminus (Y \cup Z) &= (X \setminus Y) \cap (X \setminus Z) \\ X \setminus (Y \cap Z) &= (X \setminus Y) \cup (X \setminus Z) \end{aligned}$$
6. $X \setminus (X \setminus Y) = X \cap Y$
7. se $Y \subseteq X$ allora $\complement_X \complement_X Y = Y$.

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

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

Relazioni, funzioni parziali e funzioni totali

Definizione 1.9. Siano X e Y insiemi si dice *relazione* tra X e Y, un sottinsieme $\mathcal{R} \subseteq X \times Y$. Se $\mathcal{R}$ è una relazione si scriverà anche $x\mathcal{R}y$ come sinonimo di $(x, y) \in \mathcal{R}$.

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

Definizione 1.10. Una relazione $f \subseteq X \times Y$ si dice una *funzione parziale* se per ogni $x \in X$ esiste al più un $y \in Y$ tale che $(x, y) \in f$. In simboli:
$$\forall x \in X((x, y) \in f \text{ e } (x, y') \in f) \implies y = y'$$
Si scriverà $f : X \rightharpoonup Y$ per dire che f è una funzione parziale da X a Y e in tal caso si scriverà anche $y = f(x)$ come sinonimo di $(x, y) \in f$.

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

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

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

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

Osservazione 1.11. Una funzione parziale può essere pensata come "una legge ben definita" che ad ogni elemento $x \in \mathrm{dom}(f)$ associa l'unico elemento $y \in Y$ tale che $(x, y) \in f$, questo elemento si denota con $f(x)$. Con questa interpretazione, si dà senso proprio all'uguale contenuto nella scrittura $y = f(x)$, scrittura che quindi è equivalente a $(x, y) \in f$. In questa accezione (legge che associa ad un elemento un altro elemento) verranno generalmente usate le funzioni.

Esercizio 1.5. Siano $f, g \in Y^X$ due funzioni da X in Y. Si provi che $f = g$ se e solo se $f(x) = g(x)$ per ogni $x \in X$.

Esempio 1.12. Se X è un insieme $\mathrm{id}_X = \{(x_1, x_2) \in X \times X \mid x_1 = x_2\}$ è una funzione, che viene chiamata l'*identità* di X. In altri termini $\mathrm{id}_X(x) = x$ per ogni $x \in X$.

Esempio 1.13. Se $f : X \to Y$ è una funzione e $A \subseteq X$, allora $f \cap (A \times Y)$ è anch'essa una funzione, che si denota con $f|_A$ e viene chiamata *restrizione* di f ad A.

Esempio 1.14. Se $f : A \to Y$ e $g : B \to Y$ sono funzioni, non è detto che l'unione $f \cup g \subseteq (A \cup B) \times Y$, sia ancora una funzione. In effetti, dato che $((A \setminus B) \times Y) \cap g = \varnothing$, se $x \in A \setminus B$ allora esiste un unico $y \in Y$ tale $(x, y) \in f \cup g$ e precisamente quello tale che $(x, y) \in f$. Analogamente se $x \in B \setminus A$. Se invece $x \in A \cap B$ potrebbero esisterne un unico y_1 tale che $(x, y_1(\in f$ ed esiste un unico y_2 tale che $(x, y_2) \in g$, quindi affinché $f \cup g$ sia una funzione è necessario che per ogni $x \in A \cap B$ questi due elementi coincidano, in altre parole è necessario che $\upharpoonright fa \cap B = \upharpoonright ga \cap B$.

Esercizio 1.6. Se X è un insieme, come sono fatti $X^\varnothing$ e $\varnothing^X$?

Definizione 1.15. Siano $f : X \rightharpoonup Y$ e $g : Y \rightharpoonup Z$ si chiama *composizione* di f e g la relazione tra X e Z definita da

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

Proposizione 1.16. *Se $f : X \rightharpoonup Y$ e $g : Y \rightharpoonup Z$ allora $g \circ f : X \rightharpoonup Z$. Se $f : X \to Y$ e $g : Y \to Z$ allora $g \circ f : X \to Z$.*

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

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

Osservazione 1.17. Con l'interpretazione data nell'osservazione 1.11 si ha allora che $g \circ f(x) = g(f(x))$.

Definizione 1.18. Sia $f : X \to Y$ ed $A \subseteq X$, si chiamo *immagine* di A tramite f l'insieme:

$$f(A) = \{y \in Y \mid \exists x \in A : y = f(x)\} = \{f(x) \mid x \in A\}.$$

Definizione 1.19. Sia $f : X \to Y$ ed $A \subseteq Y$, si chiamo *immagine inversa* di A tramite f l'insieme:

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

Definizione 1.20. Una funzione $f : X \to Y$ si dice:

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

Proposizione 1.21. *Sia $f : X \to Y$ una bigezione, allora esiste un'unica funzione $g : Y \to X$ tale che $f \circ g = \mathrm{id}_Y$ e $g \circ f = \mathrm{id}_X$. Tale funzione si chiama* inversa *di f e si denota con f^{-1}.*

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

Osservazione 1.22. Si osservi che rispetto alla notazione insiemistica di funzione (1.10) si ha che $f^{-1} = \{(y, x) \in Y \times X \mid (x, y) \in f\}$.

Il seguente esercizio inverte il risultato della proposizione precedente.

Esercizio 1.7. Sia $f : X \to Y$ e si supponga che esista una funzione $g : Y \to X$ tale che $g \circ f = \mathrm{id}_X$ e $f \circ g = \mathrm{id}_Y$. Si provi che allora f è bigettiva.

Esercizio 1.8. Perché se X e Y sono insiemi allora anche Y^X è un insieme?

Esercizio 1.9. Siano $f : X \rightharpoonup Y$ e $g : Y \rightharpoonup Z$, si determini $\mathrm{dom}(g \circ f)$.

Esercizio 1.10. Siano $f : X \to Y$ e $g : Y \to Z$ si provi che:

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

Esercizio 1.11. Siano X, Y, I insiemi, $f : X \to Y$ e $A_i \subseteq Y$ per ogni $i \in I$. Si provi che

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

Esercizio 1.12. Siano X, Y, I insiemi, $f : X \to Y$ e $A_i \subseteq X$ per ogni $i \in I$. Si provi che

$$f(\bigcap_{i \in I} A_i) = \bigcap_{i \in I} f(A_i) \qquad f(\bigcup_{i \in I} A_i) \subseteq \bigcup_{i \in I} f(A_i)$$

Si provi che in generale nella seconda delle due non può valere l'uguaglianza.

Lezione 2

Equipotenza di insiemi

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

Proposizione 2.2. *Valgono le seguenti proprietà:*

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

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

Osservazione 2.3. Si osservi che non abbiamo dato alcun significato alla parola cardinalità, ossia non abbiamo definito cosa sia la *cardinalità* di un insieme. In effetti ciò può essere fatto (e sarà fatto eventualmente in corsi successivi), ossia si possono definire una classe di particolari insiemi detti *cardinali* che godono della seguente proprietà:

- ogni insieme X è equipotente ad uno ed un solo cardinale, tale cardinale è usualmente denotato con $|X|$.
- due cardinali diversi non sono equipotenti tra loro.

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

Supponendo di avere fatto tutto ciò, si può allora provare il seguente

Teorema 2.4. *$X \sim Y$ se e solo se $|X| = |Y|$.*

Dimostrazione. Se $\kappa = |X| = |Y|$ allora esistono due bigezioni $f : X \to \kappa$ e $g : Y \to \kappa$ ma allora per la proposizione 2.2 si ha che $g^{-1} \circ f : X \to Y$ è una bigezione e quindi $X \sim Y$.

Viceversa sia $X \sim Y$ e sia $f : X \to Y$ una bigezione. Siano $\kappa = |X|$ e $\lambda = |Y|$, e siano $g : X \to \kappa$ e $h : Y \to \lambda$ delle bigezioni, allora $h^{-1} \circ f \circ g^{-1} : \kappa \to \lambda$ è una bigezione e quindi $\kappa = \lambda$. □

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

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

Si provi che se X e Y sono non vuoti allora

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.

Cosa resta vero se uno tra X e Y è vuoto?

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

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

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

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

I numeri naturali: gli assiomi di Peano

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

Assioma 2.5. $0 \in \mathbb{N}$

Assioma 2.6. $\mathrm{succ} : \mathbb{N} \to \mathbb{N}$ è una funzione iniettiva

Assioma 2.7. $\forall n \in \mathbb{N} \quad \mathrm{succ}(n) \neq 0$

Assioma 2.8 (di induzione). se $A \subseteq \mathbb{N}$ è un sottinsieme tale che

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

allora $A = \mathbb{N}$.

Proposizione 2.9. *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. ❑

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

Il principio di induzione (prima forma)

Una conseguenza immediata dell'assioma di induzione (2.8) è il seguente

Teorema 2.10 (prima forma dell'induzione). *Sia $P(n)$ una famiglia di proposizioni indicizzate su $\mathbb{N}$ e si supponga che*

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

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

Dimostrazione. Sia $A = \{n \mid P(n) \text{ è vera}\}$, allora $0 \in A$ e se $n \in A$ allora vale $P(n)$, quindi vale $P(\mathrm{succ}(n))$ ossia anche $succ(n) \in A$, quindi per l'assioma di induzione (2.8) $A = \mathbb{N}$. ❑

Il teorema di ricorsione

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

Teorema 2.11 (di ricorsione). *Sia X un insieme, $h : \mathbb{N} \times X \to X$ una funzione e $c \in X$. Esiste una unica funzione $f : \mathbb{N} \to X$ tale che:*

$$f(0) = c \qquad (1)$$

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

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

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

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

Proviamo ora l'esistenza. Per definizione di funzione (1.10) quello che si cerca è un insieme $f \subseteq \mathbb{N} \times X$ tale che:

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

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

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

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

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

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

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

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

Per concludere resta da provare che f verifica la (3). Procediamo per induzione su n.

Se $n = 0$. Abbiamo già visto che $(0, c) \in f$. Supponiamo per assurdo che esista $(0, d) \in f$ con $d \neq c$, e sia $f' = f - \{(0, d)\}$. Chiaramente $(0, c) \in f'$ e se $(n, x) \in f' \subseteq f$ allora $(\mathrm{succ}(n), h(n, x)) \in f$, ma allora, per il terzo assioma di Peano (2.7), $\mathrm{succ}(n) \neq 0$ per ogni $n \in \mathbb{N}$ e quindi $(\mathrm{succ}(n), h(n, x)) \neq (0, d)$, pertanto $(\mathrm{succ}(n), h(n, x) \in f'$. Quindi $f' \in \Omega$, ma ciò contraddice la (6) perché $f \not\subseteq f'$.

Supponiamo la tesi vera per n. Sia x l'unico elemento tale che $(n, x) \in f$, dato che f verifica la (5), allora $(\mathrm{succ}(n), h(n, x)) \in f$. Supponiamo per assurdo che anche $(\mathrm{succ}(n), e) \in f$ e si ponga $f' = f - \{(\mathrm{succ}(n), e)\}$. Proviamo che anche in questo caso $f' \in \Omega$ e si avrà, come prima, un assurdo. Dal terzo assioma di Peano segue che $(0, c) \in f'$. Se $(i, z) \in f' \subseteq f$ allora $(\mathrm{succ}(i), h(i, z)) \in f$. Se $i \neq n$ allora, per l'iniettività di succ (assioma 2.6) si ha che $(\mathrm{succ}(i), h(i, z)) \neq (\mathrm{succ}(n), e)$ e quindi $(\mathrm{succ}(i), h(i, z)) \in f'$. Se invece $i = n$ allora $(n, z) \in f$ implica, per l'unicità di x, che $z = x$ e quindi, dato che $h(n, z) \neq e$, $(\mathrm{succ}(i), h(i, z)) = (\mathrm{succ}(n), h(n, x)) \in f'$. Questo conclude la dimostrazione. ❑

Lezione 3

Le operazioni sui naturali

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

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

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

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

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

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

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

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

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

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

L'ordinamento dei naturali

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

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

Osservazione 3.4. Si può vedere $\leq$ come un sottinsieme di $\mathbb{N} \times \mathbb{N}$ e precisamente $\leq = \{(n,m) \in \mathbb{N} \times \mathbb{N} \mid \exists k \in \mathbb{N} : n + k = m\}$. E quindi $\leq$ è una relazione (definizione 1.9) sui naturali e quello che abbiamo definito come significato di $n \leq m$ è effettivamente lo stesso che dire $(n, m) \in \leq$.

Si può dimostrare la seguente

Proposizione 3.5. *Valgono le seguenti proprietà:*

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

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

Insiemi ordinati

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

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

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

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

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

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

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

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

L'ordinamento dei naturali e le operazioni

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

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

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

Dimostrazione. Esercizio per lo studente volenteroso. $\square$

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

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

Insiemi finiti: il Lemma dei cassetti

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

Definizione 3.10. Diremo che un insieme è *finito* se esiste $n \in \mathbb{N}$ tale che X è equipotente a I_n, in simboli$X \sim I_n$. Un insieme è detto *infinito* se non è finito

Teorema 3.11 (Lemma dei cassetti). *Siano X e Y due insiemi aventi rispettivamente $X \sim I_n$ e $Y \sim I_m$ 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 $X \sim I_{n+1}$ e sia, $Y \sim I_m$ 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 $Y' \sim I_{m-1}$, $X' \sim I_n$ e $m - 1 > n$, ciò è assurdo per ipotesi di induzione. ❑

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

Lezione 4

Cardinalità degli insiemi finiti

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

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

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

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

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

È facile provare la seguente

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

Dimostrazione. Se $|X| = |Y|$, allora esiste $n \in \mathbb{N}$ tale che X è equipotente a I_n e Y è equipotente a I_n, ma allora X e Y sono tra loro equipotenti (proposizione 2.2. Viceversa se sono equipotenti il corollario precedente mostra che hanno la stessa cardinalità. ❑

Sottinsiemi di un insieme finito

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

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

Come conseguenza si ha il seguente

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

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

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

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

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

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

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

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

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

Scommettiamo che due di voi hanno lo stesso compleanno?

Storiella. Il professore di Matematica Discreta entra nell'aula e 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 50 centesimi 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 4.5. 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 4.4 (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, ossia quel furbacchione del professore aveva una probabilità di perdere la scommessa inferiore al 0.6%. Ciò spiega perché si fa una cena gratis ogni anno (vedi figura 1).

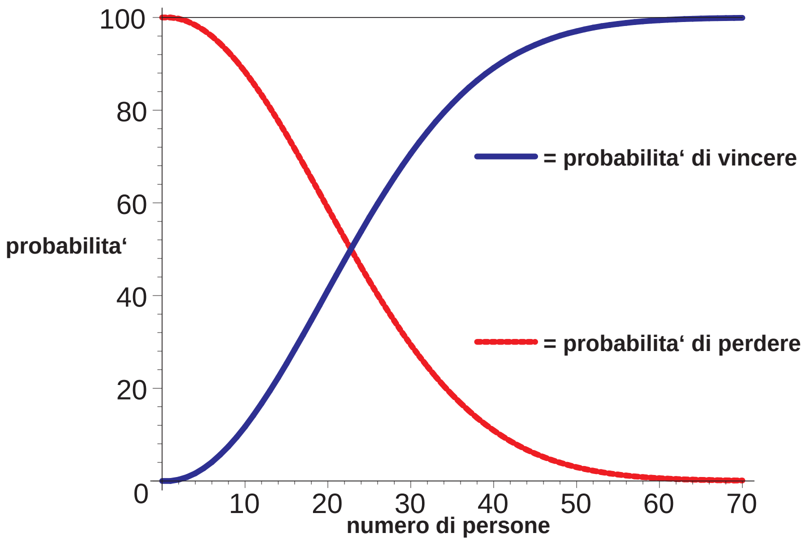

Figura 1: Grafico della probabilità di successo o di insuccesso, nella scommessa del compleanno, in funzione del numero di persone. Già con 60 persone si ha la ragionevole certezza di vincere la scommessa: la probabilità di perdere è inferiore a 6/1000, con 100 persone le probabilità di perdere scende a circa 3/10000000

Esercizio 4.6. Siano X e Y insiemi finiti entrambi di cardinalità n. Si provi che ogni funzione iniettiva $X \to Y$ è anche surgettiva.

Esercizio 4.7. Sia X un insieme finito di cardinalità n. Si determini il numero delle funzioni biunivoche di X in sé.

Lezione 5

Insiemi infiniti: l'assioma della scelta

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

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

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

tale che

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

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

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

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

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

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

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

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

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

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

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

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

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

$$g(x) = \left\langle \begin{array}{ll} x & \text{se } x \in X - Y \\ f(x) & \text{se } x \in Y \end{array} \right.$$

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

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

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

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

Lezione 6

Insiemi numerabili

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

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

Diamo ora alcune proprietà degli insiemi numerabili.

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

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

$$h(x) = \left\langle \begin{array}{ll} 2f(x) & \text{se } x \in X \\ 2g(x) + 1 & \text{se } x \in Y \end{array} \right.$$

Si verifica facilmente che h è una bigezione. ❏

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

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

$$h(x) = \left\langle \begin{array}{ll} g(x) & \text{se } x \in Y \\ f(x) + n & \text{se } x \in X \end{array} \right.$$

Si verifica facilmente che h è una bigezione.

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

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

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

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

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

$$g(x) = \left\langle \begin{array}{ll} f(x) & \text{se } x \in Z \\ x & \text{se } x \in X - Z \end{array} \right.$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Confronto di cardinalità: il Teorema di Cantor-Bernstein

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

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

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

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

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

Proposizione 6.10. *Valgono le seguenti proprietà:*

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

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

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

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

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

$$g(z) = \left\langle \begin{array}{ll} f(z) & \text{se } z \in A \\ z & \text{se } z \in Z - A \end{array} \right.$$

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

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

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

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

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

La tricotomia dei cardinali

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

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

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

Il procedimento diagonale di Cantor

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

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

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

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

$$
\begin{array}{ccccccccccc}
 & & 0 & 1 & 2 & 3 & 4 & 5 & 6 & \dots \\
 & & & & & & & & & \\
f(0) & = & \boxed{1} & 0 & 0 & 1 & 1 & 0 & 0 & \dots \\
f(1) & = & 0 & \boxed{0} & 1 & 1 & 0 & 1 & 1 & \dots \\
f(2) & = & 1 & 0 & \boxed{0} & 0 & 1 & 0 & 1 & \dots \\
f(3) & = & 1 & 1 & 1 & \boxed{1} & 0 & 0 & 0 & \dots \\
f(4) & = & 0 & 0 & 0 & 1 & \boxed{1} & 1 & 1 & \dots \\
f(5) & = & 1 & 1 & 1 & 0 & 0 & \boxed{0} & 0 & \dots \\
f(6) & = & 1 & 0 & 1 & 1 & 1 & 1 & \boxed{0} & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\
 & & & & & & & & & \\
A & = & 0 & 1 & 1 & 0 & 0 & 1 & 1 & \dots
\end{array}
$$

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

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

$$
\delta_n = \left\langle \begin{array}{ll} 1 & \text{se } \varepsilon_n \text{ è pari} \\ 2 & \text{se } \varepsilon_n \text{ è dispari} \end{array} \right.
$$

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

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

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 6.7). Si può in realtà dimostrare che $|\mathbb{R}| = 2^{\aleph_0}$ (cfr. esercizio 6.10).

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

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

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

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

Lezione 7

Operazioni tra cardinalità

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

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

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

L'esercizio precedente permette di dare la seguente

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

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

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

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

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

Esercizio 7.4. Si provino le seguenti:

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

L'assioma di buon ordinamento

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

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

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

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

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

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

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

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

Il principio di induzione (seconda forma)

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

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

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

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

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

La divisione euclidea

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

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

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

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

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

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

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

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

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

Osservazione 7.8. Si osservi che la dimostrazione del teorema 7.7, di esistenza e unicità del quoziente e del resto della divisione euclidea di due numeri naturali, permette di scrivere un algoritmo ricorsivo per il loro calcolo:

Algoritmo ricorsivo di DIVISIONE EUCLIDEA
- INPUT: n, $m \in \mathbb{N}$, $m > 0$.
- $n < m \implies$ OUTPUT: $(0, n)$
- $n \geq m \implies$ applica l'algoritmo alla coppia $(n-m, m)$ e aggiungi 1 al quoziente.

che può essere tradotto nella scrittura di un programma ricorsivo per la definizione di una funzione `DIVE` che calcoli il quoziente e resto della divisione euclidea tra due numeri:

Funzione ricorsiva `DIVE`

```
DIVE (n,m) {
  IF n < m THEN [0,n]
  ELSE [1,0] + DIVE(n-m,m)
  END IF
}
```

Esercizio 7.5. Supponendo di avere un linguaggio di programmazione con un'istruzione `WHILE`, tradurre la definizione della funzione `DIVE` in una funzione non ricorsiva (induttiva).

Lezione 8

Scrittura in base arbitraria dei naturali.

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

Osservazione 8.2. Si osservi che nessun numero è rappresentabile in base 0 (dato che $I_0 = \varnothing$) e che l'unico numero rappresentabile in base 1 è lo 0. In questo caso infatti la condizione (2) implica che ogni $\varepsilon_i = 0$.

Osservazione 8.3. La rappresentabilità in base b può essere espressa anche nel seguente modo: esiste una successione $\{\varepsilon_i\}_{i\in\mathbb{N}}$ di interi tali che:

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

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

Teorema 8.4 (rappresentazione dei naturali in base arbitraria). *Sia $b \in \mathbb{N}$, $b \ge 2$. Allora ogni $n \in \mathbb{N}$ è rappresentabile in modo unico in base b. Ossia esiste una successione $\{\varepsilon_i\}_{i\in\mathbb{N}}$ come nell'osservazione precedente (8.3) e se $\{\varepsilon'_i\}_{i\in\mathbb{N}}$ è un'altra tale successione, allora $\varepsilon_i = \varepsilon'_i$ per ogni $i \in \mathbb{N}$.*

Dimostrazione. Dimostriamo l'esistenza per induzione su n. Se $n = 0$ basta prendere $\varepsilon_i = 0$ per ogni $i \in \mathbb{N}$. Supponiamo ora $n > 0$ e che la tesi sia vera per ogni $k < n$. Siano q, r tali che $n = bq + r$ con $0 \le r < b$. Dato che $b \ge 2$ si ha che $0 \le q < bq \le bq + r = n$ e quindi per ipotesi di induzione esiste una successione definitivamente nulla $\{\delta_i\}$, costituita di interi tali che $0 \le \delta_i < b$ per ogni i e tale che $q = \sum\limits_{i=0}^{\infty} \delta_i b^i$. 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 $0 \le \varepsilon_i = \delta_{i-1} < b$ per ogni $i > 0$ e $0 \le \varepsilon_0 = r < b$.

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

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

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

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

Osservazione 8.5. Anche in questo caso la dimostrazione del teorema 8.4, di rappresentazione in base assegnata dei naturali, permette di scrivere un algoritmo ricorsivo per il calcolo della stringa degli ε_i

Algoritmo ricorsivo di RAPPRESENTAZIONE IN BASE b

- INPUT: n, $b \in \mathbb{N}$, $b \geq 2$.
- $n = 0 \implies$ OUTPUT: [ ]
- $n > 0 \implies$ calcola la divisione euclidea $n = bq + r$
  applica l'algoritmo a q, b
  aggiungi r alla stringa che hai ottenuto

algoritmo che può essere tradotto in un programma ricorsivo per la definizione di una funzione `B_RAPP` che calcoli la rappresentazione di un numero in base fissata.

Funzione ricorsiva `B_RAPP`

```
B_RAPP(n,b){
  IF n=0 THEN [ ]
  ELSE [q,r] = DIVE(n,b)
       [r,B_RAPP(q,b)]
  END IF
}
```

Il coefficiente binomiale

Definizione 8.6. Siano n, $k \in \mathbb{N}$ con $k \leq n$ si pone

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

Osservazione 8.7. È immediato verificare che $\binom{n}{k} = \binom{n}{n-k}$.

Esercizio 8.1. Provare che

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

k-sottinsiemi

Definizione 8.8. Sia X un insieme e $k \in \mathbb{N}$, un sottinsieme $A \subseteq X$ sarà detto un *k-sottinsieme* se $|A| = k$. Denoteremo con $\binom{X}{k}$ l'insieme dei k-sottinsiemi di X. I k-sottinsiemi sono anche chiamati *k-combinazioni semplici.*

Proposizione 8.9. *Se X è finito e $k \leq |X|$, allora*

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

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

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

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

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

chiaramente si ha
$$\binom{X}{k} = \mathcal{A}_1 \cup \mathcal{A}_2, \qquad \mathcal{A}_1 \cap \mathcal{A}_2 = \varnothing$$
da cui $\left|\binom{X}{k}\right| = |\mathcal{A}_1| + |\mathcal{A}_2|$)cfr esercizio4.2). Posto $X' = X - \{x_0\}$ si ha che
$$\mathcal{A}_2 = \binom{X'}{k}. \tag{7}$$
inoltre la funzione $F : \binom{X'}{k-1} \to \mathcal{A}_1$ definita da $F(A) = A \cup \{x_0\}$ è una bigezione e quindi, dato che $|X'| = |X| - 1$, per ipotesi di induzione si ha
$$\begin{aligned} |\mathcal{A}_1| \quad &=* \left|\tbinom{X'}{k-1}\right| = \tbinom{|X'|}{k-1} \\ |\mathcal{A}_2| \quad &=* \left|\tbinom{X'}{k}\right| = \tbinom{|X'|}{k} \end{aligned}$$
Ma allora, usando il risultato dell'esercizio 8.1
$$\left|\binom{X}{k}\right| = \binom{|X'|}{k-1} + \binom{|X'|}{k} = \binom{|X'|+1}{k} = \binom{|X|}{k}.$$
❏

Esercizio 8.2. Provare che
$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$

Perché non gioco al Superenalotto!

Una sestina al Superenalotto, è un sottinsieme di 6 elementi dell'insieme dei numeri naturali da 1 a 90, quindi, per la proposizione 8.9 il numero di sestine possibili è dato da:
$$\binom{90}{6} = 622614630$$
Pertanto, la probabilità di vincere giocando una sestina è pari a $1/622614630 = 0.000000161$ %. 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 0.50 Euro, mi aspetterei, in caso di successo, un premio di $0.50 \cdot 622614630 = 311307315$ Euro.

Un montepremi così alto non si è ancora visto!

Lezione 9

Divisibilità e sue prime proprietà

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

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

Proposizione 9.3.

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

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

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

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

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

Il massimo comun divisore: definizione, esistenza e unicità

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

1. $d \mid n$ e $d \mid m$;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Osservazione 9.14. 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, $m \in \mathbb{Z}$.
- $n = 0 \implies$ OUTPUT: m
- $m = 0 \implies$ 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.

tale algoritmo si può tradurre in un programma ricorsivo per la definizione di una funzione `MCD` che calcoli il M.C.D. tra due numeri naturali:

Funzione ricorsiva `MCD`

```
MCD(n,m){
  IF m=0 THEN n
  ELSE [q,r] = DIVE(n,m)
       MCD(m,r)
  END IF
}
```

Lezione 10

Proprietà dei numeri coprimi e caratterizzazione dei numeri primi

Proposizione 10.1.

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

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

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

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

Dimostrazione. Supponiamo che $p \mid nm$, dato che p è primo, se $p \nmid n$ 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 $p \mid nm \implies p \mid n$ oppure $p \mid m$, allora se $p = dh$ allora $p \mid dh$ e quindi $p \mid d$, e quindi per 9.3 si ha che $d = \pm p$ e $h = \pm 1$ oppure $p \mid h$ e quindi $h = \pm p$ e $d = \pm 1$. ❑

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

Il minimo comune multiplo: definizione, esistenza e unicità

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

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

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

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

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

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

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

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

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

Il teorema fondamentale dell'Aritmetica

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

In altre parole, ogni intero maggiore 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 10.1 esiste un j tale che $p_k \mid q_j$. Dato che sia p_k che q_j sono primi positivi, allora $p_k = q_j$. Ma allora $p_1 \dots p_{k-1} = q_1 \dots q_{j-1} q_{j+1} \dots q_h$, 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 $\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$

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

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

Esistenza di infiniti numeri primi

Corollario 10.6. *I numeri primi sono infiniti.*

Dimostrazione. Per assurdo supponiamo che $p_1, p_2, \dots, p_n$ siano tutti i primi. 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 (10.5). ❑

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

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

Lezione 11

Definizione di congruenza e prime proprietà

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

Proposizione 11.2. *Valgono le seguenti proprietà:*

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

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

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

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

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

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

1. è *riflessiva*, ossia $\forall x \in X \ x\mathcal{R}x$;

2. è *simmetrica*, ossia $\forall x, y \in X \ x\mathcal{R}y \implies y\mathcal{R}x$

3. è *transitiva*, ossia $\forall x, y, z \in X \ (x\mathcal{R}y \text{ e } y\mathcal{R}z) \implies x\mathcal{R}z$.

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

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

Classi d'equivalenza

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

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

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

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

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

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

1. *per ogni $x \in X$ $x \in [x]$*

2. *per ogni $x, y \in X$ $[x] = [y]$ se e solo se $x \sim y$.*

3. *per ogni $x, y \in X$ $[x] \cap [y] \neq \varnothing \implies [x] = [y]$.*

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

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

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

Osservazione 11.8. Le proprietà (1) e (3) assicurano che l'insieme delle classi d'equivalenza di un insieme rispetto ad una relazione d'equivalenza (il quoziente) costituisce una *partizione* dell'insieme ossia sono una collezione $\mathcal{P}$ di sottinsiemi di X (i.e. $\mathcal{P} \subset 2^X$) che hanno le seguenti proprietà:

1. sono tutti non vuoti, ovvero $\forall A \in \mathcal{P} \quad A \neq \varnothing$ (questo è garantito da (1))

2. ricoprono X, ovvero $\bigcup_{A \in \mathcal{P}} A = X$ (questo è garantito da (1))

3. sono a due a due disgiunti, ovvero $\forall A, B \in \mathcal{P} \quad A \neq B \implies A \cap B = \varnothing$ (questo è garantito da (3))

Esercizio 11.1. Sia X un insieme. Si dimostri che gli insiemi

$$R = \{\mathcal{R} \mid \mathcal{R} \text{ è una relazione d'equivalenza su } X\}$$
$$P = \{\mathcal{P} \mid \mathcal{P} \text{ è una partizione di } X\}$$

sono in bigezione.

Classi di congruenza

Definizione 11.9. Siano $a, n \in \mathbb{Z}$, si chiama classe di congruenza di a modulo n l'insieme
$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a \mod n\}.$$
Indicheremo $\mathbb{Z}/_{n\mathbb{Z}} = \left\{ [a]_n \mid a \in \mathbb{Z} \right\}$

Osservazione 11.10. Osserviamo che
$$x \equiv a \mod n \iff n \mid (x-a) \iff \exists\, k \in \mathbb{Z} : x-a = kn \iff \exists\, k \in \mathbb{Z} : x = a+kn$$
e quindi
$$[a]_n = \{a + kn \mid k \in \mathbb{Z}\}.$$

Osservazione 11.11. La classe di congruenza di a modulo n non è altro che la classe d'equivalenza di a rispetto alla relazione d'equivalenza (cfr. proposizione 11.2) $\equiv \mod n$ e $\mathbb{Z}/_{n\mathbb{Z}}$ quindi è l'insieme quoziente di $\mathbb{Z}$ rispetto a tale relazione d'equivalenza.

In virtù di questa osservazione e della proposizione 11.7 si ha la seguente:

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

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

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

Le classi modulo n sono esattamente n

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

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

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

Dimostrazione. Da 11.13 e dalla 2 di 11.12 segue immediatamente che l'insieme in questione ha al più n elementi e precisamente $[0]_n, [1]_n, \ldots, [n-1]_n$. D'altra parte se $0 \leq h < k < n$ allora $0 < k - h < n$ e quindi $n \not| (k-h)$ e quindi (sempre per la 2 di 11.12) $[h]_n \neq [k]_m$. ❑

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

Somma e prodotto di classi di congruenza

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

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

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

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

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

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

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

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

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

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

per indicare lo stesso concetto.

Esercizio 11.2. Si provino le seguenti proprietà delle operazioni tra classi di congruenza:

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

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

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

Lezione 12

Il teorema cinese del resto

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

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

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

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

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

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

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

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

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

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

Esercizio 12.1. Siano $n_1, \dots, n_k$ 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 $c + kn_1 \cdot \dots \cdot n_k]$.

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

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

Elementi invertibili modulo n

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

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

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

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

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

Dimostrazione. Dal fatto che $ax = 1$ in $\mathbb{Z}/n\mathbb{Z}$, moltiplicando entrambi i membri per y, ed usando le proprietà associativa, commutativa e dell'1 (esercizio 11.2) si ottiene

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

$\square$

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

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

Osservazione 12.6. Osserviamo che le due proposizioni precedenti permettono di definire l'invertibilità e l'inverso di una classe di congruenza: data una classe $[a]_n$ se a è invertibile, per la seconda delle proposizioni (12.4) l'insieme dei suoi inversi costituisce una classe di congruenza, mentre per la seconda (12.5) questa classe dipende non da a ma soltanto da $[a]_n$. La classe costituita dagli inversi di a viene chiamata l'*inverso* di $[a]_n$ e denotata con $[a]_n^{-1}$.

Osservazione 12.7. La definizione stessa di $[a]_n^{-1}$ mostra che tale classe è l'unica a godere della seguente proprietà:

$$[a]_n [a]_n^{-1} = [a]_n^{-1} [a]_n = [1]_n$$

Questo fatto (l'unicità di una tale classe) poteva essere provato usando soltanto le proprietà formali delle operazioni (esercizio 11.2). Supponiamo che $u \in \mathbb{Z}/n\mathbb{Z}$ e che esistano v_1, v_2 tali che $uv_1 = v_1u = 1$ e $uv_2 = v_2u = 1$. Allora

$$v_1 = v_1 \cdot 1 = v_1(uv_2) = (v_1u)v_2 = 1 \cdot v_2 = v_2$$

La proposizione 12.3 può allora essere rienunciata

Proposizione 12.8. *$[a]_n$ è invertibile se e solo se $(a, n) = 1$.*

Corollario 12.9. *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 $p \nmid a$ e quindi, dato che p è primo, $(p, a) = 1$, da cui la tesi. $\square$

Lezione 13

Equazioni lineari modulo n

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

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

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

Se p è primo tutti gli elementi non nulli sono invertibili (corollario 12.9), e quindi se $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ allora $ac = ad$ in $\mathbb{Z}/p\mathbb{Z}$ implica che $c = d$ (in $\mathbb{Z}/p\mathbb{Z}$), in particolare $ab = 0$ in $\mathbb{Z}/p\mathbb{Z}$ implica che $a = 0$ o $b = 0$.

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

$$ax \equiv b \mod n$$

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

Se x_0 è una soluzione della congruenza, allora, detto $n' = n/(a, n)$, l'insieme delle soluzioni è dato da:

$$[x_0]_{n'} = \{x_0 + kn' \mid k \in \mathbb{Z}\}$$

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

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

Proviamo ora che l'insieme delle soluzioni è proprio $[x_0]_{n'}$. Proviamo innanzitutto che se $x_1 \in [x_0]_{n'}$ allora è una soluzione della congruenza, infatti $x_1 = x_0 + kn'$ quindi $ax_1 = ax_0 + kan/(a, n)$ da cui $ax_1 - ax_0 = kan/(a, n)$ ma allora, dato che $a/(a, n) \in \mathbb{Z}$, n è un multiplo di $kan/(a, n)$, ovvero

$$ax_1 \equiv ax_0 \mod n.$$

Dato che $ax_0 \equiv b \mod n$, questo basta per concludere che anche $ax_1 \equiv b \mod n$.

Viceversa se $ax_1 \equiv b \mod n$ allora $ax_1 \equiv ax_2 \mod n$ da cui si ricava che $a(x_1 - x_0) \equiv 0 \mod n$, ovvero $n \mid a(x_1 - x_0)$. Ma allora, dato che $n' \mid n$, anche $n' \mid a'(x_1 - x_0)$, essendo $a' = a/(n, a)$. Ma allora, dato che per la proposizione 9.12 $(n', a') = 1$, usando la proposizione 10.1, $n' \mid (x_1 - x_0)$. Questo conclude la dimostrazione. ❑

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

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

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

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

Esercizio 13.2. Si provi che se $n' \mid n$ e $x \in \mathbb{Z}$ allora $[x]_n \subseteq [x]_{n'}$.
Detto $d = n/n'$ si provi che

$$[x]_{n'} = \bigcup_{i=0}^{d-1} [x + in']_n$$

e che per ogni $0 \leq i \neq j \leq d-1$ si ha che $[x + in']_n \neq [x + jn']_n$.

Esercizio 13.3. Si usi l'esercizio prexcedente per provare che se $(a, n) \mid b$ allora esistono esattamente (a, n) classi di congruenza $X \in \mathbb{Z}/_{n\mathbb{Z}}$ tali che $[a]_n X = [b]_n$.

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

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

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

Il piccolo teorema di Fermat

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

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

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

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

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

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

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

$$x_1 x_2 \ldots x_k = u x_u x_2 \ldots u x_k = u^k x_1 x_2 \ldots x_k$$

Da, questa uguaglianza, osservando che $x_1 x_2 \ldots x_k$ è invertibile (proposizione 13.6), ne segue (per quanto osservato in 13.1) che $u^k = 1$. ❑

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

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

Esercizio 13.4. Si provi che se p è un primo allora per ogni intero x si ha che $x^p \equiv x \mod p$.

Crittografia RSA

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

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

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

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

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

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

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

Chiaramente chiunque conosca c e $\Phi(m)$ è in grado di determinare la chiave di decodifica d. Ma determinare $\Phi(m)$ è molto facile se si conosce la fattorizzazione in primi di m, e fattorizzare un intero è un problema computazionalmente molto complesso. Quindi soltanto chi ha costruito m e c è in grado di determinare d facilmente. I numeri che vengono usati sono in realtà del tipo $m = pq$ con p, q primi, per i quali siha (esercizio 13.5) $\Phi(m) = (p-1)(q-1)$ e per i quali, determinare $\Phi(m)$ a partire da m è equivalente (esercizio 13.6) a determinare la fattorizzazione di m.

Esercizio 13.5. Provare che se p, q sono primi allora $\Phi(pq) = (p-1)(q-1)$

Esercizio 13.6. Supponiamo che $n = pq$ sia con p e q primi. Si provi che se si conoscono n e $\Phi(n)$ si possono determinare p e q.

Esercizio 13.7. Si risolvano, se possibile, le seguenti congruenze:

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

Lezione 14

Definizione di grafo

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

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

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

Spesso i grafi sono rappresentati graficamente mediante dei punti a rappresentare i vertici e delle linee congiungenti due vertici a rappresentare i lati. Ad esempio in figura 2 sono rappresentati i grafi G e G'definiti da

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

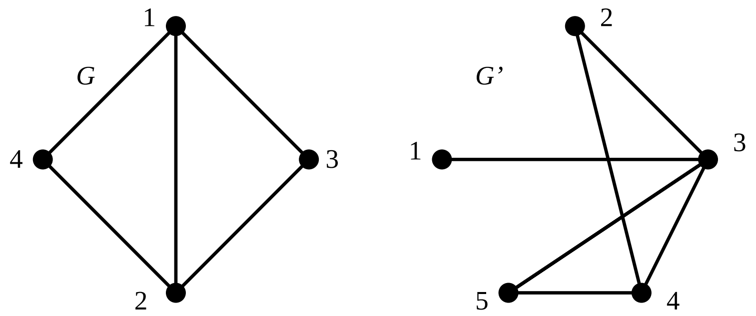

Figura 2: Esempi di grafi

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

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

Tale relazione risulta essere oviamente

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Si osservi che, a differenza dei grafi dove tra due vertici c'è 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 3).

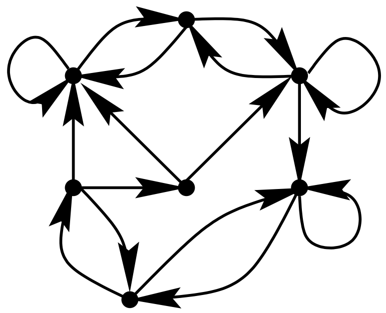

Figura 3: Un grafo diretto

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

Alcuni grafi notevoli

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

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

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

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

Indicheremo con P_∞ il grafo

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

P_n è detto il *cammino infinito.*

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

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

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

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

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

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

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

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

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

Sottografi e sottografi indotti

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

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

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

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

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

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

Morfismi ed isomorfismo di grafi

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

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

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

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

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

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

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

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

ed in questa forma può essere estesa ai grafi diretti.

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

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

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

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

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

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

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

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

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

Esercizio 14.8. Si provi che:

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

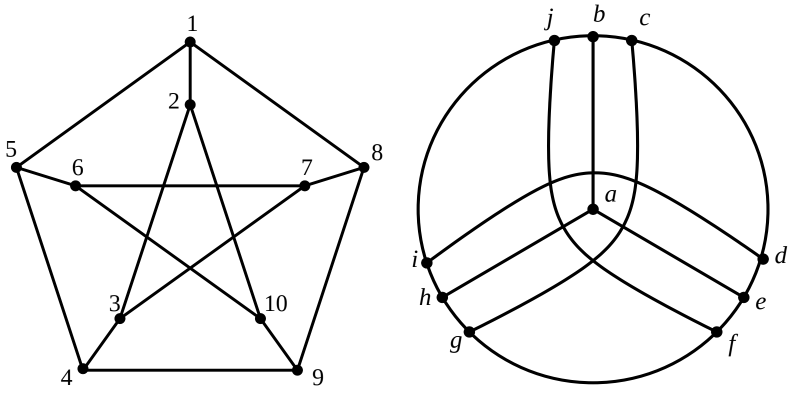

Figura 4: I grafi di esercizio 14.9

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 $G' \cong G'' \implies G \cong G''$).

Esercizio 14.9. Si provi che i due grafi rappresentati in figura 4 sono tra loro isomorfi.

Esercizio 14.10. Dire se i due grafi in figura 5 sono isomorfi oppure no.

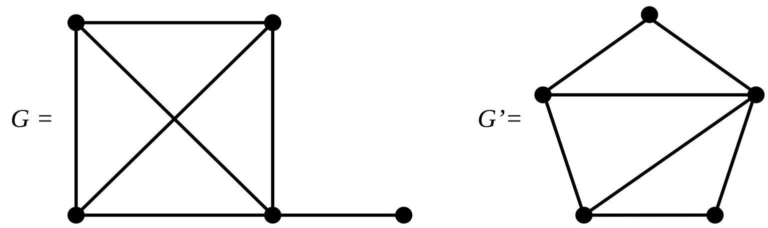

Figura 5: I grafi dell'esercizio 14.10

Esercizio 14.11. Provare che i due grafi in figura 6 non sono isomorfi.

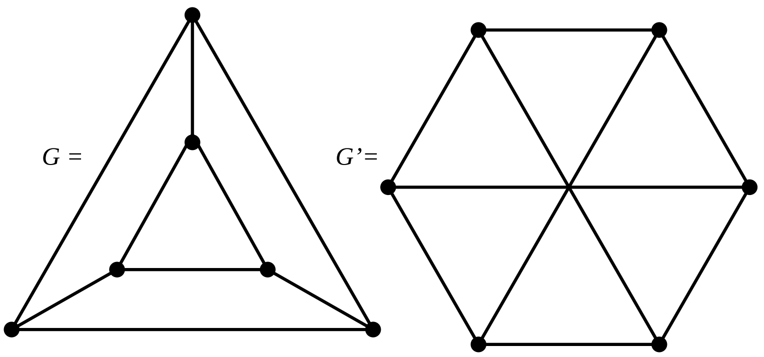

Figura 6: I grafi dell'esercizio 14.11

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

Lezione 15

Una stima del numero di grafi non isomorfi su n vertici

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

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

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

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

Dimostrazione. L'insieme $\mathcal{G}_n$ è evidentemente in bigezione con $2^{\binom{V}{2}}$ e quindi

$$2^{\binom{n}{2}} = |\mathcal{G}_n|\,,$$

in particolare allora $g_n \le |\mathcal{G}_n| = 2^{\binom{n}{2}}$, da cui passando al $\log_2$ si ha

$$\log_2(g_n) \le \binom{n}{2} = \frac{n^2}{2}\Big(1-\frac{1}{n}\Big).$$

Dato che le classi di equivalenza formano una partizione di $\mathcal{G}_n$,

$$|\mathcal{G}_n| = \sum_{x\in \mathcal{G}_n/\cong} |x|$$

ossia la cardinalità di $\mathcal{G}_n$ è la somma delle cardinalità di ciascuna classe d'isomorfismo, e quindi

$$2^{\binom{n}{2}} = \sum_{x\in \mathcal{G}_n/\cong} |x| \tag{8}$$

Osserviamo ora che dato un grafo $G \in \mathcal{G}_n$, il numero di grafi di $\mathcal{G}_n$ a lui isomorfi è al massimo $n!$ (ossia il numero di funzioni bigettive $V \to V$). Ma allora per ogni $x \in \mathcal{G}_n\big/\cong$ si ha che $|x| \le n!$. Da ciò e dalla (8) si deduce allora che

$$2^{\binom{n}{2}} \le \sum_{x\in \mathcal{G}_n/\cong} n! = n!\left|\mathcal{G}_n\big/\cong\right| = g_n n!.$$

e quindi

$$g_n \ge \frac{2^{\binom{n}{2}}}{n!}.$$

Pasando al $\log_2$ si ha che

$$\log_2(g_n) \ge \log_2\Big(\frac{2^{\binom{n}{2}}}{n!}\Big) = \log_2\big(2^{\binom{n}{2}}\big) - \log_2(n!) = \binom{n}{2} - \log_2(n!)$$

D'altra parte $n! \le n^n$, quindi $\log_2(n!) \le \log_2(n^n) = n\log_2(n)$ e perciò

$$\log_2(g_n) \ge \binom{n}{2} - n\log_2(n) = \frac{n(n-1)}{2} - n\log_2(n) = \frac{n^2}{2}\Big(1-\frac{1}{n}-\frac{2}{n}\log_2(n)\Big)$$

❑

Osservazione 15.2. La stima precedente prova $\log_2(g_n)$ ha lo stesso ordine di infinito di $n^2/2$, dato che quandi n è grande, il numero $1 - 1/n - 2\log_2(n)/n$ è molto vicino a 1. Questo prova che il problema di classificare i grafi a meno di isomorfismo è intrinsecamente difficile (anche da un punto di vista meramente computazionale) dato che il numero di classi non isomorfe è esponenziale nel numero dei vertici con esponente che ha lo stesso ordine di infinito di $n^2/2$.

Passeggiate, cammini e cicli

Definizione 15.3. Sia $G = (V, E)$ un grafo una successione finita di vertici $(v_0, \dots, v_n)$ sarà detta

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

Diremo che la passeggiata $P = (v_0, \dots, v_n)$ ha lunghezza n ed indicheremo con $\ell(P)$ la lunghezza di P.

Proposizione 15.4. *Sia G un grafo e sia $(_0, \dots, v_n)$ un cammino in G allora il grafo G' definito da:*

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

è un sottografo di G isomorfo a P_n.

Dimostrazione. Esercizio. ❑

Proposizione 15.5. *Sia G un grafo e sia $(v_0, \dots, v_n)$ un ciclo in G allora il grafo G' definito da:*

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

è un sottografo di G isomorfo a C_n.

Dimostrazione. Esercizio. ❑

Osservazione 15.6. In effetti è facile vedere che dare un cammino o un ciclo in un grafo è equivalente a dare un sottografo isomorfo a P_n o C_n per qualche n.

La relazione di essere congiungibili

Definizione 15.7. Sia $G = (V, E)$ e siano $v, w \in V$. Diremo che v e w sono *congiungibili* con un cammino [risp. una passeggiata] se e siste un cammino [risp. una passeggiata] $(v_0, \dots, v_n)$ tale che $v_0 = v$ e $v_n = w$.

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

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

Viceversa supponiamo che tra due vertici u e v esista una passeggiata. Sia $\mathcal{P} = \{P \mid P \text{ è una passegiiata tra } u \text{ e } v\}$ e sia $A = \{\ell(P) \mid P \in \mathcal{P}\}$. Dato che u e v sono congiungibili da una passeggiata, l'insieme $\mathcal{P}$ è non vuoto e quindi anche $A \neq \varnothing$. Ma allora per la proprietà di buon ordinamento (teorema 7.4) dei numeri naturali, ha minimo, ovvero esiste una passeggiata P_0 da u a v che ha lunghezza minima nel senso che

$$\forall P \in \mathcal{P} \quad \ell(P_0) \leq \ell(P).$$

Proviamo che P_0 deve essere un cammino. Sia $P_0 = (v_0, \dots, v_m)$, se per assurdo P_0 non fosse un cammino esisterebbero $i < j$ tali che $v_i = v_j$, si consideri $P_1 = (v_0, \dots, v_i, v_{j+1}, \dots, v_m)$. P_1 è una passeggiata, infatti, dato che P_0 è una passeggiata, $v_h, v_{h+1}\} \in \mathcal{E}(()G)$ per ogni $0 \leq h < m$, e dato che $v_i = v_j$, $\{v_i, v_{j+1}\} = \{v_i, v_{i+1}\} \in E(G)$. P_1 congiunge u a v, dato che $v_0 = u$ e $v_m = v$ ed essendo, quindi $P_1 \in \mathcal{P}$. Ma $\ell(P_1) = m - (j - i) < m$ e ciò contraddice la minimalità di P_0. ❑

Questa proposizione dice quindi che le due nozioni di congiungibilità che abbiamo sopra definito, sono in realtà la stessa. D'ora in poi diremo semplicemente che due punti sono congiungibili per dire che lo sono in uno dei due sensi (e quindi in tutti due i sensi) della definizione precedente.

Proposizione 15.9. *Le relazione di essere congiungibli è una relazione d'equivalenza.*

Dimostrazione. Indichiamo con $\sim$ la relazione di congiungibilità (i.e. $u \sim v$ se e solo se u è congiungibile a v). Dobbiamo provare che la relazione di essere congiungibili$\sim$ è riflessiva, simmetrica e transitiva (definizione 11.3).

La relazione è riflessiva. Invfatti per ogni $v \in V(G)$, (v) è un cammino che congiunge v a v, quindi per ogni v si ha che $v \sim v$.

La relazione è simmetrica. Se $u \sim v$ allora esiste una passeggiata $P = (v_0, \dots, v_n)$ tale che $u = v_0$ e $v = v_n$. Ma allora $P' = (v_n, v_{n-1}, \dots, v_0)$ è una passeggiata (due vertici consecutivi in P' sono adiacenti, dato che sono consecutivi —anche se in ordine scambiato— in P) il cui primo vertice è v e l'ultimo è u, ovvero

La relazione è transitiva. Se $u \sim v$ e $v \sim w$ allora esistono due passeggiate $P_1 = (v_0, \dots, v_n)$ e $P_2 = (u_0, \dots, u_m)$ tali che $u = v_0$, $v = u_n = u_0$ e $w = u_m$. Sia $Q = (v_0, \dots, v_n, u_1, \dots, u_m)$; Q è una passeggiata dato che vertici consecutivi in Q sono consecutivi o in P o in P' (si osservi che essendo $v_n = u_0$ si ha che v_n e u_1 sono consecutivi in P'), d'atra parte il primo e l'ultimo vertice di Q sono v e w, quindi $v\tilde{w}$. ❑

Lezione 16

Componenti connesse di un grafo

Definizione 16.1. Sia $G = (V, E)$ un grafo e siano $\{V_i\}_{i \in I}$ le classi d'equivalenza di V rispetto alla relazione di congiungibilità. I grafi $G[V_i]$, indotti da G sui V_i, vengono detti le *componenti connesse* di G.

Le componenti connesse sono invarianti per isomorfismo

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

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

Proposizione 16.3. *Sia $f : G \to G'$ un isomorfismo di grafi e $v, w \in V(G)$. v e w sono congiungibili se e solo se lo sono $f(v)$ e $f(w)$.*

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

Teorema 16.4. *Siano G e G' grafi isomorfi, allora hanno componenti connesse isomorfe. Più precisamente, se $\{G_i\}_{i \in I}$ e $\{G'_j\}_{j \in J}$ sono gli insiemi delle componenti connesse di G e G' rispettivamente, allora esiste una bigezione $\varphi : I \to J$ tale che $G_i \cong G'_{\varphi(i)}$.*

Dimostrazione. Siano $\{V_i\}_{i \in I}$ le classi d'equivalenza di $V(G)$ (rispetto alla congiungibilità $\sim$) e $\{V'_j\}_{j \in J}$ quelle di $V(G')$.

Proviamo innanzitutto che per ogni $i \in I$ esiste un unico $j \in J$ tale che $f(V_i) = V'_j$. Infatti sia $v \in V_i$, dato che $\{V'_j\}_{j \in J}$ è una partizione di $V(G')$, si ha che esiste un unico $j \in J$ tale che $f(v) \in V'_j$. Ma ora $u \in V_i$ se e solo se $u \sim v$ (per definizione di classe d'equivalenza (definizione 11.6)) e dato che f è un isomorfismo, per la proposizione precedente, questo equivale a dire che $f(u) \sim f(v)$ ovvero che $f(u) \in V'_j$, ovvero $f(V_i) \subseteq V'_j$. D'altra parte se $w \in V'_j$ allora $w \sim f(v)$, quindi, dato che f è un isomorfismo $f^{-1}(w) \sim v$ e quindi $f^{-1}(w) \in V_i$. Questo prova quindi che $V'_j = f(V_i)$.

Per ogni $i \in I$, indichiamo con $\varphi(i)$ l'unico j con la proprietà precedente.

Proviamo che per ogni $j \in J$ esiste un unico $i \in I$ tale che $\varphi(i) = j$, ossia $\varphi : I \to J$ è bigettiva. Dato J, sia $w \in V_j$, dato che f è bigettiva, esiste un unico $v \in V(G)$ tale che $f(v) = w$. Esiste allora un unico $i \in I$ tale che $v \in V_i$, e questo è quindi l'unico tale che $\varphi(i) = j$.

Per concludere proviamo che f induce un isomorfismo tra $G[V_i]$ e $G'[V'_\varphi(i)]$. Ma chiaramente, dato che f è bigettiva e $f(V_i) = V'_{\varphi(i)}$, anche $f|_{V_i} : V_i \to V'_{\varphi(i)}$ è bigettiva. Inoltre, se $u, v \in V_i$, per definizione di sottografo indotto (definizione 14.9), $\{u, v\} \in E(G[V_i])$ se e solo se $\{u, v\} \in E(G)$ e questo, per la proprietà di isomorfism di f equivale a dire che $\{f(u), f(v)\} \in E(G')$ e dato che $f(u), f(v) \in V'_{\varphi(i)}$, questo è a sua volta equivalente a dire che $\{f(u), f(v)\} \in E(G'[V'_{\varphi(i)}])$. E questa è la tesi. ❑

Esercizio 16.1. Si provi che se G è un grafo e $\{G_i\}_{i \in I}$ sono le sue componenti connesse, allora $E(G) = \bigcup_{i \in I} E(G_i)$.

Esercizio 16.2. Se G è un grafo finito e $G_1, \ldots, G_k$ sono le sue componenti connesse, allora $\sum_{i=1}^{k} |V(G_i)| = |V(G)|$ e $\sum_{i=1}^{k} |E(G_i)| = |E(G)|$.

Grafi connessi

Definizione 16.5. Un grafo si dice *connesso* se ha una sola componente connessa. Un grafo non connesso si dice *sconnesso*.

Osservazione 16.6. Un grafo G è connesso se e solo se per ogni $v, w \in V(G)$ v e w sono congiungibili da un cammino (risp. da una passeggiata).

Osservazione 16.7. Dal teorema 16.4 segue in particolare che se due grafi sono isomorfi, allora o sono entrambi connessi oppure sono entrambi sconnessi.

Esercizio 16.3. Si provi che se G è un grafo e G' è un sottografo di G connesso e che contiene tutti i vertici (i.e. $V(G') = V(G)$), allora anche G è connesso.

La matrice di adiacenza di un grafo finito

Definizione 16.8. Sia G un grafo finito e siano $v_1, \dots, v_n$ i sui vertici. Si chiama matrice di adiacenza di G la matrice A_G, che al posto i, j ha 1 se $\{v_i, v_j\} \in EG$ e ha 0 altrimenti.

Proposizione 16.9. *Sia A la matrice di adiacenza del grafo G, allora l'elemeto di posto i, j della matrice A^k è pari al numero di passeggiate lunghe k dal vertice v_i al vertice v_j.*

Esercizio 16.4. Si provi che un grafo finito G ha 3-cicli se e solo se la matrice A_G^3 ha elementi non nulli sulla diagonale.

Esercizio 16.5. Si provi che il numero di 3-cicli di un grafo finito G è pari a $\mathrm{tr}(A_G^3)/6$.

Lezione 17

Grado di un vertice

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

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

$$\sum_{v \in V} \deg(v) = 2\,|E| \tag{9}$$

Dimostrazione. Siano $v_1, \dots, v_n$ i vertici di G e $e_1, \dots, e_k$ i suoi lati. Per ogni $i = 1, \dots, n$ e $j = 1, \dots, k$ consideriamo il numero

$$m_{i,j} = \left\langle \begin{array}{lll} 1 & \text{se} & v_i \in e_j \\ 0 & \text{se} & v_i \notin e_j \end{array} \right.$$

Dalle proprietà associativa e commutativa della somma si ha evidentemente che

$$\sum_{i=1}^{n} \Big(\sum_{j=1}^{k} m_{i,j}\Big) = \sum_{j=1}^{k} \Big(\sum_{i=1}^{n} m_{i,j}\Big) \tag{10}$$

Ma fissato i il numero $\sum_{j=1}^{k} m_{i,j}$ è uguale alla cardinalità dell'insieme $\{j \mid m_{i,j} = 1\} = \{j \mid v_i \in e_j\}$ che è uguale al numero dei lati che contengono v_i, ossia $\sum_{j=1}^{k} m_{i,j} = \deg(v_i)$. Pertanto il lato sinistro dell'uguaglianza (10) è pari a $\sum_{i=1}^{n} \deg(v_i)$, ossia la somma dei gradi di tutti i vertici.

Invece, fissato j, il numero $\sum_{i=1}^{n} m_{i,j}$ è pari alla cardinalità dell'insieme $\{i \mid v_i \in e_j\}$, che è uguale a 2, dato che ogni lato contiene esattamente due vertici. Ne consegue che il lato destro della (10) è uguale a $2k = 2\,|E|$. ❏

Il lemma delle strette di mano

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

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

Score di un grafo

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

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

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

Osservazione 17.7. Non è vero il viceversa del precedente teorema, si vedano ad esempio i grafi i due grafi di figura 6 dell'esercizio 14.11.

Teorema dello score

Lezione 18

Definizione di grafo euleriano

Caratterizzazione dei grafi euleriani

Definizione di grafo hamiltoniano

Grafo duale di un grafo dato

G è connesso allora anche il suo duale lo è

Se G è euleriano allora il suo duale è hamiltoniano

Lezione 19

Alcune costruzioni con i grafi

Definizione 19.1. Sia $G = (V, E)$ un grafo, definiamo alcuni grafi costruiti a partire da G:

- (cancellazione di un lato) se $e \in E$ denotiamo
$$G - e = (V, E \setminus \{e\})$$
- (aggiunta di un lato) se $e \in \binom{V}{2} \setminus E$ denotiamo
$$G + e = (V, E \setminus \{e\})$$
- (cancellazione di un vertice) se $v \in V$ denotiamo
$$G - v = (V \setminus \{v\}, \{e \in E \mid v \notin e\})$$
- (divisione di un lato) se $e = \{u, v\} \in E$ denotiamo
$$G\%e = (V \cup \{z\}, E \setminus \{e\} \cup \{\{u, z\}, \{v, z\}\})$$
essendo $z \notin V$.

Esercizio 19.1. Si provi che se G è connesso, allora per ogni $e \in E(G)$, anche $G\%e$ è connesso.

Esercizio 19.2. Si provi che per ogni vertice v si ha che $C_n - v \cong P_{n-1}$.

Definizione di grafo 2-connesso

Definizione 19.2. Sia G un grafo, diremo che G è 2-connseeo se $|V(G)| \geq 3$ e per ogni $v \in V(G)$ si ha che $G - v$ è connesso.

Esercizio 19.3. Si provi che ogni grafo hamiltoniano è 2-connesso.

Esercizio 19.4. Si provi che se $f : G \to G'$ è un isomorfismo, allora per ogni $v \in V(G)$ ed $e \in E(G)$ si ha che $G - v \cong G' - f(v)$, $G - e \cong G' - f(e)$, $G\%e \cong G'\%f(e)$.

Esercizio 19.5. Si provi che se $e \in E(C_n)$ allora $C_n\%e \cong C_{n+}1$.

Esercizio 19.6. Si provi che se $e \in E(P_n)$ allora $P_n\%e \cong P_{n+1}$.

Proposizione 19.3. *Sia G un grafo 2-connesso e $e \in E(G)$. Allora $G - e$ è connesso.*

Dimostrazione. Siano $u, v \in V$. Dobbiamo provare che esiste una passeggiata tra v e u che non contiene il lato e. Si hanno due casi

1. $e \neq \{u, v\}$;

2. $e = \{u, v\}$.

Nel primo caso, sia x un estremo di e diverso da u e v (i.e. $e = \{x, y\}$ con $x \neq u$ e $x \neq v$) allora $u, v \in V(G - x)$. Dato che G è 2-connesso, $G - x$ è connesso, e quindi esiste una passeggiata in $G - x$ che congiunge u e v. Dato che $x \in e$, $e \notin E(G - x)$ quindi questa passeggiata non contenere il lato e.

Nel secondo caso, sia $w \in V(G) \setminus \{u, v\}$ (esiste perché $|V(G)| \geq 3$). Dato che G è 2-connesso esiste una passeggiata P tra u e w in $G - u$ (chiaramente tale passeggiata non passa per e). Per lo stesso motivo esiste una passeggiata tra w e v in $G - u$ (anche questa passeggiata non può contenere il lato e). Congiungendo queste due passeggiate si ottiene una passeggiata che congiunge u e v e che non passa per e. ❑

Osservazione 19.4. Dalla proposizione precedente segue in particolare che ogni grafo 2-connesso è connesso.

Prima caratterizzazione dei grafi 2-connessi

Teorema 19.5 (prima caratterizzazione dei grafi 2-connessi). *Un grafo G è 2-connesso se e solo se ogni coppia di vertici di G è contenuta in un ciclo. Ossia per ogni $v, w \in V(G)$ esiste un ciclo $(v_0, v_1, \ldots, v_n = v_0)$ in G che passa per i vertci v e w.*

Seconda caratterizzazione dei grafi 2-connessi

Lemma 19.6. *Sia G un grafo 2-connesso allora per ogni $e \in E$ anche $G\%e$ è 2-connesso.*

Dimostrazione. Sia $e = \{x, y\}$ e $v \in V(G\%e) = V(G) \cup \{z\}$. Si hanno tre casi:

1. $v = z$;

2. $v = x$ o $v = y$;

3. $v \neq x$, $v \neq y$ e $v \neq z$

Nel primo caso, $G\%e - v = G\%e - z = G - e$, infatti dalle definizioni si ha

$$\begin{aligned}
V(G\%e - z) &= V(G\%e) \setminus \{z\} = (V(G) \cup \{z\}) \setminus \{z\} = V(G) = V(G - e) \\
E(G\%e - z) &= \{a \in E(G\%e) \mid z \notin a\} = \\
&\quad \big((E(G) \setminus \{e\}) \cup \{\{z, x\}, \{z, y\}\}\big) \setminus \{a \mid z \in a\} = \\
&\quad E(G) \setminus \{e\} = E(G - e)
\end{aligned}$$

Pertanto $G\%e - v$ è connesso per la proposizione 19.3

Nel secondo caso, supponiamo che $v = y$ (l'altro caso si ottiene per simmetria, scambiando x e y). Osserviamo che $G - y$ è un sottografo di $G\%e - y$. Infatti

$$\begin{aligned}
V(G - y) &= V(G) \setminus \{y\} \\
V(G\%e - y) &= V(G\%e) \setminus \{y\} = (V(G) \cup \{z\}) \setminus \{y\} = V(G - y) \cup \{z\} \\
E(G - y) &= E(G) \setminus \{a \mid y \in a\} \\
E(G\%e - y) &= E(G\%e) \setminus \{a \mid y \in a\} = \\
&\quad \big((E(G) \setminus \{e\}) \cup \{\{z, x\}, \{z, y\}\}\big) \setminus \{a \mid y \in a\} = \\
&\quad (E(G) \setminus \{a \mid y \in a\}) \cup \{\{x, z\}\} = E(G - v) \cup \{\{x, z\}\} =
\end{aligned}$$

Ma allora dato che ogni $G - v$ è 2-connesso, $G - v$ è connesso e quindi ogni vertice di $G - v$ è congiungibile in $G - v$, e quindi in $G\%e - y$ al vertice $x \in V(G - v)$. D'altra parte, l'unico altro vertice di $G\%e - y$ è z che è congiungibile a x in $G\%e - y$, dato che $\{x, z\} \in E(G\%e - y)$. Tutti i vertici sono quindi congiungibili tra loro.

Nel terzo caso $G\%e - v = (G - v)\%e$ è connesso in quanto ottenuto dal grafo connesso $G - v$ suddividendo un suo lato (esercizio 19.1) ($G - v$ è connesso). ❑

Lemma 19.7. *Sia G un grafo 2-connesso allora per ogni $e \in \binom{V}{2} \setminus E$ anche $G + e$ è 2-connesso.*

Dimostrazione. Segue dal fatto che per ogni vertice $v \in V(G + e) = V(G)$ il grafo $(G + e) - v$ ha gli stessi vertici di $G - v$ e contiene tutti i lati di $G - v$. Dato che quest'ultimo è connesso, lo ànche $(G + e) - v$. ❑

Teorema 19.8. *Un grafo finito G è 2-connesso se e solo se è isomorfo ad un grafo ottenuto a partire da C_3 con una successione finita di suddivisioni di ed aggiunzioni di lati.*

Dimostrazione. Dato che C_3 è 2-connesso (esercizio 19.3), i due lemmi precedenti provano che ogni grafo ottenuto da C_3 aggiungendo e suddividendo lati è 2-connesso.

Proviamo l'implicazione opposta. Per semplicità diciamo che un grafo è *costruibile* se è ottenuto da C_3 con un numero finito di aggiunzioni e suddivisioni di nodi. Consideriamo l'insieme

$$\mathcal{G} = \{H \mid H \text{ è sottografo costruibile di } G\}.$$

usando l'esercizio 19.5, si prova che ogni ciclo è costruibile, d'altra parte dal primo teorema di caratterizzazione (teorema 19.5) segue, in particolare, che G contiene dei cicli. Ma allora $\mathcal{G} \neq \varnothing$. Sia allora $H_0 \in \mathcal{G}$ un grafo che massimizza il numero dei lati (G è finito!), ossia tale che

$$|E(H_0)| \geq |E(H)| \quad \forall H \in \mathcal{G}. \tag{11}$$

Proviamo che $H_0 = G$ da cui segue evidentemente la tesi.

$V(H_0) = V(G)$. Supponiamo per assurdo che esista $v \in V(G) \setminus V(H_0)$. G è connesso, esiste quindi un cammino $P = (v_0, \ldots, v_m)$ che congiunge v ad un vertice di H_0. Sia v_i il primo vertice di questo cammino tale che $v_i \in V(H_0)$. Chiamiamo

$w = v_i$ e $u = v_{i-1}$ ($i > 0$ dato che $v_0 = v \notin V(H_0)$), allora $e = \{u, w\} \in E(G)$, $w \in V(H_0)$ e $u \notin V(H_0)$.

Il grafo $G - w$ è connesso e, dato che H_0 ha almeno tre vertici, esistono vertici di H_0 diversi da w. Sia allora $Q = (u_0, \ldots, u_k)$ un cammino in $G - w$ che congiunge u ad un vertice di H_0 ed i cui altri vertici sono tutti fuori di H_0 (vedi figura 7), ossia $u_0 = u$, $u_k \in V(H_0)$ e $v_i \notin V(H_0)$ per ogni $i < k$. Consideriamo il grafo H_1 definito da:

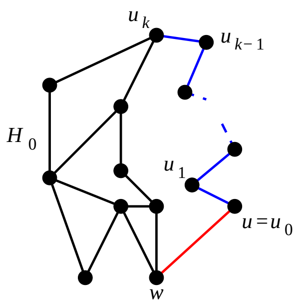

Figura 7: Come costruire un cammino che ha solo due punti in comune con H_0

$$
\begin{aligned}
V(H_1) &= V(H_0) \cup \{u = u_0, \ldots, u_{k-1}\} \\
E(H_1) &= E(H_0) \cup \{e = \{w, u_0\}, \{u_0, u_1\}, \ldots, \{u_{k-1}, u_k\}\}
\end{aligned}
$$

Chiaramente H_1 è un sottografo di G e $|E(H_1)| > |(H_0)|$. Se proviamo che H_1 è ottenuto da H_0 con un numero finito di suddivisioni e di aggiunzioni di lati si ha che $H_1 \in \mathcal{G}$ e quindi un assurdo. Ma ora si hanno due casi:

1. $\{w, u_k\} \in E(H_0)$
2. $\{w, u_k\} \notin E(H_0)$

Nel primo caso H_1 è ottenuto suddividendo k volte il lato $\{w, u_k\}$ e quindi aggiungendo di nuovo il lato $\{w, u_k\}$, nel secondo caso H_1 è ottenuto aggiungendo il lato $\{w, u_k\}$ e quindi dividendolo k volte (vedi figura 8). $E(H_0) = E(G)$. Sup-

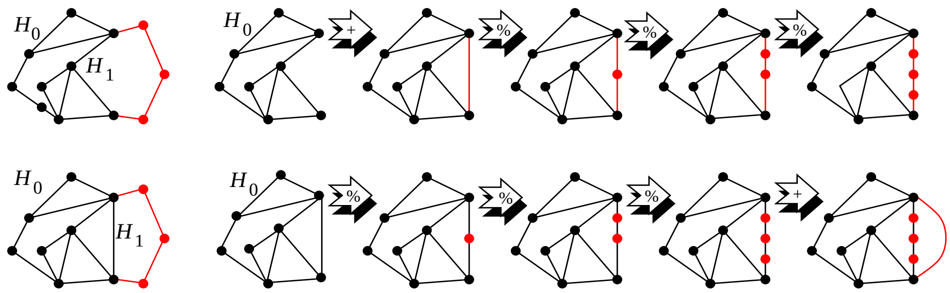

Figura 8: Il grafo H_1 è ottenuto da H_0 o aggiungendo un lato e quindi suddividendolo oppure suddividendo un lato già esistente e quindi riaggiungendolo.

poniamo per assurdo che $e \in E(G) \setminus E(H_0)$, allora, visto che per il punto precedente $V(H_0) = V(G)$, necessariamente $e \in \binom{V(H_0)}{2}$, si può allora costruire il grafo $H_1 = H_0 + e$ che è un sottografo di G. D'altra parte H_1 è ottenuto da H_0 aggiungendo un lato, quindi è costruibile, ovvero $H_1 \in \mathcal{G}$. Ma $|E(H_1)| = |E(H_0)| + 1$, che contraddice la (11). ❏

Esercizio 19.7. Siano $G = (V, E)$ e $G' = (V'.e')$ due grafi. Si denoti con $G \cup G'$ il grafo tale che $V(G \cup G') = V \cup V'$ e $E(G \cup G') = E \cup E'$. Si provi che se G e G' sono connessi e $V \cap V' \neq \varnothing$ allora $G \cup G'$ è connesso.

Esercizio 19.8. Si provi che se G e G' sono 2-connessi e $|V \cap V'| \geq 2$ allora $G \cup G'$ è 2-connesso.

Esercizio 19.9. Sia $k \geq 1$, si dice che un grafo $G = (V, E)$ è k*-connesso* se per ogni $v_1, \dots, v_{k-1} \in V$ si ha che $G - v_1 - v_2 - \cdots - v_{k-1}$ è connesso. Si osservi che 1-connesso è sinonimo di connesso.

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

Esercizio 19.10. Si determinino condizioni sufficienti affinché l'unione di due grafi k-connessi sia ancora k-connesso.

Esercizio 19.11. Per ogni $n \in \mathbb{N}$ sia $G_n = (V_n, E_n)$ un grafo connesso e si supponga che $V_n \subseteq V_{n+1}$ per ogni n. Si provi che allora $G = \bigcup_{n \in \mathbb{N}} G_n$ è connesso.

Esercizio 19.12. Per ogni $n \in \mathbb{N}$ sia $G_n = (V_n, E_n)$ un grafo connesso e si supponga che $V_n \cap V_{n+1} \neq \varnothing$ per ogni n. Si provi che allora $G = \bigcup_{n \in \mathbb{N}} G_n$ è connesso.

Esercizio 19.13. Per ogni $n \in \mathbb{N}$ sia $G_n = (V_n, E_n)$ un grafo k-connesso e si supponga che $|V_n \cap V_{n+1}| \geq k$ per ogni n. Si provi che allora $G = \bigcup_{n \in \mathbb{N}} G_n$ è k-connesso.

Lezione 20

Alberi

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

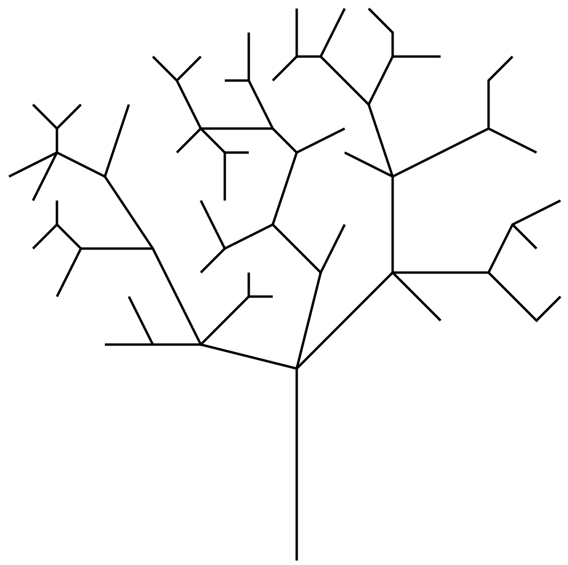

Figura 9: Un albero

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

Il teorema di caratterizzazione degli alberi

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

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

Dimostrazione. Dimostriamo le implicazioni (1) $\implies$ (2) $\implies$ (3) $\implies$ (4) $\implies$ (1).

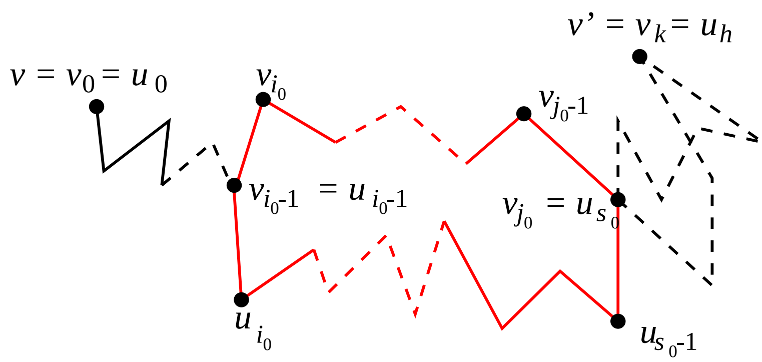

Figura 10: La costruzione del ciclo nella dimostrazione di (1) $\implies$ (2)

(1) $\implies$ (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 10).

(2) $\implies$ (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) $\implies$ (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 11).

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) $\implies$ (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

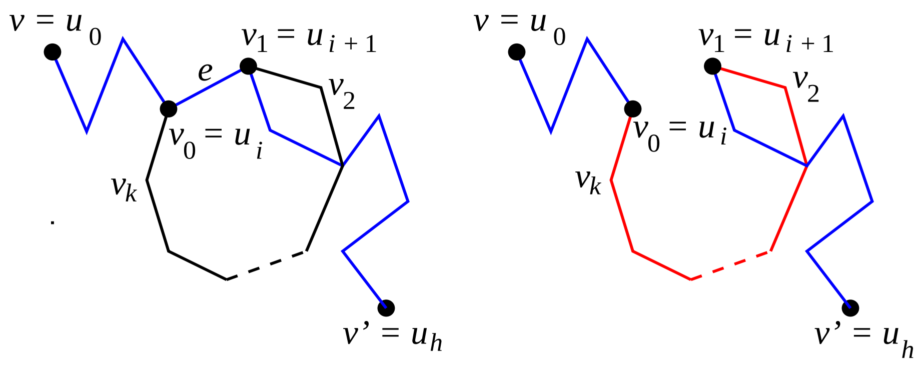

Figura 11: La costruzione della passeggiata nella dimostrazione di (3) $\implies$ (4)

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

Il teorema di caratterizzazione degli alberi finiti

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

Esercizio 20.2. Si determinino le foglie dell'albero in figura 9

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

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

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

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

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

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

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

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

1. *T è un albero*

5. *T è connesso e $|V| - 1 = |E|$*

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

$$|V(T)| - 1 - 1 = |V(T - v)| - 1 = |E(T - v)| .$$

Ma dato che $\deg(v) = 1$, $|E(T - v)| = cardE(T) - 1$ e quindi la tesi.
(5) $\implies$ (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 (proposizione 17.2), si ottiene

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

se non esistessero foglie, ogni $v \in V(T)$ dovrebbe avere $\deg(v) \geq 2$ (non possono esistere vertici di grado 0 dato che T è connesso ed ha almeno 2 lati) e si otterrebbe subito un assurdo $(2\,|V(T)| - 2 \geq 2\,|V(T)|)$. Pertanto 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 (esercizio 20.3). 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 $T - v$ contraddicendo il fatto che $T - v$ è un albero. ❑

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

Lezione 21

Albero di copertura

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

- T è un albero;
- $V(T) = V(G)$.

Osservazione 21.2. Chiaramente, se G è un grafo che possiede un albero di copertura, allora G è connesso. Dato che due vertici di G, essendo vertici di T saranno congiunti da un cammino in T, e dato che T è un sottografo di G tale cammino sarà un cammino anche in G.

Esercizio 21.1. Si dia una dimostrazione formale di quanto appena osservato (osservazione 21.2). E si provi che se G è un grafo e G' è un suo sottografo connesso tale che $V(G') = V(G)$ allora G è connesso.

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

Dimostrazione. Diamo due dimostrazioni di questo teorema, entrambe costruttive: una che costruisce un albero di copertura "partendo dal basso" ed una che lo costruisce "partendo dall'alto".

Prima dimostrazione. Si consideri l'insieme

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

$\mathcal{T} \neq \varnothing$, infatti se $v \in \mathsf{V}(G)$ allora $(\{v\}, \varnothing) \in \mathcal{T}$ (i.e. è un sottografo che è un albero). Dato che G è finito, esiste $\overline{T} \in \mathcal{T}$ con massimo numero di vertici, ossia tale che

$$|V(T)| \leq \left|V(\overline{T})\right| \quad \forall T \in \mathcal{T}.$$

Se proviamo che $V(\overline{T}) = V(G)$ avremo trovato un albero di copertura. Supponiamo che esista $v \in V(G) \setminus V(\overline{T})$, allora, usando la connessione di G con la stessa tecnica usata nella dimostrazione del teorema 19.8, è possibile determinare un vertice $w \in V(G) \setminus V(\overline{T})$ ed un vertice $u \in V(T)$ tali che $\{u, w\} \in E(G)$ (si congiunge v ad un vertice di $\overline{T}$ e si prendono il primo vertice del cammino che arriva in $\overline{T}$ ed il suo predecessore). Ma allora $T' = (V(\overline{T}) \cup \{w\}, E(\overline{T}) \cup \{\{u, w\}\})$ è evidentemente un sottografo di G ed è un albero. Quest'ultimoa asserzione si prova esattamente come nella seconda parte della dimostrazione del teorema di caratterizzazione degli alberi finiti (teorema(20.6)). In altri termini $T' \in \mathcal{T}$, d'altra parte $|V(T')| = \left|V(\overline{T})\right| + 1$ e questo è in contraddizione con la massimalità di $\overline{T}$. Questo conclude la prima dimostrazione.
Seconda dimostrazione. Si consideri l'insieme

$$\mathcal{C} = \{C \mid C \text{ è sottografo connesso di } G \text{ e } V(C) = V(G)\}$$

$\mathcal{C} \neq \varnothing$ dato che $G \in \mathcal{C}$. Data la finitezza di G esisterà un grafo $\overline{C} \in \mathcal{C}$ con il minor numero di lati, ovvero

$$\left|E(\overline{C})\right| \leq |E(C)| \quad \forall C \in \mathcal{C}$$

Proviamo che $\overline{C}$ è un albero. Infatti se non lo fosse, per la proprietà (3) del teorema di caratterizzazione degli alberi (teorema20.2) esisterebbe un lato $e \in E(\overline{C})$ tale che $\overline{C} - e$ è connesso. Ma $V(\overline{C} - e) = V(C) = V(G)$, quindi $C \in \mathcal{C}$, e d'altra parte $\left|E(\overline{C}) - e\right| = \left|E(\overline{C})\right| - 1 =$, che contraddice la minimalità di $\overline{C}$. Questo conclude la seconda dimostrazione. ❏

Osservazione 21.4. Il teorema precedente è vero anche senza l'ipotesi di finitezza, del grafo G, la sua dimostrazione nel caso infinito, richiede però degli strumenti un po' più sofisticati (si veda teorema 23.4).

Esercizio 21.2. Si traducano le due dimostrazioni del teorema precedente (teorema 21.3) in due algoritmi per la determinazione di un albero di copertura di un grafo finito.

Esercizio 21.3. Si provi che se $G = (V, E)$ è un grafo connesso finito, allora $|E| \geq |V| - 1$.

Alberi radicati

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

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

Esercizio 21.4. Si considerino i grafi in figura 12. Si provi che $T \cong T'$ ma $(T, r) \ncong (T', r')$.

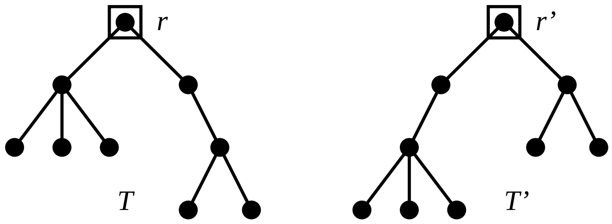

Figura 12: Gli alberi radicati dell'esercizio 21.4

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 20.2 punto 2) che congiunge r con v.

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

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

Proviamo ora che non possono valere contemporaneamente. Se vale la (1), allora $P_w = (v_0, \dots, v_k)$ con $v_0 = r$, $v_k = w$ ed esiste un i tale che $v_i = v$. Ma allora $P_v = (v_0, \dots, v_i)$. 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 $P_v = (v_0, \dots, v_i)$. ❏

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

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

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

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

Lezione 22

L'ordinamento degli alberi radicati

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

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

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

Dimostrazione. $\square$

Induzione sugli alberi radicati

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

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

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

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

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

Dimostrazione. $\square$

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

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

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

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

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

Il lemma di König

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

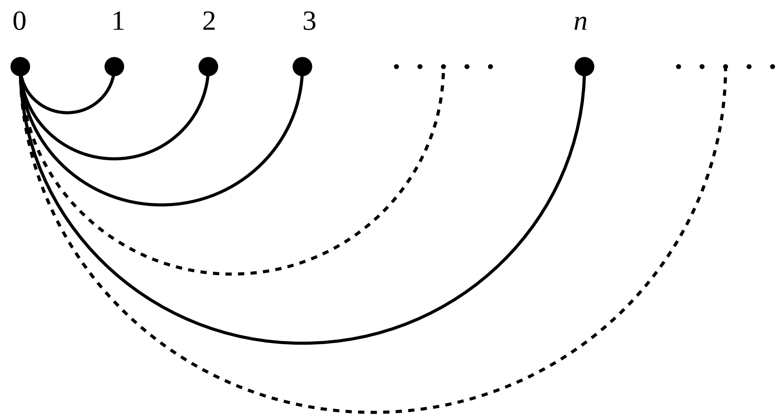

Figura 13: Un contresempio al Lemma di König, senza l'ipotesi dei gradi finiti

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

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

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

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

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

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

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

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

$$V_i = \big\{v \in V(T) \bigm| v_i \to^* v\big\}$$

Chiaramente

$$\big\{v \in V(T) \bigm| f(n) \to^* v\big\} = \{f(n)\} \cup V_1 \cup \cdots \cup V_k$$

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. ❑

Lezione 23

Il lemma di Zorn

Definizione 23.1. Sia X un insieme e sia $\preccurlyeq$ un ordinamento parziale (definizione 3.6) 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

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

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 $\to^*$ sui vertici dell'albero radicato (T, r) essendo $V(T) = \{r, a, b\}$ e $E(T) = \{\{r, a\}, \{r, b\}\}$ (vedi figura 14). Evidentemente a e b sono entrambi massimali, ma non $a \not\to^* b$ e $b \not\to^* a$.

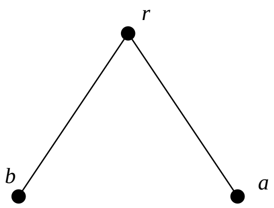

Figura 14: L'albero dell'esempio 23.2

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 (5.1), 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

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

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 $(v = v_0, \dots, v_k = w)$, 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.

Soluzione di alcuni degli esercizi proposti

Soluzione dell'esercizio 1.1 Proviamo la prima. Bisogna provare che $\forall x \quad x \in \varnothing \implies x \in X$. Ma questo è vero per quanto osservato in 1.4.

A titolo di esempio un po' più significativo, proviamo anche la quarta. Se $X = Y$, allora per il punto 1, si ha che valgono le due inclusioni. Viceversa, supponiamo che valgano le due inclusioni. Dalla prima, per definizione di inclusione *Definizione 1.5) ne segue che per ogni z, $z \in X \implies z \in Y$, dalla seconda inclusione in modo analogo segue che per ogni z, $z \in Y \implies z \in X$. Ma allora per ogni z, $z \in X \iff z \in Y$, e quindi, per estensionalità (1.1) ne segue che $X = Y$. ❑

Soluzione dell'esercizio 1.3 Proviamo la prima delle leggi di De Morgan. $x \in X \setminus (Y \cup Z)$ se e solo se $x \in X$ e $x \notin Y \cup Z$. Ma ora, dato che $x \in Y \cup Z$ se solo se $x \in Y$ o $x \in Z$, allora $x \notin Y \cup Z$ se e solo se $x \notin Y$ e $x \notin Z$. In definitiva

$$x \in X \setminus (Y \cup Z) \iff x \in X \text{ e } x \notin Y \text{ e } x \notin Z. \tag{12}$$

D'altra parte $x \in (X \setminus Y) \cap (X \setminus Z)$ se e solo se $x \in (X \setminus Y)$ e $(X \setminus Z)$ ossia se solo se $x \in X$ e $x \notin Y$ e $x \in X$ e $x \notin Z$, e quindi

$$x \in (X \setminus Y) \cap (X \setminus Z) \iff x \in X \text{ e } x \notin Y \text{ e } x \notin Z. \tag{13}$$

da 24 e 13 assieme all'assioma di separazione (1.1) segue allora la tesi. ❑

Soluzione dell'esercizio 1.4

❑

Soluzione dell'esercizio 1.5 Se $f = g$ allora per estensionalità (1.1), per ogni $(x, y) \in X \times Y$ $(x, y) \in f$. Ma allora se $x \in X$ allora $(x, f(x)) \in f = g$, e quindi $(x, f(x)) \in g$, da cui $f(x) = g(x)$.

Viceversa se $(x, y) \in f$ allora $y = f(x)$, ma allora $y = g(x)$ e quindi $(x, y) \in f$, pertanto $f \subseteq g$. Allo stesso modo si prova che anche $g \subseteq f$ e quindi si ha la tesi, ❑

Soluzione dell'esercizio 1.6 Osserviamo che $X \times \varnothing$ e $\varnothing \times X$ sono entrambi uguali a $\varnothing$. Questo perché per definixione $X \times \varnothing = \{(x, y) \mid x \in X \text{ e } y \in \varnothing\}$, ma per ogni y $y \notin \varnothing$. ❑

Soluzione dell'esercizio 1.7 f è iniettiva. Siano x_1 e $x_2 \in X$ tali che $f(x_1) = f(x_2)$, allora $g(f(x_1)) = g(f(x_2))$ ovvero $g \circ f(x_1) = g \circ f(x_2)$. Dato che $g \circ f = \mathrm{id}_X$, $g \circ f(x_1) = x_1$ e $g \circ f(x_2) = x_2$ e quindi $x_1 = x_2$.

f è suriettiva. Sia $y \in Y$, allora $g(y) \in X$ è tale che $f(g(x)) = y$, dato che $f(g(x)) = f \circ g(y) = \mathrm{id}_Y(y) = y$. ❑

Soluzione dell'esercizio 1.8 Per definizione, una funzione $f : X \to Y$ è un sottinsieme di $X \times Y$ che verifica la proprietà

$$P(f) := \forall x \in X \quad \exists \text{ unico } y \in Y : (x, y) \in f$$

ossia la collezione di tutte le funzioni da X in Y può essere descritta da:

$$Y^X = \{f \mid f \in 2^{X \times Y} \text{ e } P(f)\}$$

Dato che X e Y sono insiemi allora $X \times Y$ è un insieme. Ma allora anche $2^{X \times Y}$ è un insieme e quindi, per l'assioma di separazione (1.6), anche Y^X è un insieme. ❑

Soluzione dell'esercizio 1.9

❑

Soluzione dell'esercizio 1.10

❑

Soluzione dell'esercizio 1.11 Proviamo la prima delle due. Per definizione di immagine inversa di un insieme, $x \in f^{-1}(\bigcap_{i \in I} A_i)$ se e solo se $f(x) \in \bigcap_{i \in I} A_i$ e questo, per definizione di intersezione, equivale a dire che $f(x) \in A_i$ per ogni $i \in I$, ovvero che $x \in f^{-1}(A_i)$ per ogni $i \in I$, che equivale a dire che $x \in \bigcap_{i \in I} f^{-1}(A_i)$. Si conclude per l'assioma di estensionalità (1.1).

Del tutto analoga è la dimostrazione della seconda delle due. $x \in f^{-1}(\bigcap_{i \in I} A_i)$ se e solo se $f(x) \in \bigcup_{i \in I} A_i$ e questo, per la proprietà che caratterizza l'unione, equivale a dire che esiste $i \in I$ tale che $f(x) \in A_i$, ovvero che esiste $i \in I$ tale che $x \in f^{-1}(A_i)$, che equivale a dire che $x \in \bigcup_{i \in I} f^{-1}(A_i)$. Si conclude, anche in questo caso, per l'assioma di estensionalità (1.1). ❑

Soluzione dell'esercizio 1.12 Proviamo soltanto che nella seconda delle due non si ha in generale uguaglianza. Per fare questo, basta dare un esempio, Sia $X = \{0, 1\}$, $Y = \{0\}$ e $f : X \to Y$ l'unica funzione possibile. Sia $A_i = \{i\}$ con $i \in \{), 1\}$, allora chiaramente $\Lambda_0 \cap A_1 = \varnothing$ e quindi $f(A_0 \cap A_1) = \varnothing$. D'altra parte $f(A_i) = \{0\}$ e quindi $f(A_0) \cap f(A_1) = \{0\}$. Chiaramente questo esempio si generalizza con ogni funzione non iniettiva. ❑

Soluzione dell'esercizio 2.1 Proviamo la seconda. Supponiamo dapprima che f e g siano iniettive; se $f \times g(x, y) = f \times g(x', y')$, allora per definizione di $f \times g$, si ha che $(f(x), g(y)) = (f(x'), g(y;))$, e quindi per definizione di prodotto cartesiano, $f(x) = f(x')$ e $g(y) = g(y')$. Dato che f e g sono entrambe iniettive, questo vuol dire che $x = x'$ e $y = y'$, ovvero che $(x, y) = (x', y')$.

Viceversa, supponiamo che $f \times g$ sia iniettiva; siano x, $x' \in X$, tali che $f(x) = f(x')$, allora, prendiamo $y \in Y$ (esiste perché $Y \neq \varnothing$), allora $(f(x), g(y)) = (f(x'), g(y))$, ovvero $f \times g(x, y) = f \times g(x', y)$ e quindi $(x, y) = (x', y)$, da cui $x = x'$, ovvero f è iniettiva. In modo del tutto analogo si prova che anche g è iniettiva.

Nel caso che uno dei due insiemi X, Y sia vuoto, potrebbe succedere che la funzione prodotto sia iniettiva (o suriettiva) senza che lo sia una delle due funzioni f, g. Mostriamo questo fatto con due esempi.

Esempio 1. Si consideri $X = \varnothing$, $Y = \{1, 2\}$, $X' = Y' = \{1\}$ e f e g le uniche funzioni possibili, ovvero $f = \varnothing$ e $g(y) = 1$, per ogni $y \in Y$. Chiaramente la funzione g non è iniettiva, mentre la funzione prodotto è la funzione vuota ($f \times g = \varnothing$), che è quindi iniettiva.

Esempio 2. Si consideri $X = \varnothing$, $Y = \{1\}$, $X' = \varnothing$, $Y' = Y' = \{1, 2\}$, $f = \varnothing$ la funzione vuota e g la funzione definita da $g(1) = 1$. Chiaramente la funzione g non è suriettiva, mentre la funzione prodotto è la funzione vuota ($f \times g = \varnothing : \varnothing \to \varnothing$), che è suriettiva.

Le altre due implicazioni restano invece vere anche se X e Y sono vuoti. ❑

Soluzione dell'esercizio 2.2 Se $A \subseteq X$ definiamo la funzione $\chi_A : X \to \{0, 1\}$, ponendo

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

Questa funzione viiene chiamata funzione *caratteristica* o *indicatrice* di A.

Consideriamo la funzione $\Phi : 2^X \to \{0,1\}^X$ definita ponendo $\Phi(A) = \chi_A$, e proviamo che Φ è una bigezione.

Φ è iniettiva. Dalla definizione di χ_A si ha immediatamente che $A = \{x \mid \chi_A(x) = 1\}$. Per tanto, se $\chi_A = \chi_B$ allora

$$A = \{x \mid \chi_A(x) = 1\} = \{x \mid \chi_B(x) = 1\} = B.$$

Φ è suriettiva. Sia $\lambda : X \to \{0,1\}$. Se prendiamo $A = \{x \mid \lambda(x) = 1\}$, allora $\chi_A = \lambda$. Infatti per definizione di A si ha che $\lambda(x) = 1$ se e solo se $x \in A$, e quindi, poiché λ assume valori solo in $\{0,1\}$, se $x \notin A$, necessariamente $\lambda(x) = 0$. Ma allora λ assume gli stessi valori di χ_A e quindi coincide con χ_A. ❑

Soluzione dell'esercizio 2.3 Sia $\Phi : X^{\{0,1\}} \to X \times X$ definita da $\varphi(f) = (f(0), f(1))$ e sia $\Psi : X \times X \to X^{\{0,1\}}$ definita ponendo $\Psi(x_0, x_1)$ la funzione tale che

$$\begin{aligned} \Psi(x_0, x_1)(0) &= x_0 \\ \Psi(x_0, x_1)(1) &= x_1 \end{aligned}$$

Chiaramente $\Psi \circ \Phi(f) = \Psi(f(0), f(1)$ è, per definizione di Ψ, la funzione che in 0 vale $f(0)$ e in 1 vale $f(1)$, quindi coincide con f,

D'altra parte $\Phi \circ \Psi(x_0, x_1) = (\Psi(x_0, x_1)(0), \Psi(x_0, x_1)(1)) = (x_0, x_1)$. Ma allora per l'esercizio 1.7, Φ e Ψ sono bigezioni una inversa dell'altra, da cui la tesi. ❑

Soluzione dell'esercizio 2.4 Definiamo $\Phi : (X^Y)^Z \to X^{Y \times Z}$ nel seguente modo: se $f \in (X^Y)^Z$, e $(y, z) \in Y \times Z$ poniamo

$$\Phi(f)(y, z) = f(z)(y).$$

Quello che abbiamo scritto ha perfettamente senso, dato che $f(z)$ è una funzione $Y \to X$, ha senso quindi calcolarla in y ed il risultato è un elemento di X.

Definiamo ora $\Psi : X^{Y \times Z} \to (X^Y)^Z$ nel modo seguente: se $g \in X^{Y \times Z}$, poniamo

$$\Psi(g)(z)(y) = g(y, z)$$

ossia, fissato z, $\Psi(g)(z)$ è la funzione che calcolata in y dà per risultato $g(y, z)$.

In virtù dell'esercizio 1.7 avremo concluso se proviamo che $\Phi \circ \Psi$ e $\Psi \circ \Phi$ sono entrambe l'identità.

Sia $f \in (X^Y)^Z$ e calcoliamo il valore che assume $\Psi \circ \Phi(f)$. Per definizione di Ψ, $\Psi \circ \Phi(f)(z) = \Psi(\Phi(f))(z)$ è la funzione che calcolata in y vale $\Psi \circ \Phi(f)$. Per definizione di Ψ, $\Psi \circ \Phi(f)(z)(y) = \Phi(f)(y, z)$, e quest'ultimo, per definizione di Φ coincide con $f(z)(y)$. Ma allora per ogni z $\Psi \circ \Phi(f)(z) = f(z)$, ossia $\Psi \circ \Phi(f) = f$

Se $g \in X^{Y \times Z}$ allora, per definizione di Φ, $\Phi \circ \Psi(g)(y, z) = \Phi(\Psi(g))(y, z) = \Psi(g)(z)(y)$, che a sua volta, per definizione di Ψ, è uguale a $g(y, z)$, qualsiasi sia $(y, z)] \in Y \times Z$. Questo basta per dire che $\Phi \circ \Psi(g) = g$. ❑

Soluzione dell'esercizio 2.5 Consideriamo la funzione $\Phi : X^{Y \cup Z} \to X^Y \times X^Z$ definita da

$$\Phi(f) = (f|_Y, f|_Z)$$

Per provare che Φ è una bigezione, troviamo direttamente la sua inversa. Consideriamo $\Psi : X^Y \times X^Z \to \Phi : X^{Y \cup Z}$ definita da

$$\Psi(g_1, g_2)(x) = \left\langle \begin{array}{ll} g_1(x) & \text{se } x \in Y \\ g_2(x) & \text{se } x \in Z \end{array} \right.$$

Osserviamo innanzitutto che $\Psi(g_1, g_2)$ è ben definita, dato che $Y \cap Z = \varnothing$, e quindi non ci sono ambiguità su quale delle due scegliere per calcolare il valore in x. $\Psi(g_1, g_2)$ non è altro che l'unione $g_1 \cup g_2$ (cfr Esempio 1.14), che in questo caso è ben definita dato che $\restriction g_1 Y \cap Z = \restriction g_2 Y \cap Z = \varnothing$.

È immediato verificare che $\Phi \circ \Psi$ $\Psi \circ \Phi$ sono entrambe l'identità. ❑

Soluzione dell'esercizio 3.1 Proviamo la prima. Procediamo per induzione su n. Se $n = 0$, per definizione $0 + 0 = 0$. Supponiamo la tesi vera per n. Allora

$$0 + \mathrm{succ}(n) = \mathrm{succ}(0 + n) = \mathrm{succ}(n)$$

dove la prima uguaglianza segue dalla definizione ricorsiva di $+$ e la seconda dall'ipotesi di induzione. Questo prova la tesi.

Proviamo ora la seconda. Per induzione su n. Se $n = 0$, $1 + 0 = 1 = succ(0) = 0 + 1$ (per quanto visto nell'osservazione 3.2). Supponiamo la tesi vera per n, allora

$$1 + \mathrm{succ}(n) = \mathrm{succ}(1 + n) = \mathrm{succ}(n + 1) = \mathrm{succ}(\mathrm{succ}(n)) = \mathrm{succ}(n) + 1$$

dove la prima uguaglianza segue dalla definizione ricorsiva di $+$, la seconda dall'ipotesi di induzione ed infine la terza e la quarta da quanto visto nell'osservazione 3.2). ❑

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

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

❑

Soluzione dell'esercizio 3.3 Proviamo la prima. $k \leq h$, quindi per la prima delle proprietà di proposizione 3.9, si ha $h + m \leq h + m$. Per lo stesso motivo anche $n + k \leq m + k$. Ma allora per la proprietà commutativa della somma

$$n + k \leq m + k = k + m \leq h + m = m + h.$$

Proviamo la seconda. Chiaramente la tesi è vera se $k = 0$ o se $n = 0$. Supponiamo allora $k \geq 1$ e $n \geq 1$ (in particolare anche $m \geq 1$), allora

$$nk \leq mk = km \leq hm = mh$$

che è la tesi, ❑

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

$$h(i) = \left\langle \begin{array}{ll} f(i) & \text{se } i < n \\ g(i - n) & \text{se } n \leq i < m + n \end{array} \right.$$

è una bigezione.

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

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

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

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

sommando queste due relazioni si ottiene la tesi. ❏

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

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

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

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

❏

Soluzione dell'esercizio 4.4 Dimostriamo 1. Osserviamo che

$$X \times Y = \bigcup_{x \in X} \{x\} \times Y$$

chiaramente se $x_1 \neq x_2$ allora $(\{x_1\} \times Y) \cap (\{x_2\} \times Y) = \varnothing$ e quindi, per l'esercizio precedente (4.3),

$$|X \times Y| = \left|\bigcup_{x \in X} \{x\} \times Y\right| = \sum_{x \in X} |\{x\} \times Y| .$$

D'altra parte, per ogni $x \in X$ si ha che la funzione $Y \to \{x\} \times Y$ definita da $y \to (x, y)$ è una bigezione, e quindi $|\{x\} \times Y| = |Y|$, pertanto

$$|X \times Y| = \sum_{x \in X} |Y| = |X|\,|Y| .$$

Dimostriamo 2. Procediamo per induzione su $|X|$, Se $|X| = 0$ allora $X = \varnothing$ e $Y^X = \{\varnothing\}$ e quindi $\left|X^Y\right| = 1 = |Y|^0$, Supponiamo la tesi vera per $|X| = n$ e proviamo la tesi quando $|X| = n + 1$. Fissato un elemento $x_0 \in X$, per ogni $y \in Y$ indichiamo con $\mathcal{F}_{x_0,y} = \{f : X \to Y \mid f(x_0) = y\}$. Osserviamo che evidentemente

$$Y^X = \bigcup_{y \in Y} \mathcal{F}_{x_0,y}$$

e d'altra parte per ogni $y_1 \neq y_2$ si ha $\mathcal{F}_{x_0,y_1} \cap \mathcal{F}_{x_0,y_2} = \varnothing$, quindi

$$\left|Y^X\right| = \sum_{y \in Y} |\mathcal{F}_{x_0,y}| .$$

Ma ora, detto $X' = X - \{x_0\}$, osserviamo che per ogni $y \in Y$, l'insieme $\mathcal{F}_{x_0,y}$ è in bigezione con $Y^{X'}$, ad esempio mediante la funzione $\Phi : \mathcal{F}_{x_0,y} \to Y^{X'}$ definita da $f \to f|_{X'}$. Ma allora

$$\left|Y^X\right| = |Y| \left|Y^{X'}\right|.$$

Per concludere, osserviamo che $|X'| = |X| - 1 = n$ e quindi, per ipotesi di induzione $\left|Y^{X'}\right| = |Y|^n$ e quindi

$$\left|Y^X\right| = |Y| \, |Y|^n = \left|Y^{n+1}\right| = |Y|^{|X|}.$$

Il terzo punto dell'esercizio segue allora dal secondo e dall'esercizio 2.2. ❏

Soluzione dell'esercizio 4.5 Indichiamo con $\mathcal{I}(X,Y)$ l'insieme delle funzioni iniettive $X \to Y$. Procediamo per induzione su k. Se $k = 0$ allora $X = \varnothing$ e quindi $Y^X = \{\varnothing\}$ e la funzione $\varnothing : \varnothing \to Y$ è iniettiva. Quindi $\mathcal{I}(\varnothing, Y) = \{\varnothing\}$ ha cardinalità $1 = n!/(n-0)!$.

Supponiamo la tesi vera per k e proviamola per $k+1$. Supponiamo quindi che $|X| = k + 1 \leq |Y|$. Chiaramente $X \neq \varnothing$ e quindi esiste un elemento $x_0 \in X$. Consideriamo per ogni $y \in Y$ l'insieme

$$\mathcal{I}_y = \{f \in \mathcal{I}(X,Y) \mid f(x_0) = y\}.$$

Si ha evidentemente che

$$\mathcal{I}(X,Y) = \bigcup_{y \in Y} \mathcal{I}_y$$

e per ogni $y_1 \neq y_2$ $\mathcal{I}_{y_1} \cap \mathcal{I}_{y_2} = \varnothing$. Quindi

$$|\mathcal{I}(X,Y)| = \sum_{y \in Y} |\mathcal{I}_y|$$

Osserviamo ora che $\mathcal{I}_y$ è in bigezione con $\mathcal{I}(X \setminus \{x_0\}, Y \setminus \{y\})$ quindi, visto che $|X \setminus \{x_0\}| = k$ e $|Y \setminus \{y\}| = n - 1$, per ipotesi di induzione, si ha che $|\mathcal{I}(X \setminus \{x_0\}, Y \setminus \{y\})| = (n-1)!/(n-1-k)!$.

Ma allora

$$\begin{aligned} |\mathcal{I}(X,Y)| &= \sum_{y \in Y} |\mathcal{I}(X \setminus \{x_0\}, Y \setminus \{y\})| \\ &= \sum_{y \in Y} \frac{(n-1)!}{(n-1-k)!} = n\frac{(n-1)!}{(n-1-k)!} = \frac{n!}{(n-(k+1))!} \end{aligned}$$

❏

Soluzione dell'esercizio 4.6 Sia $f : X \to Y$ iniettiva. Se Y' è l'immagine di f allora $f : X \to Y'$ è evidentemente surgettiva e quindi bigettiva. Ma allora $X \sim Y'$ e quindi $|X| = |Y'| \leq |Y| = |X|$. Ma allora necessariamente $Y' = Y$, ovvero f è surgettiva. ❏

Soluzione dell'esercizio 4.7 Per l'esercizio precedente (4.6), l'insieme delle bigezioni di X in sé coincide con l'insieme delle funzioni iniettive $X \to X$ e quindi, si può usare la formla dell'esrcizio 4.5, che nel caso $k = n$ dà $n!/0! = n!/1 = n!$. ❏

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

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

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

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

$$g(y) = \left\langle \begin{array}{ll} x_y & \text{se } y \in f(X) \\ \overline{x} & \text{se } y \notin f(X) \end{array} \right.$$

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

Soluzione dell'esercizio 5.3

❑

Soluzione dell'esercizio 6.1

❑

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

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

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

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

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

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

Soluzione dell'esercizio 6.4

❑

Soluzione dell'esercizio 6.5
❑

Soluzione dell'esercizio 6.6
❑

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

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

$$g(x) = \left\langle \begin{array}{ll} f(x) & \text{se } x \in Y' \\ x & \text{se } x \in X - (Y \cup Y') \end{array} \right.$$

g è chiaramente una bigezione. ❑

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

Soluzione dell'esercizio 6.10
❑

Soluzione dell'esercizio 7.1
❑

Soluzione dell'esercizio 7.2
❑

Soluzione dell'esercizio 7.3
❑

Soluzione dell'esercizio 7.4
❑

Soluzione dell'esercizio 7.5

```
DIVE (n,m) {
  N=n
  M=m
  Q=0
  R=N
  WHILE N > M-1 DO
    N = N-M
    R = N
    Q = Q+1
  END WHILE
}
```

❑

Soluzione dell'esercizio 8.1 Dalla definizione del coefficiente binomiale (8.6) si ha

$$\begin{aligned}\binom{n}{k}+\binom{n}{k-1} &= \frac{n!}{k!(n-k)!}+\frac{n!}{(k-1)!(n-k+1)!} = \\ &= \frac{n!(n-k+1)+n!k}{(k)!(n-k+1)!} = \frac{n!(n+1)}{(k)!(n-k+1)!} = \binom{n+1}{k}\end{aligned}$$

❑

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

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

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

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

❑

Soluzione dell'esercizio 10.1 Procediamo per induzione su k. Se $k=1$ non c'è nulla da dimostrare. Supponiamo che la tesi sia vera per k e supponiamo che $p \mid n_1n_2\dots n_{k+1}$, ossia $p \mid (n_1n_2\dots n_k)n_{k+1}$. Per il corollario 10.2, si ha che $p \mid n_1n_2\dots n_k$ oppure $p \mid n_{k+1}$. Se si verifica la seconda eventualità abbiamo finito, altrimenti, per ipotesi di induzione esiste $i \in \{1,\dots,k\}$ tale che $p \mid n_i$, e quindi si conclude. ❑

Soluzione dell'esercizio 10.2

❑

Soluzione dell'esercizio 10.3

❑

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

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

Soluzione dell'esercizio 11.1 Per quanto visto nell'osservazione 11.8, possiamo definire l'applicazione $\Phi : R \to P$ data da $\Phi(\mathcal{R}) = X/_{\mathcal{R}}$.

Data invece una partizione $\mathcal{P} \in P$ definiamo la relazione $\overset{\mathcal{P}}{\sim}$ ponendo

$$x_1 \overset{\mathcal{P}}{\sim} x_2 \iff \exists A \in \mathcal{P} : x_1, x_2 \in A.$$

Proviamo che $\overset{\mathcal{P}}{\sim}$ è una relazione d'equivalenza.

$\overset{\mathcal{P}}{\sim}$ è riflessiva (1 di definizione 11.3). Se $x \in X$ allora, dato che $\mathcal{P}$ ricopre X (proprietà (2) di 11.8), esiste $A \in \mathcal{P}$ tale che $x \in A$ e quindi $x \overset{\mathcal{P}}{\sim} x$.

$\overset{\mathcal{P}}{\sim}$ è simmetrica (2 di definizione 11.3). Ovvio.

$\overset{\mathcal{P}}{\sim}$ è transitiva (3 di definizione 11.3). Siano $x_1 \overset{\mathcal{P}}{\sim} x_2$ e $x_2 \overset{\mathcal{P}}{\sim} x_3$, allora esistono $A, B \in \mathcal{P}$ tali che $x_1, x_2 \in A$ e $x_2, x_3 \in B$. Ma, allora $x_2 \in A \cap B$ ossia $A \cap B \neq \varnothing$ e quindi coincidono (proprietà (3) di 11.8) ossia $A = B$ e quindi $x_1, x_3 \in A$ ovvero $x_1 \overset{\mathcal{P}}{\sim} x_3$.

Definiamo allora $\Psi : P \to R$ ponendo $\Psi(\mathcal{P}) = \overset{\mathcal{P}}{\sim}$, e proviamo che $\Phi \circ \Psi = \mathrm{id}$ e $\Psi \circ \Phi = \mathrm{id}$. Ciò concluderà la dimostrazione.

Sia $\mathcal{R} \in R$, allora, per la (2) della proposizione 11.7, si ha che $x_1 \mathcal{R} x_2$ se e solo se $[x_1]_{\mathcal{R}} = [x_2]_{\mathcal{R}}$ ossia se e solo se esiste $A \in X/_{\mathcal{R}}$ tale che $x_1, x_2 \in A$ ossia se e solo se esiste $A \in \Phi(\mathcal{R})$ tale che $x_1, x_2 \in A$ ossia se e solo se $x_1 \overset{\Phi(\mathcal{R})}{\sim} x_2$ e quindi $\mathcal{R} = \Psi(\Phi(\mathcal{R}))$.

Sia invece $\mathcal{P} \in P$, allora, dato $A \in P$ sia $x \in A$, è chiaro che $[x]_{\overset{\mathcal{P}}{\sim}} = A$, ciò unito al fatto che $\mathcal{P}$ ricopre X (proprietà (2) di 11.8) permette di concludere che $X/_{\overset{\mathcal{P}}{\sim}} = \mathcal{P}$ ovvero che $\Phi(\Psi(\mathcal{P})) = \mathcal{P}$. ❑

Soluzione dell'esercizio 11.2 Proviamone l'ultima a titolo di esempio, le a ltre si dimostrano in modo completamente analogo.

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

❑

Soluzione dell'esercizio 12.1

❑

Soluzione dell'esercizio 12.2 Osserviamo che per ogni $i \in \mathbb{N}$ si ha che $10^i \equiv 1 \mod 3$. Questo perché $10 \equiv 1 \mod 3$ e quindi $10^i \equiv 1^i = 1 \mod 3$. Ma allora

$$n = \sum_{i=0}^{k} \varepsilon_i 10^i \equiv \sum_{i=0}^{k} \varepsilon_i \mod 3$$

quindi $3 \mid n$ se e solo se $n \equiv 0 \mod 3$ se e solo se $\sum_{i=0}^{k} \varepsilon_i \equiv 0 \mod 3$ se e solo se $3 \mid \sum_{i=0}^{k} \varepsilon_i$.

Del tutto analoga è la dimostrazione della seconda. Per quanto riguarda la terza si adatti la dimostrazione della prima osservando che $10 \equiv -1 \mod 11$ e quindi

$$10^i \equiv (-1)^i = \left\langle \begin{array}{ll} 1 & \text{se } x \text{ è pari} \\ -1 & \text{se } x \text{ è dispari} \end{array} \right.$$

❑

Soluzione dell'esercizio 13.1 Sia c una soluzione di $ax \equiv b \mod n$, allora $n \mid (ac-b)$ ossia $ac-b=kn$. Ma allora $a'(a,n)c-b'(a,n)=kn'(a,n)$ da cui segue che $a'c-b'=kn'$, ossia c è una soluzione della seconda congruenza.

Viceversa se c risolve $a'x \equiv b' \mod n'$ allora esiste k tale che $a'c-b'=kn'$ e quindi $ac-b=(a'c-b')(a,n)=kn'(a,n)=kn$, ossia c risolve la prima congruenza. ❑

Soluzione dell'esercizio 13.2 Se $y \in [x]_n$ allora $n \mid (x-y)$, ma dato che $n' \mid n$ allora anche $n' \mid (x-y)$, ovvero $y \in [x]_{n'}$.

Proviamo innanzitutto che $[x+in']_n \subseteq [x]_{n'}$ per ogni i. Infatti se $y \in [x+in']_n$ allora $n \mid (x-y+in')$ e quindi $n' \mid (x-y+in')$, da cui segue che $n' \mid (x-y)$ ossia che $y \in [x]_{n'}$. Da questo fatto ne consegue allora che $[x]_{n'} \supseteq \bigcup_{i=0}^{d-1}[x+in']_n$. Dimostriamo l'inclusione opposta. Sia $y \in [x]_{n'}$, e sia r il resto della divisione euclidea di $x-y$ per n, ossia $x-y=qn+r$ con $0 \leq r < n$. Allora $n' \mid x-y$ e quindi $n' \mid r$, ovvero esiste i tale che $r=in'$ e $0 \leq i \leq d-1$. Inoltre $x+r-y=nq$ e quindi $y \equiv x+r=x+id \mod n$, ossia $y \in \bigcup_{i=0}^{d-1}[x+in']_n$.

Per concludere osserviamo che affinché si abbia $[x+in']_n \neq [x+jn']_n$ deve aversi $x+in' \equiv x+jn' \mod n$, ovvero $n \mid (i-j)n'$. Supposto per assurdo che $j<i$ si ha allora che $0<i-j<d$ e quindi $0<(i-j)n'<dn'=n$, ma allora $(i-j)n'$ non potrebbe essere un multiplo di n. ❑

Soluzione dell'esercizio 13.3 Osserviamo che $X=[x]_n$ risolve l'equazione $[a]_n X=[b]_n$ se e solo se $ax \equiv b \mod n$. Per l'esercizio 13.1 se c è una soluzione intera allora tutte le soluzioni intere sono $[c]_{n'}$. Ma allora per l'esercizio precedente (13.2) $[c]_{n'}=\bigcup_{i=0}^{(a,n)-1}[x+in']_n$ e le classi $[x+in']_n$ con $i=0,\dots(a,n)-1$ sono tutte diverse. Queste sono tutte e sole le soluzioni in $\mathbb{Z}/_{n\mathbb{Z}}$ dell'equazione lineare $[a]_n X=[b]_n$. ❑

Soluzione dell'esercizio 13.4 Sia $x \in \mathbb{Z}$ allora o $p \mid x$ oppure $(x,p)=1$, ma nel primo caso $[x]_p=[0]_p$ nel secondo caso $[x]_p$ è invertibile mod p e quindi $[x]_p^{p-1}=[1]_p$ ovvero $[x]_p^{p-1}-[1]_p=[0]_p$. Ne consegue che in ogni caso il prodotto di $[x]_p$ e di $[x]_p^{p-1}-[1]_p$ è $[0]_p$ ovvero

$$\begin{aligned}
[0]_p &= [x]_p\left([x]_p^{p-1}-[1]_p\right)=\left([x]_p\left[x^{p-1}\right]_p-[1]_p\right)= \\
&= [x]_p\left[x^{p-1}-1\right]_p=\left[x(x^{p-1}-1)\right]_p=[x^p-x]_p
\end{aligned}$$

quindi $p \mid (x^p-x)$ ovvero $x^p - \equiv x \mod p$. ❑

Soluzione dell'esercizio 13.5 Osserviamo che $(a,pq) \neq 1$ se e solo se $p \mid a$ o $p \mid a$, ma i numeri più piccoli di pq che sono divisibili per p sono $p, 2p, \dots, qp$, quelli che sono divisibili per q sono invece $q, 2q, \dots, pq$ e quindi i numeri più piccoli di pq e non coprimi con pq sono $p+q-1$. Quindi $\Phi(pq)=pq-(p+q-1)=(p-1)(q-1)$. ❑

Soluzione dell'esercizio 13.6 $\Phi(n)=(p-1)(q-1)=pq-p-q+1=n-p-q+1$ da cui $p+q=n+1-\Phi(n)$. Quindi p e q sono determinati dal sistema di equazioni

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

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

Soluzione dell'esercizio 13.7

❑

Soluzione dell'esercizio 14.1 La relazione $\mathcal{R}(E)$ è simmetrica. Infatti se $v_1 \ \mathcal{R}(E) \ v_2 \iff \{v_1, v_2\} \in E$. Ma $\{v_1, v_2\} = v_2, v_1$, quindi anche $\{v_2, v_1\} \in E$ e quindi $v_2 \ \mathcal{R}(E) \ v_1$.

La relazione $\mathcal{R}(E)$ è antiriflessiva. Infatti per ogni $v \in V$ $\{v\} = \{v, v\} \notin E$ e per tanto $\neg v\mathcal{R}(E)v$.

Se $\sim$ è antiriflessiva, allora $\mathcal{E}(\sim) \subseteq \binom{V}{2}$, infatti se $e \in \mathcal{E}(\sim)$ allora, per definizione di $\mathcal{E}(\sim)$ (osservazione 14.2), $e = \{v_1, v_2\}$ con $v_1 \sim v_2$, e dato che $\sim$ è antiriflessiva, $v_1 \neq v_2$ e quindi $|e| = 2$ ovvero $e \in \binom{V}{2}$ ovvero $\mathcal{E}(\sim) \subseteq \binom{V}{2}$. ❑

Soluzione dell'esercizio 14.2 Per quanto visto nell'osservazione 14.2, la relazione $\mathcal{R}(\mathcal{E}(\sim))$ è sempre simmetrica, quindi non potrà essere uguale a $\sim$ che non lo è.

Un esempio. $X = \{0, 1\}$ e $\sim = \{(0, 1)\}$. Evidentemente $0 \sim 1$ ma $1 \not\sim 0$. ❑

Soluzione dell'esercizio 14.4 Il sottografo indotto $K_n[V]$ è isomorfo a K_m. Sia $f : \{1, \ldots, m\} \to V$ una funzione bigettiva. f è evidentemente un isomorfismo dato che tutte le coppie di elemnti di $\{1, \ldots, m\}$ sono lati di K_m e tutte le coppie di eleenti $\{v_1, v_2\}$ al variare di $v_1 \neq v_2 \in V$ sono lati di K_n e quindi di $K_n[V]$.

Volendo essere più formali, dato che K_n è completo, per ogni $1 \leq i \neq j \leq m$ il lato $\{f(i), f(j)\} \in E(K_n)$ e quindi $\{f(i), f(j)\} \in E(K_n[V])$. D'altra parte se $\{v_1, v_2\} \in E(K_n[V])$, allora esistono $1 \leq i \neq jm$ tali che $f(i) = v_1$ e $f(j) = v_2$ e dato che K_m è il grafo completo, $\{i, j\} \in E(K_m)$. ❑

Soluzione dell'esercizio 14.5

❑

Soluzione dell'esercizio 14.6

❑

Soluzione dell'esercizio 14.7

❑

Soluzione dell'esercizio 14.8

❑

Soluzione dell'esercizio 14.9 La colorazione dei lati data in figura 15 suggerisce come definire l'isomorfismo. Precismante se si definisce la funzione $f : \{1, 2, \ldots, 10\} \to \{a, b, \ldots, j\}$ ponendo

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

una semplice verifica mostra che f è un isomorfismo. ❑

Soluzione dell'esercizio 14.10

❑

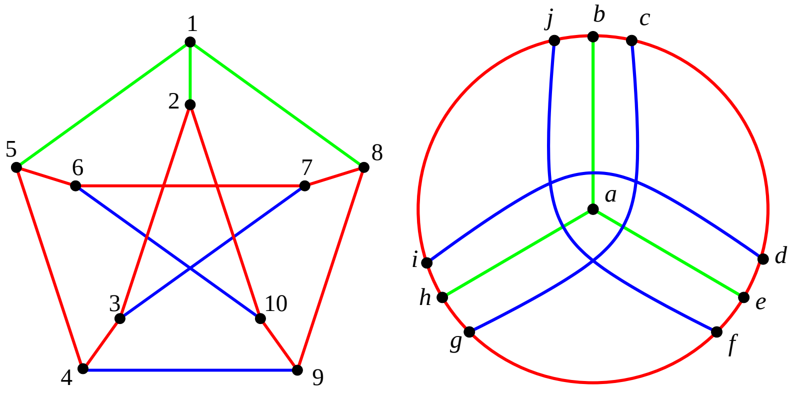

Figura 15: Soluzione grafica dell'esercizio 14.9

Soluzione dell'esercizio 14.11
❑

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

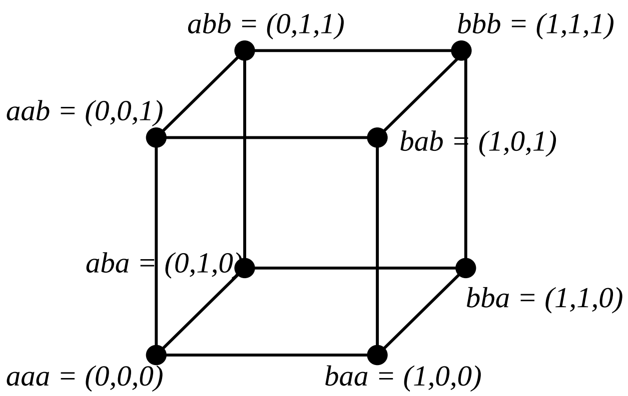

Figura 16: L'isomorfismo tra i grafi dell'esercizio 14.12

Soluzione dell'esercizio 16.1 Chiaramente $E(G) \supseteq \bigcup_{i \in I} E(G_i)$. Proviamo l'inclusione opposta. Se $e \in E(G)$ allora $e = \{u, v\}$ ed i vertici u, v sono evidentemente congiungibili. Allora sono vertici di una medesima componente connessa, ovvero esiste i tale che $u, v \in V(G_i)$. Per definizione di componente connessa (definizione 16.1) e di sottografo indotto (definizione 14.9) $e = \{u, v\} \in G_i$. Quindi, per l'arbitrarietà di $u, v \in E$ se ne deduce che $E(G) \subseteq \bigcup_{i \in I} E(G_i)$. ❑

Soluzione dell'esercizio 16.2 Segue immediatamente dall'esercizio precedente e dall'osservare che gli insiemi dei lati di due componenti diverse sono necessariamente disgiunti. ❑

Soluzione dell'esercizio 16.3 Siano $u, v \in V(G) = V(G')$, dato che G' è connesso esiste una passeggiata in G' che li congiunge, sia questa $P = (v_0, v_1, \ldots, v_n)$. Ossia $\{v_i, v_{i+1}\} \in E(G')$ per ogni i. Ma dato che G' è un sottografo di G, allora $E(G') \subseteq E(G)$ e quindi $\{v_i, v_{i+1}\} \in E(G)$ per ogni i, ossia P è una passeggiata in G, quindi u, v sono congiungibili in G. ❑

Soluzione dell'esercizio 19.1 Sia $e = \{x, y\}$ e siano $u, v \in V(G\%e) = V(G) \cup \{z\}$, si hanno due casi:

1. $u \neq z$ e $v \neq z$;
2. $u = z$ oppure $v = z$.

Nel primo caso sia $(u = v_0, v_1, \ldots, v_n = v)$ un cammino in G che congiunge u e v. Se questo non passa per il lato e, allora è un cammino anche in $G\%e$, se invece per qualche i si ha $e = \{v_i, v_{i+1}$ allora basta considerare il nuovo cammino $(v_0, \ldots, v_i, z, v_{i+1}, \ldots, v_n)$ che congiunge u a v in $G\%e$.

Nel secondo caso, supponiamo che $v = z$ allora per il passo precedente sappiamo che u è congiungibile con x in $G\%e$, d'altra parte x è congiungbile con z e quindi u è congiungibile con $z = v$. ❑

Soluzione dell'esercizio 19.2 Sia $v = i \in \{1, \ldots, n\}$, allora

$$\begin{array}{rcl} V(C_n - i) & = & \{1, \ldots, i-1\} \cup \{i+1, \ldots, n\} \\ E(C_n - i) & = & \{\{1,2\}, \ldots, \{i-2, i-1\}\} \cup \{\{i+1, i+2\}, \ldots, \{n-1, n\}, \{n, 1\}\} \end{array}$$

Ma allora la funzione $f : \{1, \ldots, n-1\} \to \{1, \ldots, i-1\} \cup \{i+1, \ldots, n\}$ definita da

$$f(j) = \left\langle \begin{array}{ll} i + j & \text{se} \quad j \leq n - i \\ j - (n - i) = j + i - n & \text{se} \quad j \geq n - i + 1 \end{array} \right.$$

è un isomorfismo. Chiaramente f è bigettiva. Inoltre

$$\{f(j), f(j+1)\} = \left\{ \begin{array}{ll} \{i + j, i + j + 1\} & \text{se} \quad j < n - i \\ \{n, 1\} & \text{se} \quad j = n - i \\ \{j + i - n, j + i - n + 1\} & \text{se} \quad j > n - i \end{array} \right.$$

da cui segue che f mette in bigezione i lati dei due grafi, ossia è un isomorfismo. ❑

Soluzione dell'esercizio 19.3 Sia G hamiltoniano, e sia H un sottografo di G isomorfo a C_n che contiene tutti i vertici di G. Allora $H - v$ è un sottografo di $G - v$ che contiene tutti i vertici di $G - v$. Ma H è isomorfo a un cammino (esercizio (19.2)) che è connesso. Si conclude allora invocando l'esercizio 16.3. ❑

Soluzione dell'esercizio 19.4

❑

Soluzione dell'esercizio 19.5 Usando l'esercizio precedente, possiamo supporre che $e = \{n, 1\}$. Ma allora si verifica immediatamente che la funzione f : $\{1, \ldots, n, n+1\} \to \{1, \ldots, n\} \cup \{z\}$ definita da

$$f(i) = \left\langle \begin{array}{ll} i & \text{se} \quad i \leq n \\ z & \text{se} \quad i = n + 1 \end{array} \right.$$

è un isomorfismo tra C_{n+1} e $C_n\%e$. ❑

Soluzione dell'esercizio 19.6 Possiamo supporre che $e = \{n-, n\}$. Ma allora si verifica immediatamente che la funzione $f : \{1, \ldots, n, n+1\} \to \{1, \ldots, n\} \cup \{z\}$ definita da

$$f(i) = \left\langle \begin{array}{lll} i & \text{se} & i \leq n-1 \\ z & \text{se} & i = n \\ n & \text{se} & i = n+1 \end{array} \right.$$

è un isomorfismo tra P_{n+1} e $P_n\%e$. ❑

Soluzione dell'esercizio 19.7
❑

Soluzione dell'esercizio 19.8
❑

Soluzione dell'esercizio 19.9
❑

Soluzione dell'esercizio 19.10
❑

Soluzione dell'esercizio 19.11
❑

Soluzione dell'esercizio 19.12
❑

Soluzione dell'esercizio 19.13
❑

Soluzione dell'esercizio 20.1
❑

Soluzione dell'esercizio 20.3 Un cammino in G 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. ❑

Soluzione dell'esercizio 20.4 Per l'esercizio precedente (esercizio 20.3) $T - v$ è connesso. D'altra parte se $T - v$ avesse un ciclo, questo sarebbe un ciclo anche in T. ❑

Soluzione dell'esercizio 20.5 Sia G un grafo connesso con n vertici, indichiamo con $f(G)$ il numero di foglie di G. Se $n = 2$ allora il numero di foglie è esattamente $f = 2$. Se $n \geq 3$ proviamo che allora il numero di foglie è $f(G) \leq n - 1$. Lo proviamo per induzione su n. Se $n = 3$ si vede facilmente, analizzando tutti i grafi connessi con 3 vertici (sono solo 2) che il massimo numero di foglie è 2 (uno ne ha 2 e l'altro non ne ha). Supponiamo la tesi vera per n e sia G un grafo connesso con $n + 1$ vertici. Se G non ha foglie allora la tesi è vera ($f(G) = 0 \leq n$) altrimenti sia $v \in V(G)$ una foglia. Il grafo $G - v$ è connesso, ha n vertici e quindi, per ipotesi di induzione, $f(G-v) \le n-1$. D'altra parte G ha al più una foglia in più di $G-v$ (il vertice v) e quindi

$$f(G) \le f(G-e) + 1 \le n - 1 + 1 = n$$

che è la tesi.

Un esempio è dato dal grafo G definito da:

$$\begin{aligned} V(G) &= \{0, 1, \ldots, n-1\} \\ E(G) &= \{\{0, i\} \mid i = 1, \ldots, n-1\} \end{aligned}$$

Si può provare che a meno di isomorfismo questo è l'unico grafo connesso con n vertici e $n-1$ foglie. Infatti sia G un tale grafo. G deve avere un vertice di grado $n-1$. Infatti se k è il grado dell'unica non foglia, allora

$$\sum_{v \in V(G)} \deg(v) = n - 1 + k = 2\,|E(G)|$$

d'altra parte se G è connesso, $|E(G)| \ge n-1$ (esercizio 21.3) quindi $k \ge n-1$. È altresì chiaro che un vertice di un grafo con n vertici può avere grado al più $n-1$ e quindi $k = n-1$. ❑

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

Soluzione dell'esercizio 21.1 Siano $v, u \in V(G) = V(G')$, allora, dato che G' è connesso, esiste una passeggiata $P = (v_0, \ldots, v_k)$ in G che congiunge U a v , ossia:

- $v_0 = u$ e $v_k = v$
- per ogni i si ha $\{v_i, v_{i+1}\} \in E(G')$.

Dato che G' è un sottografo (definizione 14.8) di G si ha che $E(G') \subseteq E(G)$ e quindi $\{v_i, v_{i+1}\} \in E(G)$ per ogni i. Di conseguenza P è una passeggiata in G che congiunge u a v. Per l'arbitrarietà di $u, v \in V(G)$ si ha la tesi. ❑

Soluzione dell'esercizio 21.2

❑

Soluzione dell'esercizio 21.3 Sia T un albero di copertura di G. Chiaramente $|V(T)| = |V(G)|$ e dato che T è un sottografo di G allora $|E(T)| \le |E(G)|$ e quindi, usando la formula che lega il numero di lati con il numero dei vertici di un albero (teorema 20.6), si ha

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

❑

Soluzione dell'esercizio 21.4

❑

Soluzione dell'esercizio 23.1

❑