



NoiStudiamo

DISPENSA DI TEORIA

Strutture Discrete

Logica, insiemi, teoria dei numeri, calcolo combinatorio,
probabilità discreta e teoria dei grafi.

A CURA DI

Gabriele Fontanarosa

Ottobre 2026

Indice dei capitoli

Logica e insiemi, teoria dei numeri, probabilità e grafi, in quattro parti.

1. Logica proposizionale	4
2. Forme normali, predicati e quantificatori	13
3. Insiemi	19
4. Metodi di dimostrazione	25
5. Famiglie di insiemi	28
6. Prodotto cartesiano e paradossi	32
7. Relazioni e funzioni	34
8. Relazioni di equivalenza e d'ordine	38
9. Hitting Set e famiglie chiuse per unione	42
10. Numeri interi e induzione	46
11. Divisione con resto e divisibilità	51
12. MCD, algoritmo di Euclide e numeri coprimi	54
13. Numeri primi e criteri di divisibilità	59
14. Congruenze e aritmetica modulare	65
15. La funzione φ di Eulero e i teoremi di Eulero e Fermat	70
16. Applicazioni dell'aritmetica modulare	75
17. Problemi aperti della teoria dei numeri	80

18. Calcolo combinatorio	85
19. Probabilità discreta	93
20. Variabili aleatorie e distribuzioni	102
21. Paradossi probabilistici	106
22. Introduzione ai grafi	110
23. Percorsi, connessione e rappresentazione dei grafi	116
24. Grafi euleriani, hamiltoniani e pesati	125
25. Grafi planari e colorazione	135
26. Alberi, complessità e problemi combinatori su grafi	142

Logica proposizionale

Il linguaggio più semplice per rappresentare affermazioni vere o false e per ragionare su di esse: connettivi, tavole di verità, equivalenze e conseguenza logica.

Il linguaggio della logica

La logica proposizionale nasce nel III secolo a.C. con la scuola degli Stoici e in particolare con Crisippo. Gran parte degli scritti originali andò perduta e il campo fu formalizzato in modo definitivo solo molti secoli dopo, grazie al lavoro di Leibniz e poi di George Boole e Augustus De Morgan, a metà dell'Ottocento. Per questo motivo la logica proposizionale è nota anche come **logica booleana**.

Una logica è un **linguaggio formale** per rappresentare informazioni da cui trarre conclusioni. Come ogni linguaggio, è composta da due parti: la **sintassi**, che stabilisce quali sequenze di simboli sono frasi (formule) del linguaggio, e la **semantica**, che stabilisce il significato delle frasi, cioè per ogni formula se è vera o falsa in una data situazione.

Le diverse logiche si distinguono per ciò che assumono come primitivo, cioè per ciò che «esiste» nel loro mondo e per i valori di verità che ammettono.

LOGICA	COSA ASSUME COME PRIMITIVO	VALORI DI VERITÀ
Proposizionale	Fatti	Vero o falso
Del primo ordine	Fatti, oggetti e relazioni tra oggetti	Vero o falso
Temporale	Fatti, oggetti, relazioni e tempo	Vero o falso
Probabilistica	Fatti, oggetti, relazioni e tempo	Grado di credenza

Tabella 1. Alcune famiglie di logiche e le loro assunzioni.

La logica proposizionale è la più semplice di tutte ed è strettamente legata al mondo binario 0 e 1 dei calcolatori. Si occupa di **proposizioni**, cioè di affermazioni di cui ha senso chiedersi se sono vere, e di come combinarle.

Proposizioni, variabili e connettivi

DEFINIZIONE: PROPOSIZIONE

Una **proposizione** è un'affermazione che è vera oppure falsa, ma non entrambe le cose.

«Roma è la capitale d'Italia» e « $3 > 2$ » sono proposizioni vere; «Catania è la capitale d'Italia» e « $2 > 3$ » sono proposizioni false. Non sono invece proposizioni una domanda come «che ora è?», un comando come «chiudi la porta» o un'espressione come « $x > 3$ », che diventa vera o falsa solo dopo aver fissato il valore di x (è un *predicato*, lo vedremo nel prossimo capitolo). Anche «questa frase è falsa» non è una proposizione ben definita: non può essere né vera né falsa senza contraddizione.

IL VOCABOLARIO

Il vocabolario della logica proposizionale è un insieme di **variabili proposizionali**, di solito indicate con $p, q, r, \dots$ oppure con $p_1, p_2, \dots$, che possono assumere solo due valori: **vero** (abbreviato V, in inglese T, oppure 1) e **falso** (abbreviato F oppure 0). Ogni variabile è già, da sola, una formula. Formule più complesse si ottengono combinando formule con i **connettivi logici**.

SIMBOLO	NOME	SI LEGGE	ESEMPIO
$\neg$	negazione	«non»	$\neg p$
$\wedge$	congiunzione	«e»	$p \wedge q$
$\vee$	disgiunzione (inclusiva)	«o» (almeno uno dei due)	$p \vee q$
$\Rightarrow$	implicazione	«se ... allora ...», «implica»	$p \Rightarrow q$
$\Leftrightarrow$	coimplicazione	«se e solo se»	$p \Leftrightarrow q$
$\oplus$	disgiunzione esclusiva (XOR)	«o l'uno o l'altro, non entrambi»	$p \oplus q$

Tabella 2. I connettivi logici. Il connettivo $\oplus$ non è primitivo: si ottiene dagli altri.

FORMULE BEN FORMATE

Le formule si costruiscono con regole ricorsive molto semplici: ogni variabile proposizionale è una formula; se P e Q sono formule, lo sono anche $\neg P$, $P \vee Q$, $P \wedge Q$, $P \Rightarrow Q$ e $P \Leftrightarrow Q$. Le formule che non nascono da queste regole non sono ammesse: « $p \wedge \vee q$ » non è una formula.

Per leggere una formula senza ambiguità si usano le parentesi e una convenzione di precedenza. La negazione $\neg$ lega più di tutti; poi viene $\wedge$, poi $\vee$, poi $\Rightarrow$ e infine $\Leftrightarrow$. Così $\neg p \vee q$ significa $(\neg p) \vee q$, cioè la negazione si applica solo a p , mentre $\neg(p \vee q)$ è la negazione dell'intera disgiunzione. Poiché non tutti gli autori seguono la stessa convenzione, nel dubbio conviene sempre scrivere le parentesi.

DA RICORDARE

La disgiunzione $\vee$ della logica è **inclusiva**: $p \vee q$ è vera anche quando sono vere entrambe. Il «o» dell'italiano quotidiano è spesso esclusivo («caffè o tè»); in logica per l'esclusivo si usa $\oplus$.

Semantica: interpretazioni e tavole di verità

DEFINIZIONE: INTERPRETAZIONE

Sia P l'insieme delle variabili proposizionali. Una **interpretazione** (o assegnazione di verità) è una funzione $I : P \rightarrow \{0, 1\}$, che a ogni variabile associa il valore vero (1) o falso (0). Il valore di una formula qualunque si ottiene da I applicando ricorsivamente le regole dei connettivi.

Le regole per calcolare il valore di verità, indicato con $I(\cdot)$, sono le seguenti.

- $I(\neg P)$ è vera se e solo se $I(P)$ è falsa.
- $I(P \wedge Q)$ è vera se e solo se $I(P)$ e $I(Q)$ sono entrambe vere.
- $I(P \vee Q)$ è vera se e solo se almeno una tra $I(P)$ e $I(Q)$ è vera.
- $I(P \Rightarrow Q)$ è vera se $I(P)$ è falsa oppure $I(Q)$ è vera; quindi è falsa soltanto quando P è vera e Q è falsa.
- $I(P \Leftrightarrow Q)$ è vera se e solo se $I(P)$ e $I(Q)$ hanno lo stesso valore, cioè se $P \Rightarrow Q$ e $Q \Rightarrow P$ sono entrambe vere.

Tutte queste regole si riassumono nelle **tavole di verità**: ogni riga corrisponde a una interpretazione delle variabili e ogni colonna a una formula.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$	$p \oplus q$
V	V	F	V	V	V	V	F
V	F	F	F	V	F	F	V
F	V	V	F	V	V	F	V
F	F	V	F	F	V	V	F

Tabella 3. Tavole di verità dei connettivi.

COME LEGGERE L'IMPLICAZIONE

L'implicazione è il connettivo che più spesso disorienta. $p \Rightarrow q$ afferma soltanto che *non si dà il caso che p sia vera e q falsa*. Se p è falsa la promessa non viene messa alla prova e l'implicazione è vera «per vacuità». Esempio: «se piove, prendo l'ombrello» è violata solo nel caso in cui piove e non prendo l'ombrello; se non piove, la frase resta vera qualunque cosa io faccia. Per lo stesso motivo la frase «se $2 > 3$ allora Catania è la capitale d'Italia» è vera: l'antecedente è falso.

Il valore di verità di una congiunzione o di una disgiunzione dipende solo dai valori delle due parti, non dal loro significato. Siano P_1 = «Roma è la capitale d'Italia» (vera), P_2 = «Catania è il capoluogo della Sicilia» (falsa: il capoluogo è Palermo) e P_3 = «Palermo è il capoluogo della Sicilia» (vera). Allora $P_1 \wedge P_3$ è vera, $P_1 \wedge P_2$ è falsa, mentre $P_1 \vee P_2$ è vera; la disgiunzione di due proposizioni false, come «Milano è la capitale d'Italia» e P_2 , è falsa.

VALORI NUMERICI

Se si identifica il vero con 1 e il falso con 0, i connettivi diventano operazioni aritmetiche, e questo spiega perché la logica booleana si implementa così bene sui calcolatori:

CONNETTIVO	OPERAZIONE SUI VALORI 0 E 1
$\neg p$	$1 - p$
$p \wedge q$	$\min(p, q)$, oppure il prodotto $p \cdot q$
$p \vee q$	$\max(p, q)$
$p \Rightarrow q$	$\max(1 - p, q)$
$p \Leftrightarrow q$	$\min(\max(1 - p, q), \max(p, 1 - q))$, oppure $1 - p - q $
$p \oplus q$	$ p - q $, cioè la somma modulo 2

Tabella 4. I connettivi come operazioni su 0 e 1.

Una formula con n variabili ha 2^n interpretazioni possibili, quindi la sua tavola di verità ha 2^n righe. Un modo sistematico per non dimenticarne nessuna è elencare le righe come i numeri binari da 0 a 2^n meno 1 (oppure, come nelle tabelle di questa dispensa, dall'alto verso il basso partendo da tutti vero).

Soddisfacibilità, validità e insoddisfacibilità

DEFINIZIONE

Una formula P è **soddisfacibile** se esiste almeno un'interpretazione I per cui $I(P)$ è vera. È **insoddisfacibile** (o contraddizione) se non ne esiste nessuna, cioè se è falsa in tutte le interpretazioni. È una **tautologia** (o formula **valida**) se è vera in tutte le interpretazioni. Una formula soddisfacibile ma non valida si dice **contingente**.

Dalla definizione segue subito un fatto utile: **una formula è valida se e solo se la sua negazione è insoddisfacibile**. Infatti P è vera in tutte le interpretazioni esattamente quando $\neg P$ è falsa in tutte. Tre esempi:

p	q	$q \vee \neg p$	$p \wedge (q \vee \neg p)$
V	V	V	V
V	F	F	F
F	V	V	F
F	F	V	F

Tabella 5. La formula $p \wedge (q \vee \neg p)$ è soddisfacibile (basta p e q vere).

p	q	$\neg p \Rightarrow q$	$p \Rightarrow (\neg p \Rightarrow q)$
V	V	V	V
V	F	V	V
F	V	V	V
F	F	F	V

Tabella 6. La formula $p \Rightarrow (\neg p \Rightarrow q)$ è una tautologia: l'ultima colonna è sempre vera.

p	q	$q \vee \neg p$	$\neg q \vee \neg p$	$p \wedge (q \vee \neg p) \wedge (\neg q \vee \neg p)$
V	V	V	F	F
V	F	F	V	F
F	V	V	V	F
F	F	V	V	F

Tabella 7. La formula $p \wedge (q \vee \neg p) \wedge (\neg q \vee \neg p)$ è insoddisfacibile: l'ultima colonna è sempre falsa.

La tabella 6 mostra un fatto curioso: da una premessa falsa si può «dedurre» qualunque cosa. Se p è falsa, $\neg p \Rightarrow q$ è vera qualunque sia q ; se p è vera, $\neg p$ è falsa e l'implicazione interna è ancora vera.

I DUE PRINCIPI FONDAMENTALI

PRINCIPI DELLA LOGICA

Principio del terzo escluso: per ogni proposizione p , la formula $p \vee \neg p$ è una tautologia (una proposizione è vera oppure è falsa, non esiste una terza possibilità).

Principio di non contraddizione: per ogni proposizione p , la formula $p \wedge \neg p$ è insoddisfacibile (una proposizione non può essere insieme vera e falsa).

Verificare se una formula con n variabili è soddisfacibile con la tavola di verità richiede, nel caso peggiore, di esaminare 2^n righe. Il problema della soddisfacibilità (SAT) è uno dei più importanti dell'informatica teorica; ne parleremo nel prossimo capitolo.

Equivalenza logica e leggi fondamentali

DEFINIZIONE: EQUIVALENZA LOGICA

Due formule P e Q sono **logicamente equivalenti**, e si scrive $P \equiv Q$, se in ogni interpretazione delle variabili che compaiono in esse hanno lo stesso valore di verità. Equivale a dire che $P \leftrightarrow Q$ è una tautologia.

ATTENZIONE

L'equivalenza logica non va confusa con l'**equisoddisfacibilità**: due formule sono equisoddisfacibili quando una è soddisfacibile se e solo se lo è l'altra, ma possono avere valori diversi nella stessa interpretazione. Per esempio p e q sono equisoddisfacibili (entrambe soddisfacibili) ma non equivalenti.

Le equivalenze che seguono si dimostrano tutte confrontando le tavole di verità dei due membri, e vanno imparate a memoria perché sono gli attrezzi di base di ogni manipolazione.

LEGGE	EQUIVALENZA
Commutatività	$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$
Associatività	$p \vee (q \vee r) \equiv (p \vee q) \vee r$ $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
Idempotenza	$p \vee p \equiv p$ $p \wedge p \equiv p$
Doppia negazione	$\neg(\neg p) \equiv p$
Distributività	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
De Morgan	$\neg(p \vee q) \equiv \neg p \wedge \neg q$ $\neg(p \wedge q) \equiv \neg p \vee \neg q$
Assorbimento	$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$
Eliminazione di $\Rightarrow$	$p \Rightarrow q \equiv \neg p \vee q$
Eliminazione di $\Leftrightarrow$	$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$
Contrapposizione	$p \Rightarrow q \equiv \neg q \Rightarrow \neg p$
Negazione di $\Rightarrow$	$\neg(p \Rightarrow q) \equiv p \wedge \neg q$
Costanti	$p \wedge V \equiv p$ $p \vee F \equiv p$ $p \wedge F \equiv F$ $p \vee V \equiv V$

Tabella 8. Le principali equivalenze logiche (V indica una formula sempre vera, F una sempre falsa).

UN ESEMPIO DI DIMOSTRAZIONE CON LA TAVOLA DI VERITÀ

Dimostriamo la prima legge di De Morgan, $\neg(p \wedge q) \equiv \neg p \vee \neg q$. Basta calcolare i due membri in tutte le interpretazioni e osservare che le colonne coincidono.

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
V	V	V	F	F	F	F
V	F	F	V	F	V	V
F	V	F	V	V	F	V
F	F	F	V	V	V	V

Tabella 9. Verifica della legge di De Morgan: le colonne quarta e ultima coincidono.

DIMOSTRARE CON UNA CATENA DI EQUIVALENZE

Quando le variabili sono molte la tavola di verità diventa lunga, ed è più comodo trasformare una formula in un'altra applicando le leggi. Questo è possibile grazie al **principio di sostituzione**: se in una formula si sostituisce una sottoformula con una sua equivalente, la formula ottenuta è equivalente all'originale. Esempio: semplifichiamo $(p \wedge q) \vee (p \wedge \neg q)$.

$$(p \wedge q) \vee (p \wedge \neg q) \equiv p \wedge (q \vee \neg q) \equiv p \wedge V \equiv p$$

Il primo passaggio usa la distributività letta al contrario, il secondo il principio del terzo escluso, il terzo la legge delle costanti.

IMPLICAZIONE: INVERSA, CONTRARIA E CONTRAPPOSTA

Data l'implicazione $p \Rightarrow q$ si chiamano **inversa** la formula $q \Rightarrow p$, **contraria** la formula $\neg p \Rightarrow \neg q$ e **contrapposta** la formula $\neg q \Rightarrow \neg p$. Solo la contrapposta è equivalente all'implicazione originale; inversa e contraria sono equivalenti tra loro ma non all'originale. Confonderle è un errore frequente (si parla di «affermazione del conseguente» e di «negazione dell'antecedente»).

FORMULA	NOME	EQUIVALENTE A $P \Rightarrow Q$?
$p \Rightarrow q$	implicazione	sì
$\neg q \Rightarrow \neg p$	contrapposta	sì
$q \Rightarrow p$	inversa	no
$\neg p \Rightarrow \neg q$	contraria	no

Tabella 10. Implicazione e formule collegate.

Esempio: «se un numero è divisibile per 4 allora è pari» è vera. La contrapposta «se un numero non è pari allora non è divisibile per 4» è vera. L'inversa «se è pari allora è divisibile per 4» è falsa (basta 6).

Conseguenza logica

DEFINIZIONE: CONSEGUENZA LOGICA

Sia Γ un insieme di formule e P una formula. Diciamo che Γ **giustifica** P , o che P è **conseguenza logica** di Γ , e scriviamo $\Gamma \models P$, se ogni interpretazione che rende vere *tutte* le formule di Γ rende vera anche P .

La conseguenza logica è la formalizzazione del ragionamento corretto: se le premesse sono vere, la conclusione non può essere falsa. Attenzione al verso: se P è vera non segue che le formule di Γ siano vere; un ragionamento può avere una conclusione vera anche con premesse false.

ESEMPIO 1: IL MODUS PONENS

Sia $\Gamma = \{p, p \Rightarrow q\}$. Mostriamo che $\Gamma \models q$. Le interpretazioni che rendono vere entrambe le premesse sono quelle in cui p è vera e $p \Rightarrow q$ è vera; ma p vera e q falsa rende falsa l'implicazione, quindi resta solo p e q entrambe vere. La tavola lo conferma:

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Tabella 11. Solo la prima riga rende vere entrambe le premesse p e $p \Rightarrow q$, e in essa anche q è vera.

ESEMPIO 2: LA REGOLA DI RISOLUZIONE

Sia $\Gamma = \{p \vee r, q \vee \neg r\}$. Mostriamo che $\Gamma \models p \vee q$. Se r è vera, la seconda premessa impone che q sia vera; se r è falsa, la prima impone che p sia vera. In entrambi i casi $p \vee q$ è vera.

p	q	r	$p \vee r$	$q \vee \neg r$	$p \vee q$
V	V	V	V	V	V
V	V	F	V	V	V
V	F	V	V	F	V
V	F	F	V	V	V
F	V	V	V	V	V
F	V	F	F	V	V
F	F	V	V	F	F
F	F	F	F	V	F

Tabella 12. Le righe in cui le due premesse sono vere hanno tutte $p \vee q$ vera.

DA RICORDARE

Per formule in numero finito, $\Gamma = \{y_1, \dots, y_n\} \models P$ se e solo se la formula $(y_1 \wedge \dots \wedge y_n) \Rightarrow P$ è una tautologia, e se e solo se l'insieme $\Gamma \cup \{\neg P\}$ è insoddisfacibile. Il secondo criterio è alla base degli algoritmi automatici di dimostrazione (dimostrazione per assurdo).

Le regole di inferenza più usate sono casi particolari di conseguenza logica, tutte verificabili con una tavola di verità:

REGOLA	PREMESSE	CONCLUSIONE
Modus ponens	$p, p \Rightarrow q$	q
Modus tollens	$\neg q, p \Rightarrow q$	$\neg p$
Sillogismo ipotetico	$p \Rightarrow q, q \Rightarrow r$	$p \Rightarrow r$
Sillogismo disgiuntivo	$p \vee q, \neg p$	q
Risoluzione	$p \vee r, q \vee \neg r$	$p \vee q$
Ex falso quodlibet	$p, \neg p$	qualunque formula q

Tabella 13. Regole di inferenza valide.

Esercizi svolti sulle tavole di verità

Costruire la tavola di verità di una formula con quattro variabili richiede 16 righe. Il modo più rapido è spezzare la formula in sottoformule, calcolare una colonna per ciascuna e poi combinarle. Svolgiamo il primo caso per esteso.

ESERCIZIO 1: $P \wedge Q \wedge (R \vee S)$

p	q	r	s	$r \vee s$	$p \wedge q \wedge (r \vee s)$
V	V	V	V	V	V
V	V	V	F	V	V
V	V	F	V	V	V
V	V	F	F	F	F
V	F	V	V	V	F
V	F	V	F	V	F
V	F	F	V	V	F
V	F	F	F	F	F
F	V	V	V	V	F
F	V	V	F	V	F
F	V	F	V	V	F
F	V	F	F	F	F
F	F	V	V	V	F
F	F	V	F	V	F
F	F	F	V	V	F
F	F	F	F	F	F

Tabella 14. Tavola di verità di $p \wedge q \wedge (r \vee s)$: vera in 3 righe su 16.

La formula è una congiunzione: è vera solo se lo sono tutti i fattori. Servono p e q vere e almeno una tra r e s vera, cioè 3 interpretazioni su 16.

GLI ALTRI TRE ESERCIZI

Per gli altri esercizi non serve compilare tutta la tabella: basta ragionare sui fattori e contare le interpretazioni che rendono vera la formula.

- $p \vee q \vee (r \wedge s)$. È falsa solo quando p e q sono false e $r \wedge s$ è falsa: sono 3 interpretazioni (le coppie (r, s) diverse da (V, V)). È quindi vera in 16 meno $3 = 13$ righe.
- $p \wedge (q \vee (s \wedge (\neg p \vee \neg q)))$. Quando p è vera la sottoformula $(\neg p \vee \neg q)$ equivale a $\neg q$, e $q \vee (s \wedge \neg q)$ equivale a $q \vee s$. La formula equivale quindi a $p \wedge (q \vee s)$, vera con p vera, almeno una tra q e s vera e r qualunque: $3 \cdot 2 = 6$ interpretazioni su 16 .
- $((p \vee \neg q \vee r) \wedge s) \vee t$ (cinque variabili, 32 righe). Se t è vera la formula è vera: 16 interpretazioni. Se t è falsa serve che s sia vera e che $p \vee \neg q \vee r$ sia vera; quest'ultima è falsa solo per p falsa, q vera e r falsa, quindi vale in 7 delle 8 scelte di (p, q, r) . La formula è dunque vera in $16 + 7 = 23$ righe su 32.

Con lo stesso metodo si dimostrano per esercizio le leggi di assorbimento e di distributività: basta una tavola con tre variabili (8 righe).

DA RICORDARE

Una tavola di verità è un algoritmo di decisione corretto ma costoso: richiede 2^n righe. Per questo, appena le variabili sono più di quattro o cinque, si preferisce trasformare le formule con le leggi di equivalenza e con le forme normali del prossimo capitolo.

Forme normali, predicati e quantificatori

Come ridurre ogni formula a una forma standard (CNF e DNF), perché il problema SAT è difficile, e come la logica si estende ai predicati con i quantificatori.

Forme normali

Nelle applicazioni informatiche le formule proposizionali vengono quasi sempre trasformate in una **forma normale**, cioè in una struttura standard su cui gli algoritmi lavorano in modo uniforme. Le due forme normali fondamentali usano gli stessi mattoni.

DEFINIZIONE: LETTERALI, CLAUSOLE E TERMINI

Un **letterale** è una variabile proposizionale (p) oppure la sua negazione ($\neg p$). Una **clausola** è una disgiunzione di letterali, per esempio $p \vee \neg r \vee s$. Un **termine** (o congiunto) è una congiunzione di letterali, per esempio $p \wedge \neg r \wedge s$.

DEFINIZIONE: CNF E DNF

Una formula è in **forma normale congiuntiva** (CNF) se è una congiunzione di clausole, per esempio $(p \vee q) \wedge (\neg p \vee \neg r \vee s)$. È in **forma normale disgiuntiva** (DNF) se è una disgiunzione di termini, per esempio $(p \wedge q) \vee (\neg p \wedge \neg r \wedge s)$.

Una singola clausola è una CNF (con una sola clausola) e anche una DNF (con tanti termini formati da un solo letterale); lo stesso vale per un termine. Una CNF è vera quando *ogni* clausola è soddisfatta; una DNF è vera quando *almeno un* termine è soddisfatto. Questo fa sì che le due forme siano comode per scopi diversi: la DNF rende evidente come soddisfare la formula, la CNF rende evidente come falsificarla (basta falsificare una clausola).

L'algoritmo di trasformazione

Ogni formula proposizionale è equivalente a una formula in CNF e a una formula in DNF, e queste si ottengono con un procedimento algoritmico in quattro fasi, che si applica ripetutamente le equivalenze del capitolo precedente.

ALGORITMO DI TRASFORMAZIONE IN FORMA NORMALE

Fase 1. Eliminare le coimplicazioni sostituendo $p \Leftrightarrow q$ con $(p \Rightarrow q) \wedge (q \Rightarrow p)$.

Fase 2. Eliminare le implicazioni sostituendo $p \Rightarrow q$ con $\neg p \vee q$.

Fase 3. Spingere le negazioni fino alle variabili con le leggi di De Morgan, eliminando le doppie negazioni.

Fase 4a (per la CNF). Distribuire $\vee$ su $\wedge$, cioè $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$, ed eliminare le clausole tautologiche (quelle che contengono p e $\neg p$) e le ripetizioni.

Fase 4b (per la DNF). Distribuire $\wedge$ su $\vee$, cioè $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$, ed eliminare i termini contraddittori (quelli che contengono p e $\neg p$) e le ripetizioni.

ESEMPIO SULLA FASE 3

La negazione $\neg(\neg p \vee \neg r \vee s)$ diventa, con De Morgan e la doppia negazione, $p \wedge r \wedge \neg s$.

ESEMPIO: DA DNF A CNF

Trasformiamo in CNF la formula in DNF $(p \wedge q) \vee (\neg p \wedge \neg r \wedge s)$. Distribuendo la disgiunzione sulla prima congiunzione, poi sulla seconda:

$$\begin{aligned} & (p \vee (\neg p \wedge \neg r \wedge s)) \wedge (q \vee (\neg p \wedge \neg r \wedge s)) \\ \equiv & (p \vee \neg p) \wedge (p \vee \neg r) \wedge (p \vee s) \wedge (q \vee \neg p) \wedge (q \vee \neg r) \wedge (q \vee s) \end{aligned}$$

La prima clausola, $p \vee \neg p$, è una tautologia e può essere eliminata, perché è l'elemento neutro della congiunzione. Resta la CNF finale:

$$(p \vee \neg r) \wedge (p \vee s) \wedge (q \vee \neg p) \wedge (q \vee \neg r) \wedge (q \vee s)$$

ESEMPIO: DA CNF A DNF

Trasformiamo in DNF la CNF $(p \vee q) \wedge (\neg p \vee \neg r)$. Distribuendo la congiunzione:

$$(p \wedge \neg p) \vee (p \wedge \neg r) \vee (q \wedge \neg p) \vee (q \wedge \neg r)$$

Il primo termine è contraddittorio ($p \wedge \neg p$ è sempre falso) e viene eliminato:

$$(p \wedge \neg r) \vee (q \wedge \neg p) \vee (q \wedge \neg r)$$

In entrambi i casi la correttezza si verifica con le tavole di verità: le due formule hanno la stessa colonna finale su tutte le interpretazioni (16 righe nel primo caso, 8 nel secondo).

ESEMPIO COMPLETO: $P \Rightarrow (Q \wedge (R \vee S))$

Eliminiamo l'implicazione: $\neg p \vee (q \wedge (r \vee s))$. Questa formula è già in una forma «mista»; ora la portiamo nelle due forme normali.

- **CNF.** Distribuiamo $\vee$ su $\wedge$: $(\neg p \vee q) \wedge (\neg p \vee r \vee s)$.
- **DNF.** Distribuiamo $\wedge$ su $\vee$ dentro la parentesi: $\neg p \vee (q \wedge r) \vee (q \wedge s)$.

Per verificare, osserviamo che se p è falsa la formula originale è vera e anche le due forme normali lo sono (contengono $\neg p$ in ogni clausola della CNF e come termine della DNF). Basta quindi controllare i soli 8 casi con p vera.

q	r	s	$p \Rightarrow (q \wedge (r \vee s))$	CNF: $(\neg p \vee q) \wedge (\neg p \vee r \vee s)$	DNF: $\neg p \vee (q \wedge r) \vee (q \wedge s)$
V	V	V	V	V	V
V	V	F	V	V	V
V	F	V	V	V	V
V	F	F	F	F	F
F	V	V	F	F	F
F	V	F	F	F	F
F	F	V	F	F	F
F	F	F	F	F	F

Tabella 1. Con p vera le tre formule coincidono su tutte e 8 le interpretazioni di q, r, s .

Forme normali canoniche da una tavola di verità

Esiste anche un metodo meccanico, che non richiede alcuna manipolazione algebrica, per scrivere una forma normale a partire dalla tavola di verità di una formula (o di una qualsiasi funzione booleana).

- **DNF canonica.** Per ogni riga in cui la formula è *vera* si scrive il termine che è vero solo in quella riga (con ogni variabile, negata se vale falso nella riga); la DNF è la disgiunzione di questi termini.
- **CNF canonica.** Per ogni riga in cui la formula è *falsa* si scrive la clausola che è falsa solo in quella riga (con ogni variabile, negata se vale vero nella riga); la CNF è la congiunzione di queste clausole.

Esempio: la funzione di **maggioranza** di tre variabili, vera quando almeno due delle tre sono vere. È vera nelle righe (V, V, V), (V, V, F), (V, F, V), (F, V, V) e falsa nelle altre quattro.

<i>p</i>	<i>q</i>	<i>r</i>	magg.(<i>p</i> , <i>q</i> , <i>r</i>)
V	V	V	V
V	V	F	V
V	F	V	V
V	F	F	F
F	V	V	V
F	V	F	F
F	F	V	F
F	F	F	F

Tabella 2. Funzione di maggioranza.

La DNF canonica ha quattro termini; semplificandola (i termini che differiscono in una sola variabile si fondono) si ottiene la forma compatta con tre termini:

$$(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \equiv (p \wedge q) \vee (p \wedge r) \vee (q \wedge r)$$

La CNF canonica, letta dalle quattro righe false, è $(p \vee q \vee r) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee q \vee r)$, che si semplifica in $(p \vee q) \wedge (p \vee r) \wedge (q \vee r)$.

DA RICORDARE

Ogni funzione booleana è esprimibile con $\neg$, $\wedge$ e $\vee$ (si dice che questi connettivi sono **funzionalmente completi**): la DNF canonica ne è la dimostrazione costruttiva. Bastano anche solo $\neg$ e $\wedge$, oppure solo il connettivo NAND ($p \text{ NAND } q = \neg(p \wedge q)$), che è la ragione per cui i circuiti digitali si possono costruire con un solo tipo di porta.

Esercizi svolti sulle forme normali

Trasformare le seguenti formule in CNF e in DNF. Le soluzioni sono state controllate confrontando le colonne finali delle tavole di verità.

ESERCIZIO 1: $\neg(P \Rightarrow (Q \wedge (R \vee S)))$

La negazione di un'implicazione è $\neg(p \Rightarrow A) \equiv p \wedge \neg A$. Quindi la formula equivale a $p \wedge \neg(q \wedge (r \vee s))$, cioè, con De Morgan, a $p \wedge (\neg q \vee (\neg r \wedge \neg s))$.

- **CNF:** $p \wedge (\neg q \vee \neg r) \wedge (\neg q \vee \neg s)$.

- **DNF:** $(p \wedge \neg q) \vee (p \wedge \neg r \wedge \neg s)$.

ESERCIZIO 2: $(Q \wedge (R \vee S)) \Rightarrow P$

Eliminando l'implicazione si ha $\neg(q \wedge (r \vee s)) \vee p$, cioè $p \vee \neg q \vee (\neg r \wedge \neg s)$. Questa è già una DNF con tre termini (p ; $\neg q$; $\neg r \wedge \neg s$).

- **DNF:** $p \vee \neg q \vee (\neg r \wedge \neg s)$.
- **CNF:** distribuendo $\vee$ su $\wedge$, $(p \vee \neg q \vee \neg r) \wedge (p \vee \neg q \vee \neg s)$.

ESERCIZIO 3: $P \wedge (Q \vee (S \wedge (\neg P \vee \neg Q)))$

Dentro la parentesi più interna, $s \wedge (\neg p \vee \neg q) \equiv (s \wedge \neg p) \vee (s \wedge \neg q)$. Moltiplicando per p il primo termine diventa contraddittorio ($p \wedge \neg p$): rimane $p \wedge (q \vee (s \wedge \neg q))$. Per assorbimento generalizzato $q \vee (s \wedge \neg q) \equiv (q \vee s) \wedge (q \vee \neg q) \equiv q \vee s$.

- **CNF:** $p \wedge (q \vee s)$.
- **DNF:** $(p \wedge q) \vee (p \wedge s)$.

ESERCIZIO 4: $((P \vee \neg Q \vee R) \wedge S) \vee T$

- **DNF:** distribuendo $\wedge$ su $\vee$ nella prima parte, $(p \wedge s) \vee (\neg q \wedge s) \vee (r \wedge s) \vee t$.
- **CNF:** distribuendo $\vee$ su $\wedge$, $(p \vee \neg q \vee r \vee t) \wedge (s \vee t)$.

DA RICORDARE

Una forma normale **non è unica**: la stessa formula ha molte CNF e molte DNF equivalenti, di lunghezze diverse. Se si vuole una forma unica si usa quella canonica, oppure una forma minimale scelta con un criterio (meno termini, meno letterali).

Il problema SAT

Il **problema SAT** chiede: data una formula proposizionale (di solito in CNF), esiste un'assegnazione di valori di verità che la rende vera? Si tratta di un problema di **decisione**, la cui risposta è sì o no, e di uno dei più studiati dell'informatica.

- Per una formula in **DNF** il problema è banale: basta cercare un termine che non contenga una variabile e la sua negazione.
- Per una formula in **CNF** con al più due letterali per clausola (2 SAT) esiste un algoritmo in tempo lineare nella dimensione della formula.
- Già per le CNF con tre letterali per clausola (3 SAT) non si conosce nessun algoritmo polinomiale: SAT e 3 SAT sono i problemi **NP completi** per eccellenza (teorema di Cook e Levin, anni 1971 e 1973).

Perché non basta allora trasformare una CNF in DNF e risolvere il caso banale? Perché la trasformazione può far crescere la formula in modo esponenziale. La CNF $(p_1 \vee q_1) \wedge (p_2 \vee q_2) \wedge \dots \wedge (p_n \vee q_n)$ ha n clausole e $2n$ letterali; la sua DNF ha un termine per ogni scelta di un letterale da ogni clausola, cioè 2^n termini, e nessuno di essi può essere eliminato perché le variabili sono tutte diverse.

Esiste una trasformazione che evita l'esplosione, ma al prezzo di cambiare il significato della formula: introducendo nuove variabili che «danno un nome» alle sottoformule (trasformazione di Tseitin) si ottiene una CNF di dimensione lineare che non è equivalente all'originale, ma **equisoddisfacibile**. È una delle ragioni per cui la distinzione tra equivalenza ed equisoddisfacibilità, vista nel capitolo precedente, è importante.

Predicati e quantificatori

La logica proposizionale non è abbastanza espressiva per parlare di insiemi e di numeri: la frase «ogni numero primo maggiore di 2 è dispari» parla di infiniti oggetti, e non si può scrivere con un numero finito di variabili proposizionali. Per questo si introducono i predicati e i quantificatori, che useremo continuamente in tutta la dispensa (per esempio nella definizione di inclusione fra insiemi).

DEFINIZIONE: PREDICATO

Un **predicato** è un'affermazione che contiene una o più variabili, e che diventa una proposizione (vera o falsa) quando alle variabili si assegnano valori in un certo **dominio**. Per esempio $P(x)$: « x è pari» sui numeri naturali, oppure $R(x, y)$: « $x < y$ ».

Partendo da un predicato si ottiene una proposizione in due modi: sostituendo un valore, oppure **quantificando** la variabile.

QUANTIFICATORE	SIMBOLO	SI LEGGE	SIGNIFICATO
Universale	$\forall$	«per ogni»	$\forall x P(x)$ è vera se $P(x)$ è vera per ogni x del dominio
Esistenziale	$\exists$	«esiste»	$\exists x P(x)$ è vera se esiste almeno un x del dominio per cui $P(x)$ è vera
Esistenza e unicità	$\exists!$	«esiste uno e uno solo»	$\exists! x P(x)$ è vera se esiste un solo x con $P(x)$ vera

Tabella 3. I quantificatori.

NEGAZIONE DEI QUANTIFICATORI

Le leggi di De Morgan si estendono ai quantificatori: negare «per ogni» significa «esiste un controesempio», e negare «esiste» significa «per ogni elemento è falso».

$$\neg \forall x P(x) \equiv \exists x \neg P(x) \quad \neg \exists x P(x) \equiv \forall x \neg P(x)$$

Esempio: la negazione di «tutti gli studenti hanno superato l'esame» è «esiste almeno uno studente che non ha superato l'esame» (non «nessuno ha superato l'esame»: questo è un errore molto comune).

L'ORDINE DEI QUANTIFICATORI

Quantificatori di tipo diverso non si possono scambiare. Sui numeri naturali, $\forall x \exists y (y > x)$ è vera (per ogni numero ne esiste uno più grande), mentre $\exists y \forall x (y > x)$ è falsa (non esiste un numero più grande di tutti, nemmeno di sé stesso). Quantificatori dello stesso tipo si possono scambiare: $\forall x \forall y$ equivale a $\forall y \forall x$, e lo stesso per $\exists$.

IL DOMINIO VUOTO

Se il dominio è vuoto, ogni affermazione universale è vera (non c'è alcun elemento che possa smentirla) e ogni affermazione esistenziale è falsa. Questa convenzione è la stessa «verità per vacuità» dell'implicazione con antecedente falso, e spiega perché l'insieme vuoto è sottoinsieme di ogni insieme.

TRADURRE DEFINIZIONI IN SIMBOLI

La capacità di scrivere e di negare correttamente una definizione quantificata è essenziale per fare dimostrazioni. Due esempi che useremo subito:

ENUNCIATO	FORMULA	NEGAZIONE
A è sottoinsieme di B	$\forall x (x \in A \Rightarrow x \in B)$	$\exists x (x \in A \wedge x \notin B)$
A e B sono uguali	$\forall x (x \in A \Leftrightarrow x \in B)$	$\exists x$ appartenente a uno solo dei due insiemi
f è iniettiva	$\forall x \forall y (x \neq y \Rightarrow f(x) \neq f(y))$	$\exists x \exists y (x \neq y \wedge f(x) = f(y))$
a_n tende a L	$\forall \varepsilon > 0 \exists N \forall n > N (a_n - L < \varepsilon)$	$\exists \varepsilon > 0 \forall N \exists n > N (a_n - L \geq \varepsilon)$

Tabella 4. Alcune definizioni scritte con i quantificatori e le loro negazioni.

DA RICORDARE

Per **dimostrare** una proposizione del tipo $\forall x P(x)$ occorre un ragionamento valido per un x generico; per **confutarla** basta un solo **controesempio**. Al contrario, per dimostrare $\exists x P(x)$ basta esibire un esempio, mentre per confutarla occorre dimostrare che $P(x)$ è falsa per ogni x .

Insiemi

Il concetto di insieme, le relazioni di appartenenza e inclusione, le operazioni fondamentali e il metodo per dimostrare uguaglianze fra insiemi.

Il concetto di insieme

La teoria degli insiemi nasce con il matematico tedesco Georg Cantor (nato nel 1845 e morto nel 1918), che dimostrò, tra le altre cose, che gli insiemi infiniti possono avere «grandezze» diverse. In queste pagine seguiamo la linea della cosiddetta **teoria ingenua degli insiemi**: un insieme è una collezione ben definita di oggetti (sinonimi usati in contesti diversi sono aggregato, classe, famiglia). La teoria assiomatica di Zermelo e Fraenkel dà a questo concetto un assetto formalmente rigoroso, ma esula dagli scopi del corso; ne ricorderemo solo alcune idee, perché l'approccio ingenuo, se usato senza cautela, porta a paradossi (ne vedremo uno nel capitolo 6).

APPARTENENZA ED ESTENSIONALITÀ

Un insieme è **univocamente caratterizzato dai suoi elementi**. Se T è un insieme, l'espressione $x \in T$ si legge « x appartiene a T » o « x è un elemento di T »; la negazione si scrive $x \notin T$.

DEFINIZIONE: UGUAGLIANZA TRA INSIEMI (ASSIOMA DI ESTENSIONALITÀ)

Due insiemi A e B sono uguali se hanno gli stessi elementi. In simboli:

$$A = B \Leftrightarrow \forall x (x \in A \Leftrightarrow x \in B).$$

Ne seguono due fatti importanti: in un insieme **l'ordine** in cui si elencano gli elementi non conta e le **ripetizioni** non contano. Perciò $\{1, 2, 3\}$, $\{3, 1, 2\}$ e $\{2, 3, 1, 2, 3\}$ sono lo stesso insieme. (Quando invece le ripetizioni contano si parla di *multinsiemi*, che non tratteremo.)

COME SI DESCRIVE UN INSIEME

Quando possibile si descrive un insieme **elencando** gli elementi tra parentesi graffe, per esempio $\{1, 2, 3\}$. In alternativa lo si descrive mediante una **proprietà** P che caratterizza i suoi elementi:

$$\{x : P(x)\}$$

La proprietà deve essere **ben definita**, cioè per ogni valore di x deve essere decidibile (almeno in linea di principio) se $P(x)$ è vera o falsa. «Essere nato il primo o l'ultimo giorno del mese» è una proprietà ben definita; lo è anche «essere un divisore di $10^{1000} + 1$ », anche se nessuno conosce esplicitamente tutti i divisori di un numero tanto grande. Non è invece ben definita «essere alto», perché non esiste una soglia che separi gli alti dai non alti: $\{x : x \text{ è alto}\}$ non è un insieme.

Due insiemi speciali: il **singolelto** $\{a\}$, formato dal solo elemento a , e l'**insieme vuoto** $\emptyset$, che non ha alcun elemento. L'insieme vuoto è unico: se $\emptyset_1$ e $\emptyset_2$ sono entrambi vuoti, l'enunciato « $x \in \emptyset_1 \Leftrightarrow x \in \emptyset_2$ » è vero per ogni x (entrambi i membri sono falsi), quindi per estensionalità sono uguali.

ATTENZIONE

$\emptyset$, $\{\emptyset\}$ e $\{\emptyset, \{\emptyset\}\}$ sono insiemi diversi: $\emptyset$ non ha elementi, $\{\emptyset\}$ ha un elemento (l'insieme vuoto), $\{\emptyset, \{\emptyset\}\}$ ne ha due. Allo stesso modo l'elemento 1 e il singoletto $\{1\}$ sono oggetti diversi: $1 \in \{1\}$, ma $1 \neq \{1\}$.

CARDINALITÀ

DEFINIZIONE: CARDINALITÀ

Il numero di elementi di un insieme A si chiama **cardinalità** e si indica con $|A|$. Se $|A|$ è un numero naturale, l'insieme è **finito**, altrimenti è **infinito**.

Per esempio $|\emptyset| = 0$, $\{|1, 2, 3|\} = 3$, $\{|a|\} = 1$, mentre l'insieme dei numeri pari ha cardinalità infinita. Più avanti (capitolo 7) preciseremo che cosa significa «contare» in termini di corrispondenze biunivoche.

GLI INSIEMI NUMERICI

SIMBOLO	INSIEME	DESCRIZIONE	STRUTTURA
$\mathbb{N}$	naturali	$\{0, 1, 2, 3, \dots\}$	discreto
$\mathbb{Z}$	interi relativi	$\{\dots, -2, -1, 0, 1, 2, \dots\}$	discreto
$\mathbb{Q}$	razionali	$\{n/m : n, m \in \mathbb{Z} \text{ e } m \neq 0\}$	né discreto né continuo (denso)
$\mathbb{R}$	reali	razionali e irrazionali	continuo
$\mathbb{C}$	complessi	$\{a + bi : a, b \in \mathbb{R}\}$	continuo

Tabella 1. Gli insiemi numerici e le inclusioni $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Un insieme è **discreto** se i suoi elementi si possono ordinare in modo che tra un elemento e il successivo non ce ne siano altri: sono elementi «isolati». Ogni insieme finito, compreso il vuoto, è discreto, come lo sono $\mathbb{N}$ e $\mathbb{Z}$. L'insieme $\mathbb{Q}$, invece, è *denso*: tra due razionali distinti ce n'è sempre un terzo. Lo studio degli insiemi discreti e delle loro strutture è esattamente l'oggetto di questo corso. In questa dispensa $\mathbb{N}$ comprende lo zero.

Inclusione e sottoinsiemi

DEFINIZIONE: INCLUSIONE

A è un **sottoinsieme** di B , e si scrive $A \subseteq B$, se ogni elemento di A è anche elemento di B :

$$A \subseteq B \Leftrightarrow \forall x (x \in A \Rightarrow x \in B).$$

In tal caso B è un **sovrainsieme** di A e si scrive $B \supseteq A$.

Poiché $A \subseteq A$, la relazione di inclusione vale anche quando i due insiemi sono uguali. Se $A \subseteq B$ ma $A \neq B$, cioè esiste almeno un elemento di B che non sta in A , si dice che A è un **sottoinsieme proprio** di B e si scrive $A \subset B$ (alcuni testi usano $\subset$ per l'inclusione in senso lato: noi useremo $\subseteq$ per l'inclusione e $\subset$ solo per quella propria).

Un sottoinsieme di un insieme dato T si specifica elencando gli elementi o, più spesso, con una proprietà: $\{x : x \in T \text{ e } P(x)\}$. Per esempio, se T è l'insieme dei numeri da 1 a 100 e $P(x)$ è « x è multiplo di 10», il sottoinsieme è $\{10, 20, 30, 40, 50, 60, 70, 80, 90, 100\}$.

DA RICORDARE

Valgono sempre: $\emptyset \subseteq A$ per ogni insieme A (l'implicazione « $x \in \emptyset \Rightarrow x \in A$ » è vera perché l'antecedente è falso); $A \subseteq A$ (riflessività); se $A \subseteq B$ e $B \subseteq C$ allora $A \subseteq C$ (transitività); se $A \subseteq B$ e $B \subseteq A$ allora $A = B$ (antisimmetria, che è la base di quasi tutte le dimostrazioni di uguaglianza).

Non vanno confuse appartenenza e inclusione. Sia $S = \{1, 2, \{1\}\}$: allora $1 \in S$ e $\{1\} \in S$ (due elementi di S), ma anche $\{1\} \subseteq S$ (perché $1 \in S$) e $\{\{1\}\} \subseteq S$ (perché $\{1\} \in S$); invece $\{2\} \in S$ è falso, mentre $\{2\} \subseteq S$ è vero.

Le operazioni tra insiemi

Le operazioni fondamentali tra insiemi, a cominciare da unione e intersezione, sono state formalizzate alla fine dell'Ottocento dal matematico e logico piemontese Giuseppe Peano (nato nel 1858 e morto nel 1932), che introdusse i simboli $\cup$, $\cap$ e $\in$. Dato un insieme universo U di cui tutti gli insiemi considerati sono sottoinsiemi, le operazioni sono le seguenti. Notare la corrispondenza con i connettivi logici: ogni operazione insiemistica è la traduzione di un connettivo applicato all'appartenenza.

OPERAZIONE	NOTAZIONE	DEFINIZIONE	CONNETTIVO
Unione	$A \cup B$	$\{x : x \in A \vee x \in B\}$	$\vee$
Intersezione	$A \cap B$	$\{x : x \in A \wedge x \in B\}$	$\wedge$
Differenza	$A \setminus B$	$\{x : x \in A \wedge x \notin B\}$	$\wedge$ con $\neg$
Complemento	A^C (anche A con un tratto sopra)	$U \setminus A = \{x \in U : x \notin A\}$	$\neg$
Differenza simmetrica	$A \Delta B$	$(A \setminus B) \cup (B \setminus A)$	$\oplus$

Tabella 2. Le operazioni fondamentali e il connettivo corrispondente.

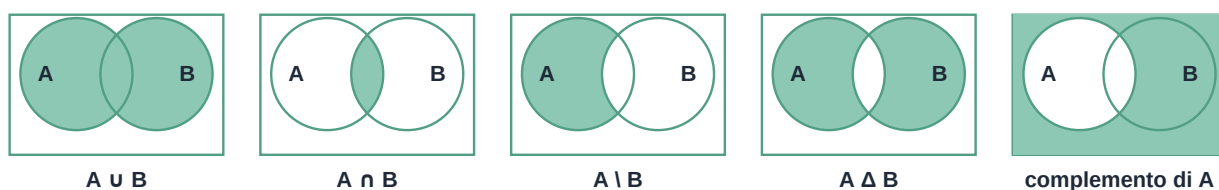


Figura 1. Le operazioni tra due insiemi: la zona colorata è il risultato (nel rettangolo, l'universo U).

UNIONE E INTERSEZIONE

L'**unione** $A \cup B$ contiene gli elementi che appartengono ad almeno uno dei due insiemi; l'**intersezione** $A \cap B$ quelli che appartengono a entrambi. Con $A = \{1, 2, 3\}$ e $B = \{3, 4, 5\}$: $A \cup B = \{1, 2, 3, 4, 5\}$ (il 3 compare una volta sola, per la definizione di insieme) e $A \cap B = \{3\}$. Due insiemi si dicono **disgiunti** se la loro intersezione è vuota. Unione e intersezione sono commutative e associative.

DIFFERENZA E COMPLEMENTO

La **differenza** $A \setminus B$ contiene gli elementi di A che non stanno in B : con gli insiemi di sopra, $A \setminus B = \{1, 2\}$ e $B \setminus A = \{4, 5\}$. La differenza non è commutativa. Il **complemento** di A rispetto all'universo U è $A^C = U \setminus A$; per esempio, con $U = \{1, 2, \dots, 10\}$ e $A = \{1, 2, 3\}$, si ha $A^C = \{4, 5, \dots, 10\}$. Dalle definizioni segue $A \setminus B = A \cap B^C$.

DIFFERENZA SIMMETRICA

La **differenza simmetrica** $A \Delta B = (A \setminus B) \cup (B \setminus A)$ contiene gli elementi che appartengono a uno solo dei due insiemi. Con gli insiemi di sopra, $A \Delta B = \{1, 2, 4, 5\}$: l'elemento 3, presente in entrambi, è tolto dall'unione. Vale anche $A \Delta B = (A \cup B) \setminus (A \cap B)$ (lo dimostreremo tra poco). La differenza simmetrica è commutativa e associativa, ed è l'operazione corrispondente al connettivo $\oplus$: $x \in A \Delta B$ se e solo se $x \in A \oplus x \in B$.

Le proprietà delle operazioni

Le proprietà seguenti si ricavano da quelle dei connettivi logici (capitolo 1), applicate alla relazione di appartenenza. Valgono per qualsiasi A, B, C sottoinsiemi di U .

PROPRIETÀ	PER L'UNIONE	PER L'INTERSEZIONE
Commutativa	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associativa	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
Idempotenza	$A \cup A = A$	$A \cap A = A$
Distributiva	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Assorbimento	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Elemento neutro	$A \cup \emptyset = A$	$A \cap U = A$
Elemento assorbente	$A \cup U = U$	$A \cap \emptyset = \emptyset$
Complemento	$A \cup A^C = U$	$A \cap A^C = \emptyset$
De Morgan	$(A \cap B)^C = A^C \cup B^C$	$(A \cup B)^C = A^C \cap B^C$

Tabella 3. Le proprietà formali delle operazioni insiemistiche. Inoltre il complemento del complemento di A è A .

FORMULE PER LE CARDINALITÀ

Per insiemi finiti si ottengono formule che permettono di contare senza elencare:

QUANTITÀ	FORMULA
Unione	$ A \cup B = A + B - A \cap B $ (se disgiunti: $ A + B $)
Differenza	$ A \setminus B = A - A \cap B $
Complemento	$ A^C = U - A $
Differenza simmetrica	$ A \Delta B = A + B - 2 A \cap B $
Unione di tre insiemi	$ A \cup B \cup C = A + B + C - A \cap B - A \cap C - B \cap C + A \cap B \cap C $

Tabella 4. Cardinalità delle operazioni (la formula per tre insiemi è il caso base del principio di inclusione ed esclusione, capitolo 18).

La prima formula si spiega così: sommando $|A|$ e $|B|$ gli elementi dell'intersezione vengono contati due volte, quindi si sottrae una volta $|A \cap B|$. La quarta segue dalla definizione: $|A \Delta B| = |A \setminus B| + |B \setminus A| = (|A| - |A \cap B|) + (|B| - |A \cap B|)$.

Esempio. In una classe di 40 studenti, 25 seguono il corso di inglese (A), 18 quello di spagnolo (B) e 7 entrambi. Gli studenti che seguono almeno un corso sono $25 + 18 - 7 = 36$; quelli che non ne seguono nessuno sono $40 - 36 = 4$; quelli che seguono un solo corso sono $|A \Delta B| = 25 + 18 - 14 = 29$.

I DIAGRAMMI DI VENN

I diagrammi di Venn, dal nome del matematico inglese John Venn (nato nel 1834 e morto nel 1923), rappresentano gli insiemi come regioni del piano. Per tre insiemi A , B , C il diagramma è composto da **otto regioni**, corrispondenti ai modi di appartenere o non appartenere a ciascun insieme. In generale il diagramma di n insiemi ha 2^n regioni (alcune possono essere vuote per gli insiemi dati).

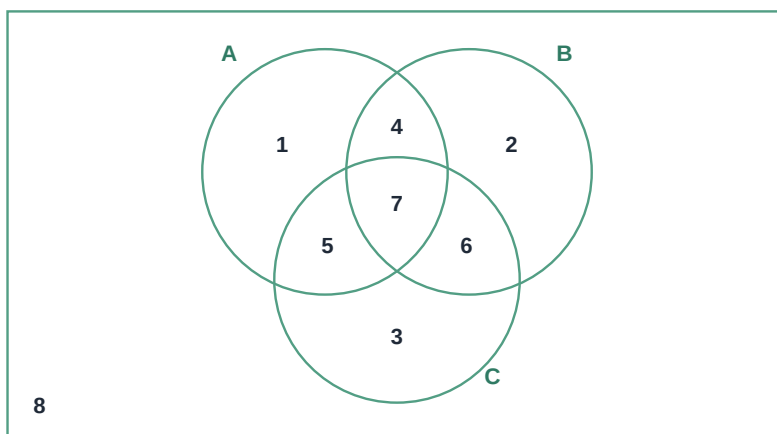


Figura 2. Le otto regioni del diagramma di Venn di tre insiemi (la regione 8 è l'esterno).

REGIONE	DESCRIZIONE	REGIONE	DESCRIZIONE
1	$A \setminus (B \cup C)$	5	$(A \cap C) \setminus B$
2	$B \setminus (A \cup C)$	6	$(B \cap C) \setminus A$
3	$C \setminus (A \cup B)$	7	$A \cap B \cap C$
4	$(A \cap B) \setminus C$	8	né in A, né in B, né in C

Tabella 5. Descrizione delle otto regioni.

Come si dimostrano le uguaglianze fra insiemi

Quasi tutte le dimostrazioni di questo capitolo sono di uno di tre tipi: dimostrare che $A \subseteq B$, che $A = B$, oppure che $A = \emptyset$.

- Per dimostrare $A \subseteq B$ si prende un elemento *generico* $x \in A$ e si dimostra che $x \in B$.
- Per dimostrare $A = B$ si usa l'estensionalità: si dimostra $A \subseteq B$ e $B \subseteq A$ (**doppia inclusione**), oppure si dimostra direttamente una catena di equivalenze « $x \in A \Leftrightarrow \dots \Leftrightarrow x \in B$ ».
- Per dimostrare $A = \emptyset$ si mostra che l'ipotesi $x \in A$ porta a una contraddizione.

ESEMPIO CON LA DOPPIA INCLUSIONE

Dimostriamo che $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$, cioè le due descrizioni della differenza simmetrica coincidono.

Prima inclusione ($\subseteq$). Sia $x \in (A \setminus B) \cup (B \setminus A)$. Ci sono due casi. Se $x \in A \setminus B$, allora $x \in A$ e $x \notin B$: da $x \in A$ segue $x \in A \cup B$, e da $x \notin B$ segue $x \notin A \cap B$; quindi $x \in (A \cup B) \setminus (A \cap B)$. Se $x \in B \setminus A$, il ragionamento è analogo a parti scambiate.

Seconda inclusione ($\supseteq$). Sia $x \in (A \cup B) \setminus (A \cap B)$: quindi x è in A o in B ma non in entrambi. Se $x \in A$, allora $x \notin B$ e dunque $x \in A \setminus B$; se $x \in B$, allora $x \notin A$ e $x \in B \setminus A$. In entrambi i casi $x \in (A \setminus B) \cup (B \setminus A)$. Le due inclusioni provano l'uguaglianza. ■

IL METODO DELLE EQUIVALENZE LOGICHE

Una strada più rapida traduce ogni appartenenza in una variabile proposizionale: si pone $a = \langle x \in A \rangle$, $b = \langle x \in B \rangle$, $c = \langle x \in C \rangle$, e l'uguaglianza fra insiemi diventa un'equivalenza logica fra formule in a, b, c , che si verifica con le leggi del capitolo 1. Per esempio, per $(A \setminus B) \cup (C \setminus B) = (A \cup C) \setminus B$ si ha:

$$(a \wedge \neg b) \vee (c \wedge \neg b) \equiv (a \vee c) \wedge \neg b$$

che è la distributività della congiunzione sulla disgiunzione letta a rovescio. Il metodo funziona perché ogni uguaglianza tra insiemi costruiti con $\cup$, $\cap$, $\setminus$ e complemento è vera se e solo se lo è l'equivalenza logica corrispondente.

ESERCIZI SVOLTI

Con il metodo delle equivalenze, ponendo a , b , c come sopra, si dimostrano le dieci uguaglianze seguenti.

UGUAGLIANZA	DIMOSTRAZIONE (FORMULE SU A, B, C)
$(A \setminus B) \cup (C \setminus B) = (A \cup C) \setminus B$	$(a \wedge \neg b) \vee (c \wedge \neg b) \equiv (a \vee c) \wedge \neg b$ (distributività)
$(A \setminus B) \cap (C \setminus B) = (A \cap C) \setminus B$	$(a \wedge \neg b) \wedge (c \wedge \neg b) \equiv a \wedge c \wedge \neg b$ (idempotenza di $\neg b$)
$(A \setminus B) \setminus C = A \setminus (B \cup C)$	$(a \wedge \neg b) \wedge \neg c \equiv a \wedge \neg(b \vee c)$ (De Morgan)
$A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap B \cap C)$	$a \wedge \neg(b \wedge \neg c) \equiv a \wedge (\neg b \vee c) \equiv (a \wedge \neg b) \vee (a \wedge c) \equiv (a \wedge \neg b) \vee (a \wedge b \wedge c)$, perché la parte $a \wedge c \wedge \neg b$ è già contenuta in $a \wedge \neg b$
$(A \setminus C) \cap (B \setminus C) \cap (A \setminus B) = \emptyset$	contiene $b \wedge \neg b$ (da $B \setminus C$ si ha b , da $A \setminus B$ si ha $\neg b$): contraddizione
$(A \cap B)^C = A^C \cup B^C$	$\neg(a \wedge b) \equiv \neg a \vee \neg b$ (De Morgan)
$(A \cup B)^C = A^C \cap B^C$	$\neg(a \vee b) \equiv \neg a \wedge \neg b$ (De Morgan)
$A \Delta (B \Delta C) = (A \Delta B) \Delta C$	$a \oplus (b \oplus c) \equiv (a \oplus b) \oplus c$: entrambe sono vere quando il numero di variabili vere è dispari
$(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$	$(a \wedge \neg b) \vee (b \wedge \neg a) \equiv (a \vee b) \wedge \neg(a \wedge b)$ (esattamente una delle due è vera)
$(A \cup B) \setminus (A \Delta B) = A \cap B$	$(a \vee b) \wedge \neg(a \oplus b) \equiv (a \vee b) \wedge (a \leftrightarrow b) \equiv a \wedge b$

Tabella 6. Dieci uguaglianze tra insiemi e la verifica logica corrispondente.

DA RICORDARE

Il metodo delle equivalenze logiche è comodo, ma la doppia inclusione resta il metodo di base, perché si applica anche a insiemi definiti da proprietà più complesse (dove non basta tradurre in connettivi). Per confutare un'uguaglianza basta un controesempio concreto con insiemi piccoli.

Esercizi proposti

Dimostrare, con la doppia inclusione o con le equivalenze logiche, che per ogni insieme A, B, C : $(A \cap B) \cup (A \cap B^C) = A$; $A \cup (B \setminus A) = A \cup B$; $A \subseteq B$ se e solo se $A \cap B = A$ se e solo se $A \cup B = B$; $A \Delta A = \emptyset$ e $A \Delta \emptyset = A$. Trovare un controesempio all'affermazione « $A \setminus (B \setminus C) = (A \setminus B) \setminus C$ ».

Metodi di dimostrazione

Che cosa è una dimostrazione e quali schemi di ragionamento useremo in tutto il corso: dimostrazione diretta, per contrapposizione, per assurdo, per casi, controesempi.

Teoremi, lemmi e congetture

La matematica procede enunciando affermazioni e dimostrandole. Una **dimostrazione** è una successione finita di passaggi, ciascuno giustificato da una definizione, da un assioma o da un risultato già dimostrato, che porta dalle **ipotesi** alla **tesi**. Il vocabolario è il seguente.

TERMINE	SIGNIFICATO
Definizione	Stabilisce il significato di un termine; non si dimostra.
Assioma	Affermazione assunta come vera, punto di partenza della teoria.
Teorema	Affermazione importante, dimostrata.
Proposizione	Affermazione dimostrata, di rilievo minore o più specifica di un teorema.
Lemma	Risultato preparatorio, usato per dimostrare un teorema.
Corollario	Conseguenza immediata di un teorema già dimostrato.
Congettura	Affermazione che si ritiene vera ma di cui non si ha ancora una dimostrazione (o una confutazione).

Tabella 1. Il vocabolario delle dimostrazioni.

La maggior parte dei teoremi ha la forma di un'implicazione *ipotesi* $\Rightarrow$ *tesi*, spesso con quantificatori: «per ogni x , se $P(x)$ allora $Q(x)$ ». Per dimostrarla si lavora su un x **generico**, di cui si sa soltanto che soddisfa P , e si arriva a Q usando solo ciò che è noto. Dimostrare per esempi (anche molti) non dimostra nulla: un esempio non basta per un enunciato universale, mentre un solo controesempio basta per confutarlo.

Dimostrazione diretta

Si parte dall'ipotesi P e, con una catena di implicazioni $P \Rightarrow R_1 \Rightarrow R_2 \Rightarrow \dots \Rightarrow Q$, si arriva alla tesi. È lo schema che abbiamo già usato nel capitolo sugli insiemi per dimostrare $A \subseteq B$: si prende $x \in A$ e si mostra che $x \in B$.

Esempio. *La somma di due numeri pari è pari.* Siano m e n pari: per definizione di numero pari esistono interi a e b tali che $m = 2a$ e $n = 2b$. Allora $m + n = 2a + 2b = 2(a + b)$, che è il doppio di un intero, quindi pari. ■

Dimostrazione per contrapposizione

Poiché $P \Rightarrow Q$ è equivalente alla sua contrapposta $\neg Q \Rightarrow \neg P$, per dimostrare un'implicazione si può dimostrare la contrapposta. Conviene quando la negazione della tesi dà un'ipotesi più utile della tesi stessa.

Esempio. *Se n^2 è pari, allora n è pari.* Dimostriamo la contrapposta: se n non è pari, cioè è dispari, allora n^2 non è pari. Se $n = 2k + 1$, allora $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, che è dispari. ■

Attenzione a non confondere la contrapposta con l'inversa: dimostrare «se n è dispari allora n^2 è dispari» è utile solo perché, in questo caso, è proprio la contrapposta; l'inversa dell'enunciato di partenza sarebbe «se n è pari allora n^2 è pari», una cosa diversa.

Dimostrazione per assurdo

Per dimostrare un enunciato S si **assume che sia falso**, cioè si assume $\neg S$, e se ne deduce una contraddizione, cioè una formula del tipo $R \wedge \neg R$. Poiché da premesse vere non si può dedurre una contraddizione, l'assunzione $\neg S$ era sbagliata, e quindi S è vera. Per un'implicazione $P \Rightarrow Q$ si assume che valga P e che Q sia falsa ($\neg(P \Rightarrow Q) \equiv P \wedge \neg Q$).

Esempio classico. $\sqrt{2}$ non è un numero razionale. Supponiamo per assurdo che $\sqrt{2} = a/b$ con a e b interi positivi **primi tra loro** (frazione ridotta ai minimi termini). Elevando al quadrato, $a^2 = 2b^2$, quindi a^2 è pari e, per il risultato dimostrato sopra, anche a è pari: $a = 2k$. Sostituendo, $4k^2 = 2b^2$, cioè $b^2 = 2k^2$, quindi anche b è pari. Ma allora a e b sono entrambi divisibili per 2, contro l'ipotesi che fossero primi tra loro. L'assunzione era falsa. ■

DA RICORDARE

Nella dimostrazione per assurdo la contraddizione può essere con l'ipotesi, con un fatto già noto o con l'assunzione stessa. Ciò che conta è indicare chiaramente quale assunzione si nega e dove nasce la contraddizione. Lo stesso schema è alla base della prova che i primi sono infiniti (capitolo 13).

Dimostrazione per casi

Se un'ipotesi si può spezzare in casi che si escludono e che coprono tutte le possibilità, basta dimostrare la tesi in ciascun caso. È la regola logica $(P \vee Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow R) \Rightarrow R$.

Esempio. Il quadrato di ogni intero, diviso per 4, dà resto 0 oppure 1. Ogni intero n è pari o dispari. Se $n = 2k$, allora $n^2 = 4k^2$ ha resto 0. Se $n = 2k + 1$, allora $n^2 = 4(k^2 + k) + 1$ ha resto 1. In nessun caso il resto è 2 o 3. ■ Da qui segue, per esempio, che nessun numero della forma $4m + 3$ è somma di due quadrati: la somma di due quadrati ha resto 0, 1 o 2 divisa per 4.

Controesempi

Per confutare un enunciato universale $\forall x P(x)$ basta trovare **un** valore di x per cui $P(x)$ è falsa. Il polinomio di Eulero $n^2 + n + 41$ produce un numero primo per tutti gli n da 0 a 39 (41, 43, 47, 53, ...), e viene da pensare che lo faccia sempre: ma per $n = 40$ si ottiene $1681 = 41^2$, che non è primo. La congettura « $n^2 + n + 41$ è sempre primo» è dunque falsa, e questo esempio mostra quanto siano insidiosi i controlli su pochi casi, anche quaranta.

Esistenza e unicità

Per dimostrare che esiste un oggetto con una certa proprietà si può **costruirlo** (dimostrazione costruttiva) oppure provarne l'esistenza senza costruirlo (non costruttiva). Esempio non costruttivo: *esistono due numeri irrazionali a e b tali che a^b è razionale*. Si consideri $\sqrt{2}^{\sqrt{2}}$. Se è razionale, basta $a = b = \sqrt{2}$. Se è irrazionale, si prenda $a = \sqrt{2}^{\sqrt{2}}$ e $b = \sqrt{2}$: allora $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$, che è razionale. In entrambi i casi la tesi è vera, anche se non sappiamo dire quale dei due casi si verifichi.

Per dimostrare l'**unicità** si suppongono due oggetti con la proprietà e si dimostra che coincidono. Esempio: l'insieme vuoto è unico, come visto nel capitolo precedente.

Il principio di induzione

Per gli enunciati che riguardano tutti i numeri naturali esiste uno schema specifico, il **principio di induzione**: si dimostra il caso base e il passo induttivo. Lo introdurremo, con numerosi esempi, nel capitolo 10, quando parleremo dei numeri interi; qui ne anticipiamo la struttura.

METODO	SCHEMA	QUANDO CONVIENE
Diretta	$P \Rightarrow \dots \Rightarrow Q$	La tesi si ricava dall'ipotesi con passaggi naturali.
Contrapposizione	dimostrare $\neg Q \Rightarrow \neg P$	La negazione della tesi è più maneggevole della tesi.
Assurdo	assumere $\neg S$ e giungere a una contraddizione	Enunciati di impossibilità o di non esistenza.
Per casi	dividere in casi esaustivi	L'ipotesi ammette poche situazioni distinte.
Controesempio	esibire un solo x con $P(x)$ falsa	Per confutare un enunciato universale.
Induzione	caso base e passo induttivo	Enunciati su tutti i numeri naturali.

Tabella 2. Riepilogo dei metodi di dimostrazione.

Errori frequenti

- **Affermare il conseguente.** Da $P \Rightarrow Q$ e Q non si può concludere P (se piove la strada è bagnata; la strada è bagnata, ma potrebbe averla lavata qualcuno).
- **Ragionamento circolare.** Usare nella dimostrazione, anche in modo nascosto, la tesi stessa.
- **Generalizzare da un caso.** Verificare un enunciato su alcuni valori e dichiararlo dimostrato.
- **Dividere per zero** o semplificare un fattore che può annullarsi senza tenerne conto.
- **Non dichiarare cosa è generico.** Una dimostrazione su un x particolare, scelto con una proprietà in più rispetto a quelle ammesse, non vale per tutti.

DA RICORDARE

Una buona dimostrazione scritta ha sempre la stessa struttura: **(1)** si enunciano ipotesi e tesi; **(2)** si dichiara il metodo (diretta, per assurdo, per induzione, ...); **(3)** si svolgono i passaggi giustificando ciascuno; **(4)** si chiude indicando che la tesi è raggiunta, tradizionalmente con il simbolo ■.

Famiglie di insiemi

Insiemi i cui elementi sono a loro volta insiemi: insieme delle parti, unione e intersezione di famiglie, chiusura rispetto alle operazioni e partizioni.

L'insieme delle parti

Un insieme i cui elementi sono insiemi si chiama **famiglia di insiemi**. L'esempio fondamentale è l'insieme delle parti di un insieme T .

DEFINIZIONE: INSIEME DELLE PARTI

L'**insieme delle parti** (o insieme potenza) di T , indicato con $P(T)$ oppure $\text{pow}(T)$, è l'insieme di tutti i sottoinsiemi di T , compresi $\emptyset$ e T stesso.

Per $T = \{1, 2, 3\}$ si ha $P(T) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$: otto elementi, ciascuno dei quali è un insieme. Altri esempi, da controllare con attenzione perché mescolano appartenenza e inclusione:

- $P(\emptyset) = \{\emptyset\}$, un insieme con un elemento (l'insieme vuoto);
- $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$, un insieme con due elementi;
- $P(\{a, \{a, b\}\}) = \{\emptyset, \{a\}, \{\{a, b\}\}, \{a, \{a, b\}\}\}$, perché a e $\{a, b\}$ sono due elementi distinti del tutto indipendenti.

QUANTI SONO I SOTTOINSIEMI

Procedendo per piccoli casi si osserva che ogni volta che si aggiunge un elemento il numero di sottoinsiemi raddoppia: $|P(\emptyset)| = 1$, e poi 2, 4, 8, ... Vale in generale:

TEOREMA

Se T è un insieme finito con n elementi, allora $P(T)$ ha 2^n elementi, cioè $|P(T)| = 2^{|T|}$.

Dimostrazione. Sia $T = \{t_1, \dots, t_n\}$. Un sottoinsieme S di T è individuato dalle n risposte alla domanda « t_i appartiene a S ?», ciascuna sì o no. Associando 1 al sì e 0 al no si ottiene una stringa di n bit, e viceversa ogni stringa di n bit definisce un sottoinsieme. Questa corrispondenza tra sottoinsiemi e stringhe è biunivoca, e le stringhe di n bit sono $2 \cdot 2 \cdot \dots \cdot 2 = 2^n$ (due scelte per ciascuna posizione). ■

La stessa idea dà una struttura dati: se $T = \{0, 1, \dots, n-1\}$, ogni sottoinsieme si rappresenta con un numero binario di n bit, e la rappresentazione dei sottoinsiemi come interi da 0 a 2^n meno 1 è ciò che si usa in programmazione (maschere di bit). Ritroveremo questa dimostrazione per induzione nel capitolo 10.

PROPRIETÀ DELL'INSIEME DELLE PARTI

Tra le proprietà dell'insieme delle parti ce ne sono due che interessano il comportamento rispetto a intersezione e unione.

PROPOSIZIONE

Per ogni coppia di insiemi A e B valgono:

(P1) $P(A \cap B) = P(A) \cap P(B)$;

(P2) $P(A \cup B) \supseteq P(A) \cup P(B)$, e in generale l'inclusione è **stretta**. L'uguaglianza vale se e solo se $A \subseteq B$ oppure $B \subseteq A$.

Dimostrazione di P1. ($\subseteq$) Se $X \in P(A \cap B)$, allora $X \subseteq A \cap B$, quindi $X \subseteq A$ e $X \subseteq B$: dunque $X \in P(A)$ e $X \in P(B)$. ($\supseteq$) Se $X \in P(A) \cap P(B)$, allora $X \subseteq A$ e $X \subseteq B$, quindi $X \subseteq A \cap B$, cioè $X \in P(A \cap B)$. ■

Dimostrazione di P2. Se $X \in P(A) \cup P(B)$, allora $X \subseteq A$ oppure $X \subseteq B$; in entrambi i casi $X \subseteq A \cup B$, quindi $X \in P(A \cup B)$. L'inclusione può essere stretta: con $A = \{1, 2\}$ e $B = \{1, 3\}$, l'insieme $\{2, 3\}$ (e lo stesso $A \cup B = \{1, 2, 3\}$) è sottoinsieme di $A \cup B$ ma non è né sottoinsieme di A né di B . Più in generale, se $A \not\subseteq B$ e $B \not\subseteq A$, scelti $a \in A \setminus B$ e $b \in B \setminus A$, l'insieme $\{a, b\}$ sta in $P(A \cup B)$ ma non in $P(A) \cup P(B)$. Se invece, per esempio, $A \subseteq B$, allora $A \cup B = B$ e $P(A) \subseteq P(B)$, per cui entrambi i membri valgono $P(B)$. ■

Famiglie finite e infinite, unione e intersezione

Una famiglia è **finita** se ha un numero finito di elementi, **infinita** altrimenti. La definizione non dice nulla sulla cardinalità degli insiemi che la compongono: la famiglia $\{P, D\}$ formata dall'insieme dei pari e dall'insieme dei dispari è una famiglia finita (due elementi) di insiemi infiniti. Al contrario la famiglia $\{P_1, P_2, P_3, \dots\}$ con $P_i = \{2^1, \dots, 2^i\}$ è una famiglia infinita di insiemi finiti.

Spesso gli elementi di una famiglia sono numerati da un insieme di **indici** I , e la famiglia si scrive $\{A_i : i \in I\}$. Unione e intersezione, che per due insiemi abbiamo già visto, si estendono a famiglie qualsiasi, anche infinite.

DEFINIZIONE: UNIONE E INTERSEZIONE DI UNA FAMIGLIA

Sia F una famiglia non vuota di insiemi. La **unione** di F è l'insieme degli elementi che appartengono a *qualcuno* degli insiemi di F ; l'**intersezione** è l'insieme degli elementi che appartengono a *tutti* gli insiemi di F :

$$\bigcup_{X \in F} X = \{x : \exists X \in F \text{ con } x \in X\} \quad \bigcap_{X \in F} X = \{x : \forall X \in F \text{ si ha } x \in X\}$$

Esempi. Per $A_n = \{k \in \mathbb{N} : k \geq n\}$, con $n \in \mathbb{N}$, la famiglia è decrescente ($A_0 \supseteq A_1 \supseteq A_2 \supseteq \dots$): l'unione è $A_0 = \mathbb{N}$ e l'intersezione è $\emptyset$ (un numero k non appartiene a A_{k+1}). Per M_n = multipli di n , l'intersezione di M_2 e M_3 sono i multipli di 6.

DA RICORDARE

L'intersezione di una famiglia *vuota* non è definita come insieme senza fissare un universo (sarebbe «l'insieme di tutto»), mentre la sua unione è $\emptyset$. Per questo la definizione richiede una famiglia non vuota. Le leggi di De Morgan valgono anche per famiglie infinite: il complemento dell'unione è l'intersezione dei complementi, e viceversa.

Insiemi chiusi rispetto a un'operazione

Sia U un insieme e sia data un'operazione definita su elementi di U . Si dice che U è **chiuso** rispetto all'operazione se il risultato dell'operazione, applicata a elementi di U , è sempre un elemento di U . Esempi:

- $\mathbb{N}$ è chiuso rispetto alla somma, ma non rispetto alla sottrazione (3 meno 5 non è un numero naturale).
- $\mathbb{Z}$ è chiuso rispetto alla sottrazione, ma non rispetto alla divisione (1 diviso 2 non è intero).
- $X = \{1, 2, 3\}$ non è chiuso rispetto al minimo comune multiplo ($\text{mcm}(2, 3) = 6$ non sta in X), mentre $X = \{1, 2, 3, 6\}$ lo è.

Famiglie chiuse per unione e intersezione

DEFINIZIONE

Una famiglia di insiemi F è **chiusa rispetto all'unione** se per ogni coppia X, Y di insiemi di F anche $X \cup Y$ appartiene a F ; è **chiusa rispetto all'intersezione** se anche $X \cap Y$ appartiene sempre a F .

Esempio: $F = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}\}$ è chiusa rispetto all'unione ($\{1, 2\} \cup \{1, 3\} = \{1, 2, 3\} \in F$ e le altre unioni sono ovvie), ma non rispetto all'intersezione, perché $\{1, 2\} \cap \{1, 3\} = \{1\}$ non appartiene a F .

Fissato un universo U , data una famiglia $F \subseteq P(U)$ si definisce la **famiglia dei complementi** $F^C = \{X^C : X \in F\}$, dove $X^C = U \setminus X$. Evidentemente $(F^C)^C = F$. Le leggi di De Morgan danno un'utile dualità.

TEOREMA (DUALITÀ)

F è chiusa rispetto all'unione se e solo se F^C è chiusa rispetto all'intersezione. Analogamente, F è chiusa rispetto all'intersezione se e solo se F^C lo è rispetto all'unione.

Dimostrazione. Sia F chiusa rispetto all'unione, e siano $X, Y \in F^C$: esistono $A, B \in F$ con $X = A^C$ e $Y = B^C$. Per De Morgan $X \cap Y = A^C \cap B^C = (A \cup B)^C$, e poiché $A \cup B \in F$ si ha $(A \cup B)^C \in F^C$. Quindi F^C è chiusa rispetto all'intersezione. Viceversa, se F^C è chiusa rispetto all'intersezione e $A, B \in F$, allora $A^C, B^C \in F^C$ e $A^C \cap B^C = (A \cup B)^C \in F^C$, cioè $A \cup B \in (F^C)^C = F$. Il secondo enunciato si ottiene applicando il primo a F^C . ■

Una famiglia chiusa contemporaneamente rispetto a unione, intersezione e complemento (e che contiene $\emptyset$ e U) si chiama **algebra di insiemi**: è la struttura su cui si fonda la teoria della probabilità, che incontreremo nel capitolo 19.

La chiusura di una famiglia

DEFINIZIONE: CHIUSURA

Sia F una famiglia finita di sottoinsiemi di U e $*$ un'operazione binaria tra insiemi (per esempio $\cup$ o $\cap$). La **chiusura** di F rispetto a $*$ è la più piccola famiglia $F_* \supseteq F$ che sia chiusa rispetto a $*$.

In concreto, la chiusura contiene gli insiemi di F e tutti quelli che si ottengono applicando l'operazione a due o più insiemi di F . Per unione e intersezione:

$$F_{\cup} = \left\{ \bigcup_{X \in F} X : F \subseteq F, F \neq \emptyset \right\} \quad F_{\cap} = \left\{ \bigcap_{X \in F} X : F \subseteq F, F \neq \emptyset \right\}$$

Esempio. Sia $F = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 4\}\}$, che non è chiusa per l'unione. Le uniche unioni nuove sono $\{1, 2\} \cup \{2, 4\} = \{1, 2, 4\}$ e $\{1, 3\} \cup \{2, 4\} = \{1, 2, 3\} \cup \{2, 4\} = \{1, 2, 3, 4\}$. Dunque la chiusura è

$$F_{\cup} = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{1, 2, 4\}, \{1, 2, 3, 4\}\}$$

La famiglia F' ottenuta aggiungendo anche $\{1, 3, 4\}$ è ancora chiusa rispetto all'unione e contiene F , ma non è la chiusura: la chiusura è la più piccola, e $\{1, 3, 4\}$ non si ottiene come unione di insiemi di F .

UN ALGORITMO PER CALCOLARE LA CHIUSURA

Per calcolare $F_{\cup}$ si può, per definizione, formare le unioni di tutti i 2^m meno 1 sottofamiglie non vuote di F (con $m = |F|$); è un metodo costoso. Un metodo più economico costruisce la chiusura per passi: si parte da F e si aggiungono ripetutamente le unioni di coppie, finché nessuna coppia produce insiemi nuovi. Il processo termina perché i sottoinsiemi di U sono finiti.

```
def chiusura(F, op):
    risultato = {frozenset(X) for X in F}
    cambiato = True
    while cambiato:
        cambiato = False
        for X in list(risultato):
            for Y in list(risultato):
                Z = op(X, Y)          # X | Y per l'unione, X & Y per l'intersezione
                if Z not in risultato:
                    risultato.add(Z)
                    cambiato = True
    return risultato
```

La stessa procedura vale per l'intersezione. Notare che nell'intersezione può comparire $\emptyset$ (due insiemi disgiunti) e che la chiusura rispetto all'unione ha sempre come massimo l'unione di tutti gli insiemi di F .

ESERCIZI SVOLTI

Sia $U = \{1, 2, \dots, 10\}$. Applicando l'algoritmo alle tre famiglie assegnate si ottiene:

FAMIGLIA	CHIUSURA RISPETTO ALL'INTERSEZIONE	CHIUSURA RISPETTO ALL'UNIONE
$F_1 = \{\{1,2,3\}, \{4,5,6\}, \{7,8\}, \{9,10\}, \{1,4,5\}, \{2,6,8\}, \{3,5\}, \{1,10\}\}$	17 insiemi: i dati e, in più, $\emptyset, \{1\}, \{2\}, \{3\}, \{5\}, \{6\}, \{8\}, \{10\}, \{4,5\}$	112 insiemi, il massimo è $\{1, \dots, 10\}$
$F_2 = \{\{1,2\}, \{1,3,4\}, \{4,5,6\}, \{6,7,8\}, \{8,9,10\}, \{5,8,9\}\}$	13 insiemi: i dati e, in più, $\emptyset, \{1\}, \{4\}, \{5\}, \{6\}, \{8\}, \{8,9\}$	51 insiemi, il massimo è $\{1, \dots, 10\}$
$F_3 = \{\{1,2\}, \{2,3,4\}, \{4,5\}, \{5,6\}, \{3,8,9\}, \{6,9\}, \{7,8\}, \{7,10\}\}$	17 insiemi: i dati e, in più, $\emptyset, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}, \{7\}, \{8\}, \{9\}$	135 insiemi, il massimo è $\{1, \dots, 10\}$

Tabella 1. Chiusure delle tre famiglie (calcolate con l'algoritmo; i numeri sono le cardinalità delle chiusure).

Le chiusure rispetto all'unione sono molto più grandi perché già poche unioni mescolano molti elementi: per F_1 le sottofamiglie non vuote sono 255 e producono 112 unioni distinte. Per esempio, in F_1 si ottengono $\{1, 2, 3, 4, 5, 6\} = \{1, 2, 3\} \cup \{4, 5, 6\}$ e $\{1, 3, 4, 5\} = \{1, 4, 5\} \cup \{3, 5\}$. Il fatto che queste famiglie non siano chiuse non è una proprietà negativa, ma l'indicazione che l'operazione fa uscire dalla famiglia.

Partizioni e coperture

DEFINIZIONE: PARTIZIONE

Una famiglia F di sottoinsiemi di U è una **partizione** di U se: **(1)** ogni $X \in F$ è non vuoto; **(2)** l'unione di tutti gli insiemi di F è U ; **(3)** due insiemi distinti di F sono disgiunti. Gli insiemi di F si chiamano **parti**, **classi** o **blocchi**.

Una partizione «copre» U senza sovrapposizioni. Esempio: con $U = \{1, \dots, 12\}$ (i mesi dell'anno), la famiglia $\{\{1, 3, 5, 7, 8, 10, 12\}, \{2\}, \{4, 6, 9, 11\}\}$ è la partizione dei mesi in base alla loro durata: mesi di 31 giorni, mesi con meno di 30 giorni (febbraio) e mesi di 30 giorni. Una famiglia che soddisfa solo la condizione (2) si chiama **copertura**: i blocchi possono sovrapporsi.

Il numero di partizioni di un insieme di n elementi si chiama **numero di Bell**: per $n = 1, 2, 3, 4, 5$ vale 1, 2, 5, 15, 52. Per esempio le cinque partizioni di $\{1, 2, 3\}$ sono $\{\{1,2,3\}\}, \{\{1,2\},\{3\}\}, \{\{1,3\},\{2\}\}, \{\{2,3\},\{1\}\}, \{\{1\},\{2\},\{3\}\}$. Le partizioni sono strettamente legate alle relazioni di equivalenza, tema del capitolo 8.

Prodotto cartesiano e paradossi

Copie ordinate, insieme prodotto e n uple; il paradosso di Russell e il teorema di Cantor come limite dell'idea ingenua di insieme.

Copie ordinate

Nell'insieme $\{x, y\}$ l'ordine non conta; a volte però serve distinguere un *primo* elemento da un *secondo*. Date due entità x e y , non necessariamente distinte, si indica con (x, y) la **coppia ordinata** con primo elemento x e secondo elemento y . Il suo comportamento è catturato da una sola proprietà:

$$(x, y) = (x', y') \text{ se e solo se } x = x' \text{ e } y = y'$$

Perciò $(x, y) \neq (y, x)$ a meno che $x = y$, e la coppia (x, y) è un oggetto diverso dall'insieme $\{x, y\}$. Se si vuole ridurre tutto agli insiemi, si può *definire* (x, y) come l'insieme $\{\{x\}, \{x, y\}\}$ (definizione di Kuratowski), per il quale la proprietà precedente si dimostra, ma nell'uso corrente basta sapere la proprietà.

Il prodotto cartesiano

DEFINIZIONE: INSIEME PRODOTTO

Dati due insiemi A e B , il loro **prodotto cartesiano** $A \times B$ è l'insieme di tutte le coppie ordinate con il primo elemento in A e il secondo in B :

$$A \times B = \{(x, y) : x \in A \text{ e } y \in B\}.$$

Se A e B sono finiti, $|A \times B| = |A| \cdot |B|$: per ogni scelta di x in A ($|A|$ modi) si può scegliere y in B ($|B|$ modi). Se uno dei due insiemi è vuoto il prodotto è vuoto. Il prodotto non è commutativo: $A \times B \neq B \times A$ in generale, anche se hanno la stessa cardinalità.

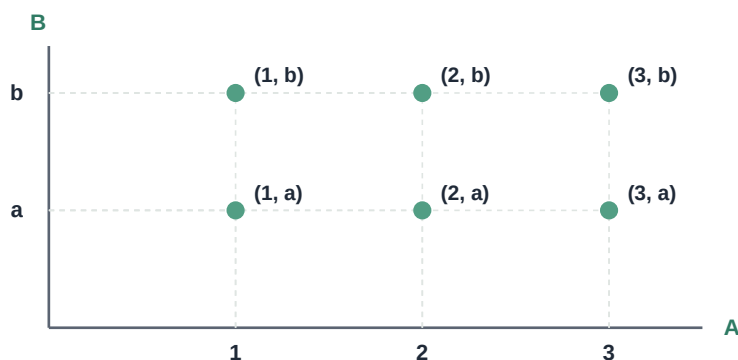


Figura 1. Il prodotto $\{1, 2, 3\} \times \{a, b\}$: sei coppie ordinate, come $|A| \cdot |B| = 3 \cdot 2 = 6$.

Il caso più noto è il **piano cartesiano** $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, i cui punti sono le coppie ordinate di numeri reali. Anche una tabella di un database è, in sostanza, un sottoinsieme di un prodotto: ogni riga è una coppia (o una n upla) i cui elementi appartengono ai domini delle colonne.

PRODOTTI DI PIÙ INSIEMI

La definizione si estende a n insiemi $A_1, \dots, A_n$: il prodotto $A_1 \times \dots \times A_n$ è l'insieme delle **n uple ordinate** $(x_1, \dots, x_n)$ con $x_i \in A_i$ e la sua cardinalità è il prodotto delle cardinalità. Il prodotto di n copie dello stesso insieme si scrive A^n . Per esempio $\mathbb{R}^n$ è l'insieme delle n uple di numeri reali e $\{0, 1\}^n$ l'insieme delle stringhe di n bit, che ha 2^n elementi: questa è la ragione per cui un insieme di n elementi ha 2^n sottoinsiemi.

DA RICORDARE

Per contare le coppie, le terne, le n uple si moltiplicano le cardinalità: $|A_1 \times \dots \times A_n| = |A_1| \cdot \dots \cdot |A_n|$. Questa è la forma più semplice del **principio moltiplicativo** del calcolo combinatorio (capitolo 18).

Il paradosso di Russell

Finora abbiamo usato l'idea intuitiva di insieme come collezione definita da una proprietà. All'inizio del Novecento la speranza di fondare tutta la matematica sulla teoria degli insiemi ricevette un colpo apparentemente mortale dal matematico, filosofo e logico inglese Bertrand Russell (nato nel 1872 e morto nel 1970), che comunicò nel 1902 a Gottlob Frege una scoperta devastante.

In generale un insieme non appartiene a sé stesso (l'insieme dei numeri pari non è un numero pari). Ma si può immaginare qualche insieme che appartiene a sé stesso: l'insieme di tutti gli insiemi con infiniti elementi è infinito, quindi appartiene a sé stesso. Se ogni proprietà potesse definire un insieme, si potrebbe allora formare l'insieme degli insiemi che *non* appartengono a sé stessi:

$$S = \{A : A \text{ è un insieme e } A \notin A\}$$

Domanda: $S \in S$? Se la risposta è sì, allora S soddisfa la proprietà che definisce gli elementi di S , cioè $S \notin S$: contraddizione. Se la risposta è no, cioè $S \notin S$, allora S soddisfa la proprietà e quindi deve appartenere a S : contraddizione. Entrambe le risposte portano a un assurdo.

UNA VERSIONE DIVULGATIVA

In un villaggio il barbiere rade tutti e soli gli uomini che non si radono da sé. Chi rade il barbiere? Se si rade da sé, allora non dovrebbe (perché rade solo chi non si rade da sé); se non si rade da sé, allora dovrebbe radersi. Il barbiere che soddisfa tale regola semplicemente non può esistere: allo stesso modo, l'insieme S non esiste.

COME SI EVITA LA CONTRADDIZIONE

Una via d'uscita consiste nell'imporre che un insieme si possa definire con una proprietà solo come **sottoinsieme di un insieme già noto**. Questo è l'**assioma di separazione** della teoria di Zermelo e Fraenkel: dati un insieme U e una proprietà P , esiste l'insieme $\{x \in U : P(x)\}$. Con questa regola il tentativo di Russell diventa $S = \{A \in U : A \notin A\}$, e il ragionamento di prima, riletto, **dimostra** che S non può appartenere a U . L'«insieme di tutti gli insiemi» non esiste. L'uso quotidiano degli insiemi non ne risente, perché le proprietà definiscono sempre sottoinsiemi di insiemi noti, come $\mathbb{N}$ o $\mathbb{R}$.

Il teorema di Cantor

Il ragionamento del paradosso di Russell ha una versione più precisa, dovuta a Cantor, che mostra che l'insieme delle parti è sempre «più grande» dell'insieme di partenza.

TEOREMA DI CANTOR

Per ogni insieme A non esiste alcuna funzione surgettiva da A in $P(A)$. In particolare, A e $P(A)$ non possono essere messi in corrispondenza biunivoca.

Dimostrazione. Sia $f : A \rightarrow P(A)$ una funzione qualsiasi, e consideriamo l'insieme $D = \{x \in A : x \notin f(x)\}$, formato dagli elementi che non appartengono al sottoinsieme che f associa loro. D è un sottoinsieme di A . Se f fosse surgettiva, esisterebbe $d \in A$ con $f(d) = D$. Ma allora $d \in D$ se e solo se $d \notin f(d) = D$: contraddizione. Dunque f non è surgettiva. ■

Per insiemi finiti il risultato è ovvio ($2^n > n$), ma per gli insiemi infiniti è sorprendente: esiste una gerarchia infinita di «infiniti» sempre più grandi, $\mathbb{N}$, $P(\mathbb{N})$, $P(P(\mathbb{N}))$, ..., e l'insieme dei numeri reali ha la stessa cardinalità di $P(\mathbb{N})$.

Relazioni e funzioni

Relazioni binarie e loro proprietà, funzioni iniettive, surgettive e biettive, e il legame tra funzioni e cardinalità degli insiemi.

Relazioni binarie

DEFINIZIONE: RELAZIONE BINARIA

Una **relazione binaria** da un insieme A a un insieme B è un sottoinsieme $R \subseteq A \times B$. Se $A = B = U$ si parla di relazione su U , cioè $R \subseteq U \times U$. L'insieme delle coppie (x, y) per cui la relazione è verificata si chiama **grafico** della relazione.

Scriveremo indifferentemente $R(x, y)$, $(x, y) \in R$ oppure $x R y$ per dire che x e y sono in relazione. Una relazione è dunque un predicato in due variabili: « x divide y », « $x \leq y$ », « x è figlio di y », « $X \subseteq Y$ » sono tutte relazioni binarie, definite su insiemi diversi.

Esempio. Su $U = \{1, 2, 3, 4, 6\}$ la relazione « x divide y » è l'insieme $\{(1,1), (1,2), (1,3), (1,4), (1,6), (2,2), (2,4), (2,6), (3,3), (3,6), (4,4), (6,6)\}$, un sottoinsieme di $U \times U$ con 12 delle 25 coppie possibili. La **relazione inversa** di R è $R^{-1} = \{(y, x) : (x, y) \in R\}$; l'inversa di «divide» è «è multiplo di».

LE PROPRIETÀ DELLE RELAZIONI

DEFINIZIONE

Sia R una relazione su U . Si dice:

riflessiva se $\forall x \in U$ vale $R(x, x)$;

simmetrica se $\forall x, y$, da $R(x, y)$ segue $R(y, x)$;

antisimmetrica se $\forall x, y$, da $R(x, y)$ e $R(y, x)$ segue $x = y$;

transitiva se $\forall x, y, z$, da $R(x, y)$ e $R(y, z)$ segue $R(x, z)$.

Simmetria e antisimmetria non sono l'una la negazione dell'altra: l'uguaglianza è sia simmetrica sia antisimmetrica, mentre «essere diversi» è simmetrica e non antisimmetrica, e « $\leq$ » è antisimmetrica ma non simmetrica. Le relazioni riflessive, simmetriche e transitive sono le **relazioni di equivalenza** (capitolo 8); quelle riflessive, antisimmetriche e transitive sono le **relazioni d'ordine**.

RELAZIONE	RIFLESSIVA	SIMMETRICA	ANTISIMMETRICA	TRANSITIVA
$x = y$ (uguaglianza)	sì	sì	sì	sì
$x \leq y$ sugli interi	sì	no	sì	sì
$x < y$ sugli interi	no	no	sì	sì
x divide y sui naturali positivi	sì	no	sì	sì
$X \subseteq Y$ tra sottoinsiemi	sì	no	sì	sì
$x \neq y$ (diversi)	no	sì	no	no
X e Y disgiunti	no	sì	no	no

Tabella 1. Proprietà di alcune relazioni. La relazione « $<$ » è antisimmetrica per vacuità: la premessa non si verifica mai.

DA RICORDARE

Per **dimostrare** che una relazione ha una proprietà si ragiona su elementi generici; per **escluderla** basta un controesempio. Nel dubbio, controllare sempre i casi limite: elementi uguali, insieme vuoto, elementi ripetuti.

Funzioni

DEFINIZIONE: FUNZIONE

Una relazione $f \subseteq A \times B$ è una **funzione** (o applicazione) da A (**dominio**) in B (**codominio**) se per ogni $x \in A$ esiste *uno e uno solo* $y \in B$ con $(x, y) \in f$. Si scrive $f : A \rightarrow B$ e l'unico y si indica con $f(x)$, valore di f in x .

In una funzione ogni elemento del dominio ha esattamente *una* freccia in uscita; nel quarto riquadro della figura, la relazione non è una funzione perché 1 ha due immagini e 2 non ne ha nessuna.

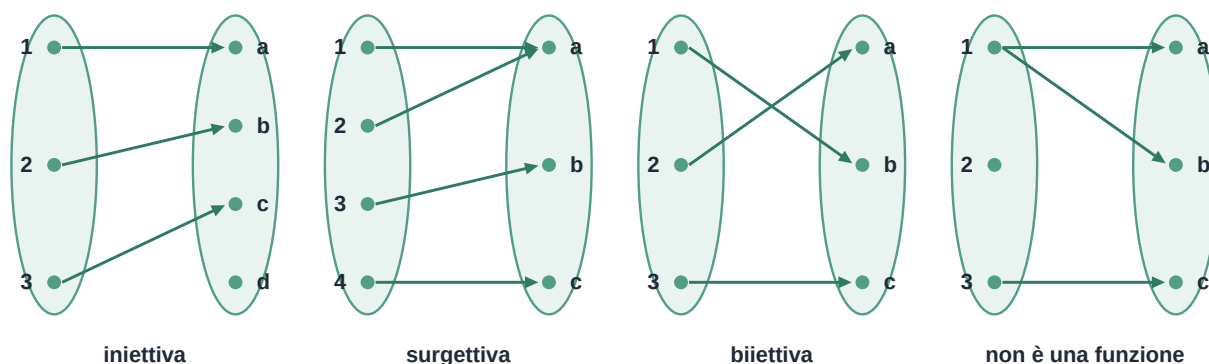


Figura 1. Tre funzioni e una relazione che non è funzione.

Per $X \subseteq A$ si chiama **immagine** di X l'insieme $f(X) = \{y \in B : \exists x \in X \text{ con } f(x) = y\}$; l'insieme $f(A)$ è l'immagine di f . Per $Y \subseteq B$ la **controimmagine** è $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$; attenzione: la controimmagine esiste sempre, anche se la funzione non è invertibile. Una funzione è **costante** se la sua immagine ha un solo elemento.

FUNZIONI PARTICOLARI

- La **funzione identica** $I_A : A \rightarrow A$, $I_A(x) = x$.
- Le **proiezioni canoniche** $A \times B \rightarrow A$, $(x, y) \mapsto x$, e $A \times B \rightarrow B$, $(x, y) \mapsto y$.
- La **funzione successore** $\mathbb{N} \rightarrow \mathbb{N}$, $n \mapsto n + 1$.

INIETTIVE, SURGETTIVE, BIETTIVE

DEFINIZIONE

Una funzione $f : A \rightarrow B$ si dice:

iniettiva se punti distinti hanno immagini distinte: $\forall x, y \in A, x \neq y \Rightarrow f(x) \neq f(y)$ (equivalentemente $f(x) = f(y) \Rightarrow x = y$);

surgettiva se $f(A) = B$, cioè ogni elemento di B ha almeno una controimmagine;

biiettiva (o corrispondenza biunivoca) se è iniettiva e surgettiva: ogni elemento di B ha esattamente una controimmagine.

Esempi: l'identità è biiettiva; la funzione successore è iniettiva ma non surgettiva (0 non è immagine di nessun numero); la funzione $\mathbb{N} \rightarrow \{\text{numeri pari}\}$, $n \mapsto 2n$ è biiettiva. Per la funzione $x \mapsto x^2$ si ha: da $\mathbb{R}$ a $\mathbb{R}$ non è né iniettiva

(1 e meno 1 hanno la stessa immagine) né surgettiva (i negativi non sono immagini); da $\mathbb{R}_{\geq 0}$ a $\mathbb{R}$ è iniettiva; da $\mathbb{R}$ a $\mathbb{R}_{\geq 0}$ è surgettiva; da $\mathbb{R}_{\geq 0}$ a $\mathbb{R}_{\geq 0}$ è biiettiva (con $\mathbb{R}_{\geq 0}$ insieme dei reali non negativi).

COMPOSIZIONE E INVERSA

Date $f: A \rightarrow B$ e $g: B \rightarrow C$, la **composizione** $g \circ f: A \rightarrow C$ è definita da $(g \circ f)(x) = g(f(x))$. La composizione di funzioni iniettive è iniettiva, quella di surgettive è surgettiva, quella di biiettive è biiettiva. Una funzione f è biiettiva se e solo se ammette una **funzione inversa** $f^{-1}: B \rightarrow A$ tale che $f^{-1} \circ f = I_A$ e $f \circ f^{-1} = I_B$.

Funzioni e cardinalità

La nozione di corrispondenza biunivoca è alla base del concetto stesso di numero: **contare** significa stabilire una corrispondenza biunivoca fra gli oggetti da contare e un insieme «campione». Posto $I_n = \{0, 1, \dots, n-1\}$, un insieme X è **finito** con n elementi se esiste una biiezione $X \rightarrow I_n$, e si scrive $|X| = n$; se non esiste alcun n del genere X è infinito.

TEOREMA

Siano A e B insiemi finiti. Se esiste una funzione iniettiva $f: A \rightarrow B$, allora $|A| \leq |B|$. Se esiste una funzione surgettiva, allora $|A| \geq |B|$. Se esiste una funzione biiettiva, allora $|A| = |B|$.

Dimostrazione. Se f è iniettiva, ogni elemento di $f(A)$ ha una sola controimmagine, quindi $f(A)$ ha tanti elementi quanti A . Poiché $f(A) \subseteq B$, si ha $|A| = |f(A)| \leq |B|$. Se f è surgettiva, ogni elemento di B ha almeno una controimmagine, e controimmagini di elementi diversi sono disgiunte (perché f è una funzione), quindi A contiene almeno $|B|$ elementi. Il terzo caso segue dai primi due. ■

TEOREMA (INSIEMI FINITI DELLA STESSA CARDINALITÀ)

Se A e B sono finiti con $|A| = |B|$ e $f: A \rightarrow B$, allora f è iniettiva $\Leftrightarrow f$ è surgettiva $\Leftrightarrow f$ è biiettiva.

Questo fatto, falso per gli insiemi infiniti (la funzione successore su $\mathbb{N}$ è iniettiva e non surgettiva), è alla base del principio dei cassetti (capitolo 18). Per gli insiemi infiniti il fenomeno è proprio il contrario: un insieme infinito può essere messo in corrispondenza biunivoca con una sua parte propria. Per esempio $n \mapsto 2n$ è una biiezione tra $\mathbb{N}$ e l'insieme dei pari, che è un sottoinsieme proprio di $\mathbb{N}$; anche $\mathbb{Z}$ si può mettere in corrispondenza biunivoca con $\mathbb{N}$ ($0, 1, -1, 2, -2, \dots$). Gli insiemi infiniti in biiezione con $\mathbb{N}$ si dicono **numerabili**; per il teorema di Cantor (capitolo 6) $P(\mathbb{N})$ e $\mathbb{R}$ non lo sono.

QUANTE FUNZIONI CI SONO

TIPO DI FUNZIONE DA A A B	QUANTE (CON $ A = K, B = N$)
Tutte le funzioni	n^k (una scelta in B per ciascun elemento di A)
Iniettive (con $k \leq n$)	$n(n-1)\dots(n-k+1)$
Biiettive (con $k = n$)	$n! = n(n-1)\dots 2 \cdot 1$
Funzioni da A in $\{0, 1\}$	2^k , quanti i sottoinsiemi di A (funzioni caratteristiche)

Tabella 2. Conteggio delle funzioni tra insiemi finiti (si approfondirà nel capitolo 18).

Esercizi svolti sulle relazioni

UNIONE E INTERSEZIONE DI RELAZIONI

Siano R e S due relazioni su U . Per ogni proprietà vediamo se si conserva passando a $R \cap S$ e a $R \cup S$ (ricordiamo che sono insiemi di coppie).

PROPRIETÀ	$R \cap S$	$R \cup S$
Riflessiva	sì: (x, x) sta in entrambe, quindi nell'intersezione	sì: (x, x) sta già in R
Simmetrica	sì: se (x, y) sta in entrambe, anche (y, x) sta in entrambe	sì: se (x, y) sta in R o in S , anche (y, x) vi sta
Transitiva	sì: se (x, y) , (y, z) stanno in entrambe, (x, z) sta in entrambe	no : $R = \{(1,2)\}$ e $S = \{(2,3)\}$ sono transitive ma $R \cup S$ non contiene $(1,3)$

Tabella 3. Unione e intersezione di relazioni.

ALCUNE RELAZIONI CONCRETE

RELAZIONE	RIFL.	SIMM.	TRANS.	MOTIVO
x vive a meno di 10 km da y (cittadini italiani)	sì	sì	no	tre città in fila a 8 km l'una dall'altra: la prima e la terza distano 16 km
X e Y sono disgiunti (sottoinsiemi di U)	no	sì	no	$X \cap X = X$ è vuoto solo per $X = \emptyset$; con $\{1\}$, $\{2\}$, $\{1\}$ si rompe la transitività
X e Y hanno intersezione non vuota	no	sì	no	$\emptyset$ non è in relazione con sé stesso; $\{1\}$, $\{1, 2\}$, $\{2\}$: i primi due e gli ultimi due si intersecano, il primo e l'ultimo no
$ X \setminus Y \geq Y \setminus X $	sì	no	sì	equivale a $ X \geq Y $, perché $ X \setminus Y $ meno $ Y \setminus X = X $ meno $ Y $; non è simmetrica ($\{1\}$ e $\emptyset$)

Tabella 4. Quattro relazioni e le loro proprietà (le risposte sono state verificate esaustivamente su piccoli insiemi).

DA RICORDARE

Una relazione si può rappresentare con una **matrice di 0 e 1** (riga x , colonna y , valore 1 se $R(x, y)$) oppure con un **grafo orientato** (una freccia da x a y). In questa lettura la riflessività significa «tutti i cappi presenti», la simmetria «matrice simmetrica», la transitività «ogni percorso di due frecce ha la scorciatoia». Ne ripareremo nel capitolo 8 e nella parte sui grafi.

Relazioni di equivalenza e d'ordine

Le due grandi classi di relazioni: quelle che raggruppano gli elementi in classi (equivalenza) e quelle che li confrontano (ordine); inoltre la rappresentazione degli insiemi finiti al calcolatore.

Relazioni di equivalenza

DEFINIZIONE: RELAZIONE DI EQUIVALENZA

Una relazione R su U riflessiva, simmetrica e transitiva si dice **relazione di equivalenza**. Si scrive $x \approx y$ per $R(x, y)$ e si legge « x è equivalente a y ».

Una relazione di equivalenza astrae il concetto di «essere uguali rispetto a una certa caratteristica». Esempi: avere lo stesso anno di nascita; avere la stessa lunghezza (per le stringhe); avere lo stesso resto nella divisione per 3 (per gli interi); dare lo stesso risultato sotto una funzione f ($x \approx y$ se $f(x) = f(y)$). Tre esempi con cui si impara a controllare le proprietà:

- **Stessa parità** su $\mathbb{Z}$: $x \approx y$ se x meno y è pari. Riflessiva (x meno $x = 0$ è pari), simmetrica (se x meno y è pari, lo è anche y meno x), transitiva (la somma di due pari è pari). È una relazione di equivalenza.
- **Essere amici** su un insieme di persone: simmetrica, ma in generale non transitiva (l'amico di un amico può non essere amico); quindi non è di equivalenza.
- **Dividere** su $\mathbb{N}$ positivi: riflessiva e transitiva, ma non simmetrica; è una relazione d'ordine, non di equivalenza.

CLASSI DI EQUIVALENZA

DEFINIZIONE: CLASSE DI EQUIVALENZA

Sia $\approx$ una relazione di equivalenza su U . La **classe di equivalenza** di x è l'insieme di tutti gli elementi equivalenti a x :

$$[x] = \{y \in U : x \approx y\}.$$

TEOREMA

Due classi di equivalenza sono o disgiunte o coincidenti.

Dimostrazione. Siano $[x]$ e $[z]$ due classi con un elemento w in comune: $x \approx w$ e $z \approx w$. Per simmetria $w \approx z$, e per transitività $x \approx z$. Sia ora $y \in [x]$, cioè $x \approx y$; da $z \approx x$ (simmetria di $x \approx z$) e $x \approx y$ si ottiene per transitività $z \approx y$, cioè $y \in [z]$. Dunque $[x] \subseteq [z]$; scambiando i ruoli si ha $[z] \subseteq [x]$, quindi $[x] = [z]$. Se invece le due classi non hanno elementi in comune sono disgiunte. ■

Poiché ogni x appartiene alla propria classe ($[x] \neq \emptyset$ per riflessività), le classi di equivalenza sono non vuote, disgiunte e coprono tutto U : sono una **partizione** di U , detta **insieme quoziente** e indicata $U/\approx$. La corrispondenza è biunivoca:

TEOREMA (EQUIVALENZE E PARTIZIONI)

Ogni relazione di equivalenza su U individua una partizione di U (le sue classi); viceversa, ogni partizione F di U individua una relazione di equivalenza ponendo $x \approx y$ se e solo se x e y stanno nello stesso blocco di F .

Quindi «relazione di equivalenza» e «partizione» sono due modi di dire la stessa cosa, e il numero di relazioni di equivalenza su un insieme di n elementi è il numero di Bell (1, 2, 5, 15, 52 per n da 1 a 5). L'applicazione che a ogni x associa la sua classe $[x]$ è una funzione surgettiva $U \rightarrow U/\approx$, detta **applicazione canonica** sul quoziente.



Figura 1. La relazione «stesso resto nella divisione per 3» sull'insieme $\{1, \dots, 10\}$ ha tre classi.

Esempio importante: i numeri razionali. Sull'insieme delle coppie (a, b) di interi con $b \neq 0$ si pone $(a, b) \approx (c, d)$ se e solo se $ad = bc$. È una relazione di equivalenza, e una classe è proprio un numero razionale: la classe di $(1, 2)$ contiene $(2, 4)$, $(3, 6)$, (meno 1, meno 2), e rappresenta $1/2$. I razionali sono dunque le frazioni «a meno di semplificazione».

Preordini e relazioni d'ordine

DEFINIZIONE: PREORDINE, ORDINE

Una relazione riflessiva e transitiva si dice **preordine**. Un preordine antisimmetrico, cioè tale che da $x \leq y$ e $y \leq x$ segue $x = y$, si dice **ordinamento** (o ordine parziale). Un insieme su cui è definito un ordinamento si dice **insieme ordinato**.

Se $\leq$ è un ordinamento si pone $x < y$ quando $x \leq y$ e $x \neq y$. Ogni relazione di equivalenza è un preordine (e anche un ordine solo nel caso banale in cui coincide con l'uguaglianza); l'usuale $\leq$ sui numeri e l'inclusione $\subseteq$ tra sottoinsiemi di U sono ordinamenti; la divisibilità sui naturali positivi è un ordinamento.

La differenza essenziale con i numeri è che in un ordine *parziale* due elementi possono essere **non confrontabili**: in $P(\{1, 2\})$ gli insiemi $\{1\}$ e $\{2\}$ non sono uno incluso nell'altro, e tra 2 e 3 non c'è relazione di divisibilità. Se invece per ogni coppia x, y vale $x \leq y$ oppure $y \leq x$, l'ordine è **totale** (o lineare).

MASSIMO, MINIMO, MASSIMALE, MINIMALE

DEFINIZIONE

Sia $(U, \leq)$ un insieme ordinato. Un elemento M è il **massimo** se $x \leq M$ per ogni $x \in U$; è **massimale** se non esiste alcun $x \in U$ con $M < x$. Analogamente m è il **minimo** se $m \leq x$ per ogni x , ed è **minimale** se non esiste x con $x < m$.

Ogni massimo è massimale, ma non viceversa. Un insieme ordinato può avere più elementi massimali (minimali) ma al più un massimo (minimo): se ci fossero due massimi M e M' , si avrebbe $M \leq M'$ e $M' \leq M$, quindi $M = M'$ per antisimmetria.

Esempio. Su $U = \{2, 3, 4, 5, 6, 12\}$ con la relazione «divide», gli elementi minimali sono 2, 3 e 5 (nessun altro elemento di U li divide), i massimali sono 5 e 12 (nessun elemento di U è multiplo proprio di essi); non ci sono né massimo né minimo. Aggiungendo 1 all'insieme si ottiene il minimo 1; aggiungendo 60 si ottiene il massimo 60.

DIAGRAMMI DI HASSE

Un ordine parziale finito si disegna con il **diagramma di Hasse**: ogni elemento è un nodo, x è posto più in basso di y se $x < y$, e si traccia un segmento da x a y solo se y **copre** x , cioè $x < y$ e non esiste z con $x < z < y$. Le relazioni ottenibili per transitività e i cappi (riflessività) non si disegnano.

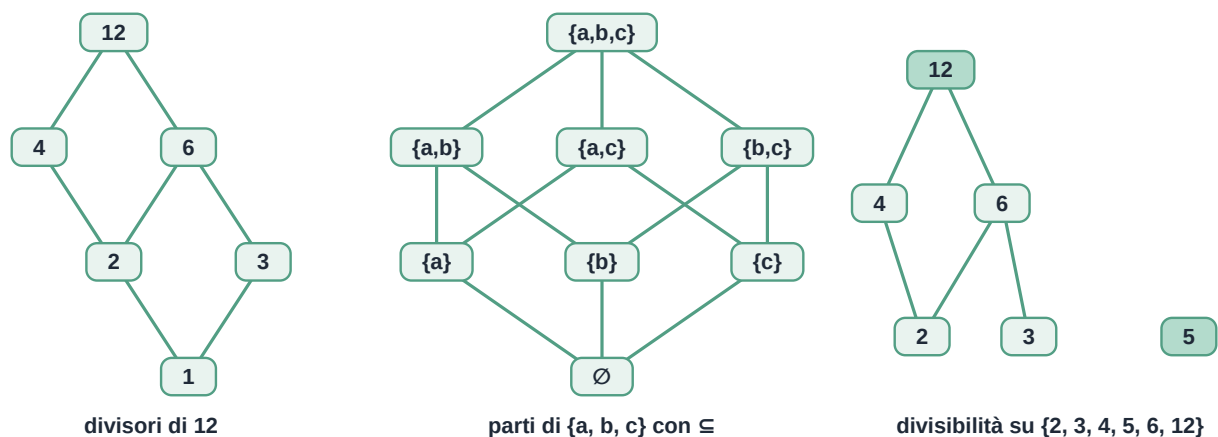


Figura 2. Diagrammi di Hasse: i divisori di 12; l'insieme delle parti di $\{a, b, c\}$ con l'inclusione; la divisibilità su $\{2, 3, 4, 5, 6, 12\}$ (i due massimali sono evidenziati).

Nel diagramma di sinistra, 1 è il minimo e 12 il massimo; nel diagramma centrale il minimo è $\emptyset$ e il massimo $\{a, b, c\}$, e i tre livelli intermedi mostrano che i sottoinsiemi di uguale cardinalità sono a pari altezza. Interessante: i divisori di $30 = 2 \cdot 3 \cdot 5$ con la divisibilità hanno lo stesso diagramma di $P(\{a, b, c\})$: divisore $\leftrightarrow$ sottoinsieme dei fattori primi.

MAGGIORANTI, MINORANTI, ESTREMI

Dato $S \subseteq U$, un **maggiorante** di S è un elemento $u \in U$ con $s \leq u$ per ogni $s \in S$; il più piccolo dei maggioranti, se esiste, si chiama **estremo superiore** (sup) di S . Analogamente per i **minoranti** e l'**estremo inferiore** (inf). Per l'inclusione tra insiemi, $\sup\{A, B\} = A \cup B$ e $\inf\{A, B\} = A \cap B$; per la divisibilità sui naturali positivi $\sup\{a, b\} = \text{mcm}(a, b)$ e $\inf\{a, b\} = \text{MCD}(a, b)$. Sono gli stessi oggetti che incontreremo nel capitolo 12.

CATENE E ANTICATENE

Un sottoinsieme di un insieme ordinato in cui tutti gli elementi sono confrontabili si chiama **catena**; uno in cui nessuna coppia è confrontabile si chiama **anticatena**. Per esempio, in $P(\{a, b, c\})$ i tre insiemi $\{a\}$, $\{b\}$, $\{c\}$ formano un'anticatena e $\emptyset \subset \{a\} \subset \{a, b\} \subset \{a, b, c\}$ è una catena di lunghezza massima.

DA RICORDARE

Ogni ordine parziale finito si può «estendere» a un ordine totale, cioè disporre gli elementi in una lista in cui ogni elemento compare dopo quelli che lo precedono nell'ordine: è l'ordinamento topologico, usato per pianificare compiti con dipendenze (prima di seguire il corso B bisogna aver seguito il corso A). Si ottiene scegliendo ripetutamente un elemento minimale, mettendolo in lista e rimuovendolo.

Rappresentare gli insiemi finiti

Un calcolatore deve rappresentare gli insiemi con strutture dati. Sia $A \subseteq \mathbb{N}$ un insieme finito, contenuto in $I_m = \{0, 1, \dots, m-1\}$. Le due rappresentazioni principali sono le seguenti.

- **Rappresentazione binaria** (vettore caratteristico): un vettore di m bit X con $X[i] = 1$ se $i \in A$ e $X[i] = 0$ altrimenti.
- **Rappresentazione estesa**: un vettore (o una lista concatenata) Y di $n = |A|$ interi, con $Y[i] = x_i$, dove $A = \{x_0, \dots, x_{n-1}\}$.

OPERAZIONE	ETTORE DI BIT	ETTORE DI INTERI NON ORDINATO	ETTORE DI INTERI ORDINATO
Test $x \in A$	tempo costante	tempo lineare in n	tempo logaritmico (ricerca binaria)
Unione, intersezione	m operazioni su bit (OR, AND)	circa n^2 confronti	circa $n + n'$ passi (fusione)
Memoria per $A = \{10, 3, 99\}$	100 bit	3 interi	3 interi
Memoria in generale	m bit, qualunque sia $ A $	n interi	n interi

Tabella 1. Confronto tra le rappresentazioni di un insieme finito.

La rappresentazione binaria è molto efficiente quando l'universo è piccolo o l'insieme è «denso»; quella estesa conviene quando l'universo è enorme ma l'insieme è piccolo (per $A = \{10, 3, 99\}$ servono 3 interi invece di 100 bit). Se l'universo è $I_n = \{0, \dots, n-1\}$, ogni sottoinsieme è una stringa di n bit, cioè un numero binario compreso tra 0 e $2^n - 1$: ritroviamo che $P(I_n)$ ha 2^n elementi.

Con i sottoinsiemi di un universo rappresentati da interi (maschere di bit), le operazioni insiemistiche diventano operazioni bit a bit del processore: l'unione è l'OR, l'intersezione è l'AND, il complemento è il NOT, la differenza simmetrica è lo XOR, e l'inclusione $A \subseteq B$ si verifica controllando che $A \text{ AND } (\text{NOT } B)$ sia zero.

```

A = 0b00110101      # {0, 2, 4, 5}: bit 0, 2, 4, 5 accesi
B = 0b00011100      # {2, 3, 4}
unione              = A | B          # {0, 2, 3, 4, 5}
intersezione        = A & B          # {2, 4}
differenza           = A & ~B        # {0, 5}
simmetrica           = A ^ B         # {0, 3, 5}
incluso              = (A & ~B) == 0 # A e' sottoinsieme di B? falso

```

Anche una relazione su un insieme finito si rappresenta con una **matrice booleana** M di 0 e 1: $M[i][j] = 1$ se i è in relazione con j . La riflessività equivale ad avere tutti 1 sulla diagonale, la simmetria al fatto che M sia uguale alla sua trasposta, e la composizione di relazioni corrisponde al prodotto di matrici (con OR al posto della somma e AND al posto del prodotto).

Hitting Set e famiglie chiuse per unione

Un problema computazionalmente difficile sulle famiglie di insiemi, il calcolo di un hitting set, e un caso di studio su un problema aperto: la congettura di Frankl.

Il problema dell'Hitting Set

Dato un insieme finito U e una famiglia A di sottoinsiemi non vuoti di U , ci si chiede quali elementi di U si debbano scegliere per «colpire» ogni insieme della famiglia, cioè perché ogni insieme contenga almeno uno degli elementi scelti. Il problema ha molte applicazioni: scegliere il minor numero di sensori che sorveglino ogni zona, il minor numero di domande che coprano tutti gli argomenti d'esame, il minor numero di test che distinguano ogni guasto.

DEFINIZIONE: HITTING SET

Siano U un insieme finito, A una famiglia di sottoinsiemi non vuoti di U e $H \subseteq U$. H è un **hitting set** (HS) per A se e solo se $A \cap H \neq \emptyset$ per ogni $A \in A$.

H è **minimale** se è un HS ma per ogni $x \in H$ l'insieme $H \setminus \{x\}$ non è più un HS. H è **minimo** se ha la cardinalità più piccola tra tutti gli HS.

Ogni HS minimo è minimale, ma non viceversa. Poiché ogni insieme della famiglia è non vuoto, U stesso è sempre un HS: il problema interessante è trovarne uno piccolo.

Esempio. Sia $U = \{a, b, c, d, e\}$ e $A = \{\{a, b, c\}, \{a, d, e\}, \{b, c, d\}, \{c, d, e\}\}$. L'insieme $\{a, b, c\}$ è un HS ma non minimale, perché $\{a, c\}$ è ancora un HS. Invece $\{b, c\}$ non è un HS (non colpisce $\{a, d, e\}$) e nemmeno $\{d, e\}$ lo è (non colpisce $\{a, b, c\}$). Nessun elemento da solo appartiene a tutti e quattro gli insiemi, quindi nessun HS ha cardinalità 1, e $\{a, c\}$ è minimo. Gli HS minimi sono sei: $\{a, c\}, \{a, d\}, \{b, d\}, \{b, e\}, \{c, d\}, \{c, e\}$.

INSIEME	A	B	C	D	E
$\{a, b, c\}$	1	1	1	0	0
$\{a, d, e\}$	1	0	0	1	1
$\{b, c, d\}$	0	1	1	1	0
$\{c, d, e\}$	0	0	1	1	1

Tabella 1. Matrice di incidenza dell'esempio: ogni colonna è un elemento di U . Scegliendo le colonne a e c ogni riga contiene almeno un 1.

UN PROBLEMA EQUIVALENTE SU GRAFI

Se tutti gli insiemi di A hanno due elementi, A è l'insieme degli archi di un grafo e un HS è un insieme di vertici che tocca ogni arco: è il problema del **vertex cover** (copertura dei vertici), che incontreremo nel capitolo sui grafi. Dualmente, il problema dell'HS equivale al problema classico della **copertura di insiemi** (set cover).

Come trovare un hitting set minimo

Un algoritmo c'è, ed è semplice: provare tutti i sottoinsiemi di U per cardinalità crescente e fermarsi al primo che è un HS. Il problema è il costo: i sottoinsiemi non vuoti di U sono $2^{|U|} - 1$. Per $|U| = 100$ si hanno circa $1,27 \cdot 10^{30}$ sottoinsiemi; anche con un computer che ne controlla un miliardo al secondo servirebbero circa $1,27 \cdot 10^{21}$ secondi, cioè circa $3,5 \cdot 10^{17}$ ore, $1,5 \cdot 10^{16}$ giorni, oltre 40 mila miliardi di anni. Conviene assumere di non avere tanto tempo.

Si può fare di meglio? Non si sa. Il problema dell'HS minimo (nella versione decisionale: esiste un HS con al più k elementi?) è **NP completo**, e quindi appartiene alla vasta classe di problemi per i quali nessuno conosce un algoritmo che impieghi un numero polinomiale di operazioni nella dimensione dell'input (capitolo 26). Si studiano allora casi particolari e algoritmi che producono soluzioni buone, ma non necessariamente ottime.

CASI PARTICOLARI

- **Insiemi disgiunti.** Se gli insiemi di A sono a due a due disgiunti (per esempio se A è una partizione) un HS minimo si ottiene scegliendo un elemento qualsiasi per ciascun insieme; ogni HS deve avere almeno un elemento in ciascuno degli $|A|$ insiemi disgiunti, quindi ha almeno $|A|$ elementi.
- **Insiemi con un solo elemento.** Se $\{x\} \in A$, ogni HS deve contenere x . Si può quindi inserire x nell'HS, eliminare da A tutti gli insiemi che contengono x e ripetere sul resto. Esempio: $U = \{a, b, c, d, e\}$, $A = \{\{a, b, c\}, \{a, d, e\}, \{c, d\}, \{c, d, e\}, \{d\}, \{e\}\}$. Gli insiemi $\{d\}$ e $\{e\}$ forzano d ed e ; resta da colpire $\{a, b, c\}$ con un elemento qualsiasi. Un HS minimo è $\{a, d, e\}$; $\{d, e\}$ non lo è perché non interseca $\{a, b, c\}$.
- **Insiemi con due elementi.** È il vertex cover, già NP completo in generale.

UN ALGORITMO DI APPROSSIMAZIONE SEMPLICE

Se ogni insieme di A ha al più d elementi, si può trovare rapidamente un HS non più grande di d volte il minimo. Si scelgono, uno dopo l'altro, insiemi della famiglia che non intersecano quelli già scelti, finché è possibile: si ottengono t insiemi a due a due disgiunti e *maximal* (ogni altro insieme di A interseca almeno uno di essi). L'unione H di questi t insiemi è un HS, con al più $d \cdot t$ elementi. Ma ogni HS, per il caso degli insiemi disgiunti, ha almeno t elementi: dunque $|H| \leq d \cdot t$ (cardinalità del minimo).

L'ALGORITMO GOLOSO

Un metodo molto usato è l'**algoritmo goloso** (greedy): a ogni passo si sceglie l'elemento che appartiene al maggior numero di insiemi non ancora colpiti, lo si inserisce nell'HS e si eliminano gli insiemi colpiti, fino a esaurirli.

```
def hitting_set_goloso(F, U):
    H = set()
    da_colpire = [set(A) for A in F]
    while da_colpire:
        x = max(U, key=lambda e: sum(e in A for A in da_colpire))
        H.add(x)
        da_colpire = [A for A in da_colpire if x not in A]
    return H
```

Esempio. Siano $U = \{a, b, c, d, e, f\}$ e $A = \{\{a, b, e\}, \{a, b, f\}, \{b, d\}, \{a, c, f\}, \{a, c, e\}, \{c, e, f\}\}$. L'elemento a appartiene a 4 insiemi, più di ogni altro, e viene scelto. Restano due insiemi disgiunti, $\{b, d\}$ e $\{c, e, f\}$, e da ciascuno dobbiamo scegliere un elemento, per esempio d e f . Si ottiene $H = \{a, d, f\}$, che è un HS minimale, ma **non minimo**: l'HS minimo è $\{b, c\}$, di soli due elementi. A seconda delle scelte tra elementi a pari merito, l'algoritmo potrebbe anche restituire $\{a, b, c\}$, che non è nemmeno minimale (si può eliminare a).

DA RICORDARE

L'algoritmo goloso è veloce e fornisce sempre un HS, ma non garantisce il minimo. Si dimostra però che, con $m = |A|$ insiemi, l'HS prodotto è al più $(1 + \ln m)$ volte più grande del minimo, un risultato classico dovuto a Johnson, Lovász e Chvátal negli anni Settanta; e non ci si aspetta di poter fare molto meglio in tempo polinomiale.

ESERCIZI SVOLTI

Con $U = \{1, 2, \dots, 10\}$, un HS minimo per ciascuna delle tre famiglie già usate nel capitolo 5 si trova controllando i sottoinsiemi per cardinalità crescente (il calcolo, fatto con un programma, dà anche il numero di HS minimi).

FAMIGLIA	CARDINALITÀ MINIMA	UN HS MINIMO	QUANTI HS MINIMI
$F_1 = \{\{1,2,3\}, \{4,5,6\}, \{7,8\}, \{9,10\}, \{1,4,5\}, \{2,6,8\}, \{3,5\}, \{1,10\}\}$	4	$\{1, 5, 8, 9\}$	6
$F_2 = \{\{1,2\}, \{1,3,4\}, \{4,5,6\}, \{6,7,8\}, \{8,9,10\}, \{5,8,9\}\}$	3	$\{1, 4, 8\}$	5
$F_3 = \{\{1,2\}, \{2,3,4\}, \{4,5\}, \{5,6\}, \{3,8,9\}, \{6,9\}, \{7,8\}, \{7,10\}\}$	4	$\{2, 5, 7, 9\}$	1

Tabella 2. Hitting set minimi delle tre famiglie.

Per la prima famiglia, i quattro insiemi $\{4, 5, 6\}$, $\{7, 8\}$, $\{9, 10\}$ e $\{1, 2, 3\}$ sono a due a due disgiunti: servono quindi almeno 4 elementi, e $\{1, 5, 8, 9\}$ li ottiene (colpisce anche $\{1, 4, 5\}$, $\{2, 6, 8\}$, $\{3, 5\}$ e $\{1, 10\}$). Per la seconda, $\{1, 2\}$, $\{4, 5, 6\}$ e $\{8, 9, 10\}$ sono disgiunti: servono almeno 3 elementi, e $\{1, 4, 8\}$ basta. Per la terza, $\{1, 2\}$, $\{4, 5\}$, $\{6, 9\}$ e $\{7, 10\}$ sono a due a due disgiunti: servono almeno 4 elementi, e l'unica quaterna che funziona è $\{2, 5, 7, 9\}$.

Caso di studio: la congettura delle famiglie chiuse per unione

Lo studio delle famiglie chiuse rispetto all'unione, introdotte nel capitolo 5, nasconde uno dei problemi aperti più celebri della combinatoria. Una famiglia F di insiemi finiti è chiusa per unione se $X \cup Y \in F$ per ogni $X, Y \in F$. Un elemento è **abbondante** in F se compare in almeno la metà degli insiemi di F .

CONGETTURA (FRANKL, 1979)

Sia F una famiglia finita, chiusa per unione, che contiene almeno un insieme non vuoto. Allora esiste un elemento che appartiene ad almeno la metà degli insiemi di F (cioè ad almeno $|F|/2$ di essi).

La congettura è nota anche come **congettura di Frankl**, dal nome di Péter Frankl che la propose nel 1979 (o, in modo equivalente, come «congettura degli insiemi chiusi per unione»). Per esempio, la famiglia $\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{1, 2, 4\}, \{1, 2, 3, 4\}\}$, chiusura dell'esempio del capitolo 5, ha 6 insiemi: l'elemento 1 compare in 5 di essi, l'elemento 2 in 5, l'elemento 3 in 3, l'elemento 4 in 3; quindi 1 e 2 sono abbondanti.

UNA VERSIONE DUALE

Per il teorema di dualità del capitolo 5, F è chiusa per unione se e solo se la famiglia dei complementi F^C è chiusa per intersezione, e un elemento compare in almeno la metà degli insiemi di F se e solo se compare in *al più* la metà degli insiemi di F^C . La congettura equivale dunque a: *in una famiglia chiusa per intersezione, con almeno due insiemi, esiste un elemento che compare in al più la metà degli insiemi*. Una terza formulazione riguarda i reticoli (cioè gli insiemi ordinati del capitolo 8 in cui ogni coppia ha estremo superiore e inferiore): in ogni reticolo finito con più di un elemento esiste un elemento «irriducibile per il sup» con al più metà degli elementi sopra di sé.

UN CASO CHE SI DIMOSTRA

Se F contiene un insieme con un solo elemento $\{x\}$, la congettura vale e l'elemento abbondante è proprio x . Infatti consideriamo l'applicazione $S \mapsto S \cup \{x\}$, definita sugli insiemi di F che *non* contengono x . Poiché F è chiusa per unione e $\{x\} \in F$, l'immagine sta in F , e contiene x . L'applicazione è iniettiva, perché da $S \cup \{x\}$ si recupera S togliendo x . Dunque gli insiemi che contengono x sono almeno tanti quanti quelli che non lo contengono, cioè almeno $|F|/2$. ■

Per il caso in cui F contiene un insieme di due elementi esistono dimostrazioni nella letteratura, ma richiedono argomenti molto più elaborati e non le riportiamo qui; il caso generale è invece aperto.

CHE COSA SI SA

La congettura ha resistito per oltre quarant'anni. Un cambio di passo è avvenuto a novembre 2022, quando Justin Gilmer ha dimostrato con metodi di teoria dell'informazione che esiste sempre un elemento che appartiene ad almeno una frazione costante degli insiemi, pari a 0,01. In pochi giorni diversi gruppi (Alweiss, Huang e Sellke; Chase e Lovett; Sawin; Pebody) hanno migliorato il metodo portando la costante a $(3 - \sqrt{5})/2 \approx 0,38197$. Successivamente Sawin, e poi Yu e Cambie, hanno ottenuto circa 0,38234, e nel 2023 Liu ha ottenuto circa 0,38271 con un procedimento che si appoggia in parte a verifiche numeriche. Siamo dunque vicini, ma non ancora a $1/2 = 0,5$: **la congettura di Frankl è, a quanto risulta all'autore, ancora aperta.**

DA RICORDARE

Il valore della congettura sta anche nella sua semplicità: si enuncia con la sola nozione di insieme, di unione e di cardinalità, eppure nessuno è riuscito a dimostrarla. Il caso è un buon esempio di come i problemi aperti della matematica discreta non richiedano strumenti avanzati per essere capiti.

Numeri interi e induzione

Gli insiemi numerici, le operazioni sugli interi, la definizione di Peano dei naturali, il buon ordinamento e il principio di induzione, con molti esempi di dimostrazioni.

Gli insiemi numerici

Cominciamo dai numeri che tutti conosciamo, fissando le notazioni che useremo in questa e nelle prossime parti. In questo corso **lo zero è un numero naturale**.

INSIEME	NOME	DEFINIZIONE	UN ELEMENTO CHE NON STA NEL PRECEDENTE
$\mathbb{N}$	naturali	$\{0, 1, 2, 3, \dots\}$	(è il primo della catena)
$\mathbb{Z}$	interi relativi	$\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$	-1
$\mathbb{Q}$	razionali	$\{n/m : n, m \in \mathbb{Z} \text{ e } m \neq 0\}$	1/2
$\mathbb{R}$	reali	numeri razionali e irrazionali	$\sqrt{2}$
$\mathbb{C}$	complessi	numeri reali e immaginari, cioè $a + bi$ con $a, b \in \mathbb{R}$	i , con $i^2 = -1$

Tabella 1. Gli insiemi numerici e la catena di inclusioni strette.

Vale quindi la catena di inclusioni strette

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

dove ogni insieme contiene il precedente e almeno un elemento in più. Per indicare i soli naturali positivi si scrive $\mathbb{N}^+ = \{1, 2, 3, \dots\}$; analogamente $\mathbb{Z}^+$ e $\mathbb{R}^+$ indicano gli elementi positivi di $\mathbb{Z}$ e $\mathbb{R}$.

NUMERI IRRAZIONALI E SCUOLA PITAGORICA

La scuola pitagorica fu fondata da Pitagora a Crotone intorno al 530 a.C. ed era, insieme, una scuola di matematica e filosofia e una comunità di carattere religioso, con regole rigide e l'obbligo di non divulgare le scoperte. Ai pitagorici, oltre al teorema che porta il loro nome, si attribuisce la scoperta che il lato di un quadrato e la sua diagonale sono **incommensurabili**: non esiste alcuna unità di misura di cui entrambi siano multipli interi. Poiché la diagonale di un quadrato di lato 1 misura $\sqrt{2}$, questo equivale a dire che $\sqrt{2}$ non è razionale, fatto che abbiamo dimostrato nel capitolo 4. Per chi credeva che tutto fosse misurabile con i numeri interi e le loro frazioni fu uno shock. La tradizione racconta che Ippaso, uno degli allievi, fu punito con la morte per aver divulgato il segreto; la vicenda è però incerta e le fonti antiche non concordano, quindi è da considerarsi una leggenda. Il numero $\sqrt{2}$ è detto anche **costante di Pitagora**.

Operazioni sugli interi

Su $\mathbb{N}$ sono definite due operazioni, la **somma** $+$: $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ e il **prodotto** $\cdot$: $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, che a ogni coppia (n, m) associano $n + m$ e $n \cdot m$. Su $\mathbb{Z}$ si aggiunge la **differenza** $-$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, che a (n, m) associa $n - m$, cioè $n + (-m)$. Su $\mathbb{N}$ la differenza non è definita in modo diretto: $n - m$ ha senso come numero naturale solo quando $n \geq m$ ($3 - 5$ non è un naturale). La **divisione** non è invece un'operazione su $\mathbb{Z}$: $7/2$ non è intero. Il capitolo 11 la sostituisce con la divisione con resto.

PROPRIETÀ FORMALI DI SOMMA E PRODOTTO

Per ogni $a, b, c \in \mathbb{Z}$ valgono le proprietà seguenti, che useremo senza richiamarle ogni volta.

PROPRIETÀ	SOMMA	PRODOTTO
Commutativa	$a + b = b + a$	$a \cdot b = b \cdot a$
Associativa	$(a + b) + c = a + (b + c)$	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Elemento neutro	$a + 0 = a$	$a \cdot 1 = a$
Distributiva	$a \cdot (b + c) = a \cdot b + a \cdot c$	(prodotto rispetto alla somma)
Opposto	$a + (-a) = 0$	(solo ± 1 hanno un inverso in $\mathbb{Z}$)
Elemento zero	nessuna	$a \cdot 0 = 0$; e se $a \cdot b = 0$ allora $a = 0$ oppure $b = 0$

Tabella 2. Proprietà formali delle operazioni su $\mathbb{Z}$.

L'ultima proprietà (*legge di annullamento del prodotto*) sembra ovvia, ma non vale in ogni struttura numerica: nei calcoli con le congruenze del capitolo 14 troveremo prodotti nulli con fattori non nulli, come $2 \cdot 3 = 6 \equiv 0$ modulo 6.

PRIORITÀ DEGLI OPERATORI

Il prodotto ha priorità più alta di somma e differenza, che hanno la stessa priorità e si calcolano da sinistra verso destra (**associatività a sinistra**). Questo è importante soprattutto per la differenza, che non è associativa:

$$a - b - c = (a - b) - c \text{ e non } a - (b - c)$$

Esempi: $10 + 3 \cdot 5 - 5 = 10 + 15 - 5 = 20$; $20 - 3 \cdot 5 - 5 = 20 - 15 - 5 = 0$; $5 - 1 - 2 + 3 = 4 - 2 + 3 = 2 + 3 = 5$, mentre $5 - (1 - 2) + 3 = 5 + 1 + 3 = 9$.

VALORE ASSOLUTO

DEFINIZIONE: VALORE ASSOLUTO

Il **valore assoluto** (o **modulo**) di un intero n è l'intero non negativo $|n|$ definito da $|n| = n$ se $n \geq 0$, e $|n| = -n$ se $n < 0$.

Per ogni $n, m \in \mathbb{Z}$ valgono le proprietà seguenti. Le dimostrazioni si fanno per casi sul segno.

- $|n| = 0$ se e solo se $n = 0$. Infatti se $n \neq 0$ allora $|n|$ è n oppure $-n$, entrambi diversi da 0.
- $|n \cdot m| = |n| \cdot |m|$. Se i due segni sono concordi il prodotto è ≥ 0 e $|n \cdot m| = n \cdot m = |n| \cdot |m|$ (se $n, m \geq 0$ è ovvio; se entrambi negativi, $(-n)(-m) = n \cdot m$); se sono discordi $|n \cdot m| = -(n \cdot m) = |n| \cdot |m|$.
- $n + |n| \geq 0$, e vale 0 se e solo se $n \leq 0$. Se $n \geq 0$ la somma è $2n \geq 0$, e nulla solo per $n = 0$; se $n < 0$ la somma è $n + (-n) = 0$.
- **Disuguaglianza triangolare:** $|n + m| \leq |n| + |m|$. Da $-|n| \leq n \leq |n|$ e $-|m| \leq m \leq |m|$ si ottiene, sommando, $-(|n| + |m|) \leq n + m \leq |n| + |m|$.

I numeri naturali secondo Peano

Il matematico e logico piemontese Giuseppe Peano (nato nel 1858 e morto nel 1932), lo stesso che introdusse molti dei simboli insiemistici che usiamo, diede una definizione assiomatica dei numeri naturali: invece di *costruirli*, ne elenca le proprietà fondamentali, a partire dalle quali si ricava tutto il resto.

ASSIOMI DI PEANO

1. Esiste un numero naturale 0.
2. Ogni naturale a ha un **successore** $S(a)$, anch'esso naturale.
3. Nessun naturale ha 0 come successore.
4. Naturali distinti hanno successori distinti: se $a \neq b$ allora $S(a) \neq S(b)$.
5. (Induzione) Se un insieme di naturali contiene 0 e contiene il successore di ogni suo elemento, allora è tutto $\mathbb{N}$.

Si pone $1 = S(0)$, $2 = S(1)$, e così via; la somma e il prodotto si definiscono per ricorsione sul secondo argomento, ponendo $a + 0 = a$ e $a + S(b) = S(a + b)$, poi $a \cdot 0 = 0$ e $a \cdot S(b) = a \cdot b + a$. Per esempio $2 + 2 = 2 + S(1) = S(2 + 1) = S(2 + S(0)) = S(S(2 + 0)) = S(S(2)) = 4$. Con queste definizioni $S(a) = a + 1$ per ogni a . Ogni naturale n diverso da 0 è il successore di un unico naturale, il suo **predecessore** $n - 1$.

L'ordine si definisce a partire dalla somma: $a \leq b$ se esiste $c \in \mathbb{N}$ con $a + c = b$, e $a < b$ se vale $a \leq b$ e $a \neq b$. In particolare $a < S(a)$, e l'ordine è transitivo: se $a < b$ e $b < c$ allora $a < c$.

IL BUON ORDINAMENTO

ASSIOMA DEL BUON ORDINAMENTO

Ogni insieme non vuoto S di numeri naturali ha un **elemento minimo**: esiste $s \in S$ tale che $s \leq t$ per ogni $t \in S$.

È una proprietà specifica dei naturali, che non vale per gli altri insiemi numerici. In $\mathbb{Z}$ l'insieme dei pari negativi non ha minimo; l'insieme dei razionali positivi non ha minimo, perché per ogni $q > 0$ si ha $q/2 > 0$ e $q/2 < q$; lo stesso accade per i reali strettamente positivi. Questo assioma ci servirà per dimostrare il principio di induzione e, nel capitolo 11, l'esistenza della divisione con resto.

Il principio di induzione

Il quinto assioma di Peano è il **principio di induzione**. Nella forma in cui lo si usa per dimostrare enunciati, parla di *proprietà* invece che di insiemi: se $P(n)$ è un'affermazione riguardante il naturale n , l'insieme dei naturali per cui P è vera è un sottoinsieme di $\mathbb{N}$, e il quinto assioma dice quando è tutto $\mathbb{N}$.

PRINCIPIO DI INDUZIONE

Sia $P(n)$ un'affermazione sui numeri naturali. Se

(a) $P(0)$ è vera (**caso base**) e

(b) per ogni naturale n , se $P(n)$ è vera allora è vera anche $P(n + 1)$ (**passo induttivo**; l'ipotesi « $P(n)$ è vera» si chiama **ipotesi induttiva**),

allora $P(n)$ è vera per ogni naturale n .

L'immagine classica è quella di una fila infinita di tessere del domino: se la prima cade (caso base) e ogni tessera, cadendo, fa cadere la successiva (passo), allora cadono tutte. Il principio può anche essere *dimostrato* a partire dal buon ordinamento, e questo mostra che i due sono, in pratica, due facce della stessa proprietà.

Dimostrazione. Per assurdo, supponiamo che (a) e (b) valgano ma che P sia falsa per qualche naturale. Allora l'insieme $S = \{n \in \mathbb{N} : P(n) \text{ è falsa}\}$ non è vuoto e, per il buon ordinamento, ha un minimo s . Poiché $P(0)$ è vera, $s \neq 0$, quindi $s > 0$ e ha un predecessore $s - 1$. Poiché $s - 1 < s$ e s è il minimo di S , $s - 1 \notin S$, cioè $P(s - 1)$ è vera. Ma allora, per (b), è vera anche $P(s)$, contro il fatto che $s \in S$. Contraddizione. ■

DA RICORDARE

Una dimostrazione per induzione ha sempre due parti: il **caso base** e il **passo induttivo**. Nel passo si assume $P(n)$ per un n generico e si deduce $P(n+1)$, usando l'ipotesi induttiva in un punto preciso del ragionamento. Se la proprietà vale solo da un certo n_0 in poi, il caso base è $P(n_0)$ (per gli interi positivi, spesso $n_0 = 1$).

SECONDA FORMA (INDUZIONE FORTE)

Nella seconda forma, nel passo induttivo si può usare l'ipotesi per *tutti* i numeri precedenti, non solo per l'ultimo.

PRINCIPIO DI INDUZIONE (SECONDA FORMA)

Se $P(0)$ è vera e, per ogni $n > 0$, la verità di $P(k)$ per tutti i $k < n$ implica la verità di $P(n)$, allora P è vera per ogni naturale.

La dimostrazione è identica alla precedente: il minimo s di S ha $P(k)$ vera per ogni $k < s$, quindi anche $P(s)$ è vera, assurdo. La seconda forma è più comoda quando $P(n+1)$ non dipende da $P(n)$ ma da casi più piccoli, come negli esempi 7 e 8 qui sotto.

Esempi di dimostrazioni per induzione

Esempio 1: la somma di Gauss. Per ogni $n \geq 1$: $1 + 2 + \dots + n = n(n+1)/2$.

Caso base ($n = 1$): $1 = 1 \cdot 2/2$. **Passo:** supponiamo $1 + \dots + n = n(n+1)/2$. Allora $1 + \dots + n + (n+1) = n(n+1)/2 + (n+1) = [n(n+1) + 2(n+1)]/2 = (n+1)(n+2)/2$, che è la formula per $n+1$. ■ (Si dice che Gauss, da bambino, trovò la formula osservando che sommando il primo e l'ultimo termine, il secondo e il penultimo, e così via, si ottiene sempre $n+1$.)

Esempio 2: la progressione geometrica. Per $x \neq 1$ e ogni $n \geq 0$: $1 + x + x^2 + \dots + x^n = (1 - x^{n+1})/(1 - x)$.

Caso base ($n = 0$): il primo membro è 1 e il secondo è $(1 - x)/(1 - x) = 1$. **Passo:** sommando x^{n+1} alla formula per n si ha $(1 - x^{n+1})/(1 - x) + x^{n+1} = [1 - x^{n+1} + x^{n+1}(1 - x)]/(1 - x) = (1 - x^{n+2})/(1 - x)$. ■ Per $x = 2$ si ottiene $1 + 2 + \dots + 2^n = 2^{n+1} - 1$, la formula che conta, per esempio, i valori massimi rappresentabili con $n+1$ bit.

Esempio 3: la somma dei primi dispari. Per ogni $n \geq 1$: $1 + 3 + 5 + \dots + (2n-1) = n^2$. **Caso base:** $1 = 1^2$. **Passo:** $n^2 + (2n+1) = (n+1)^2$. ■

Esempio 4: un fattoriale supera una potenza. Per ogni $n \geq 4$: $n! > 2^n$. Si noti che la proprietà è falsa per $n = 3$ ($6 < 8$), per questo il caso base è $n = 4$. **Caso base:** $4! = 24 > 16 = 2^4$. **Passo:** se $n! > 2^n$ con $n \geq 4$, allora $(n+1)! = (n+1) \cdot n! > (n+1) \cdot 2^n \geq 2 \cdot 2^n = 2^{n+1}$, dove si è usato $n+1 \geq 2$. ■

Esempio 5: il numero dei sottoinsiemi. Se A è un insieme finito, $|P(A)| = 2^{|A|}$ (induzione sulla cardinalità $n = |A|$). **Caso base** ($n = 0$): $A = \emptyset$ e $P(\emptyset) = \{\emptyset\}$ ha $1 = 2^0$ elementi. **Passo:** sia $|A| = n \geq 1$ e fissiamo $a \in A$; l'insieme $A' = A \setminus \{a\}$ ha $n-1$ elementi, quindi per ipotesi $|P(A')| = 2^{n-1}$. I sottoinsiemi di A si dividono in due gruppi disgiunti: quelli che *non* contengono a , che sono esattamente gli elementi di $P(A')$, e quelli che contengono a . La funzione $X \mapsto X \cup \{a\}$ è una corrispondenza biunivoca tra $P(A')$ e i sottoinsiemi che contengono a (l'inversa è $Y \mapsto Y \setminus \{a\}$); quindi anche questi sono 2^{n-1} . In totale $|P(A)| = 2 \cdot 2^{n-1} = 2^n$. ■

Esempio 6: una divisibilità. Per ogni $n \geq 0$, $n^3 - n$ è divisibile per 3. **Caso base:** 0. **Passo:** $(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 = (n^3 - n) + 3(n^2 + n)$, somma di due multipli di 3. ■ (Il fatto è vero anche per n negativo, e lo dimostreremo con le congruenze nel capitolo 14.)

Esempio 7 (seconda forma): i francobolli da 4 e da 5. Ogni importo $n \geq 12$ si può ottenere con monete da 4 e da 5 centesimi. Servono *quattro* casi base: $12 = 4 + 4 + 4$, $13 = 4 + 4 + 5$, $14 = 4 + 5 + 5$, $15 = 5 + 5 + 5$. Per $n \geq 16$ si ha $n - 4 \geq 12$ e, per ipotesi, $n - 4$ si ottiene con monete da 4 e da 5; aggiungendo una moneta da 4 si ottiene n . ■ L'importo 11 non è ottenibile, quindi 12 è il minimo possibile.

Esempio 8 (seconda forma): fattorizzazione. Un naturale $p \geq 2$ è **primo** se i suoi unici divisori positivi sono 1 e p . Ogni naturale $n \geq 2$ è primo oppure prodotto di numeri primi. Se n è primo non c'è nulla da dimostrare. Altrimenti $n = a \cdot b$ con $1 < a, b < n$; per ipotesi induttiva (valida per tutti i naturali tra 2 e $n - 1$) a e b sono primi o prodotti di primi, e quindi lo è anche n . ■ Qui l'induzione semplice non basterebbe, perché a e b non sono $n - 1$.

GLI ERRORI TIPICI

Il caso base e il passo sono entrambi indispensabili. Senza caso base si «dimostra» che $n = n + 1$: se vale per n allora, sommando 1, vale per $n + 1$, ma non vale mai. Senza passo basta verificare qualche valore, come accade con $n^2 + n + 41$, che è primo per $n = 0, 1, \dots, 39$ e non lo è per $n = 40$ ($1681 = 41^2$). Un errore più subdolo è quello del «paradosso dei cavalli»: la tesi «in ogni gruppo di n cavalli tutti i cavalli hanno lo stesso colore» ha caso base $n = 1$ evidente, e il «passo» considera un gruppo di $n + 1$ cavalli, toglie un cavallo, poi un altro, e conclude che i due gruppi di n si sovrappongono. Ma per $n = 1$ (da 1 a 2 cavalli) i due gruppi di un cavallo non hanno elementi in comune, quindi il passo non funziona proprio per il primo valore, e tutta la dimostrazione crolla. Moraltà: il passo induttivo deve valere per **ogni** n dal caso base in poi.

Parte intera inferiore e superiore

Per un numero reale x si definiscono due interi.

DEFINIZIONE: FLOOR E CEILING

La **parte intera inferiore** (floor) $\lfloor x \rfloor$ è il più grande intero minore o uguale a x . La **parte intera superiore** (ceiling) $\lceil x \rceil$ è il più piccolo intero maggiore o uguale a x .

x	$\lfloor x \rfloor$	$\lceil x \rceil$
3,8	3	4
-3,8	-4	-3
-3	-3	-3
0,2	0	1

Tabella 3. Esempi di floor e ceiling.



Figura 1. Floor e ceiling per $x = -3,8$ e $x = 3,8$: sono i due interi consecutivi tra cui x è compreso.

Attenzione ai numeri negativi: $\lfloor -3,8 \rfloor$ è -4 e non -3 , perché -3 è maggiore di $-3,8$. Le proprietà fondamentali, per x reale e n intero, sono:

- $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$, e $\lfloor x \rfloor - 1 < x \leq \lfloor x \rfloor$;
- $\lfloor x \rfloor = \lceil x \rceil$ se e solo se x è un intero; altrimenti $\lceil x \rceil = \lfloor x \rfloor + 1$;
- $\lfloor x \rfloor = -\lceil -x \rceil$ e $\lceil x \rceil = -\lfloor -x \rfloor$;
- $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ e $\lceil x + n \rceil = \lceil x \rceil + n$;
- $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$ (per n pari valgono entrambi $n/2$, per n dispari valgono $(n - 1)/2$ e $(n + 1)/2$).

Servono per passare da un reale a un intero: le pagine per 53 righe da 10 sono $\lceil 53/10 \rceil = 6$, i bit per scrivere n in binario sono $\lfloor \log_2 n \rfloor + 1$. Le ritroveremo nei capitoli 11 e 18.

Divisione con resto e divisibilità

Il teorema della divisione con quoziente e resto, anche con numeri negativi, e le proprietà della relazione «m divide n».

La divisione con resto

Nel capitolo precedente abbiamo visto che la divisione non è un'operazione su $\mathbb{Z}$: 17 diviso 5 non è un intero. Possiamo però chiederci *quante volte 5 sta in 17 e quanto avanza*: $17 = 3 \cdot 5 + 2$. Questa idea è formalizzata nel teorema seguente, che è alla base di tutta la teoria dei numeri.

TEOREMA DELLA DIVISIONE CON RESTO

Dati due interi a e b con $b \neq 0$, detti **dividendo** e **divisore**, esistono e sono **unici** due interi q e r , detti **quoziente** e **resto**, tali che

$$a = q \cdot b + r \text{ con } 0 \leq r < |b|.$$

Il resto si indica anche con $a \bmod b$.

Si noti che il resto è **sempre non negativo** e strettamente minore del valore assoluto del divisore, anche quando a o b sono negativi. Se $b > 0$ il quoziente è $q = \lfloor a/b \rfloor$, se $b < 0$ è $q = \lceil a/b \rceil$; in entrambi i casi il resto è poi $r = a - qb$.



Figura 1. Divisione di 23 per 5: $23 = 4 \cdot 5 + 3$. Il quoziente è il numero di multipli interi di 5 che precedono a , il resto è la distanza dall'ultimo.

DIMOSTRAZIONE DELL'ESISTENZA

Trattiamo prima il caso $b > 0$ e a intero qualunque. Consideriamo l'insieme

$$S = \{a - kb : k \in \mathbb{Z} \text{ e } a - kb \geq 0\}$$

dei resti «candidati». S è un insieme di naturali ed è non vuoto: se $a \geq 0$ contiene a (per $k = 0$); se $a < 0$ contiene $a - ab = a(1 - b) = |a|(b - 1) \geq 0$ (per $k = a$). Per il buon ordinamento S ha un minimo $r = a - qb \geq 0$. Resta da mostrare che $r < b$. Se fosse $r \geq b$, allora $r - b = a - (q + 1)b$ sarebbe un elemento di S più piccolo di r , contro la minimalità. Dunque $0 \leq r < b$. Se invece $b < 0$, si applica quanto appena visto a a e $|b|$: $a = q'|b| + r$ con $0 \leq r < |b|$, e poiché $|b| = -b$ si ottiene $a = (-q')b + r$, cioè $q = -q'$ e lo stesso resto. ■

DIMOSTRAZIONE DELL'UNICITÀ

Siano $a = q_1b + r_1 = q_2b + r_2$ con $0 \leq r_1, r_2 < |b|$. Sottraendo, $b(q_2 - q_1) = r_1 - r_2$, e passando ai valori assoluti $|b| \cdot |q_2 - q_1| = |r_1 - r_2|$. Poiché r_1 e r_2 stanno entrambi tra 0 e $|b|$, la loro differenza ha valore assoluto strettamente minore di $|b|$. Quindi $|b| \cdot |q_2 - q_1| < |b|$, cioè $|q_2 - q_1| < 1$; essendo un intero, è 0. Allora $q_1 = q_2$ e, dalla prima uguaglianza, $r_1 = r_2$. ■

COME SI CALCOLANO QUOZIENTE E RESTO

Il metodo pratico è dividere i **valori assoluti** e poi correggere i segni. Si calcolano $q' = \lfloor |a|/|b| \rfloor$ e $r' = |a| - q'|b|$, e poi:

SEGNI	QUOZIENTE Q	RESTO R
$a \geq 0, b > 0$	q'	r'
$a \geq 0, b < 0$	$-q'$	r'
$a < 0, b > 0$	$-q'$ se $r' = 0$, altrimenti $-q' - 1$	0 se $r' = 0$, altrimenti $b - r'$
$a < 0, b < 0$	q' se $r' = 0$, altrimenti $q' + 1$	0 se $r' = 0$, altrimenti $-b - r'$

Tabella 1. Ricetta per la divisione con resto a partire dai valori assoluti.

Il caso $r' = 0$ va trattato a parte: se a è un multiplo di b , il resto è 0 e non $|b|$. Ecco gli esempi, con $a = qb + r$.

A	B	Q	$R = A \bmod B$	VERIFICA
13	10	1	3	$13 = 1 \cdot 10 + 3$
13	-10	-1	3	$13 = -1 \cdot (-10) + 3$
-13	10	-2	7	$-13 = -2 \cdot 10 + 7$
-13	-10	2	7	$-13 = 2 \cdot (-10) + 7$
29	7	4	1	$29 = 4 \cdot 7 + 1$
-29	7	-5	6	$-29 = -5 \cdot 7 + 6$
29	-7	-4	1	$29 = -4 \cdot (-7) + 1$
-29	-7	5	6	$-29 = 5 \cdot (-7) + 6$
20	5	4	0	$20 = 4 \cdot 5 + 0$
-20	5	-4	0	$-20 = -4 \cdot 5 + 0$

Tabella 2. Esempi di divisione con resto con tutte le combinazioni di segni.

In particolare, per ogni coppia di interi positivi $n < m$ si ha $n \bmod m = n$ e $(-n) \bmod m = m - n$; quindi $-1 \bmod 10 = 9$ e $-2 \bmod 7 = 5$.

ATTENZIONE AI LINGUAGGI DI PROGRAMMAZIONE

Nella matematica il resto è sempre non negativo. In molti linguaggi (C, C++, Java) l'operatore % restituisce invece un resto con il **segno del dividendo**: $-7 \% 3$ vale -1 , mentre matematicamente $(-7) \bmod 3 = 2$ (perché $-7 = (-3) \cdot 3 + 2$). In Python, invece, $-7 \% 3$ vale 2. Inoltre, tra interi l'operatore / dà il quoziente della divisione intera ($3/2$ vale 1 se gli operandi sono interi, 1,5 se sono numeri in virgola mobile), e in C e Java il quoziente di numeri negativi è arrotondato verso zero, non verso il basso: $-7/3$ vale -2 .

QUALCHE APPLICAZIONE

- **Parità.** Un intero è pari se il resto della divisione per 2 è 0, dispari se è 1; i pari sono i numeri della forma $2k$, i dispari quelli della forma $2k + 1$.
- **Cicli periodici.** Se oggi è venerdì, tra 100 giorni sarà il giorno corrispondente a $100 \bmod 7 = 2$ giorni dopo, cioè domenica. Quindici ore dopo le 20 sono le $(20 + 15) \bmod 24 = 11$.
- **Cambio di base.** Le cifre di un numero in base b si trovano con divisioni successive per b , leggendo i resti dall'ultimo al primo: $37 = 18 \cdot 2 + 1$, $18 = 9 \cdot 2 + 0$, $9 = 4 \cdot 2 + 1$, $4 = 2 \cdot 2 + 0$, $2 = 1 \cdot 2 + 0$, $1 = 0 \cdot 2 + 1$, da cui $37 = 100101$ in base 2.

- **Dimostrazioni per casi.** Nella divisione per m ogni intero n ha uno solo degli m resti $0, 1, \dots, m-1$, quindi si può dimostrare un enunciato distinguendo m casi. Per esempio, $n(n+1)$ è sempre pari (se n è pari lo è il primo fattore, se è dispari lo è $n+1$), e $n(n+1)(n+2)$ è sempre un multiplo di 3: se n ha resto 0 nella divisione per 3 lo è n , se ha resto 2 lo è $n+1$, se ha resto 1 lo è $n+2$.

La divisibilità

DEFINIZIONE: DIVISIBILITÀ

Dati $m, n \in \mathbb{Z}$, si dice che m **divide** n (o che m è un **divisore** di n , o che n è un **multiplo** di m) se esiste $k \in \mathbb{Z}$ tale che $n = k \cdot m$. Si scrive $m \mid n$; se m non divide n si scrive $m \nmid n$.

Se $m \neq 0$, dire che $m \mid n$ equivale a dire che il resto della divisione di n per m è 0. Esempi: $2 \mid 8$, $-5 \mid 15$, $5 \nmid 16$, $3 \nmid -7$ (il resto di -7 diviso 3 è 2). Un numero è **pari** se è divisibile per 2, **dispari** altrimenti.

DA RICORDARE

$m \mid n$ è una *relazione* tra due interi che è vera o falsa; non va confusa con la frazione m/n o con la barra della divisione. Si legge « m divide n » e non « n diviso m ».

LE PRIME PROPRIETÀ

TEOREMA (PROPRIETÀ DELLA DIVISIBILITÀ)

Per ogni $a, b, c \in \mathbb{Z}$:

(Somma) se $a \mid b$ e $a \mid c$ allora $a \mid (b+c)$.

(Prodotto) se $a \mid b$ allora $a \mid bc$.

(Transitività) se $a \mid b$ e $b \mid c$ allora $a \mid c$.

Dimostrazione. *Somma:* esistono x e y con $b = ax$ e $c = ay$, quindi $b+c = a(x+y)$, che è un multiplo di a .

Prodotto: da $b = ax$ segue $bc = a(xc)$. *Transitività:* da $b = ax$ e $c = by$ segue $c = a(xy)$. ■

Da queste proprietà seguono subito i risultati seguenti.

- **Quadrato:** se $a \mid b$ allora $a \mid b^2$ (caso particolare del prodotto, con $c = b$).
- **Combinazione lineare:** se $a \mid b$ e $a \mid c$ allora $a \mid (hb+kc)$ per ogni $h, k \in \mathbb{Z}$. Infatti $a \mid hb$ e $a \mid kc$ per il prodotto, e si applica la somma. È la base dell'algoritmo di Euclide e di Bézout (capitolo 12).
- **Contrapposta della somma:** se $a \mid b$ e $a \nmid c$ allora $a \nmid (b+c)$. Infatti, se per assurdo $a \mid (b+c)$, allora a divide anche $(b+c) - b = c$, contro l'ipotesi.

ZERO, DIVISORI BANALI E ANTISIMMETRIA

- **Ogni intero divide 0**, perché $0 = 0 \cdot a$. Invece 0 divide solo 0: se $0 \mid a$ allora $a = x \cdot 0 = 0$.
- **Divisori banali:** ogni intero a è divisibile per 1, -1 , a e $-a$. I divisori diversi da questi sono «non banali» (capitolo 13).
- **Antisimmetria:** se $a \mid b$ e $b \mid a$ allora $|a| = |b|$, cioè $a = \pm b$. Infatti $b = ax$ e $a = by$ danno $a = axy$, cioè $a(1-xy) = 0$. Se $a = 0$ anche $b = 0$; altrimenti $xy = 1$, quindi x e y sono entrambi 1 o entrambi -1 , e $a = \pm b$. ■
- **Confronto:** se $a \mid b$ e $b \neq 0$ allora $|a| \leq |b|$, perché $b = ak$ con $k \neq 0$ intero, quindi $|k| \geq 1$. Quindi un numero non nullo ha un numero finito di divisori.

Su $\mathbb{N}$ la divisibilità è riflessiva, antisimmetrica e transitiva: è una **relazione d'ordine parziale** (capitolo 8), con minimo 1 e massimo 0, non totale (2 e 3 non sono confrontabili). In $\mathbb{Z}$ non è antisimmetrica: $-3 \mid 3$ e $3 \mid -3$ ma $3 \neq -3$. I divisori comuni a due numeri, e quindi il massimo comune divisore e il minimo comune multiplo, sono il tema del capitolo 12.

MCD, algoritmo di Euclide e numeri coprimi

Il massimo comune divisore, l'algoritmo di Euclide e la sua complessità, l'identità di Bézout, i numeri coprimi e il minimo comune multiplo.

Il massimo comune divisore

Dati due interi a e b , un **divisore comune** è un intero che divide sia a sia b . Se i due numeri non sono entrambi nulli, i divisori comuni sono in numero finito e ne esiste uno più grande degli altri. La definizione che adottiamo è però leggermente più forte di «il più grande», ed è quella che funziona bene anche negli ambienti in cui non c'è un ordine.

DEFINIZIONE: MASSIMO COMUNE DIVISORE

Siano $a, b \in \mathbb{Z}$ non entrambi nulli. Un **massimo comune divisore** di a e b è un intero d tale che:

- (1) $d \mid a$ e $d \mid b$ (d è un divisore comune);
- (2) ogni divisore comune x (cioè $x \mid a$ e $x \mid b$) divide d (d è multiplo di ogni altro divisore comune).

Il massimo comune divisore è unico a meno del segno: se d e d' soddisfano entrambi la definizione, ciascuno divide l'altro e, per l'antisimmetria della divisibilità (capitolo 11), $d' = \pm d$. Per convenzione si sceglie quello positivo, che si indica con $\text{MCD}(a, b)$ (in inglese gcd, *greatest common divisor*). Con questa convenzione $\text{MCD}(a, b)$ è davvero il più grande dei divisori comuni, perché per la proprietà (2) ogni divisore comune x divide d e quindi $|x| \leq d$.

Esempio. I divisori positivi di 330 sono 1, 2, 3, 5, 6, 10, 11, 15, 22, 30, 33, 55, 66, 110, 165, 330; quelli di 156 sono 1, 2, 3, 4, 6, 12, 13, 26, 39, 52, 78, 156. I divisori comuni sono 1, 2, 3, 6: il più grande è 6 e, come richiesto dalla definizione, tutti gli altri lo dividono. Dunque $\text{MCD}(330, 156) = 6$.

Alcune osservazioni immediate: $\text{MCD}(a, b) = \text{MCD}(|a|, |b|)$, $\text{MCD}(a, b) = \text{MCD}(b, a)$, $\text{MCD}(a, 0) = |a|$ per $a \neq 0$ (ogni intero divide 0), e $\text{MCD}(a, b) = |b|$ se $b \mid a$. Per tre o più numeri si procede a coppie: $\text{MCD}(a, b, c) = \text{MCD}(\text{MCD}(a, b), c)$.

Il metodo imparato a scuola, scomporre i numeri in fattori primi e prendere i fattori comuni con l'esponente minore, è corretto ma richiede di fattorizzare, che è un'operazione molto costosa quando i numeri sono grandi. L'algoritmo di Euclide calcola il MCD senza fattorizzare, ed è uno dei più antichi algoritmi ancora in uso.

L'algoritmo di Euclide

Descritto negli *Elementi* di Euclide (tra la fine del IV e l'inizio del III secolo a.C.), l'algoritmo si basa su un'osservazione semplice.

LEMMA DI EUCLIDE PER IL MCD

Se $a = qb + r$ con a, b, q, r interi, allora gli insiemi dei divisori comuni di a e b e dei divisori comuni di b e r coincidono. In particolare $\text{MCD}(a, b) = \text{MCD}(b, r)$.

Dimostrazione. Se d divide a e b , allora divide $r = a - qb$ (combinazione lineare, capitolo 11). Viceversa, se d divide b e r , allora divide $a = qb + r$. I due insiemi di divisori coincidono, e quindi hanno lo stesso elemento massimo. ■

Prendiamo $a \geq b > 0$. Se r è il resto della divisione di a per b , con $0 \leq r < b$, allora $\text{MCD}(a, b) = \text{MCD}(b, r)$: si è passati a una coppia più piccola. Si ripete finché il resto è 0; a quel punto $\text{MCD}(x, 0) = x$. In formule, si costruisce la successione

$$x_1 = a, x_2 = b, x_{k+1} = \text{resto della divisione di } x_{k-1} \text{ per } x_k$$

che si ferma sul primo resto nullo; l'ultimo resto non nullo è il MCD. Ecco il codice, in versione iterativa e ricorsiva (in Python; l'operatore % dà il resto e, per numeri non negativi, coincide con il resto matematico).

```
def euclide(a, b):          # versione iterativa
    while b != 0:
        a, b = b, a % b
    return a

def euclide_ric(a, b):      # versione ricorsiva
    if b == 0:
        return a
    return euclide_ric(b, a % b)
```

Esempio. Calcoliamo $\text{MCD}(330, 156)$, con una riga per ciascuna divisione.

PASSO	DIVISIONE	RESTO
1	$330 = 2 \cdot 156 + 18$	18
2	$156 = 8 \cdot 18 + 12$	12
3	$18 = 1 \cdot 12 + 6$	6
4	$12 = 2 \cdot 6 + 0$	0

Tabella 1. L'algoritmo di Euclide su 330 e 156: l'ultimo resto non nullo, 6, è il MCD.

Verifica: $330 = 6 \cdot 55$ e $156 = 6 \cdot 26$, con $55 = 5 \cdot 11$ e $26 = 2 \cdot 13$ senza fattori in comune. Un altro esempio classico è $\text{MCD}(1071, 462)$: $1071 = 2 \cdot 462 + 147$, $462 = 3 \cdot 147 + 21$, $147 = 7 \cdot 21 + 0$, quindi il MCD è 21. Se $b \mid a$ l'algoritmo si ferma subito: $\text{MCD}(a, b) = b$.



Figura 1. L'algoritmo di Euclide come piastrellatura: un rettangolo 330×156 si riempie con 2 quadrati di lato 156, poi con 8 di lato 18, 1 di lato 12 e 2 di lato 6. Il lato dell'ultimo quadrato, 6, è il MCD.

CORRETTEZZA E TERMINAZIONE

La **correttezza** segue dal lemma: a ogni passo il MCD della coppia non cambia, e quando $b = 0$ il MCD è a (per induzione sul numero di passi). La **terminazione** è garantita perché i resti formano una successione strettamente decrescente di numeri naturali, $0 \leq r < b$, e per il buon ordinamento non può decrescere all'infinito. Se $a < b$ il primo passo scambia i due numeri (il resto di a diviso b è a stesso). Per numeri negativi basta usare i valori assoluti. L'unico caso non definito è $\text{MCD}(0, 0)$: per convenzione si può porre 0, ed è il valore che il codice restituisce.

QUANTO È VELOCE

Il numero di divisioni è piccolo anche per numeri enormi. Se $b \leq a/2$, dopo un passo il primo parametro è almeno dimezzato. Se invece $b > a/2$, il quoziente è 1 e il resto $a - b$ è minore di $a/2$, quindi dopo due passi il primo parametro è comunque più piccolo di $a/2$. Perciò il primo parametro si dimezza almeno ogni due passi e il numero di divisioni è al più circa $2 \cdot \log_2 a$: per un numero di 100 cifre decimali (circa 332 bit) non sono più di 664 divisioni.

Si può essere più precisi. Il **teorema di Lamé** (1844) afferma che se con $a > b > 0$ l'algoritmo esegue N divisioni, allora $a \geq F_{N+2}$, dove F_n è l' n -esimo numero di Fibonacci (1, 1, 2, 3, 5, 8, 13, ...). Il caso peggiore si ha quindi con due numeri di Fibonacci consecutivi, in cui tutti i quozienti valgono 1: per esempio $\text{MCD}(89, 55)$ richiede 9 divisioni, ciascuna con quoziente 1 tranne l'ultima. Poiché F_n cresce come φ^n , con $\varphi = (1 + \sqrt{5})/2 \approx 1,618$, ne segue che il numero di divisioni è al più circa 4,8 volte il numero di cifre decimali di a , contro le circa 6,6 volte della stima per dimezzamento: per un numero di 100 cifre, al massimo circa 480 divisioni.

L'identità di Bézout

Ripercorrendo l'algoritmo a ritroso si scopre una cosa notevole: il MCD si può scrivere come combinazione lineare dei due numeri. Per 330 e 156: $6 = 18 - 12 = 18 - (156 - 8 \cdot 18) = 9 \cdot 18 - 156 = 9 \cdot (330 - 2 \cdot 156) - 156 = 9 \cdot 330 - 19 \cdot 156$. Infatti $9 \cdot 330 = 2970$, $19 \cdot 156 = 2964$ e la differenza è 6.

TEOREMA (IDENTITÀ DI BÉZOUT)

Siano $a, b \in \mathbb{Z}$ non entrambi nulli. Esistono due interi h, k tali che

$$\text{MCD}(a, b) = a \cdot h + b \cdot k.$$

Dimostrazione. Si lavora con l'algoritmo di Euclide, che produce $r_1 = a$, $r_2 = b$, e poi i resti successivi r_i . Mostriamo per induzione che ogni resto r_i è combinazione lineare di a e b . Per $r_1 = 1 \cdot a + 0 \cdot b$ e $r_2 = 0 \cdot a + 1 \cdot b$ è vero. Se $r_{i-1} = s_{i-1}a + t_{i-1}b$ e $r_i = s_i a + t_i b$, allora il resto successivo è $r_{i+1} = r_{i-1} - q_i r_i = (s_{i-1} - q_i s_i)a + (t_{i-1} - q_i t_i)b$, ancora una combinazione. In particolare lo è l'ultimo resto non nullo, cioè il MCD. ■

La dimostrazione è anche un metodo di calcolo, l'**algoritmo di Euclide esteso**: si affiancano ai resti i coefficienti s, t tali che $r = s \cdot 330 + t \cdot 156$, con la regola «nuovo = precedente - quoziente $\times$ corrente» applicata a resti e coefficienti.

i	QUOZIENTE Q	RESTO R_i	S_i	T_i	VERIFICA
1		330	1	0	$1 \cdot 330 + 0 \cdot 156 = 330$
2		156	0	1	$0 \cdot 330 + 1 \cdot 156 = 156$
3	2	18	1	-2	$1 \cdot 330 + -2 \cdot 156 = 18$
4	8	12	-8	17	$-8 \cdot 330 + 17 \cdot 156 = 12$
5	1	6	9	-19	$9 \cdot 330 + -19 \cdot 156 = 6$
6	2	0	-26	55	$-26 \cdot 330 + 55 \cdot 156 = 0$

Tabella 2. Algoritmo di Euclide esteso per 330 e 156. L'ultimo resto non nullo, 6, è $9 \cdot 330 - 19 \cdot 156$.

I coefficienti non sono unici: se (h, k) è una soluzione, lo sono anche $(h + t \cdot b/d, k - t \cdot a/d)$ per ogni intero t , dove $d = \text{MCD}(a, b)$. Per 330 e 156 si hanno le coppie $(9, -19)$, $(35, -74)$, $(-17, 36)$, ... Un'altra utile caratterizzazione è la seguente.

MCD COME MINIMO POSITIVO

$\text{MCD}(a, b)$ è il **più piccolo intero positivo** della forma $ah + bk$ con $h, k \in \mathbb{Z}$.

Infatti sia m il minimo positivo di questo tipo (esiste per il buon ordinamento) e sia $d = \text{MCD}(a, b)$. Per Bézout d è di quella forma, quindi $m \leq d$. D'altra parte d divide a e b , quindi divide $m = ah + bk$, da cui $d \leq m$. Dunque $m = d$.

EQUAZIONI LINEARI IN DUE INCOGNITE

L'identità di Bézout risolve completamente le equazioni diofantee lineari $ax + by = c$ da risolvere in interi: **c'è una soluzione se e solo se $\text{MCD}(a, b)$ divide c** . Se $d \nmid c$ non può esserci soluzione, perché d divide il primo membro. Se $c = dm$, si moltiplicano per m i coefficienti di Bézout. Per esempio $330x + 156y = 12$: poiché $12 = 2 \cdot 6$, una soluzione è $x = 18, y = -38$ (infatti $5940 - 5928 = 12$), mentre $330x + 156y = 10$ non ha soluzioni intere perché $6 \nmid 10$. Queste equazioni ritorneranno nelle congruenze (capitolo 14), dove servono a calcolare gli inversi.

Numeri coprimi

DEFINIZIONE: NUMERI COPRIMI

Due interi a e b non entrambi nulli sono **coprimi** (o primi tra loro) se $\text{MCD}(a, b) = 1$, cioè se i loro unici divisori comuni sono 1 e -1 .

Per l'identità di Bézout, se a e b sono coprimi esistono h, k con $ah + bk = 1$. Vale anche il viceversa, che è utilissimo.

TEOREMA (CRITERIO DI COPRIMALITÀ)

Se esistono $h, k \in \mathbb{Z}$ con $ah + bk = 1$, allora $\text{MCD}(a, b) = 1$.

Dimostrazione. Sia $d = \text{MCD}(a, b)$. Poiché $d \mid a$ e $d \mid b$, d divide $ah + bk = 1$, e l'unico divisore positivo di 1 è 1. Quindi $d = 1$. ■

Il criterio dà in un colpo solo dimostrazioni eleganti delle tre proprietà seguenti, che sono la ragione dell'importanza dei numeri coprimi.

TEOREMA (PROPRIETÀ DEI COPRIMI)

(P1) Due interi consecutivi sono coprimi.

(P2) Se $c \mid ab$ e c è coprimo con a , allora $c \mid b$.

(P3) Se $a \mid c$ e $b \mid c$ e a, b sono coprimi, allora $ab \mid c$.

Dimostrazione. (P1) Da $1 \cdot (n + 1) + (-1) \cdot n = 1$ e dal criterio, n e $n + 1$ sono coprimi.

(P2) Da $c \mid ab$ si ha $ab = ch$ per qualche h , e da $\text{MCD}(c, a) = 1$ si ha $ka + k'c = 1$. Moltiplicando per b : $b = kab + k'cb = kch + k'cb = c(kh + k'b)$, quindi $c \mid b$.

(P3) Siano $c = ah = bk$ e $ah' + bk' = 1$. Moltiplicando per c : $c = ah'c + bk'c = ah'(bk) + bk'(ah) = ab(h'k + k'h)$, quindi $ab \mid c$. ■

L'ipotesi di coprimalità non si può togliere. Per (P2): $9 \mid 3 \cdot 6 = 18$ ma $9 \nmid 3$ e $9 \nmid 6$, e infatti 9 non è coprimo né con 3 né con 6 (il MCD è 3 in entrambi i casi). Per (P3): $4 \mid 12$ e $6 \mid 12$, ma $4 \cdot 6 = 24 \nmid 12$, e infatti $\text{MCD}(4, 6) = 2$. In generale, (P2) e (P3) sono il motivo per cui si possono «semplificare» i fattori coprimi, e (P3) si usa per i criteri di

divisibilità composti: un numero è divisibile per 6 se e solo se lo è per 2 e per 3, che sono coprimi, ma non è sufficiente che lo sia per 2 e per 4.

Il minimo comune multiplo

DEFINIZIONE: MINIMO COMUNE MULTIPOLO

Siano $a, b \in \mathbb{Z}$ **entrambi non nulli**. Il **minimo comune multiplo** $\text{mcm}(a, b)$ è l'intero positivo m tale che:

- (1) $a \mid m$ e $b \mid m$ (m è un multiplo comune);
- (2) ogni multiplo comune x di a e b è un multiplo di m .

Se uno dei due numeri è 0 l'unico multiplo comune è 0, e non esiste un multiplo comune positivo: per questo si richiede che entrambi siano diversi da 0 (ci si limita a coppie di numeri non nulli, a differenza del MCD). La proprietà (2) dice che m è non solo il più piccolo ma divide tutti gli altri multipli comuni. Il legame con il MCD è semplice e molto comodo.

TEOREMA

Per ogni coppia di interi non nulli: $\text{MCD}(a, b) \cdot \text{mcm}(a, b) = |ab|$.

Dimostrazione. Sia $d = \text{MCD}(a, b)$ e scriviamo $a = da'$, $b = db'$. Allora a' e b' sono coprimi (se avessero un divisore comune $e > 1$, de sarebbe un divisore comune di a e b più grande di d). Poniamo $m = da'b' = |ab|/d$, che è positivo se prendiamo i valori assoluti. È un multiplo comune: $m = ab' = ba'$ (a meno del segno). Sia ora x un multiplo comune: $x = au = bv$, cioè $da'u = db'v$, da cui $a'u = b'v$. Quindi a' divide $b'v$ e, essendo coprimo con b' , divide v per (P2): $v = a't$. Allora $x = bv = db'a't = mt$, multiplo di m . ■

Esempio. $\text{mcm}(330, 156) = 330 \cdot 156/6 = 51480/6 = 8580$. Il calcolo del mcm si riduce così a quello del MCD, e quindi all'algoritmo di Euclide (conviene dividere prima: $330/6 \cdot 156 = 55 \cdot 156 = 8580$, per non lavorare con numeri inutilmente grandi). Se a e b sono coprimi, $\text{mcm}(a, b) = |ab|$: per esempio $\text{mcm}(4, 9) = 36$. Per più numeri si procede a coppie: $\text{mcm}(a, b, c) = \text{mcm}(\text{mcm}(a, b), c)$.

UN'APPLICAZIONE TIPICA

Due luci lampeggiano ogni 12 e ogni 18 secondi e sono ora accese insieme. Si riaccenderanno insieme dopo $\text{mcm}(12, 18) = 12 \cdot 18/6 = 36$ secondi. Lo stesso ragionamento serve per la sincronizzazione di processi periodici e per sommare frazioni con denominatori diversi, usando come denominatore comune il mcm.

Numeri primi e criteri di divisibilità

I numeri primi, il teorema fondamentale dell'aritmetica, l'infinità dei primi, la loro distribuzione, il crivello di Eratostene, i test di primalità e i criteri di divisibilità.

Numeri primi

DEFINIZIONE: NUMERO PRIMO

Un intero $p \geq 2$ è **primo** se i suoi unici divisori positivi sono 1 e p . Un intero $n \geq 2$ che non è primo si dice **composto**: si scrive $n = ab$ con $1 < a, b < n$.

I primi sono dunque 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ... (sotto 100 ce ne sono 25). Il numero 1 non è primo e nemmeno composto, e 2 è l'unico primo pari. In $\mathbb{Z}$ si potrebbero chiamare primi anche gli opposti $-2, -3, \dots$, cioè gli interi che hanno solo i divisori banali ± 1 e $\pm p$, ma la definizione tradizionale, e quella che useremo, riguarda i naturali.

Se p è primo e a è un intero qualunque, $\text{MCD}(p, a)$ è un divisore positivo di p , quindi vale 1 oppure p : o p divide a , oppure p e a sono coprimi. Questa dicotomia dà la proprietà che rende speciali i primi.

LEMMA DI EUCLIDE

Se un primo p divide un prodotto ab , allora p divide almeno uno dei due fattori. Più in generale, se $p \mid a_1 a_2 \dots a_n$ allora $p \mid a_i$ per qualche i .

Dimostrazione. Se $p \nmid a$, allora $\text{MCD}(p, a) = 1$, e per la proprietà (P2) dei coprimi (capitolo 12) $p \mid b$. Per più fattori si procede per induzione su n : se $p \mid (a_1 \dots a_{n-1})a_n$, allora p divide a_n oppure divide il prodotto dei primi $n-1$ fattori, e in questo caso si applica l'ipotesi induttiva. ■

Il lemma *non vale* per i numeri composti: $6 \mid 3 \cdot 4 = 12$ ma $6 \nmid 3$ e $6 \nmid 4$. È una caratteristica dei primi, ed è la chiave della prossima dimostrazione.

Il teorema fondamentale dell'aritmetica

TEOREMA DI FATTORIZZAZIONE

Ogni intero $n \geq 2$ si scrive come prodotto di numeri primi, e in modo **unico** a meno dell'ordine dei fattori. Cioè se $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ con tutti i p_i e q_j primi, allora $r = s$ e, riordinando, $p_i = q_i$ per ogni i .

Un primo conta come prodotto di un solo fattore. Raggruppando i fattori uguali si scrive $n = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$ con $p_1 < \dots < p_k$ primi ed esponenti $e_i \geq 1$: è la **fattorizzazione canonica**. Per esempio $330 = 2 \cdot 3 \cdot 5 \cdot 11$, $156 = 2^2 \cdot 3 \cdot 13$, $360 = 2^3 \cdot 3^2 \cdot 5$.

Esistenza. Per assurdo, se esistessero interi ≥ 2 non prodotto di primi, per il buon ordinamento ci sarebbe un minimo s tra essi. Non è primo (un primo è prodotto di se stesso), quindi $s = dc$ con $1 < d, c < s$. Ma d e c sono minori di s , quindi sono prodotti di primi, e allora lo è anche s : assurdo. ■

Unicità. Per induzione su r . Se $r = 1$, $n = p_1$ è primo e $p_1 = q_1 q_2 \dots q_s$: q_1 divide il primo p_1 ed è maggiore di 1, quindi $q_1 = p_1$; se fosse $s > 1$, semplificando resterebbe $1 = q_2 \dots q_s > 1$, assurdo. Dunque $s = 1$. Passo induttivo: sia $n = p_1 \dots p_{r+1} = q_1 \dots q_s$. Il primo p_1 divide $q_1 \dots q_s$, quindi per il lemma di Euclide divide un q_j , e poiché questo è primo, $p_1 = q_j$. Riordinando, $p_1 = q_1$; semplificando si ottiene $p_2 \dots p_{r+1} = q_2 \dots q_s$. Il primo membro è un prodotto di $r \geq 1$ primi, quindi è maggiore di 1 e il secondo membro non è vuoto ($s \geq 2$). Per ipotesi induttiva $r = s - 1$ e i fattori

coincidono a meno dell'ordine. ■

PERCHÉ NON È OVVIO

L'unicità sembra scontata, ma non vale in ogni contesto numerico. Nell'insieme dei numeri $a + b\sqrt{-5}$ con a, b interi si ha $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, due scomposizioni in fattori che non si possono scomporre ulteriormente e sono diverse. Nei naturali l'unicità dipende dal lemma di Euclide, cioè dalla teoria del MCD.

CONSEGUENZE DELLA FATTORIZZAZIONE

- **MCD e mcm.** Se a e b sono scritti con gli stessi primi (ammettendo esponenti nulli), $\text{MCD}(a, b)$ è il prodotto dei primi con l'esponente *minimo* e $\text{mcm}(a, b)$ quello con l'esponente *massimo*. Per $330 = 2 \cdot 3 \cdot 5 \cdot 11$ e $156 = 2^2 \cdot 3 \cdot 13$: $\text{MCD} = 2 \cdot 3 = 6$ e $\text{mcm} = 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 = 8580$, come già trovato con Euclide. Poiché $\min + \max =$ somma degli esponenti, si ritrova $\text{MCD} \cdot \text{mcm} = ab$.
- **Divisori.** I divisori positivi di $n = p_1^{e_1} \dots p_k^{e_k}$ sono esattamente i numeri $p_1^{f_1} \dots p_k^{f_k}$ con $0 \leq f_i \leq e_i$, quindi ne esistono $(e_1 + 1) \dots (e_k + 1)$. Per $360 = 2^3 \cdot 3^2 \cdot 5$ sono $4 \cdot 3 \cdot 2 = 24$.
- **Quadrati.** n è un quadrato perfetto se e solo se tutti gli esponenti sono pari. Da qui una seconda dimostrazione che $\sqrt{2}$ non è razionale: se $a^2 = 2b^2$, l'esponente di 2 nella fattorizzazione sarebbe pari a sinistra e dispari a destra, in contraddizione con l'unicità. Lo stesso argomento mostra che $\sqrt{n}$ è irrazionale per ogni n che non sia un quadrato perfetto.

I numeri primi sono infiniti

TEOREMA DI EUCLIDE

Esistono infiniti numeri primi.

Dimostrazione. Supponiamo per assurdo che i primi siano finiti, $p_1 = 2, p_2 = 3, \dots, p_n$, e consideriamo $N = p_1 p_2 \dots p_n + 1$. Poiché $N \geq 2$, per il teorema di fattorizzazione ha un divisore primo p , che deve essere uno dei p_i . Ma allora p divide sia N sia il prodotto $p_1 \dots p_n$, e quindi divide la loro differenza, che è 1: assurdo. ■

Attenzione a un'imprecisione diffusa: la dimostrazione *non* dice che $p_1 \dots p_n + 1$ è primo. Per esempio $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$, che è composto: dice solo che ha un fattore primo che non è nella lista. La stessa idea mostra che esistono intervalli arbitrariamente lunghi di numeri consecutivi composti: gli $n - 1$ numeri $n! + 2, n! + 3, \dots, n! + n$ sono tutti composti, perché $n! + k$ è divisibile per k (per $2 \leq k \leq n$).

Come sono distribuiti i primi

I primi sono infiniti, ma quanti ce ne sono fino a un certo n ? Sia $\pi(n)$ il numero dei primi minori o uguali a n . Il **teorema dei numeri primi** (dimostrato nel 1896, indipendentemente, da Hadamard e de la Vallée Poussin) afferma che $\pi(n)$ si comporta come $n/\ln n$, nel senso che

$$\lim_{n \rightarrow \infty} \pi(n) / (n / \ln n) = 1$$

Ne segue che $\pi(n)$ è compresa tra $c_1 n/\ln n$ e $c_2 n/\ln n$ per due costanti positive c_1 e c_2 (risultato che Chebyshev aveva già dimostrato a metà dell'Ottocento). In termini pratici, un numero scelto a caso intorno a n è primo con probabilità circa $1/\ln n$: per numeri di 100 cifre, circa 1 su 230. Per questo è facile trovare primi grandi, purché si abbia un buon test di primalità.

n	$\pi(n)$ effettivo	$n / \ln n$	Rapporto
10^2	25	22	1,151
10^3	168	145	1,161
10^4	1.229	1.086	1,132
10^5	9.592	8.686	1,104
10^6	78.498	72.382	1,084

Tabella 1. Primi fino a n e stima del teorema dei numeri primi: il rapporto tende lentamente a 1.

Un risultato più elementare è il **teorema di Bertrand e Chebyshev** (il «postulato di Bertrand», dimostrato da Chebyshev nel 1852): per ogni $n \geq 2$ esiste un primo p con $n < p < 2n$. Per $n = 10$, per esempio, i primi tra 10 e 20 sono 11, 13, 17, 19. Dal teorema si ricava di nuovo che i primi sono infiniti, e che il primo successivo a un primo p è minore di $2p$. Esistono invece moltissime questioni aperte sulla distribuzione dei primi, come la congettura dei primi gemelli, che vedremo nel capitolo 17.

Test di primalità per divisioni successive

Come si verifica se n è primo? Controllando che non abbia divisori non banali. Basta cercarli tra 2 e $\sqrt{n}$. Infatti se n è composto, $n = ab$ con $1 < a \leq b$, e allora $a^2 \leq ab = n$, cioè $a \leq \sqrt{n}$. Per esempio, per stabilire che 97 è primo basta controllare i divisori fino a 9 (cioè 2, 3, 5, 7), perché $10^2 > 97$.

```
def primo(x):
    if x < 2:
        return False
    d = 2
    while d * d <= x:
        if x % d == 0:
            return False
        d += 1
    return True
```

Il metodo è corretto ma lento: per un numero di D cifre servono circa $10^{D/2}$ divisioni, un tempo esponenziale nella lunghezza dell'input. Con 100 cifre sarebbero circa 10^{50} divisioni, che a un miliardo di divisioni al secondo richiederebbero circa $3 \cdot 10^{33}$ anni. Nelle applicazioni crittografiche si usano primi di molte centinaia di cifre (per RSA, oggi, di 1024 bit, cioè 309 cifre decimali) e si ricorre a test molto più veloci, come il **test di Miller e Rabin**, probabilistico, e l'algoritmo **AKS** (Agrawal, Kayal e Saxena, 2002), il primo test deterministico di durata polinomiale. Questi metodi esulano dallo scopo del corso.

Il crivello di Eratostene

Se serve l'elenco di *tutti* i primi fino a n conviene un algoritmo molto antico, attribuito a Eratostene di Cirene (vissuto all'incirca tra il 276 e il 194 a.C., noto anche per aver misurato con ottima approssimazione la circonferenza della Terra). Si scrivono i numeri da 2 a n , poi si ripete: si prende il primo numero non ancora cancellato, lo si lascia e si cancellano tutti i suoi multipli. Ci si ferma quando il numero preso supera $\sqrt{n}$. I numeri non cancellati sono i primi.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figura 1. Il crivello di Eratostene per $n = 100$: in verde i 25 primi; gli altri numeri sono cancellati dai multipli di 2, 3, 5 e 7 (il più grande primo $\leq \sqrt{100} = 10$).

Perché funziona: un numero composto $m \leq n$ ha un fattore primo $p \leq \sqrt{m} \leq \sqrt{n}$ ed è quindi cancellato come multiplo di p (o prima); un primo non è mai cancellato, perché non è multiplo di nessun altro primo. Si può partire a cancellare da p^2 , perché i multipli più piccoli di p hanno un fattore primo minore e sono già stati cancellati. Il numero di operazioni è dell'ordine di $n \cdot \ln \ln n$, quasi lineare. Un'implementazione:

```
def crivello(n):
    primo = [True] * (n + 1)
    primo[0] = False
    if n >= 1:
        primo[1] = False
    d = 2
    while d * d <= n:
        if primo[d]:
            for m in range(d * d, n + 1, d):
                primo[m] = False
        d += 1
    return [k for k in range(2, n + 1) if primo[k]]
```

Criteri di divisibilità

Per alcuni divisori m si può stabilire se $m \mid n$ guardando le cifre di n senza fare la divisione. Scriviamo n in base 10 come $n = a_k 10^k + \dots + a_1 10 + a_0$, dove a_0 è la cifra delle unità, e come $n = 10q + r$, dove $r = a_0$ è la cifra delle unità e q il numero che si ottiene togliendola.

DIVISORE	CRITERIO	PERCHÉ
2	ultima cifra 0, 2, 4, 6, 8	$2 \mid 10$, quindi $2 \mid n$ se e solo se $2 \mid r$
5	ultima cifra 0 oppure 5	$5 \mid 10$, quindi $5 \mid n$ se e solo se $5 \mid r$
4, 25	le ultime due cifre formano un multiplo di 4 (di 25: 00, 25, 50, 75)	$n = 100Q + u$, con u ultime due cifre, e $4 \mid 100$, $25 \mid 100$
8	le ultime tre cifre formano un multiplo di 8	$8 \mid 1000$
3, 9	la somma delle cifre è multipla di 3 (di 9)	$n - (\text{somma cifre})$ è multiplo di 9
11	differenza tra somma delle cifre di posto dispari e di posto pari è multipla di 11	$10^j - (-1)^j$ è multiplo di 11 (vedi sotto)

DIVISORE	CRITERIO	PERCHÉ
7, 13, 17, 19, 23	$q + ar$ è multiplo del primo, con a della tabella 3	teorema sotto
6, 12, 15	divisibile per 2 e 3 (3 e 4; 3 e 5)	(P3) dei coprimi: i fattori sono coprimi

Tabella 2. I principali criteri di divisibilità.

IL CASO DI 3 E DI 9

Sia m la somma delle cifre di n . Per ogni $i \geq 1$ il numero $10^i - 1$ è formato da i cifre uguali a 9, quindi $10^i - 1 = 9b_i$, dove $b_i = 11...1$ (i cifre uguali a 1). Allora

$$n - m = \sum a_i(10^i - 1) = 9 \cdot \sum a_i b_i$$

è un multiplo di 9. Poiché $n = (n - m) + m$, per la proprietà della somma n è divisibile per 9 se e solo se lo è m ; lo stesso vale per 3, perché $3 \mid 9$. Se si ripete la somma delle cifre fino ad avere una sola cifra si ottiene la **radice numerica** $\rho(n)$ di n (per $n > 0$). Per esempio $\rho(198) = 1 + 9 + 8 \rightarrow 1 + 8 \rightarrow 9$, $\rho(239) = 14 \rightarrow 5$, $\rho(1137) = 12 \rightarrow 3$. Dato che a ogni passo si sottrae un multiplo di 9, $n - \rho(n)$ è sempre multiplo di 9. Quindi $n > 0$ è divisibile per 3 se e solo se $\rho(n)$ è 3, 6 o 9, ed è divisibile per 9 se e solo se $\rho(n) = 9$. Da qui: 198 è divisibile per 9, 1137 per 3 ma non per 9, 239 per nessuno dei due.

La proprietà $n - m$ multiplo di 9 vale per ogni n , anche non divisibile per 9: $199 - 19 = 180$, $640 - 10 = 630$, $1129 - 13 = 1116$, tutti multipli di 9.

IL CASO DI 11

Per ogni i il numero $10^i - (-1)^i$ è multiplo di 11, perché per ogni x, y e $i \geq 1$ si ha $x^i - y^i = (x - y)(x^{i-1} + x^{i-2}y + \dots + y^{i-1})$, e qui $x - y = 10 + 1 = 11$. Perciò n differisce da $a_0 - a_1 + a_2 - \dots$ (somma alternata delle cifre, a partire dalle unità) per un multiplo di 11, e $11 \mid n$ se e solo se 11 divide la somma alternata. Basta quindi sommare le cifre di posto dispari e quelle di posto pari e fare la differenza: per 2805 si ha $(2 + 0) - (8 + 5) = -11$, multiplo di 11; per 14894 si ha $(1 + 8 + 4) - (4 + 9) = 0$. Se il numero di cifre è pari, contare le posizioni da sinistra o da destra cambia al più il segno della differenza, che è irrilevante. Casi speciali: i numeri con cifre a coppie uguali (112233) e i palindromi con un numero pari di cifre (12344321) sono multipli di 11.

I CRITERI PER 7, 13, 17, 19, 23

TEOREMA (CRITERIO CON LA CIFRA DELLE UNITÀ)

Siano $n = 10q + r$ con $0 \leq r \leq 9$, p un intero ≥ 2 e a un intero tale che $10a - 1$ sia multiplo di p . Allora $p \mid n$ se e solo se $p \mid (q + ar)$.

Dimostrazione. Poniamo $10a = 1 + pm$. Allora $an = 10aq + ar = (1 + pm)q + ar = (q + ar) + pmq$. Se $p \mid n$, allora p divide an e quindi anche $an - pmq = q + ar$. Viceversa, se $p \mid q + ar$, allora $p \mid an$. Dall'uguaglianza $10a - pm = 1$ e dal criterio di coprimialità, a e p sono coprimi, e per (P2) $p \mid n$. ■

Il coefficiente a è un numero che moltiplicato per 10 dà un risultato di una unità più grande di un multiplo di p : è sufficiente cercarlo a mano, oppure trovarlo con l'identità di Bézout applicata a 10 e p (per questo p non può dividere 10).

p	3	7	9	11	13	17	19	23	29	31
a	1	-2	1	-1	4	-5	2	7	3	-3

Tabella 3. Il coefficiente a del criterio « $q + ar$ » per alcuni divisori.

Esempi. Per 7: $2247 \rightarrow 224 - 2 \cdot 7 = 210 = 7 \cdot 30$, quindi $7 \mid 2247$; $161 \rightarrow 16 - 2 = 14 = 7 \cdot 2$. Per un numero grande si ripete la riduzione, come si fa con 96577 ($q = 9657$, $r = 7$):

- per 13: $9657 + 4 \cdot 7 = 9685 \rightarrow 968 + 20 = 988 \rightarrow 98 + 32 = 130 \rightarrow 13 + 0 = 13$: multiplo di 13;
- per 17: $9657 - 5 \cdot 7 = 9622 \rightarrow 962 - 10 = 952 \rightarrow 95 - 10 = 85 \rightarrow 8 - 25 = -17$: multiplo di 17;
- per 19: $9657 + 2 \cdot 7 = 9671 \rightarrow 967 + 2 = 969 \rightarrow 96 + 18 = 114 \rightarrow 11 + 8 = 19$: multiplo di 19;
- per 23: $9657 + 7 \cdot 7 = 9706 \rightarrow 970 + 42 = 1012 \rightarrow 101 + 14 = 115 \rightarrow 11 + 35 = 46 = 2 \cdot 23$: multiplo di 23.

In effetti $96577 = 13 \cdot 17 \cdot 19 \cdot 23$. Il criterio funziona perché ogni passo sostituisce il numero con uno più piccolo e con lo stesso comportamento rispetto alla divisibilità per p ; ci si ferma quando si riconosce un multiplo di p (o si capisce che non lo è).

ESERCIZI SVOLTI

Esempio. 525 è divisibile per 3 (somma delle cifre 12), per 5 (termina con 5) e per 7 ($52 - 2 \cdot 5 = 42 = 7 \cdot 6$), non lo è per 9 (12 non è multiplo di 9), per 11 ($(5 + 5) - 2 = 8$), per 13 ($52 + 4 \cdot 5 = 72$, e $7 + 4 \cdot 2 = 15$, $1 + 4 \cdot 5 = 21$ non è multiplo di 13), per 17 ($52 - 25 = 27$), per 19 ($52 + 10 = 62$) e per 23 ($52 + 35 = 87 = 3 \cdot 23 + 18$). Infatti $525 = 3 \cdot 5^2 \cdot 7$.

La tabella seguente applica i criteri a sei coppie di numeri consecutivi e conferma, in ciascuna, la proprietà (P1) del capitolo 12: i due numeri non hanno fattori primi in comune.

NUMERO	DIVISIBILE PER (TRA 2, 3, 5, 7, 9, 11, 13, 17, 19, 23)	FATTORIZZAZIONE
119	7, 17	$7 \cdot 17$
120	2, 3, 5	$2^3 \cdot 3 \cdot 5$
195	3, 5, 13	$3 \cdot 5 \cdot 13$
196	2, 7	$2^2 \cdot 7^2$
231	3, 7, 11	$3 \cdot 7 \cdot 11$
232	2	$2^3 \cdot 29$
399	3, 7, 19	$3 \cdot 7 \cdot 19$
400	2, 5	$2^4 \cdot 5^2$
437	19, 23	$19 \cdot 23$
438	2, 3	$2 \cdot 3 \cdot 73$
532	2, 7, 19	$2^2 \cdot 7 \cdot 19$
533	13	$13 \cdot 41$

Tabella 4. Divisibilità e fattorizzazione di sei coppie di interi consecutivi.

Congruenze e aritmetica modulare

La congruenza modulo m come relazione di equivalenza, le classi di resto, il calcolo con i resti, le potenze modulari e l'inverso modulare.

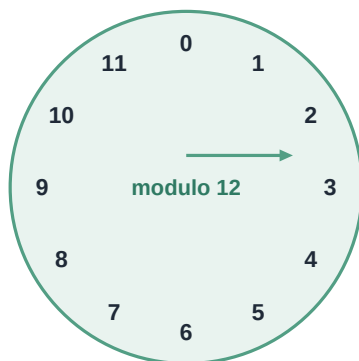
Congruenza modulo m

L'aritmetica modulare è il calcolo sui **resti** della divisione per un numero fissato. Si usa tutti i giorni: se sono le 10 e passano 5 ore, sono le 3 e non le 15, perché sull'orologio a 12 ore i numeri che differiscono di un multiplo di 12 indicano la stessa posizione. L'idea è di considerare *equivalenti* due interi che hanno lo stesso resto rispetto a un divisore fissato, detto **modulo**.

DEFINIZIONE: CONGRUENZA MODULO m

Fissato un intero m , due interi a e b si dicono **congruenti modulo m** , e si scrive $a \equiv b \pmod{m}$, se m divide la loro differenza: $m \mid (a - b)$. Se questo non accade si scrive $a \not\equiv b \pmod{m}$.

Equivalentemente, per $m \neq 0$, $a \equiv b \pmod{m}$ se e solo se a e b hanno lo **stesso resto** nella divisione per m , cioè $a \bmod m = b \bmod m$. Infatti se entrambi hanno resto r , $a = q_1 m + r$ e $b = q_2 m + r$, quindi $a - b = (q_1 - q_2)m$. Viceversa, se $a - b = km$ e $b = qm + r$ con $0 \leq r < |m|$, allora $a = (q + k)m + r$ e, per l'unicità del resto, anche a ha resto r . In particolare $a \equiv (a \bmod m) \pmod{m}$, perché $a - (a \bmod m) = qm$.



$$15 \equiv 3 \pmod{12}$$

$$27 \equiv 3 \pmod{12}$$

$$-9 \equiv 3 \pmod{12}$$

ore che differiscono di un multiplo di 12
segnano la stessa posizione sul quadrante

Figura 1. L'orologio a 12 ore: gli interi che differiscono di un multiplo di 12 cadono nella stessa posizione, cioè sono congrui modulo 12.

Esempi. $12 \equiv 9 \pmod{3}$, perché $3 \mid 3$ (entrambi hanno resto 0). $-15 \equiv 9 \pmod{4}$, perché $-15 - 9 = -24 = 4 \cdot (-6)$; infatti $-15 \bmod 4 = 1$ e $9 \bmod 4 = 1$. $7 \not\equiv 1 \pmod{4}$, perché $7 \bmod 4 = 3$ e $1 \bmod 4 = 1$. $-7 \equiv 1 \pmod{4}$, perché $-7 \bmod 4 = 1$.

DA RICORDARE

La scrittura $a \equiv b \pmod{m}$ è una *relazione* (vera o falsa) tra a e b , mentre $a \bmod m$ è un *numero*, il resto, compreso tra 0 e $|m| - 1$. Le due cose sono legate da: $a \equiv b \pmod{m}$ se e solo se $a \bmod m = b \bmod m$. Il modulo m si può prendere ≥ 0 , perché la congruenza modulo m e modulo $-m$ coincidono (se $a - b = km$ allora $a - b = (-k)(-m)$).

UNA RELAZIONE DI EQUIVALENZA

Per ogni m fissato la congruenza modulo m è una relazione di equivalenza su $\mathbb{Z}$ (capitolo 8), e quindi ci sono infinite relazioni di equivalenza, una per ogni m .

- **Riflessiva:** $a \equiv a \pmod{m}$ perché $a - a = 0$ è multiplo di m .

- **Simmetrica:** se $a - b = km$ allora $b - a = (-k)m$.
- **Transitiva:** se $a - b = hm$ e $b - c = km$, sommando $a - c = (h + k)m$.

LE CLASSI DI RESTO

Indichiamo con $[a]_m = \{b \in \mathbb{Z} : b \equiv a \pmod{m}\}$ la classe di equivalenza di a . Tre casi particolari.

- **Modulo 0:** $a \equiv b \pmod{0}$ significa $a - b = 0$, cioè $a = b$. È l'uguaglianza, e ogni classe ha un solo elemento.
- **Modulo 1:** ogni intero è multiplo di 1, quindi tutti gli interi sono congrui tra loro e c'è un'unica classe, $\mathbb{Z}$.
- **Modulo 2:** $a \equiv b \pmod{2}$ se e solo se $a - b$ è pari, quindi ci sono due classi: i numeri pari $[0]_2$ e i dispari $[1]_2$.

TEOREMA (CLASSI DI RESTO)

Fissato $m > 1$, la congruenza modulo m ha esattamente m classi di equivalenza, e sono $[0]_m, [1]_m, \dots, [m-1]_m$.

Dimostrazione. Ogni intero a si scrive $a = qm + r$ con $0 \leq r \leq m-1$, quindi $a \equiv r$ e $a \in [r]_m$: le classi sono al più quelle elencate. Sono tutte distinte: se fosse $[x]_m = [y]_m$ con $0 \leq y < x \leq m-1$, allora $m \mid x - y$ con $0 < x - y < m$, ma tra 0 e m (estremi esclusi) non ci sono multipli di m . ■

Il resto r è il **rappresentante canonico** della classe, e le classi si chiamano **classi resto modulo m** . Per sapere in quale classe cade a basta dividere: modulo 5 si ha $22 = 4 \cdot 5 + 2$, quindi $[22]_5 = [2]_5$. In $[0]_m$ stanno i multipli di m . L'insieme delle m classi si indica con $\mathbb{Z}_m$ (o $\mathbb{Z}/m\mathbb{Z}$).

CLASSE	ALCUNI ELEMENTI	FORMA GENERALE
$[0]_5$	-10, -5, 0, 5, 10	$n = 5q + 0$
$[1]_5$	-9, -4, 1, 6, 11	$n = 5q + 1$
$[2]_5$	-8, -3, 2, 7, 12	$n = 5q + 2$
$[3]_5$	-7, -2, 3, 8, 13	$n = 5q + 3$
$[4]_5$	-6, -1, 4, 9, 14	$n = 5q + 4$

Tabella 1. Le cinque classi resto modulo 5.

Congruenze e operazioni

TEOREMA (COMPATIBILITÀ CON SOMMA E PRODOTTO)

Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, allora

$a + c \equiv b + d \pmod{m}$ e $a \cdot c \equiv b \cdot d \pmod{m}$.

Dimostrazione. Sia $a - b = k_1m$ e $c - d = k_2m$. Allora $(a + c) - (b + d) = (k_1 + k_2)m$. Per il prodotto, $a = b + k_1m$ e $c = d + k_2m$ danno $ac - bd = (b + k_1m)(d + k_2m) - bd = (bk_2 + dk_1 + k_1k_2m)m$. ■

Ne segue che si può **sostituire ogni numero con uno congruo** senza cambiare il risultato di somme e prodotti. In particolare, poiché $a \equiv a \pmod{m}$, per a, b naturali:

- (P1) $(a + b) \pmod{m} = ((a \pmod{m}) + (b \pmod{m})) \pmod{m}$;
- (P2) $(a \cdot b) \pmod{m} = ((a \pmod{m}) \cdot (b \pmod{m})) \pmod{m}$;
- (P3) $a^n \pmod{m} = ((a \pmod{m})^n) \pmod{m}$, per ogni esponente naturale n (si applica P2 più volte);
- (P4) $a^h \cdot b^k \pmod{m} = ((a \pmod{m})^h \cdot (b \pmod{m})^k) \pmod{m}$.

Ciò permette di lavorare con numeri piccoli. Qualche esempio.

- $60 \bmod 7 = (50 + 10) \bmod 7 = (1 + 3) \bmod 7 = 4$, e anche $60 \bmod 7 = (6 \cdot 10) \bmod 7 = (6 \cdot 3) \bmod 7 = 18 \bmod 7 = 4$.
- $13^2 \bmod 10 = (13 \bmod 10)^2 \bmod 10 = 3^2 \bmod 10 = 9$, e infatti $13^2 = 169$.
- $41503 \bmod 5$: poiché $41503 = 11^2 \cdot 7^3$, vale $(11 \bmod 5)^2 \cdot (7 \bmod 5)^3 \bmod 5 = 1^2 \cdot 2^3 \bmod 5 = 8 \bmod 5 = 3$.
- $3^{10} \bmod 11$: $3^4 = 81 \equiv 4$ e $3^6 = 3^3 \cdot 3^3 \equiv 5 \cdot 5 = 25 \equiv 3 \pmod{11}$, quindi $3^{10} \equiv 4 \cdot 3 = 12 \equiv 1$. Infatti $3^{10} - 1 = 59048 = 11 \cdot 5368$.
- **Ultima cifra di una potenza** (cioè potenza modulo 10): $11^{333} \equiv 1^{333} = 1$; $9^{333} \equiv (-1)^{333} = -1 \equiv 9$; $48^{10} \equiv (-2)^{10} = 1024 \equiv 4 \pmod{10}$.

PROVA DEL NOVE

Poiché $10 \equiv 1 \pmod{9}$, ogni intero è congruo modulo 9 alla somma delle sue cifre (capitolo 13). Se un calcolo $a \cdot b = c$ è giusto, allora le somme delle cifre (ridotte modulo 9) devono verificare la stessa uguaglianza: è la «prova del nove» imparata alle elementari. Per $37 \cdot 24 = 888$: $37 \rightarrow 10 \rightarrow 1$, $24 \rightarrow 6$, $1 \cdot 6 = 6$; $888 \rightarrow 24 \rightarrow 6$. Coincidono. Attenzione: la prova scopre molti errori ma non tutti (per esempio non vede uno scambio di cifre).

POTENZE MODULARI VELOCI

Per calcolare $a^n \bmod m$ con n grande non si calcola mai a^n , che avrebbe moltissime cifre, ma si riduce modulo m a ogni passo. Con il metodo dei **quadrati ripetuti** bastano circa $\log_2 n$ passi: si scrive n in binario e si moltiplicano le potenze $a, a^2, a^4, a^8, \dots$ (ciascuna ottenuta elevando al quadrato la precedente) corrispondenti alle cifre 1. Per $2^{20} \bmod 11$: $2^1 = 2$, $2^2 = 4$, $2^4 = 16 \equiv 5$, $2^8 \equiv 25 \equiv 3$, $2^{16} \equiv 9$; poiché $20 = 16 + 4$, $2^{20} \equiv 9 \cdot 5 = 45 \equiv 1 \pmod{11}$. Infatti $2^{20} - 1 = 1048575 = 11 \cdot 95325$.

```
def potenza_mod(a, n, m):
    r = 1
    a = a % m
    while n > 0:
        if n % 2 == 1:
            r = (r * a) % m
        a = (a * a) % m
        n = n // 2
    return r
```

In Python la stessa cosa si ottiene con la funzione predefinita `pow(a, n, m)`. Questo calcolo è la base della crittografia RSA (capitolo 16), dove gli esponenti hanno centinaia di cifre.

Cosa non si può fare: dividere

Se si *sottrae* lo stesso numero da entrambi i membri una congruenza resta vera (è un caso della compatibilità con la somma). Per il prodotto, invece, **non si può semplificare** un fattore comune: $2 \cdot 3 \equiv 2 \cdot 1 \pmod{4}$ (entrambi sono congrui a 2) ma $3 \not\equiv 1 \pmod{4}$. La situazione è esattamente quella della legge di annullamento: modulo 6 si ha $2 \cdot 3 \equiv 0$ pur con $2 \not\equiv 0$ e $3 \not\equiv 0$.

TEOREMA (SEMPLIFICAZIONE)

Se $ac \equiv bc \pmod{m}$ e $d = \text{MCD}(c, m)$, allora $a \equiv b \pmod{m/d}$. In particolare, se c e m sono **coprimi**, si può semplificare c : $a \equiv b \pmod{m}$.

Dimostrazione. Da $m \mid c(a - b)$, scrivendo $c = dc'$ e $m = dm'$ con c' e m' coprimi, si ottiene $m' \mid c'(a - b)$ e, per la proprietà (P2) dei coprimi (capitolo 12), $m' \mid a - b$. ■ Nell'esempio, $d = \text{MCD}(2, 4) = 2$ e si conclude solo $3 \equiv 1 \pmod{2}$.

addizione modulo 5						moltiplicazione modulo 6						
+	0	1	2	3	4	·	0	1	2	3	4	5
0	0	1	2	3	4	0	0	0	0	0	0	0
1	1	2	3	4	0	1	0	1	2	3	4	5
2	2	3	4	0	1	2	0	2	4	0	2	4
3	3	4	0	1	2	3	0	3	0	3	0	3
4	4	0	1	2	3	4	0	4	2	0	4	2
						5	0	5	4	3	2	1

Figura 2. A sinistra l'addizione in $\mathbb{Z}_5$, a destra la moltiplicazione in $\mathbb{Z}_6$: qui $2 \cdot 3 = 0$ e $3 \cdot 4 = 0$, e le righe di 2, 3, 4 non contengono 1, cioè questi elementi non hanno inverso.

Conseguenze: numeri consecutivi

TEOREMA

Tra $m \geq 2$ interi consecutivi ce n'è **esattamente uno** divisibile per m .

Dimostrazione. Siano $n, n+1, \dots, n+m-1$ gli interi. Poniamo $k = \lceil n/m \rceil$: km è il più piccolo multiplo di m maggiore o uguale a n , e poiché $(k-1)m < n$ si ha $km < n+m$: è nella sequenza. Altri multipli distano da km almeno m , quindi non possono stare nella sequenza, che ha ampiezza $m-1$. (Con le classi di resto: $n \equiv i$ e $n+(m-i) \equiv 0$ se $i > 0$.) ■

Da qui discendono molti fatti utili: tra 2 numeri consecutivi uno è pari; tra 3 consecutivi uno è multiplo di 3 e almeno uno è pari, quindi il prodotto di tre interi consecutivi è multiplo di 6. In generale il prodotto di k interi consecutivi è sempre divisibile per $k!$ (per $k=5$, per esempio, per $5! = 120$, e non solo per 60 come si vede con una stima più grossolana: tra cinque consecutivi uno è multiplo di 5, uno di 3 almeno, due sono pari e uno di questi è multiplo di 4, quindi c'è il fattore $5 \cdot 3 \cdot 8 = 120$).

DUE ESERCIZI SVOLTI

E1. Per ogni intero n , $n^3 - n$ è multiplo di 6. Infatti $n^3 - n = n(n^2 - 1) = (n-1)n(n+1)$ è il prodotto di tre interi consecutivi.

E2. Se $n > 3$ e sia n sia $n+2$ sono primi, allora $n+1$ è multiplo di 6. Tra $n, n+1, n+2$ almeno uno è pari: non può essere n né $n+2$ (sono primi maggiori di 2), quindi è $n+1$. Inoltre uno dei tre è multiplo di 3: non possono essere n e $n+2$ (primi maggiori di 3), quindi è $n+1$. Dunque $n+1$ è multiplo di 2 e di 3, cioè di 6 (P3 del capitolo 12). Per esempio 5, 7; 11, 13; 17, 19. Le coppie di primi di questo tipo si chiamano *primi gemelli*.

L'inverso modulare

In $\mathbb{Q}$ ogni numero non nullo a ha un inverso x con $ax = 1$. In $\mathbb{Z}$ questo non accade, ma modulo m è spesso possibile avere $ax \equiv 1 \pmod{m}$.

TEOREMA (ESISTENZA DELL'INVERSO MODULARE)

Siano a, b interi positivi. Esiste x tale che $ax \equiv 1 \pmod{b}$ se e solo se a e b sono **coprime**. Un tale x si dice **inverso di a modulo b** e si indica con $a^{-1} \pmod{b}$.

Dimostrazione. ($\Rightarrow$) Se a e b sono coprimi esistono h, k con $ha + kb = 1$ (Bézout, capitolo 12). Allora $ha = 1 - kb \equiv 1 \pmod{b}$ e $x = h$ è un inverso. ($\Leftarrow$) Se $xa \equiv 1 \pmod{b}$, esiste k con $xa - 1 = kb$, cioè $xa + (-k)b = 1$, e per il criterio di coprimialità $\text{MCD}(a, b) = 1$. ■

L'inverso, quando esiste, è **unico modulo b** : se $ax \equiv ax' \equiv 1$, moltiplicando per x si ottiene $x \equiv x'$. Lo si calcola con l'algoritmo di Euclide esteso (capitolo 12) e poi lo si riduce modulo b , oppure, come vedremo nel capitolo 15, con il teorema di Eulero.

Esempi. L'inverso di 5 modulo 3 è 2 ($2 \cdot 5 = 10 \equiv 1$); quello di 9 modulo 7 è 4 ($36 = 5 \cdot 7 + 1$); quello di 9 modulo 11 è 5 ($45 = 4 \cdot 11 + 1$). Invece 14 non ha inverso modulo 6: i multipli di 14 hanno resti 2, 4, 0, 2, 4, 0, ... (14 e 6 hanno MCD 2). Un inverso si ottiene anche da Bézout: per 7 modulo 11, $7 \cdot 8 = 56 = 5 \cdot 11 + 1$, quindi $7^{-1} = 8$.

CONGRUENZE LINEARI

L'inverso permette di risolvere le equazioni $ax \equiv c \pmod{m}$. Se $\text{MCD}(a, m) = 1$, moltiplicando per a^{-1} si ottiene l'unica soluzione $x \equiv a^{-1}c \pmod{m}$. Per esempio $7x \equiv 3 \pmod{11}$: essendo $7^{-1} = 8$, $x \equiv 24 \equiv 2$, e infatti $7 \cdot 2 = 14 \equiv 3$. Se $d = \text{MCD}(a, m) > 1$, c'è soluzione se e solo se $d \mid c$, e in tal caso si divide tutto per d ottenendo $a'x \equiv c' \pmod{m'}$ con a' e m' coprimi: ci sono d soluzioni modulo m . Per $6x \equiv 4 \pmod{10}$: $d = 2$ divide 4, si ottiene $3x \equiv 2 \pmod{5}$, inverso di 3 modulo 5 è 2, $x \equiv 4 \pmod{5}$, cioè $x \equiv 4$ o $9 \pmod{10}$. Invece $6x \equiv 3 \pmod{10}$ non ha soluzioni, perché $2 \nmid 3$.

La funzione φ di Eulero e i teoremi di Eulero e Fermat

Quanti numeri sono coprimi con n , come si calcola $\varphi(n)$, il teorema di Eulero, il piccolo teorema di Fermat, gli esponenti grandi e un secondo metodo per l'inverso modulare.

La funzione φ di Eulero

Leonhard Euler (Eulero, nato nel 1707 e morto nel 1783, nato in Svizzera e vissuto soprattutto a San Pietroburgo e Berlino) è stato uno dei più grandi matematici di tutti i tempi, con contributi fondamentali al calcolo infinitesimale, alla teoria dei grafi e alla teoria dei numeri. In questa parte ci interessa una funzione che porta il suo nome.

DEFINIZIONE: FUNZIONE Φ DI EULERO

Per ogni intero $n \geq 1$, $\varphi(n)$ è il **numero degli interi x con $1 \leq x \leq n$ che sono coprimi con n** :

$$\varphi(n) = |\{x \in \mathbb{N} : 1 \leq x \leq n \text{ e } \text{MCD}(n, x) = 1\}|.$$

Per esempio $\varphi(1) = 1$ ($\text{MCD}(1, 1) = 1$), $\varphi(2) = 1$ (solo 1; 2 ha MCD 2 con se stesso), $\varphi(3) = 2$ (1, 2), $\varphi(4) = 2$ (1, 3), $\varphi(5) = 4$ (1, 2, 3, 4), $\varphi(6) = 2$ (1, 5). I valori fino a 20 sono nella tabella.

n	$\varphi(n)$	n	$\varphi(n)$	n	$\varphi(n)$	n	$\varphi(n)$
1	1	6	2	11	10	16	8
2	1	7	6	12	4	17	16
3	2	8	4	13	12	18	6
4	2	9	6	14	6	19	18
5	4	10	4	15	8	20	8

Tabella 1. I primi venti valori di $\varphi(n)$.

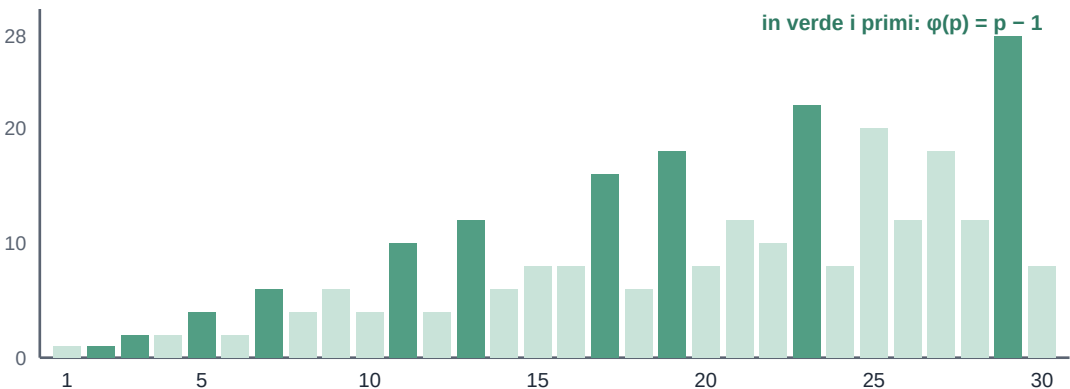


Figura 1. I valori di $\varphi(n)$ per n da 1 a 30: per n primo $\varphi(n) = n - 1$ (barre verdi), il massimo possibile.

Come si calcola $\varphi(n)$

CASO 1: N PRIMO

Se p è primo tutti i numeri $1, 2, \dots, p-1$ sono coprimi con p e p non lo è: $\varphi(p) = p-1$. Per esempio $\varphi(7) = 6$, $\varphi(11) = 10$, $\varphi(13) = 12$.

CASO 2: N POTENZA DI UN PRIMO

Se $n = p^k$ con $k \geq 1$, un numero x non è coprimo con n se e solo se è multiplo di p . Tra 1 e p^k i multipli di p sono $p, 2p, \dots, p^{k-1} \cdot p$, cioè p^{k-1} . Quindi

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

Per esempio $\varphi(2^3) = 8 - 4 = 4$ (i coprimi con 8 sono 1, 3, 5, 7), $\varphi(3^3) = 27 - 9 = 18$ (tutti i numeri da 1 a 27 tranne i multipli di 3), $\varphi(5^3) = 125 - 25 = 100$.

CASO 3: PRODOTTO DI DUE NUMERI COPRIMI

TEOREMA (MOLTIPLICATIVITÀ)

Se h e k sono interi positivi coprimi, allora $\varphi(hk) = \varphi(h) \cdot \varphi(k)$.

Dimostrazione. Per $hk > 1$ consideriamo gli interi x con $0 \leq x < hk$ e associamo a ciascuno la coppia $(x \bmod h, x \bmod k)$. L'associazione è *iniettiva*: se due interi x e y hanno la stessa coppia, $h \mid x-y$ e $k \mid x-y$, quindi per (P3) dei coprimi $hk \mid x-y$, e dato che $|x-y| < hk$ si ha $x=y$. Gli insiemi di partenza e di arrivo hanno entrambi hk elementi, perciò l'associazione è anche *suriettiva*: ogni coppia (u, v) con $0 \leq u < h$ e $0 \leq v < k$ proviene da uno e un solo x . Ora x è coprimo con hk se e solo se è coprimo sia con h sia con k : un divisore comune di x e di h (o di k) è anche un divisore comune di x e hk ; viceversa, se $ax + bh = 1$ e $cx + dk = 1$, moltiplicando le due uguaglianze si ottiene $x(\dots) + bdhk = 1$, quindi $\text{MCD}(x, hk) = 1$. E x è coprimo con h se e solo se lo è $x \bmod h$ ($\text{MCD}(x, h) = \text{MCD}(h, x \bmod h)$). Quindi gli x coprimi con hk corrispondono esattamente alle coppie (u, v) con u coprimo con h e v coprimo con k , che sono $\varphi(h) \cdot \varphi(k)$. ■

Per due primi distinti p, q si ottiene $\varphi(pq) = (p-1)(q-1)$: per esempio $\varphi(2 \cdot 3) = 1 \cdot 2 = 2$ (cioè 1, 5) e $\varphi(3 \cdot 5) = 2 \cdot 4 = 8$ (cioè 1, 2, 4, 7, 8, 11, 13, 14). Questo è il caso che interviene nella crittografia RSA (capitolo 16). Due altri esempi: $\varphi(4 \cdot 9) = \varphi(2^2) \cdot \varphi(3^2) = 2 \cdot 6 = 12$ (1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35) e $\varphi(5 \cdot 8) = \varphi(5) \cdot \varphi(2^3) = 4 \cdot 4 = 16$ (1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39). Attenzione all'ipotesi: $\varphi(4 \cdot 6) = \varphi(24) = 8$, mentre $\varphi(4) \cdot \varphi(6) = 2 \cdot 2 = 4$, perché 4 e 6 non sono coprimi.

FORMULA GENERALE

TEOREMA (FORMULA DI EULERO)

Se $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_m^{k_m}$ è la fattorizzazione canonica di $n > 1$, allora

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdot \dots \cdot (p_m^{k_m} - p_m^{k_m-1}),$$

$$\text{equivalentemente } \varphi(n) = n \cdot (1 - 1/p_1) \cdot \dots \cdot (1 - 1/p_m).$$

Dimostrazione. Per induzione sul numero m di primi distinti. Per $m = 1$ è il caso 2. Per $m > 1$ sia $n' = p_1^{k_1} \cdot \dots \cdot p_{m-1}^{k_{m-1}}$: n' e $p_m^{k_m}$ sono coprimi, quindi per la moltiplicatività $\varphi(n) = \varphi(n') \cdot \varphi(p_m^{k_m})$, e si applica l'ipotesi induttiva a $\varphi(n')$. ■

Esempi: $42 = 2 \cdot 3 \cdot 7$, $\varphi(42) = 1 \cdot 2 \cdot 6 = 12$. $220 = 2^2 \cdot 5 \cdot 11$, $\varphi(220) = 2 \cdot 4 \cdot 10 = 80$. $1000 = 2^3 \cdot 5^3$, $\varphi(1000) = 4 \cdot 100 = 400$. Il calcolo di $\varphi(n)$ richiede quindi la fattorizzazione di n , che è difficile per n grande: è la ragione della sicurezza di RSA.

DUE PROPRIETÀ UTILI

1. Per $n \geq 3$, $\varphi(n)$ è pari: gli interi coprimi con n si dividono in coppie $\{x, n - x\}$ con $x \neq n - x$ ($\text{MCD}(x, n) = \text{MCD}(n - x, n)$).
2. (Gauss) Sommando $\varphi(d)$ su tutti i divisori positivi d di n si ottiene n . Per $n = 12$: $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$. Infatti, dividendo gli interi $1, \dots, n$ secondo il valore di $\text{MCD}(x, n) = n/d$, quelli con quel MCD sono tanti quanti i numeri coprimi con d tra 1 e d , cioè $\varphi(d)$.

Il teorema di Eulero

TEOREMA DI EULERO

Siano n e m interi positivi con $\text{MCD}(n, m) = 1$. Allora

$$n^{\varphi(m)} \equiv 1 \pmod{m}.$$

Esempi: $n = 12, m = 5$: $\varphi(5) = 4$ e $12^4 = 20736 \equiv 1 \pmod{5}$. $n = 21, m = 20$: $\varphi(20) = \varphi(4) \cdot \varphi(5) = 2 \cdot 4 = 8$, quindi $21^8 \equiv 1 \pmod{20}$; infatti $21^8 = 37\,822\,859\,361 = 20 \cdot 1\,891\,142\,968 + 1$.

Dimostrazione. Sia $m > 1$ (per $m = 1$ tutto è congruo) e sia $C_m = \{x : 0 < x < m, \text{MCD}(x, m) = 1\}$, un insieme di $\varphi(m)$ elementi. Consideriamo la funzione $f(x) = (nx) \bmod m$.

- **f manda C_m in C_m .** Se x è coprimo con m , anche nx lo è (prodotto di due numeri coprimi con m : moltiplicando le due identità di Bézout), e $\text{MCD}(nx \bmod m, m) = \text{MCD}(nx, m) = 1$; inoltre $(nx) \bmod m \neq 0$, perché $m > 1$ non è coprimo con 0.
- **f è iniettiva.** Se $nx \equiv ny \pmod{m}$ con n coprimo con m , per il teorema di semplificazione $x \equiv y \pmod{m}$, e poiché $0 < x, y < m$, $x = y$.
- Una funzione iniettiva da un insieme finito in sé stesso è **biunivoca**: f permuta gli elementi di C_m .

Sia P il prodotto di tutti gli elementi di C_m . Poiché f è una permutazione, anche i prodotti dei valori $f(x)$ danno P . Ma per la compatibilità con il prodotto, il prodotto degli nx è congruo a $n^{\varphi(m)} \cdot P$ (ci sono $\varphi(m)$ fattori n). Quindi

$$n^{\varphi(m)} \cdot P \equiv P \pmod{m}$$

Ora P è un prodotto di numeri coprimi con m , quindi è coprimo con m , e si può semplificare: $n^{\varphi(m)} \equiv 1 \pmod{m}$. ■

Nel corso del ragionamento abbiamo dimostrato anche che $x \mapsto (nx) \bmod m$ è una permutazione degli «invertibili» modulo m . Un esempio: con $m = 10$, $C_{10} = \{1, 3, 7, 9\}$ e $n = 13$ si ottiene $\{13 \bmod 10, 39 \bmod 10, 91 \bmod 10, 117 \bmod 10\} = \{3, 9, 1, 7\}$, cioè gli stessi elementi in un altro ordine. Con $m = 12$, $C_{12} = \{1, 5, 7, 11\}$ e $n = 13 \equiv 1$, ogni elemento va in sé stesso. Lo stesso insieme è anche chiuso rispetto all'inversione: in C_5 gli inversi di 1, 2, 3, 4 sono 1, 3, 2, 4; in C_{10} gli inversi di 1, 3, 7, 9 sono 1, 7, 3, 9; in C_{12} ogni elemento è inverso di sé stesso.

Il piccolo teorema di Fermat

Pierre de Fermat (vissuto tra il 1601 circa e il 1665), giurista francese e matematico dilettante di genio, è noto soprattutto per l'«ultimo teorema di Fermat»: l'equazione $a^n + b^n = c^n$ non ha soluzioni intere positive per $n > 2$. Fermat annotò di averne una dimostrazione, ma con ogni probabilità si sbagliava: fu dimostrato oltre tre secoli dopo da Andrew Wiles (con un contributo di Richard Taylor), nel 1994, e pubblicato nel 1995. Con Blaise Pascal fu anche tra i fondatori della teoria della probabilità (capitolo 19).

PICCOLO TEOREMA DI FERMAT

Se p è primo e a non è multiplo di p (cioè $\text{MCD}(a, p) = 1$), allora $a^{p-1} \equiv 1 \pmod{p}$. Equivalentemente, per ogni intero a : $a^p \equiv a \pmod{p}$.

È il teorema di Eulero con $m = p$ primo, per cui $\varphi(p) = p - 1$. La seconda forma si ottiene moltiplicando per a , e vale anche se $p \mid a$ (entrambi i membri sono $\equiv 0$). Esempi: $10^2 = 100 \equiv 1 \pmod{3}$; $12^4 \equiv 1 \pmod{5}$; $40^{16} \equiv 1 \pmod{17}$, perché $40 \equiv 6$ e $6^{16} \equiv 1$.

FERMAT COME TEST DI PRIMALITÀ (E PERCHÉ NON BASTA)

Il teorema dà una condizione necessaria: se esiste a coprimo con n con $a^{n-1} \not\equiv 1 \pmod{n}$, allora n è **composto**. Il viceversa è falso: $2^{340} \equiv 1 \pmod{341}$ ma $341 = 11 \cdot 31$; 341 è detto *pseudoprimo* in base 2 (e $3^{340} \not\equiv 1$ mostra che è composto). Esistono addirittura numeri composti, detti **numeri di Carmichael**, per cui la congruenza vale per ogni a coprimo: il più piccolo è $561 = 3 \cdot 11 \cdot 17$. Test più raffinati, come quello di Miller e Rabin, correggono questo difetto.

Esponenti grandi

TEOREMA

Se $\text{MCD}(a, n) = 1$, allora per ogni $x \geq 0$: $a^x \equiv a^{x \bmod \varphi(n)} \pmod{n}$.

Dimostrazione. Sia $x = q \varphi(n) + r$ con $r = x \bmod \varphi(n)$. Allora $a^x = (a^{\varphi(n)})^q \cdot a^r \equiv 1^q \cdot a^r = a^r \pmod{n}$ per il teorema di Eulero. ■

Esempi. $12^{50} \bmod 5$: $\varphi(5) = 4$ e $50 \bmod 4 = 2$, quindi $12^{50} \equiv 12^2 = 144 \equiv 4 \pmod{5}$. Per $3^{100} \cdot 7^{200} \bmod 10$: $\varphi(10) = 4$, 100 e 200 sono multipli di 4, quindi $3^{100} \equiv 3^0 = 1$ e $7^{200} \equiv 1$; il prodotto è 1 (mod 10).

Attenzione: l'ipotesi $\text{MCD}(a, n) = 1$ è essenziale. Per $a = 2$, $n = 12$ ($\varphi(12) = 4$) si ha $2^4 = 16 \equiv 4 \pmod{12}$, mentre $2^{4 \bmod 4} = 2^0 = 1$.

Calcolare l'inverso con Eulero

Se n e m sono coprimi, dal teorema di Eulero $n \cdot n^{\varphi(m)-1} \equiv 1 \pmod{m}$, quindi $n^{\varphi(m)-1}$ è un inverso di n modulo m . Possiamo ridurre prima la base: l'inverso *normalizzato* (tra 0 e $m - 1$) è $((n \bmod m)^{\varphi(m)-1}) \bmod m$, calcolabile con i quadrati ripetuti. È un metodo alternativo all'algoritmo di Euclide esteso del capitolo 12 (e quando $\varphi(m)$ è noto, come per m primo, è comodo).

- Inverso di 11 modulo 7: $\varphi(7) = 6$, $11 \bmod 7 = 4$ e $4^5 = 1024 \equiv 2 \pmod{7}$; infatti $2 \cdot 11 = 22 \equiv 1$.
- Inverso di 30 modulo 11: $\varphi(11) = 10$, $30 \bmod 11 = 8$ e $8^9 \equiv 7 \pmod{11}$; infatti $7 \cdot 30 = 210 = 19 \cdot 11 + 1$.
- Inverso di 45 modulo 16: $45 = 3^2 \cdot 5$ è coprimo con $16 = 2^4$; $\varphi(16) = 8$, $45 \bmod 16 = 13$ e $13^7 \equiv 5 \pmod{16}$; infatti $45 \cdot 5 = 225 = 14 \cdot 16 + 1$.
- Inverso di 70 modulo 9: $\varphi(9) = 6$, $70 \bmod 9 = 7$ e $7^5 \equiv 4 \pmod{9}$; infatti $4 \cdot 70 = 280 = 31 \cdot 9 + 1$.

ESERCIZI SVOLTI: INVERSI

A	MODULO	A MOD MODULO	INVERSO	VERIFICA
49	23	3	8	$49 \cdot 8 = 392 = 17 \cdot 23 + 1$
51	16	3	11	$51 \cdot 11 = 561 = 35 \cdot 16 + 1$
63	10	3	7	$63 \cdot 7 = 441 = 44 \cdot 10 + 1$
72	5	2	3	$72 \cdot 3 = 216 = 43 \cdot 5 + 1$
83	10	3	7	$83 \cdot 7 = 581 = 58 \cdot 10 + 1$
97	11	9	5	$97 \cdot 5 = 485 = 44 \cdot 11 + 1$
100	23	8	3	$100 \cdot 3 = 300 = 13 \cdot 23 + 1$

Tabella 2. Gli inversi modulari richiesti dagli esercizi: a ogni riga si è ridotta la base e verificato il prodotto.

ESERCIZI SVOLTI: POTENZE

Potenza	Ragionamento	Risultato
$9^{100} \bmod 8$	$9 \equiv 1 \pmod{8}$, quindi $9^{100} \equiv 1^{100} = 1$	1
$15^{80} \bmod 16$	$15 \equiv -1 \pmod{16}$ e l'esponente è pari: $(-1)^{80} = 1$	1
$13^{40} \bmod 19$	$\varphi(19) = 18$, $40 \bmod 18 = 4$; $13^2 = 169 \equiv -2$, quindi $13^4 \equiv 4$	4
$11^{57} \bmod 23$	$\varphi(23) = 22$, $57 \bmod 22 = 13$; $11^2 \equiv 6$, $11^4 \equiv 13$, $11^8 \equiv 8$, quindi $11^{13} = 11^8 \cdot 11^4 \cdot 11 \equiv 8 \cdot 13 \cdot 11 = 1144 \equiv 17$	17
$7^{50} \bmod 11$	$\varphi(11) = 10$ e 50 è multiplo di 10: $7^{50} \equiv 1$	1
$40^{60} \cdot 60^{40} \bmod 31$	$\varphi(31) = 30$: $40^{60} = (40^{30})^2 \equiv 1$. Poi $60 \equiv -2$ e $60^{40} \equiv 2^{40} = 2^{30} \cdot 2^{10} \equiv 1024 \equiv 1$ ($1024 = 33 \cdot 31 + 1$)	1
$29^{101} \bmod 31$	$\varphi(31) = 30$, $101 \bmod 30 = 11$; $29 \equiv -2$ e $(-2)^{11} = -2048 \equiv -2 \equiv 29$ ($2048 = 66 \cdot 31 + 2$)	29

Tabella 3. Potenze modulari calcolate con il teorema di Eulero.

Applicazioni dell'aritmetica modulare

Prova del nove, codici ISBN e carte di credito, cifrari di Cesare e affini, tabelle hash e crittografia RSA: l'aritmetica dei resti al lavoro.

L'aritmetica modulare ha applicazioni in matematica e, soprattutto, in informatica, per la gestione dei dati e per la sicurezza. In questo capitolo ne vediamo cinque: la prova del nove, i codici di controllo (ISBN e carte di credito), i cifrari a sostituzione, le tabelle hash e, per finire, un'introduzione alla crittografia RSA, che usa insieme tutti gli strumenti dei capitoli precedenti.

La prova del nove

La prova del nove è una verifica del risultato di una somma o di un prodotto, che confronta le **radici numeriche** (capitolo 13) di operandi e risultato. Si fonda sul fatto che ogni naturale è congruo modulo 9 alla somma delle sue cifre, quindi alla sua radice numerica: $n \equiv p(n) \pmod{9}$. Per la compatibilità delle congruenze con somma e prodotto vale allora

$$p(n \cdot m) = p(p(n) \cdot p(m)) \text{ e } p(n + m) = p(p(n) + p(m))$$

(per $n, m > 0$). Si chiama «del nove» perché la radice numerica si ottiene «scartando i nove» dalla somma delle cifre: $3 + 4 + 7 = 14$, e togliendo 9 si ha 5, come sommando le cifre di 14.

Esempio. È giusto $123 \cdot 347 = 42671$? Si ha $p(123) = 6$ e $p(347) = 5$, quindi $p(6 \cdot 5) = p(30) = 3$, ma $p(42671) = p(20) = 2$. I due valori sono diversi: il calcolo è **sbagliato**. Infatti $123 \cdot 347 = 42681$ e $p(42681) = 3$. Allo stesso modo, $123 + 347 = 472$ è sbagliato ($p(6 + 5) = 2$, $p(472) = 4$), perché la somma giusta è 470 con $p(470) = 2$.

ATTENZIONE: LA PROVA FUNZIONA SOLO IN UN VERSO

Se i due numeri sono **diversi**, il calcolo è certamente sbagliato. Se sono **uguali**, il calcolo *può* essere giusto, ma non è garantito. Per esempio $123 \cdot 347 = 42771$ supera la prova ($p(42771) = 3$), eppure è sbagliato. La prova non scopre gli errori di una quantità multipla di 9 (per esempio lo scambio di due cifre adiacenti) né quelli che si compensano. Un calcolo che supera la prova è «probabilmente» giusto, non certamente.

Esattamente lo stesso vale per la prova dell'undici, che usa la differenza alternata delle cifre invece della somma, e per qualunque modulo: si calcola il risultato modulo m in due modi e si confrontano.

Codici di controllo: ISBN

Il codice **ISBN** (*International Standard Book Number*) identifica in modo univoco un libro. Dal 2007 ha 13 cifre, prima aveva 10 caratteri (l'ultimo poteva essere la lettera X, che vale 10). L'ultimo carattere è di **controllo**: è scelto in modo che una certa combinazione lineare delle cifre sia congrua a 0, e permette di accorgersi della maggior parte degli errori di battitura.

ISBN A 10 CIFRE

Se i caratteri sono $a_{10} a_9 \dots a_1$ (da sinistra a destra, con X = 10), il codice è formalmente corretto se

$$a_1 + 2a_2 + 3a_3 + \dots + 9a_9 + 10a_{10} \equiv 0 \pmod{11}.$$

Per 2468864212 si ha $10 \cdot 2 + 9 \cdot 4 + 8 \cdot 6 + 7 \cdot 8 + 6 \cdot 8 + 5 \cdot 6 + 4 \cdot 4 + 3 \cdot 2 + 2 \cdot 1 + 1 \cdot 2 = 264 = 11 \cdot 24$: il codice è corretto. Per 2468864211 la somma è 263, che non è multiplo di 11: il codice è errato. Un esempio di ISBN reale è 0 306 40615 2: $10 \cdot 0 + 9 \cdot 3 + 8 \cdot 0 + 7 \cdot 6 + 6 \cdot 4 + 5 \cdot 0 + 4 \cdot 6 + 3 \cdot 1 + 2 \cdot 5 + 1 \cdot 2 = 132 = 11 \cdot 12$.

ISBN A 13 CIFRE

Se le cifre sono $a_1, a_2, \dots, a_{13}$, il codice è corretto se

$$a_1 + 3a_2 + a_3 + 3a_4 + \dots + a_{11} + 3a_{12} + a_{13} \equiv 0 \pmod{10}.$$

Per 2468864211129 la somma è $2 + 12 + 6 + 24 + 8 + 18 + 4 + 6 + 1 + 3 + 1 + 6 + 9 = 100$, multiplo di 10, quindi il codice è corretto; per 2468864211128 la somma è 99 e il codice è errato. (Il codice reale 978 0 306 40615 7 è la versione a 13 cifre del precedente: i codici veri iniziano con 978 o 979.)

QUALI ERRORI SCOPRE

Perché il modulo 11 funziona così bene? Perché 11 è **primo**. Se si cambia una sola cifra a_i in a'_i , la somma pesata cambia di $i(a'_i - a_i)$: il peso i (da 1 a 10) e la differenza (non nulla, in valore assoluto al più 10) non sono multipli di 11, e per il lemma di Euclide (capitolo 13) nemmeno il prodotto lo è: l'errore è **sempre scoperto**. Anche lo scambio di due cifre diverse in posizioni i e j cambia la somma di $(i - j)(a_j - a_i)$, prodotto di due numeri non multipli di 11: anche questo errore è **sempre scoperto**.

L'ISBN a 13 cifre usa il modulo 10, che non è primo, e perde qualcosa: i pesi 1 e 3 sono coprimi con 10, quindi ogni errore su una cifra è scoperto, ma lo scambio di due cifre adiacenti a e b cambia la somma di $\pm 2(a - b)$, che è multiplo di 10 se e solo se $a - b$ è multiplo di 5, cioè se le due cifre differiscono di 5 (0 e 5, 1 e 6, ...): questi scambi **non** sono scoperti. L'ISBN a 13 cifre coincide con il codice a barre EAN 13 dei prodotti, ed è per questa compatibilità che si è accettato un controllo un po' più debole.

Codici di controllo: carte di credito

Anche il numero di 16 cifre di una carta di credito contiene una cifra di controllo, calcolata con la **formula di Luhn**. Partendo dall'*ultima* cifra (quella di controllo), si raddoppia una cifra ogni due, cioè si moltiplicano per 2 la penultima, la terzultima..., avanti di due; se il doppio supera 9 lo si sostituisce con la somma delle sue cifre (la sua radice numerica, cioè il doppio meno 9). Si sommano tutte le cifre così ottenute. Il numero è formalmente corretto se la somma $S \equiv 0 \pmod{10}$.

Per una carta a 16 cifre scritta a gruppi di 4, $a_1 b_1 a_2 b_2 a_3 b_3 a_4 b_4 \dots$, si raddoppiano quindi le cifre in posizione dispari $a_1, \dots, a_8$ (contando da sinistra) e $S = \sum p(2a_i) + \sum b_i$.

Esempio 1. 1234 5678 8765 4321. Le cifre di posto dispari sono 1, 3, 5, 7, 8, 6, 4, 2; raddoppiate e ridotte danno 2, 6, 1, 5, 7, 3, 8, 4 (infatti $2 \cdot 5 = 10 \rightarrow 1$, $2 \cdot 7 = 14 \rightarrow 5$, $2 \cdot 8 = 16 \rightarrow 7$, $2 \cdot 6 = 12 \rightarrow 3$), con somma 36. Le cifre di posto pari sono 2, 4, 6, 8, 7, 5, 3, 1, con somma 36. In totale 72: non è multiplo di 10, e il numero **non** è valido.

Esempio 2. 1111 1212 1212 1212. Le cifre di posto dispari sono tutte 1 e, raddoppiate, danno $8 \cdot 2 = 16$; le cifre di posto pari sono 1, 1, 2, 2, 2, 2, 2, 2, con somma 14. Il totale 30 è un multiplo di 10: il numero è **formalmente valido**.

Il controllo di Luhn scopre tutti gli errori su una singola cifra (raddoppiare e ridurre è una funzione iniettiva sulle cifre) e quasi tutti gli scambi di cifre adiacenti, con la sola eccezione dello scambio di 0 e 9. Non è un meccanismo di sicurezza: serve a scoprire errori di battitura, non a impedire la contraffazione, perché chiunque può calcolare una cifra di controllo valida.

UNA PRECISAZIONE SULL'ORDINE

Contare le cifre dall'ultima è il modo corretto in generale, perché funziona per qualunque lunghezza. Per i numeri di 16 cifre equivale a raddoppiare le posizioni dispari da sinistra, come nella descrizione precedente; per i numeri di 15 cifre (alcune carte) le posizioni da raddoppiare, contate da sinistra, sono quelle pari.

Cifrari a sostituzione

La **crittografia** studia come rendere un messaggio comprensibile solo al destinatario. Un esempio storico usato da Giulio Cesare per comunicare con i suoi generali è il **cifrario di Cesare**: ogni lettera viene sostituita dalla lettera che la segue di 3 posizioni nell'alfabeto, ricominciando da capo dopo la z (con l'alfabeto moderno di 26 lettere). Per esempio «ce la faremo» diventa «fhodiduhpr» (si ignorano gli spazi).

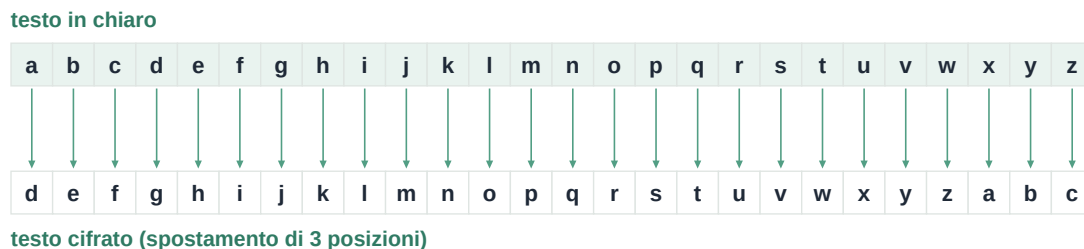


Figura 1. Il cifrario di Cesare con chiave 3: ogni lettera è sostituita da quella che la segue di tre posizioni (x, y, z diventano a, b, c).

È un cifrario a **sostituzione monoalfabetica**, cioè un cifrario in cui a ogni lettera del testo in chiaro corrisponde sempre la stessa lettera del testo cifrato; è diverso da un cifrario a *trasposizione*, in cui le lettere restano le stesse ma cambiano di posto. Un altro esempio è il **ROT13**, usato sul web per nascondere soluzioni e spoiler: lo spostamento è di 13 posizioni e, siccome $13 + 13 = 26$, applicarlo due volte riporta al testo originale (cifrare e decifrare sono la stessa operazione).

IL CIFRARIO COME ARITMETICA MODULARE

Si associa a ogni lettera il numero d'ordine partendo da zero: $a = 0, b = 1, \dots, z = 25$. Scelta una **chiave** intera k con $0 < k < 26$, un messaggio $m_1 m_2 \dots m_s$ si cifra con la funzione

$$f(m_i) = (m_i + k) \bmod 26,$$

e si decifra con $g(m_i) = (m_i - k) \bmod 26$. Per esempio, con $k = 3$: $c (2) \rightarrow 5 = f$, $e (4) \rightarrow 7 = h$, $l (11) \rightarrow 14 = o$, $a (0) \rightarrow 3 = d$. Ecco il codice per le lettere minuscole (ord restituisce il codice del carattere, e il resto per 26 dà il numero d'ordine da 0 a 25):

```
def cesare(testo, k):
    ris = ''
    for c in testo:
        if 'a' <= c <= 'z':
            ris += chr((ord(c) + k) % 26 + 97)
        else:
            ris += c
    return ris

# per decifrare: cesare(cifrato, 25 * k), perche 25 e congruo a meno 1 modulo 26
```

Il cifrario di Cesare è però **debolissimo**: le chiavi possibili sono solo 25, e si possono provare tutte; inoltre la lettera più frequente del testo cifrato corrisponde con grande probabilità alla più frequente della lingua (la e, in italiano), il che rivela la chiave a colpo d'occhio (*analisi delle frequenze*).

IL CIFRARIO AFFINE

Un miglioramento naturale è cifrare con $f(x) = (ax + b) \bmod 26$. Perché si possa decifrare, la funzione deve essere biunivoca, e questo accade esattamente quando a è **coprimo con 26**: allora esiste l'inverso a^{-1} modulo 26 e $x = a^{-1}(y - b) \bmod 26$. I valori ammessi per a sono $\phi(26) = 12$ (1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25), quindi le chiavi sono $12 \cdot 26 = 312$. Con $a = 5, b = 8$ (inverso di 5 modulo 26: 21, perché $5 \cdot 21 = 105 = 4 \cdot 26 + 1$) la parola «ciao» diventa «swia»: $c (2) \rightarrow 5 \cdot 2 + 8 = 18 = s$, $i (8) \rightarrow 48 \bmod 26 = 22 = w$, $a (0) \rightarrow 8 = i$, $o (14) \rightarrow 78 \bmod 26 = 0 = a$. Anche questo cifrario si rompe facilmente: lo spazio delle chiavi è minuscolo. I cifrari moderni (AES) sono su un'altra scala di complessità, e per la cifratura a chiave pubblica serve un'idea diversa, quella di RSA.

Tabelle hash

Immaginiamo di dover gestire in un archivio le automobili circolanti in Italia, ciascuna identificata dalla targa (2 lettere, 3 cifre, 2 lettere). Il numero di targhe possibili è enorme: con 26 lettere sarebbe $26^4 \cdot 10^3 = 456\,976\,000$ (impareremo a calcolarlo nel capitolo 18); in realtà le targhe italiane non usano le lettere I, O, Q, U e le combinazioni sono $22^4 \cdot 10^3 = 234\,256\,000$. Il parco auto è di circa 50 milioni di veicoli: riservare un posto a ogni targa possibile sarebbe uno spreco.

Si usa allora una struttura con n posizioni, e ad ogni auto, la cui targa è convertita in un intero a , si associa la posizione

$$h(a) = a \bmod n$$

Una funzione di questo tipo si chiama **funzione di hash**: calcola direttamente dove cercare la chiave, senza scorrere l'elenco. Poiché le chiavi sono più delle posizioni, due chiavi diverse possono avere la stessa posizione (**collisione**); la gestione delle collisioni (catene, indirizzamento aperto) si vedrà in altri corsi. In pratica n si sceglie primo, perché la funzione distribuisce meglio le chiavi: con $n = 7$, le chiavi 15, 28, 47, 33, 5 vanno nelle posizioni 1, 0, 5, 5, 5, e le ultime tre collidono. Se le chiavi sono multipli di uno stesso numero e n ha un fattore in comune con quel numero, molte posizioni restano vuote: è un'altra conseguenza del fatto che moltiplicare per c è biunivoco modulo n solo se c è coprimo con n .

Una introduzione alla crittografia RSA

La crittografia **a chiave pubblica** risolve un problema che i cifrari precedenti non risolvono: come scambiarsi messaggi segreti senza essersi prima accordati su una chiave segreta. Il sistema **RSA** (dalle iniziali di Rivest, Shamir e Adleman, 1977) usa due chiavi: una *pubblica*, che chiunque può conoscere e serve per cifrare, e una *privata*, segreta, che serve per decifrare. Si basa su tre fatti dei capitoli precedenti: le potenze modulari si calcolano in fretta (quadrati ripetuti), il teorema di Eulero, e il fatto che moltiplicare due primi enormi è facile mentre fattorizzare il prodotto è, per quanto si sa, molto difficile (capitolo 13).

GENERAZIONE DELLE CHIAVI

1. Si scelgono due primi molto grandi e distinti p e q e si pone $n = pq$; allora $\varphi(n) = (p-1)(q-1)$.
2. Si sceglie un intero e con $1 < e < \varphi(n)$ coprimo con $\varphi(n)$ (spesso $e = 65537$).
3. Si calcola d , l'inverso di e modulo $\varphi(n)$: $ed \equiv 1 \pmod{\varphi(n)}$.

Chiave pubblica: (n, e) . **Chiave privata:** d (e p, q vanno distrutti o tenuti segreti).

CIFRATURA E DECIFRATURA

Un messaggio è un intero m con $0 \leq m < n$. Si cifra con $c = m^e \bmod n$ e si decifra con $m = c^d \bmod n$.

Perché funziona. Poiché $ed \equiv 1 \pmod{(p-1)(q-1)}$, si può scrivere $ed = 1 + k(p-1)(q-1)$ per un intero $k \geq 0$. Mostriamo che $m^{ed} \equiv m$ sia modulo p sia modulo q . Modulo p : se $p \mid m$ entrambi i membri sono $\equiv 0$; altrimenti, per il piccolo teorema di Fermat $m^{p-1} \equiv 1$ e quindi $m^{ed} = m \cdot (m^{p-1})^{k(q-1)} \equiv m \pmod{p}$. Lo stesso vale modulo q . Dunque p e q dividono entrambi $m^{ed} - m$, e poiché sono coprimi il loro prodotto n lo divide (proprietà (P3) dei coprimi): $m^{ed} \equiv m \pmod{n}$. Perciò $(m^e)^d \equiv m$, e poiché $0 \leq m < n$, il resto è proprio m . ■

Un esempio con numeri piccoli. Siano $p = 61$ e $q = 53$: $n = 3233$ e $\varphi(n) = 60 \cdot 52 = 3120$. Scegliamo $e = 17$, coprimo con 3120. L'inverso di 17 modulo 3120 è $d = 2753$, perché $17 \cdot 2753 = 46801 = 15 \cdot 3120 + 1$. Per cifrare $m = 65$ si calcola $65^{17} \bmod 3233 = 2790$. Per decifrare si calcola $2790^{2753} \bmod 3233 = 65$. (I calcoli si fanno con i quadrati ripetuti; in Python con `pow(65, 17, 3233)` e `pow(2790, 2753, 3233)`.) Si verifica anche che la decifratura restituisce il messaggio per ognuno dei 3233 messaggi possibili.

PERCHÉ È SICURO (PER QUANTO SI SA)

Chi conosce solo la chiave pubblica (n , e) deve trovare d , cioè l'inverso di e modulo $\varphi(n)$, e per farlo gli serve $\varphi(n)$. Ma calcolare $\varphi(n)$ conoscendo n è equivalente a fattorizzare n (da n e $\varphi(n) = n - (p + q) + 1$ si ricava $p + q$, e quindi p e q come radici di un'equazione di secondo grado). Per n di 2048 bit (due primi di 1024 bit, circa 309 cifre ciascuno) nessun algoritmo di fattorizzazione noto è abbastanza veloce. Non è stato però dimostrato che fattorizzare sia difficile: è un'ipotesi, legata alle questioni di complessità del capitolo 26.

AVVERTENZE

L'esempio è **didattico**: con numeri così piccoli si fattorizza a mente, e la versione «da manuale» di RSA descritta qui non è sicura nella pratica (messaggi uguali danno cifrature uguali, e certi messaggi piccoli si decifrano facilmente). I sistemi reali aggiungono casualità e imbottiture (padding, per esempio OAEP) e usano RSA soprattutto per scambiare una chiave di un cifrario simmetrico veloce, che cifra poi il messaggio vero. Non si deve mai realizzare un sistema di sicurezza con codice scritto da sé: si usano librerie collaudate.

Problemi aperti della teoria dei numeri

Primi di Mersenne e numeri perfetti, primi gemelli, la congettura di Goldbach e il problema $3x + 1$ di Collatz: questioni semplici da enunciare e ancora irrisolte.

La teoria dei numeri studia le proprietà degli interi, ed è ricca di problemi che si enunciano con le conoscenze del primo anno e che resistono, alcuni da secoli, ai tentativi di soluzione, soprattutto quando coinvolgono i numeri primi. In questo capitolo ne vediamo alcuni tra i più celebri, usando gli strumenti dei capitoli precedenti. Molti problemi chiedono se una certa successione di interi è infinita: per le successioni note esiste una grande raccolta in rete, la *Online Encyclopedia of Integer Sequences* (OEIS, oeis.org), in cui ogni successione ha un codice (per esempio A000040 per i numeri primi) e una scheda con proprietà e riferimenti storici.

Numeri primi di Mersenne

Marin Mersenne (nato nel 1588 e morto nel 1648), religioso, filosofo e matematico francese, studiò i numeri della forma $M_n = 2^n - 1$ e ne propose un elenco di quelli che riteneva primi. I **numeri primi di Mersenne** sono i primi di questa forma. I primi cinque sono

$$M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127, M_{13} = 8191.$$

In tutti questi casi l'esponente è primo, e non è un caso.

TEOREMA

Se $2^n - 1$ è primo, allora n è primo.

Dimostrazione. Per contrapposizione: se $n = hk$ con $h, k \geq 2$, vale l'identità $2^{hk} - 1 = (2^h - 1)(1 + 2^h + 2^{2h} + \dots + 2^{(k-1)h})$, che si verifica sviluppando il prodotto (somma geometrica, capitolo 10). Il primo fattore è maggiore di 1 (perché $h \geq 2$) e minore di $2^n - 1$, quindi $2^n - 1$ è composto. ■

Il viceversa è falso: $2^{11} - 1 = 2047 = 23 \cdot 89$ è composto, pur essendo 11 primo. Perciò gli esponenti da provare sono i primi, e per decidere se M_p è primo si usa un test molto veloce, il **test di Lucas e Lehmer**: per p primo dispari si pone $s_0 = 4$ e $s_{k+1} = (s_k^2 - 2) \bmod M_p$; allora M_p è primo se e solo se $s_{p-2} = 0$ (non lo dimostriamo). Per $p = 5$ ($M = 31$) la successione è 4, 14, 8, 0: primo. Per $p = 7$ ($M = 127$) è 4, 14, 67, 42, 111, 0: primo. Per $p = 11$ l'ultimo termine non è 0, coerentemente con $2047 = 23 \cdot 89$. I primi di Mersenne con esponente più piccolo di 2300 sono quelli con $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281$ (la lista di Mersenne conteneva errori: includeva 67 e 257, che non danno primi, e ometteva 61, 89 e 107).

Si conoscono soltanto **52** primi di Mersenne. Il più grande, $2^{136279841} - 1$, scoperto il 12 ottobre 2024 da Luke Durant nell'ambito del progetto di calcolo distribuito GIMPS (*Great Internet Mersenne Prime Search*), ha 41 024 320 cifre decimali, ed è il più grande numero primo conosciuto. Non si sa se i primi di Mersenne siano infiniti.

Numeri perfetti

DEFINIZIONE: FUNZIONE Σ E NUMERI PERFETTI

Per $n \geq 1$, $\sigma(n)$ è la **somma di tutti i divisori positivi** di n . Un numero n si dice **perfetto** se $\sigma(n) = 2n$, cioè se è uguale alla somma dei suoi divisori propri (tutti i divisori tranne n stesso).

Si ha $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 4$, $\sigma(4) = 7$, $\sigma(5) = 6$, $\sigma(6) = 12$, e in generale $\sigma(p) = p + 1$ se p è primo. Il primo numero perfetto è $6 = 1 + 2 + 3$ ($\sigma(6) = 12$), poi $28 = 1 + 2 + 4 + 7 + 14$ e 496. Se a e b sono coprimi, $\sigma(ab) = \sigma(a)\sigma(b)$ (ogni divisore di ab si scrive in modo unico come prodotto di un divisore di a e di uno di b , per l'unicità

della fattorizzazione); inoltre $\sigma(2^k) = 1 + 2 + \dots + 2^k = 2^{k+1} - 1$.

TEOREMA DI EUCLIDE E EULER

Un numero pari n è perfetto se e solo se $n = 2^{p-1}(2^p - 1)$ con $2^p - 1$ primo, cioè con $2^p - 1$ un primo di Mersenne.

Dimostrazione (Euclide). Se $M = 2^p - 1$ è primo, 2^{p-1} e M sono coprimi, quindi $\sigma(2^{p-1}M) = \sigma(2^{p-1}) \cdot \sigma(M) = (2^p - 1)(M + 1) = M \cdot 2^p = 2 \cdot 2^{p-1}M$. Il numero è perfetto.

Dimostrazione (Eulero). Sia n pari e perfetto e scriviamo $n = 2^k m$ con $k \geq 1$ e m dispari. Allora $\sigma(n) = (2^{k+1} - 1)\sigma(m)$ deve valere $2n = 2^{k+1}m$. Poiché $2^{k+1} - 1$ è coprimo con 2^{k+1} , divide m : $m = (2^{k+1} - 1)t$, e quindi $\sigma(m) = 2^{k+1}t$. Ora $m + t = (2^{k+1} - 1)t + t = 2^{k+1}t = \sigma(m)$. Ma m ha almeno i divisori 1, t , m ; se $t \neq 1$ questi sono tre divisori distinti (perché $2^{k+1} - 1 > 1$) e $\sigma(m) \geq 1 + t + m > m + t$, assurdo. Quindi $t = 1$, $m = 2^{k+1} - 1$ e i suoi soli divisori sono 1 e m : m è primo e $n = 2^k(2^{k+1} - 1)$ ha la forma di Euclide con $p = k + 1$. ■

p	Forma	Numero perfetto
2	$2^1 \cdot (2^2 - 1)$	6
3	$2^2 \cdot (2^3 - 1)$	28
5	$2^4 \cdot (2^5 - 1)$	496
7	$2^6 \cdot (2^7 - 1)$	8 128
13	$2^{12} \cdot (2^{13} - 1)$	33 550 336
17	$2^{16} \cdot (2^{17} - 1)$	8 589 869 056
19	$2^{18} \cdot (2^{19} - 1)$	137 438 691 328
31	$2^{30} \cdot (2^{31} - 1)$	2 305 843 008 139 952 128

Tabella 1. I primi otto numeri perfetti, uno per ogni primo di Mersenne con esponente p .

Dunque i numeri perfetti *pari* corrispondono uno a uno ai primi di Mersenne: se ne conoscono 52 (il più grande ha 82 048 640 cifre). Per i numeri perfetti *dispari* non si sa nulla: **non si conosce nessun numero perfetto dispari**, e si sa solo che, se esiste, è maggiore di 10^{1500} (Ochem e Rao, 2012). Non si sa neppure se i numeri perfetti siano infiniti.

L'ULTIMA CIFRA DEI NUMERI PERFETTI PARI

Tutti i numeri perfetti pari terminano con 6 o con 8, come si osserva dalla tabella. Infatti $n = 2^{p-1}(2^p - 1)$ con p primo. Se $p = 2$, $n = 6$. Se $p \geq 3$, 2^{p-1} è una potenza di 2 con $p - 1 \geq 2$, quindi termina con 2, 4, 6, 8 (mai con 0, altrimenti sarebbe multiplo di 5), e allora 2^p termina con 4, 8, 2, 6 rispettivamente, e $2^p - 1$ con 3, 7, 1, 5. L'ultima cifra 5 è impossibile, perché un multiplo di 5 maggiore di 5 non è primo. Restano le coppie di ultime cifre (2, 3), (4, 7), (6, 1), che danno prodotti terminanti in 6, 8, 6. ■

Primi gemelli

Due primi si dicono **gemelli** se differiscono di 2: (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), ... Per $p > 3$ il numero $p + 1$ che sta in mezzo (il «separatore») è multiplo di 6, come visto nel capitolo 13. La congettura sui primi gemelli afferma che **ne esistono infiniti**; è attribuita tradizionalmente a Euclide, ma non compare negli *Elementi*, ed è ancora aperta.

Fino a n	Coppie di primi gemelli
10^2	8
10^3	35
10^4	205
10^5	1 224
10^6	8 169

Tabella 2. Coppie di primi gemelli fino a 10^2 , ..., 10^6 (calcolate con un programma).

- **Congettura di Polignac** (1849): per ogni intero pari $2k$ esistono infinite coppie di primi che differiscono di $2k$. Per $k = 1$ si ha la congettura dei primi gemelli; per $2k = 4$ si hanno i *primi cugini* $((3, 7), (7, 11), (13, 17), \dots)$.
- **Teorema di Brun** (1915): la somma degli inversi dei primi gemelli converge. Quindi, anche se fossero infiniti, i primi gemelli sarebbero «rari», molto più rari dei primi, per i quali la somma degli inversi diverge.
- **Zhang, Maynard, Tao, Polymath** (dal 2013): Yitang Zhang dimostrò che esiste un intero N (inizialmente minore di 70 milioni) tale che infinite coppie di primi consecutivi differiscono di meno di N ; il lavoro di James Maynard e del progetto collaborativo Polymath ha ridotto il valore a 246. Si è quindi vicini, ma non a 2.
- **Congettura di Hardy e Littlewood**: il numero di coppie di gemelli fino a x è circa $2C_2 x/(\ln x)^2$, con la «costante dei primi gemelli» $C_2 = \prod (1 - 1/(p-1)^2) \approx 0,66016$, prodotto su tutti i primi $p \geq 3$.
- La più grande coppia di primi gemelli conosciuta (dal 2016, secondo le liste pubbliche) è $2996863034895 \cdot 2^{1290000} \pm 1$, con 388 342 cifre.

La congettura di Goldbach

Nel 1742 Christian Goldbach, matematico prussiano, scrisse a Eulero una lettera in cui avanzava due affermazioni sulle somme di primi; Eulero la riformulò nella forma che conosciamo.

CONGETTURA DI GOLDBACH

Ogni numero pari maggiore di 2 è somma di due numeri primi.

Esempi: $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7 = 5 + 5$, $12 = 5 + 7$, $14 = 3 + 11 = 7 + 7$, $16 = 3 + 13 = 5 + 11$, $18 = 5 + 13 = 7 + 11$. Il numero delle scritture cresce con il numero: 10 ha 2 rappresentazioni come somma di due primi (a meno dell'ordine), 100 ne ha 6, 1000 ne ha 28, 10000 ne ha 127, 100000 ne ha 810.

- **Verifiche al computer**: la congettura è stata verificata per tutti i pari fino a $4 \cdot 10^{18}$ (Oliveira e Silva e collaboratori, 2013). Nessun controesempio è noto.
- **Perché ci si crede**: per il teorema dei numeri primi, ci sono circa $n/\ln n$ primi minori di n , quindi circa $n^2/(2 \ln^2 n)$ coppie di primi minori di n , le cui somme sono tutti numeri minori di $2n$ e dunque tra n numeri pari. Poiché $n < n^2/(2 \ln^2 n)$ per $n \geq 14$, ci sono, in media, molte più coppie che numeri pari, e il numero di rappresentazioni di un pari cresce. Questo ragionamento euristico non è una dimostrazione.
- **Risultati parziali**: il teorema di Chen (1973) dice che ogni pari sufficientemente grande è somma di un primo e di un numero che è un primo o prodotto di due primi. La versione «debole» (ogni dispari maggiore di 5 è somma di tre primi) è stata dimostrata da Harald Helfgott nel 2013 e la dimostrazione è comunemente accettata. La versione forte, sopra, è ancora aperta.

DUE RIFORMULAZIONI E LA «DISTANZA DI GOLDBACH»

Se $p_1 + p_2 = 2x$ allora x è il punto medio dei due primi: $x = (p_1 + p_2)/2$. La congettura equivale allora a ciascuna delle due affermazioni seguenti.

- **G1**: per ogni intero $x \geq 2$ esiste un intero $d \geq 0$ tale che $x - d$ e $x + d$ sono entrambi primi;
- **G2**: per ogni intero $x \geq 2$ esistono due primi p_1, p_2 con $x = (p_1 + p_2)/2$.

Se x è primo basta prendere $d = 0$, cioè $p_1 = p_2 = x$. Dato n , il minimo d per cui $n - d$ e $n + d$ sono primi si chiama **distanza di Goldbach** $d(n)$, ed è definita per ogni n se e solo se la congettura è vera. Si ha $d(n) = 0$ se n è primo, $d(n) = 1$ se n è il separatore di due primi gemelli. Per $n = 2, \dots, 10$: d vale 0, 0, 1, 0, 1, 0, 3, 2, 3 (per esempio $d(8) = 3$ perché $8 - 3 = 5$ e $8 + 3 = 11$ sono primi, mentre 7 e 9, 6 e 10 non lo sono). Chiamiamo G_k l'insieme degli n con $d(n) = k$.

- G_0 = i numeri primi;
- $G_1 = \{4, 6, 12, 18, 30, 42, 60, 72, 102, 108, \dots\}$, i separatori dei gemelli (multipli di 6 tranne 4);
- $G_2 = \{9, 15, 21, 39, 45, 69, 81, 99, 105, 111, \dots\}$;
- $G_3 = \{8, 10, 14, 16, 20, 26, 34, 40, 44, 50, 56, 64, \dots\}$;
- $G_4 = \{27, 33, 57, 63, 75, 93, 135, 153, 177, 237, \dots\}$.

Gli insiemi G_k sono a due a due disgiunti, e la congettura di Goldbach equivale a dire che la loro unione è l'insieme di tutti gli interi ≥ 2 . Se n non è primo, n e $d(n)$ sono **coprimi**: se un $h > 1$ dividesse entrambi, dividerebbe $n - d(n)$ e $n + d(n)$, che sono primi, e quindi coinciderebbe con tutti e due, cioè $d(n) = 0$ (e n primo). (Per n primo, invece, $d(n) = 0$ e $\text{MCD}(n, 0) = n$, quindi la proprietà vale solo per n composti.) Non si sa se gli insiemi G_k siano infiniti (per G_1 è proprio la congettura sui gemelli) né se qualcuno sia vuoto.

Un altro insieme per cui la congettura vale per costruzione è quello degli **interprimi**, i punti medi di due primi consecutivi: $(p_n + p_{n+1})/2$ per $n \geq 2$, cioè 4, 6, 9, 12, 15, 18, 21, 26, 30, 34, ... Contiene i separatori dei primi gemelli e, più in generale, i punti medi delle coppie di primi consecutivi che differiscono di $2k$; non contiene 8 e 10.

La congettura di Collatz

La congettura di Collatz, o problema « $3x + 1$ », fu proposta da Lothar Collatz, matematico tedesco, nel 1937. Si definisce una funzione sugli interi positivi: se n è pari si divide per 2, se è dispari lo si moltiplica per 3 e si aggiunge 1; e si ripete finché si arriva a 1.

```
def collatz(x):
    traiettoria = [x]
    while x > 1:
        if x % 2 == 0:
            x = x // 2
        else:
            x = 3 * x + 1
        traiettoria.append(x)
    return traiettoria
```

CONGETTURA DI COLLATZ

Per ogni intero $x \geq 1$ l'algoritmo termina, cioè la successione parte da x e raggiunge 1.

La successione di numeri generata a partire da n si chiama **traiettoria** (o successione «grandine», perché sale e scende come i chicchi in una nube). Per esempio: $3 \rightarrow 10, 5, 16, 8, 4, 2, 1$; $6 \rightarrow 3, 10, 5, 16, 8, 4, 2, 1$; $7 \rightarrow 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1$. Il numero di *passi* necessari per arrivare a 1 è, per $n = 1, 2, \dots, 10$: 0, 1, 7, 2, 5, 8, 16, 3, 19, 6. La congettura non è stata né dimostrata né confutata: non si è mai trovato un numero la cui traiettoria diverga o cada in un ciclo diverso da 4, 2, 1.

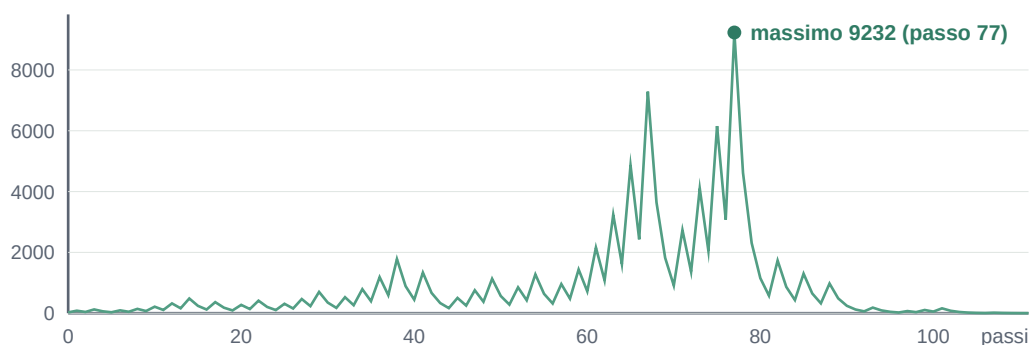


Figura 1. La traiettoria di 27: 111 passi, con un massimo di 9232 al passo 77, prima di precipitare a 1.

QUALCHE FENOMENO CURIOSO

- **Traiettorie lunghe.** Per alcuni interi la traiettoria è più lunga del numero stesso: 3, 6, 7, 9, 11, 14, 15, 18, 19, 27, 31, 41, ... Il numero 27 richiede 111 passi.
- **Valori massimi.** I valori massimi raggiunti per $n = 1, \dots, 16$ sono 1, 2, 16, 4, 16, 16, 52, 8, 52, 16, 52, 16, 40, 52, 160, 16. Per 27 e 31 il massimo è 9232, molto più grande dei loro quadrati (729 e 961). I numeri che stabiliscono un nuovo record di massimo sono 1, 2, 3, 7, 15, 27, 255, 447, 639, 703, 1819, ...
- **Versione abbreviata.** Poiché per x dispari $3x + 1$ è pari, si può passare direttamente a $(3x + 1)/2$, ottenendo traiettorie più corte (per 3: 3, 5, 8, 4, 2, 1).
- **Potenze di 2.** Basta raggiungere una potenza di 2, perché poi si scende fino a 1 dimezzando: la congettura equivale a «ogni traiettoria incontra una potenza di 2». Non si passa però sempre per 16: la traiettoria di 21 è 21, 64 e quella di 85 è 85, 256.

Perché 21 → 64 e 85 → 256? Se h è pari, $2^h \equiv (-1)^h = 1 \pmod{3}$, perché $2 \equiv -1 \pmod{3}$; quindi $2^h - 1 = 3k$ per un intero k , e k è dispari perché $3k$ è dispari. Allora a partire da k si ottiene $3k + 1 = 2^h$: $21 = (2^6 - 1)/3$ e $85 = (2^8 - 1)/3$.

COSA SI SA

- Al calcolatore la congettura è stata verificata per tutti gli interi di partenza fino ad almeno $2^{68} \approx 2,95 \cdot 10^{20}$ (Barina, 2020); aggiornamenti recenti riportano circa $2^{71} \approx 2,4 \cdot 10^{21}$.
- Un'euristica probabilistica rende plausibile la congettura: nella versione abbreviata un passo dispari moltiplica per circa $3/2$ e un passo pari per $1/2$, e se i due casi sono equiprobabili ogni coppia di passi moltiplica in media per $\sqrt{(3/2 \cdot 1/2)} = \sqrt{3}/2 \approx 0,87 < 1$, quindi i valori «tendono a decrescere». È un'argomentazione di plausibilità, non una dimostrazione.
- Nel 2019 Terence Tao ha dimostrato che «quasi tutte» le traiettorie (in un senso preciso, la densità logaritmica) scendono sotto qualsiasi funzione che tende all'infinito, per quanto lentamente; è il risultato più forte noto, ma lontano dalla congettura.
- Paul Erdős, uno dei più importanti matematici delle strutture discrete, commentò che «la matematica potrebbe non essere ancora pronta per problemi di questo tipo».

Calcolo combinatorio

Contare gli oggetti che ci interessano senza elencarli uno per uno: regole della somma e del prodotto, disposizioni, permutazioni, combinazioni, teorema binomiale, combinazioni con ripetizione e principio dei cassetti.

Perché contare

Una delle capacità più importanti per un informatico, o un matematico, è **contare**: sapere quanti sono gli oggetti o i casi di un certo tipo senza doverli elencare uno per uno. Non è un caso che la parola inglese *computer* derivi dal verbo *to compute*, cioè «calcolare». I problemi, però, sono spesso meno semplici di quanto sembri. Per esempio:

- quanti sono i codici PIN di una carta a 5 cifre, e quanto tempo serve a un programma per provare tutte le password di 8 simboli?
- quante squadre di calcio diverse si possono formare da un gruppo di 50 studenti?
- qual è la probabilità di un poker d'assi servito, o che in un'aula di 23 persone due compiano gli anni lo stesso giorno?

In questo capitolo costruiamo gli strumenti per rispondere alle domande di conteggio; le domande di probabilità, che dei conteggi fanno largo uso, sono nei capitoli 19, 20 e 21.

Regola della somma e regola del prodotto

REGOLA DELLA SOMMA

REGOLA DELLA SOMMA

Se A e B sono insiemi **disgiunti** (senza elementi in comune), allora $|A \cup B| = |A| + |B|$. Più in generale, se $A_1, \dots, A_k$ sono a due a due disgiunti, il numero degli elementi della loro unione è la somma delle loro cardinalità.

Le lettere dell'alfabeto inglese, minuscole e maiuscole, sono $26 + 26 = 52$; aggiungendo le 10 cifre si ottengono $52 + 10 = 62$ caratteri alfanumerici.

SE GLI INSIEMI NON SONO DISGIUNTI: INCLUSIONE ED ESCLUSIONE

Se A e B hanno elementi in comune, la somma $|A| + |B|$ conta due volte quelli di $A \cap B$, che vanno quindi sottratti una volta:

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

Per tre insiemi la formula, detta **principio di inclusione ed esclusione**, diventa

$$|A \cup B \cup D| = |A| + |B| + |D| - |A \cap B| - |A \cap D| - |B \cap D| + |A \cap B \cap D|$$

Perché funziona. Un elemento che sta in esattamente j dei tre insiemi (con j uguale a 1, 2 o 3) viene contato j volte nella prima somma, sottratto $C(j, 2)$ volte nella seconda e aggiunto $C(j, 3)$ volte nell'ultima. Il totale è 1 in ogni caso: $1; 2 - 1 = 1; 3 - 3 + 1 = 1$. Ogni elemento dell'unione è dunque contato esattamente una volta. Il principio si estende a un numero qualsiasi di insiemi, alternando i segni.

Esempio. Quanti sono i numeri da 1 a 100 divisibili per 2, per 3 o per 5? I multipli di 2 sono 50, di 3 sono 33, di 5 sono 20; i multipli comuni di 2 e 3 (cioè di 6) sono 16, di 2 e 5 (cioè di 10) sono 10, di 3 e 5 (cioè di 15) sono 6, e i multipli di 30 sono 3. Quindi $50 + 33 + 20 - 16 - 10 - 6 + 3 = 74$. Gli altri 26 numeri sono quelli non divisibili per nessuno dei tre.

REGOLA DEL COMPLEMENTO

Quando è più facile contare ciò che *non* interessa, si usa $|A| = |U| - |U \setminus A|$. Tipico è il caso di «almeno uno»: gli oggetti con almeno una certa proprietà sono tutti meno quelli che non ne hanno nessuna. Per esempio, i sottoinsiemi di $\{1, \dots, 10\}$ con 5 elementi che contengono almeno un numero pari sono $C(10, 5) - C(5, 5) = 252 - 1 = 251$, perché l'unico sottoinsieme di 5 elementi senza numeri pari è $\{1, 3, 5, 7, 9\}$.

REGOLA DEL PRODOTTO

REGOLA DEL PRODOTTO

Se dobbiamo eseguire k scelte in successione, la prima in n_1 modi, la seconda in n_2 modi, ..., la k esima in n_k modi, dove ogni numero non dipende dalle scelte precedenti, allora le scelte complessive sono $n_1 \cdot n_2 \cdot \dots \cdot n_k$.

Il caso di due insiemi è il prodotto cartesiano del capitolo 6: $|A \times B| = |A| \cdot |B|$. Le coppie di caratteri alfanumerici sono quindi $62 \cdot 62 = 3.844$. Attenzione al significato della condizione: a contare non sono le scelte disponibili ma il *loro numero*, che deve essere sempre lo stesso a prescindere da ciò che si è scelto prima. Per esempio, i PIN di 4 cifre che non iniziano per 0 e non hanno cifre ripetute sono $9 \cdot 9 \cdot 8 \cdot 7 = 4.536$: la prima cifra si sceglie in 9 modi (da 1 a 9), la seconda in 9 (le 10 cifre tranne quella già usata, e ora lo 0 è ammesso), la terza in 8 e la quarta in 7. Le scelte possibili cambiano a seconda dei casi, ma il loro numero no.

I PIN di 5 cifre sono $10^5 = 100.000$. Anche le targhe italiane si contano con il prodotto: hanno la forma LL 000 LL (due lettere, tre cifre, due lettere); con 26 lettere sarebbero $26^4 \cdot 10^3 = 456.976.000$, ma poiché non si usano le lettere I, O, Q, U ne restano 22 e le targhe possibili sono $22^4 \cdot 10^3 = 234.256.000$.

QUANTO CI METTE UN PROGRAMMA A TROVARE UNA PASSWORD?

Le password di 8 simboli scelti tra n simboli possibili sono n^8 . Il tempo per provarle tutte, a una velocità data, dipende dall'alfabeto in modo drammatico, come mostra la tabella (in media si trova la password dopo aver provato metà dei casi, ma l'ordine di grandezza resta lo stesso).

ALFABETO	PASSWORD DI 8 SIMBOLI	A 1.000 AL SECONDO	A 1 MILIARDO AL SECONDO
10 cifre	100.000.000	circa 28 ore	meno di un secondo
26 lettere minuscole	208.827.064.576	circa 7 anni	circa 3 minuti
36 (lettere minuscole e cifre)	2.821.109.907.456	circa 89 anni	circa 47 minuti
62 (maiuscole, minuscole, cifre)	218.340.105.584.896	circa 6.900 anni	circa 61 ore

Tabella 1. Tempo necessario per provare tutte le password di 8 simboli (distinguendo o meno maiuscole e minuscole).

Con le sole lettere minuscole e le cifre (36 simboli) servono circa 89 anni a 1.000 tentativi al secondo, ma meno di un'ora a un miliardo al secondo. Distinguere maiuscole e minuscole (62 simboli) moltiplica i casi per $(62/36)^8 \approx 77$, e a un miliardo di tentativi al secondo bastano comunque circa 61 ore. Ne segue una regola pratica: per rendere sicura una password conviene soprattutto aumentarne la *lunghezza*, perché l'esponente pesa molto più della base.

Disposizioni, permutazioni e combinazioni

Quattro problemi di conteggio ricorrono continuamente. Dati due insiemi A e B , con $|A| = k$ e $|B| = n$:

1. quante sono le applicazioni di A in B ? Il loro numero è detto numero delle **disposizioni con ripetizione** di n elementi di classe k ;
2. quante sono le applicazioni *iniettive* di A in B ? È il numero delle **disposizioni semplici** di n elementi di classe k , indicato con $D_{n,k}$;

3. quanti sono i sottoinsiemi di B con k elementi? È il numero delle **combinazioni** semplici, indicato con $C_{n,k}$ o con $C(n, k)$;
4. quanti sono i monomi di grado k , con coefficiente 1, nelle n variabili di B ? È il numero delle **combinazioni con ripetizione**.

DISPOSIZIONI CON RIPETIZIONE

TEOREMA: APPLICAZIONI TRA INSIEMI FINITI

Se $|A| = k$ e $|B| = n$, il numero delle applicazioni da A a B è n^k .

Dimostrazione. Per ciascuno dei k elementi di A dobbiamo scegliere la sua immagine tra gli n elementi di B , e le scelte sono indipendenti: per la regola del prodotto sono $n \cdot n \cdot \dots \cdot n = n^k$. ■

Equivalentemente, un'applicazione di A in B equivale a una k upla di elementi di B , cioè a un elemento di B^k (si veda il capitolo 6): le k uple si dicono disposizioni con ripetizione perché lo stesso elemento di B può comparire più volte. Se $B = \{a, b\}$, le disposizioni di classe 1 sono (a), (b); quelle di classe 2 sono (a, a), (a, b), (b, a), (b, b); quelle di classe 3 sono 8, e così via.

Esempio: assegnazioni di verità. Le funzioni da un insieme di k variabili in $\{0, 1\}$ sono 2^k : sono i modi di assegnare un valore di verità alle variabili, cioè le righe della tavola di verità. Non vanno confuse con le *funzioni booleane* di k variabili, che sono funzioni da $\{0, 1\}^k$ in $\{0, 1\}$: il dominio ha 2^k elementi e quindi le funzioni sono 2^{2^k} . Per $k = 2$ sono 16 (le sedici tavole di verità dei connettivi a due ingressi), per $k = 3$ sono 256, per $k = 4$ sono 65.536.

DISPOSIZIONI SEMPLICI

Un'applicazione iniettiva da A a B può esistere solo se $k \leq n$. In tal caso la scelta delle immagini si fa in successione: la prima in n modi, la seconda in $n - 1$ (non si può riusare l'immagine già scelta), ..., la k esima in $n - k + 1$ modi. Per la regola del prodotto

$$D_{n,k} = n \cdot (n - 1) \cdot \dots \cdot (n - k + 1) = n! / (n - k)!$$

dove $n!$ (fattoriale di n) è il prodotto $1 \cdot 2 \cdot \dots \cdot n$, con la convenzione $0! = 1$. Le disposizioni semplici sono le k uple di elementi *distinti* di B . Per $B = \{a, b, c\}$, quelle di classe 2 sono (a, b), (a, c), (b, a), (b, c), (c, a), (c, b), cioè $D_{3,2} = 3 \cdot 2 = 6$.

Esempio. Da un gruppo di 50 studenti si può formare una squadra di calcio di 11 giocatori in $D_{50,11} = 50 \cdot 49 \cdot \dots \cdot 40 \approx 1,49 \cdot 10^{18}$ modi, se si considerano diverse due squadre formate dagli stessi giocatori ma ordinati in modo diverso (per esempio perché ciascuno ha un ruolo).

PERMUTAZIONI

Le **permutazioni** di un insieme di n elementi sono le disposizioni semplici di classe n : $D_{n,n} = n \cdot (n - 1) \cdot \dots \cdot 1 = n!$. Un'applicazione iniettiva tra insiemi finiti con la stessa cardinalità è anche surgettiva, quindi le permutazioni sono le biezioni di un insieme in sé stesso, e si può vedere ciascuna come un riordinamento degli n elementi. Le permutazioni di $\{1, 2, 3\}$ sono $3! = 6$: (1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1).

Il fattoriale cresce più velocemente di qualsiasi potenza: $5! = 120$, $10! = 3.628.800$, $20! = 2.432.902.008.176.640.000 \approx 2,4 \cdot 10^{18}$, e i modi di ordinare un mazzo di 52 carte sono $52! \approx 8,07 \cdot 10^{67}$, un numero con 68 cifre. Per questo gli algoritmi che provano tutte le permutazioni sono praticabili solo per n molto piccolo (si veda il capitolo 24 per il problema del commesso viaggiatore).

COMBINAZIONI

Se non interessa l'ordine, ma solo *quali* elementi sono stati scelti, bisogna contare i sottoinsiemi. Consideriamo le $D_{n,k}$ applicazioni iniettive di A (con k elementi) in B (con $n \geq k$ elementi) e diciamo che due di esse, f e g , sono equivalenti se hanno la stessa immagine: $f(A) = g(A)$. È una relazione di equivalenza (capitolo 8), e le sue classi corrispondono ai sottoinsiemi di B con k elementi: sono quindi $C_{n,k}$. Ciascuna classe contiene tante applicazioni quante sono le biezioni di A sull'immagine, cioè $k!$. Contando le applicazioni in due modi,

$$D_{n,k} = C_{n,k} \cdot k! \quad \text{e dunque} \quad C(n, k) = n! / (k! (n - k)!)$$

I numeri $C(n, k)$, che si leggono « n su k », sono detti **coefficienti binomiali**. Poiché $0! = 1$ la formula vale anche per $k = 0$ e $k = n$, con $C(n, 0) = C(n, n) = 1$ (l'unico sottoinsieme senza elementi è l'insieme vuoto, e l'unico con tutti gli elementi è B). Dalla formula si vede subito la simmetria $C(n, k) = C(n, n - k)$: scegliere gli elementi da prendere equivale a scegliere quelli da lasciare.

Esempio. I sottoinsiemi di un insieme con 6 elementi hanno cardinalità da 0 a 6, e il loro numero è, rispettivamente, 1, 6, 15, 20, 15, 6, 1. La somma è $64 = 2^6$, in accordo con il fatto che un insieme con n elementi ha 2^n sottoinsiemi. Tornando alla squadra di calcio: se non interessa l'ordine, da 50 studenti si ottengono $C(50, 11) = 37.353.738.800$ squadre diverse, cioè $11! = 39.916.800$ volte meno di prima.

IDENTITÀ DI PASCAL

Per $1 \leq k \leq n - 1$ vale $C(n, k) = C(n - 1, k - 1) + C(n - 1, k)$.

Dimostrazione. Fissiamo un elemento x dell'insieme B di n elementi. I sottoinsiemi con k elementi si dividono in quelli che contengono x , che sono tanti quanti i sottoinsiemi con $k - 1$ elementi di $B \setminus \{x\}$, cioè $C(n - 1, k - 1)$, e quelli che non lo contengono, che sono i sottoinsiemi con k elementi di $B \setminus \{x\}$, cioè $C(n - 1, k)$. ■

L'identità permette di costruire tutti i coefficienti binomiali con sole addizioni, riga dopo riga: è il **triangolo di Pascal**, in cui ogni numero è la somma dei due che lo sovrastano e le righe sono simmetriche.

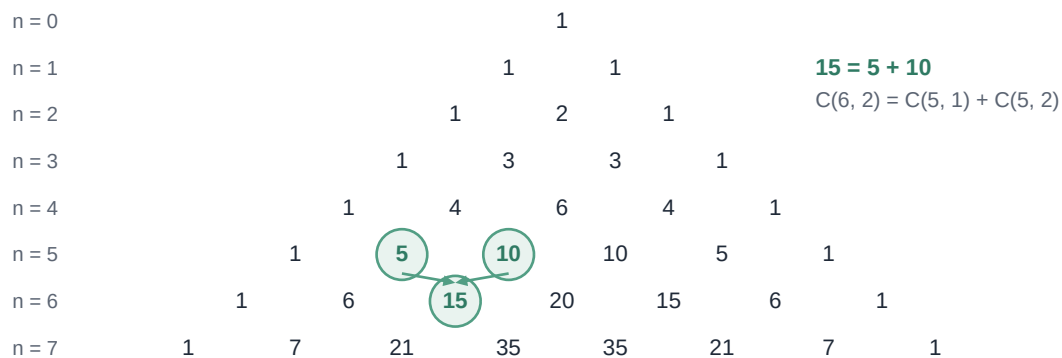


Figura 1. Il triangolo di Pascal fino alla riga 7: la riga n contiene i numeri $C(n, 0), \dots, C(n, n)$.

```
def riga_di_pascal(n):
    riga = [1]
    for _ in range(n):
        # ogni nuovo numero e' la somma dei due che lo sovrastano
        riga = [a + b for a, b in zip([0] + riga, riga + [0])]
    return riga

print(riga_di_pascal(6))  # [1, 6, 15, 20, 15, 6, 1]
```

ANAGRAMMI: PERMUTAZIONI CON ELEMENTI RIPETUTI

Quando alcuni oggetti sono uguali tra loro, le permutazioni si riducono. Gli **anagrammi** della parola CATANIA (che ha 7 lettere, di cui tre A) si contano scegliendo prima i 3 posti delle A, in $C(7, 3) = 35$ modi, e poi disponendo le altre 4 lettere distinte (C, T, N, I) nei posti rimasti, in $4! = 24$ modi: in tutto $35 \cdot 24 = 840 = 7!/3!$. In generale, se in una lista di n oggetti ce ne sono n_1 di un tipo, n_2 di un altro, ..., n_r dell'ultimo (con $n_1 + \dots + n_r = n$), le disposizioni distinte sono

$$n! / (n_1! \cdot n_2! \cdot \dots \cdot n_r!)$$

detto **coefficiente multinomiale**. Con due soli tipi si ritrovano i coefficienti binomiali: le sequenze di n simboli con k simboli «1» e $n - k$ simboli «0» sono $C(n, k)$.

Il teorema binomiale

Una delle scoperte più importanti di Isaac Newton, pubblicata alla fine del Seicento, è la formula che permette di elevare a una potenza qualsiasi un binomio, cioè una somma di due termini. La versione per esponenti interi non negativi, che qui interessa, era in realtà già nota ad altri matematici prima di lui; la sua geniale estensione riguarda gli esponenti non interi.

TEOREMA BINOMIALE

Per ogni coppia di numeri reali a e b e per ogni intero $n \geq 0$,

$$(a + b)^n = \sum_{k=0}^n C(n, k) \cdot a^{n-k} \cdot b^k.$$

Dimostrazione. La potenza $(a + b)^n$ è il prodotto di n fattori tutti uguali a $(a + b)$. Sviluppando il prodotto si ottiene una somma di monomi di grado n in a e b , della forma $a^{n-k} b^k$ con $0 \leq k \leq n$: da ciascun fattore si sceglie o a o b . Il monomio $a^{n-k} b^k$ compare tante volte quanti sono i modi di scegliere i k fattori da cui si prende b (gli altri $n - k$ forniscono a), cioè $C(n, k)$. In particolare a^n e b^n compaiono una volta sola, e $a^{n-1} b$ compare n volte. ■

Per esempio, usando le righe 4 e 5 del triangolo di Pascal, $(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$ e $(a + b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$. Il nome «coefficienti binomiali» viene proprio da qui.

CONSEGUENZE

- Per $a = b = 1$ si ottiene $\sum_{k=0}^n C(n, k) = 2^n$: la somma di una riga del triangolo di Pascal è il numero di tutti i sottoinsiemi di un insieme con n elementi.
- Per $a = 1$ e $b = 10$ si ottiene $\sum_{k=0}^n C(n, k) \cdot 10^k = 11^n$, un modo per leggere le potenze di 11 nel triangolo di Pascal.
- Per $a = 1$ e $b = -1$, e $n \geq 1$, si ottiene $\sum_{k=0}^n (-1)^k C(n, k) = 0$: i sottoinsiemi con un numero pari di elementi sono tanti quanti quelli con un numero dispari, cioè 2^{n-1} ciascuno.

Combinazioni con ripetizione

Quanti sono i monomi di grado k nelle n variabili $x_1, \dots, x_n$? Un monomio come $x_1^2 x_3 x_4^3$ (di grado 6) è determinato dagli esponenti, cioè da una n upla di interi non negativi la cui somma è k ; in altre parole è una scelta di k variabili, con possibili ripetizioni e senza interessare l'ordine. Con tre variabili x, y, z i monomi di grado 2 sono 6: $xy, xz, yz, x^2, y^2, z^2$.

COMBINAZIONI CON RIPETIZIONE

Il numero dei monomi di grado k in n variabili, cioè delle scelte non ordinate di k oggetti tra n tipi con ripetizione ammessa, è

$$C_{n,k}^r = C(n + k - 1, k) = (n + k - 1)! / (k! (n - 1)!).$$

Dimostrazione (metodo dei pallini e delle barre). Rappresentiamo un monomio con una riga di k pallini (uno per ogni fattore) separati da $n - 1$ barre, che dividono i pallini in n gruppi: il i esimo gruppo contiene tanti pallini quant'è l'esponente di x_i . Per esempio, con $n = 3$ variabili a, b, c e $k = 5$, la riga $\bullet \bullet \mid \bullet \mid \bullet \bullet$ rappresenta $a^2 b c^2$. Ogni monomio corrisponde a una e una sola riga di $k + n - 1$ posti, di cui $n - 1$ occupati dalle barre, e viceversa. Le righe si contano scegliendo i posti delle barre: $C(k + n - 1, n - 1) = C(n + k - 1, k)$. ■

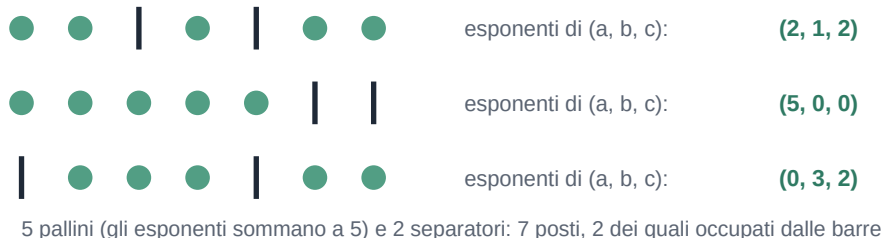


Figura 2. Tre monomi di grado 5 in tre variabili a, b, c e le corrispondenti righe di pallini e barre.

Lo stesso risultato conta le **soluzioni intere non negative** dell'equazione $x_1 + \dots + x_n = k$: sono $C(n + k - 1, k)$. Se si richiede invece $x_i \geq 1$ per ogni i , basta sottrarre 1 a ogni incognita e le soluzioni diventano $C(k - 1, n - 1)$. Per esempio, i monomi di grado 3 in 5 variabili sono $C(7, 3) = 35$: 10 con tre variabili distinte (come abc), 20 con una variabile al quadrato e un'altra al primo grado (come a^2b) e 5 cubi (come a^3).

IL QUADRO D'INSIEME

Le quattro situazioni nascono da due domande: l'ordine conta? lo stesso elemento può comparire più volte? Si parla anche di estrazioni da un'urna con n palline numerate, ordinate o no, con o senza reinserimento (capitolo 19).

Scelta di k elementi da n	Con ripetizione	Senza ripetizione
L'ordine conta	n^k	$n!/(n - k)!$
L'ordine non conta	$C(n + k - 1, k)$	$C(n, k)$

Tabella 2. Le quattro formule fondamentali di conteggio.

In Python la libreria *itertools* genera esattamente questi oggetti, ed è utile per controllare i conti su casi piccoli:

```
from itertools import product, permutations, combinations
from itertools import combinations_with_replacement
from math import comb, perm

n, k = 5, 3
print(len(list(product(range(n), repeat=k))))          # 125 = 5 alla 3
print(len(list(permutations(range(n), k))), perm(n, k)) # 60 60
print(len(list(combinations(range(n), k))), comb(n, k)) # 10 10
print(len(list(combinations_with_replacement(range(n), k)))) # 35 = comb(7, 3)
```

Esempi svolti

Il domino. Un domino è formato da tessere divise in due parti, ciascuna con un numero da 0 a 6; i due numeri possono coincidere. Le tessere con numeri diversi sono $C(7, 2) = 21$, perché una tessera è un sottoinsieme di due numeri tra i 7 possibili; a queste si aggiungono le 7 tessere con numeri uguali: in tutto 28. Lo stesso valore si ottiene come combinazioni con ripetizione di classe 2 di 7 elementi: $C(8, 2) = 28$.

Gruppi di persone. Un'azienda deve assumere 4 persone tra 8 candidati, 5 uomini e 3 donne. I gruppi possibili sono $C(8, 4) = (8 \cdot 7 \cdot 6 \cdot 5)/4! = 70$. I gruppi di soli uomini sono $C(5, 4) = 5$; i gruppi che contengono tutte e tre le

donne si formano scegliendo l'uomo mancante, in $C(5, 1) = 5$ modi: i due numeri sono uguali.

Parole con le lettere di CATANIA. Le lettere distinte della parola sono $\{C, A, T, N, I\}$. Le parole di quattro lettere distinte sono $5 \cdot 4 \cdot 3 \cdot 2 = D_{5,4} = 120$: si scelgono le 4 lettere, in $C(5, 4) = 5$ modi, e per ciascun gruppo si hanno $4! = 24$ ordinamenti ($5 \cdot 24 = 120$).

Gelato per tutti. Venti studenti vanno da un gelataio. Ci sono 8 gusti e ogni cono ha 3 porzioni, anche dello stesso gusto, senza interessare l'ordine. I coni diversi sono le combinazioni con ripetizione di classe 3 di 8 elementi: $C(10, 3) = 120$. Poiché $120 \geq 20$, è possibile che ogni studente abbia un cono diverso.

Il principio dei cassetti

Il **principio dei cassetti** (o della piccionaia, in inglese *pigeonhole principle*) fu usato sistematicamente dal matematico tedesco Peter Gustav Lejeune Dirichlet, ed è uno degli argomenti più semplici ed efficaci del calcolo combinatorio. Nella forma più semplice afferma che, se si devono sistemare $n + 1$ piccioni in n cassette, almeno una cassetta contiene più di un piccione.

PRINCIPIO DEI CASSETTI (FORMA GENERALE)

Se m oggetti sono distribuiti in n cassette, almeno un cassetto contiene almeno $\lceil m/n \rceil$ oggetti. In particolare, se $m = kn + 1$ allora un cassetto contiene almeno $k + 1$ oggetti.

Dimostrazione. Se ogni cassetto contenesse al più $\lceil m/n \rceil - 1$ oggetti, che è un numero minore di m/n , il totale degli oggetti sarebbe minore di $n \cdot (m/n) = m$: assurdo. Per $m = kn + 1$ si ha $\lceil m/n \rceil = k + 1$. ■

Il principio è non costruttivo: dimostra che qualcosa esiste senza dire dove si trova. Ecco alcune applicazioni.

La coppia di calzini. In un cassetto ci sono calzini neri e blu. Prendendone al buio 3, almeno 2 hanno lo stesso colore: i colori sono i «cassetti» e $3 = 2 \cdot 1 + 1$.

I capelli. Una persona ha, in media, circa 110.000 capelli, con un massimo che si può stimare, esagerando, in 200.000. La provincia di Catania ha più di un milione di abitanti, quindi, poiché i possibili numeri di capelli sono al più 200.001 (da 0 a 200.000), esistono almeno $\lceil 1.000.001 / 200.001 \rceil = 5$ persone con esattamente lo stesso numero di capelli.

Differenza multipla di n . Se S è un insieme di $n + 1$ interi distinti, esistono due interi $a, b \in S$ la cui differenza $a - b$ è un multiplo di n . Infatti i resti della divisione per n sono solo n (da 0 a $n - 1$), quindi due dei $n + 1$ interi hanno lo stesso resto e la loro differenza è divisibile per n (capitolo 14).

Numero di amici. In una stanza con $n \geq 2$ persone ce ne sono almeno due con lo stesso numero di amici (tra i presenti; l'amicizia è reciproca). Il numero di amici di ciascuno è un valore tra 0 e $n - 1$, ma i valori 0 e $n - 1$ non possono comparire insieme: se qualcuno è amico di tutti gli altri, nessuno ha 0 amici. Quindi i valori possibili sono al più $n - 1$, e le persone sono n : due coincidono.

Classi di resto. Se S è un insieme di m interi positivi e $0 < n < m$, almeno $\lceil m/n \rceil$ elementi di S hanno lo stesso resto nella divisione per n : i resti sono i cassetti. Con $m = 100$ interi ce ne sono almeno $\lceil 100/7 \rceil = 15$ con lo stesso resto modulo 7, almeno 20 modulo 5 e almeno 10 modulo 11. Se $m = qn + r$ con $0 \leq r < n$, il numero $\lceil m/n \rceil$ è q se $r = 0$ e $q + 1$ se $r > 0$.

Tre amici o tre estranei. In un gruppo di 6 persone ce ne sono sempre 3 che si conoscono tutte tra loro oppure 3 che non si conoscono affatto. Prendiamo una persona x : ognuna delle altre 5 la conosce oppure no, quindi, per il principio dei cassetti, almeno $\lceil 5/2 \rceil = 3$ appartengono alla stessa categoria. Supponiamo che x ne conosca 3, a, b, c (l'altro caso è simmetrico). Se due di loro si conoscono, per esempio a e b , allora x, a, b si conoscono tutti. Altrimenti a, b, c sono a due a due estranei. ■ Il numero 6 non si può abbassare: con 5 persone sedute attorno a un tavolo, ciascuna conoscente soltanto dei due vicini, non ci sono né tre conoscenti né tre estranei. Questo è il primo caso della teoria di Ramsey, che studia quanto «disordine» è impossibile evitare in strutture abbastanza grandi (si veda il capitolo 22 per il linguaggio dei grafi).

Esercizi di riepilogo svolti

QUESITO	SOLUZIONE	RISULTATO
Sottoinsiemi di 3 elementi di $\{1, \dots, 15\}$ con un solo numero primo	I primi sono 2, 3, 5, 7, 11, 13 (6) e i non primi 9: $6 \cdot C(9, 2)$	216
50 studenti: due nati lo stesso giorno del mese? lo stesso mese? lo stesso giorno e mese?	Cassetti: 31 giorni, 12 mesi, 366 date. Con $50 > 31$ e $50 > 12$ sì ai primi due; $50 < 366$ non è garantito il terzo	sì, sì, no
Funzioni iniettive da un insieme di 4 elementi a uno di 10	$10 \cdot 9 \cdot 8 \cdot 7$	5.040
Tra 90 interi, quanti hanno certamente lo stesso resto modulo 13?	$[90/13]$	7
Monomi di grado 4 in 5 variabili	$C(5 + 4 - 1, 4) = C(8, 4)$	70
Insiemi di 5 elementi, 2 da A (4 elementi) e 3 da B (6 elementi), con A e B disgiunti	$C(4, 2) \cdot C(6, 3)$	120
PIN di 4 cifre senza ripetizioni e che non cominciano per 0	$9 \cdot 9 \cdot 8 \cdot 7$	4.536
40 studenti da CT, SR, ME, RG; se quelli di CT sono meno di 10, ce ne sono almeno 11 da una stessa altra provincia	Gli altri sono almeno 31 in 3 province: $[31/3] = 11$	dimostrato
Sottoinsiemi di 5 elementi di $\{1, \dots, 10\}$ con almeno un numero pari	$C(10, 5) - C(5, 5)$	251
Esiste una funzione iniettiva dai sottoinsiemi di 5 elementi di $\{1, \dots, 9\}$ ai sottoinsiemi di 7 elementi di $\{1, \dots, 10\}$?	I primi sono $C(9, 5) = 126$, i secondi $C(10, 7) = 120$, e $126 > 120$	no

Tabella 3. Esercizi di riepilogo con le soluzioni.

Probabilità discreta

Spazio dei campioni, eventi, assiomi di Kolmogorov, probabilità condizionata, indipendenza, teorema di Bayes, problemi d'urna e alcuni celebri problemi con le loro soluzioni.

Le origini del calcolo delle probabilità

Lo studio sistematico della probabilità nasce tra la fine del Cinquecento e il Seicento da problemi legati al gioco d'azzardo, in particolare al gioco dei dadi. Tra i fondatori c'è il medico, matematico e filosofo italiano Gerolamo Cardano, autore del *Liber de ludo aleae*, in cui compaiono i concetti fondamentali della teoria (e anche alcune indicazioni su come barare). Su richiesta del Granduca di Toscana, Galileo Galilei scrisse un breve trattato sulle *scoperte dei dadi*, dove mostra che con tre dadi la somma 10 o 11 è più probabile della somma 9 o 12 (lo ricalcoleremo più avanti). Poco dopo un nobile francese, accanito giocatore, pose a Blaise Pascal questo problema: è più probabile ottenere almeno un 6 lanciando un dado 4 volte, oppure almeno un doppio 6 lanciando due dadi 24 volte? Pascal ne scrisse a Pierre de Fermat, e dalla loro corrispondenza nacquero le prime leggi della probabilità.

La risposta si trova con il passaggio al complemento: la probabilità di non ottenere mai un 6 in 4 lanci è $(5/6)^4$, quindi il primo evento ha probabilità $1 - (5/6)^4 \approx 0,5177$; la probabilità di non ottenere mai un doppio 6 in 24 lanci è $(35/36)^{24}$, quindi il secondo evento ha probabilità $1 - (35/36)^{24} \approx 0,4914$. Il primo gioco è favorevole al giocatore, il secondo no, di poco.

Spazio dei campioni ed eventi

La probabilità è definita su uno **spazio dei campioni** (o spazio campionario) S : l'insieme di tutti gli esiti possibili di un esperimento casuale. Gli elementi di S sono gli **esiti** o **eventi elementari**; un **evento** è un qualsiasi sottoinsieme di S , cioè un insieme di esiti. S stesso è l'**evento certo** e $\emptyset$ è l'**evento impossibile**. Due eventi E_1 e E_2 sono **mutuamente esclusivi** se $E_1 \cap E_2 = \emptyset$, cioè se non possono verificarsi insieme. Le operazioni sugli eventi sono quelle sugli insiemi del capitolo 3: l'unione è « A oppure B », l'intersezione è « A e B », il complemento è «non A ».

Esempio. Lanciando due monete (T per testa, C per croce) lo spazio dei campioni è $S = \{TT, TC, CT, CC\}$. L'evento «si ottiene una testa e una croce» è $E = \{TC, CT\}$. Lanciando un dado, $S = \{1, 2, 3, 4, 5, 6\}$ e l'evento «esce un numero minore di 3» è $\{1, 2\}$.

In questo corso lo spazio dei campioni è finito, o al più numerabile (**probabilità discreta**). In tal caso una distribuzione di probabilità è determinata assegnando a ogni esito ω un numero $p(\omega) \geq 0$, in modo che la somma di tutti i $p(\omega)$ sia 1; la probabilità di un evento A è la somma delle probabilità dei suoi esiti: $P(A) = \sum_{\omega \in A} p(\omega)$.

Che cosa significa «probabilità»?

Il concetto ha una storia di definizioni successive, ciascuna con pregi e limiti.

- **Definizione classica** (Laplace). La probabilità di un evento A è il rapporto tra il numero dei casi favorevoli f e il numero dei casi possibili n : $P(A) = f/n$. Per «esce un numero minore di 3» con un dado è $2/6 = 1/3$. La definizione presuppone che tutti i casi siano *ugualmente possibili*, e quindi in un certo senso è circolare: usa il concetto di probabilità per definirlo.
- **Definizione frequentista** (Richard von Mises, matematico austriaco poi statunitense, a cui si attribuisce anche il primo enunciato del problema del compleanno). Si ripete l'esperimento n volte e si definisce $P(A)$ come il limite della frequenza relativa f_A/n al crescere di n . Non richiede casi equiprobabili, ma non si applica agli

esperimenti non ripetibili: qual è la probabilità che nei prossimi 100 anni un meteorite colpisca la Terra provocando un'estinzione di massa?

- **Definizione soggettiva** (Bruno de Finetti, matematico italiano). La probabilità misura il grado di fiducia di un individuo nel verificarsi di un evento, e può essere definita come il prezzo che si è disposti a pagare per ricevere 1 se l'evento si verifica. Le valutazioni devono essere *coerenti*: non deve essere possibile costruire una scommessa che dia una vincita o una perdita certa. Chi gioca ignorando questa coerenza è destinato a perdere.
- **Definizione assiomatica** (Andrej Kolmogorov, 1933). Inserita nella teoria della misura, non dice *come* calcolare le probabilità ma elenca le proprietà che esse devono soddisfare; è quindi compatibile sia con l'approccio oggettivista sia con quello soggettivista, ed è quella usata oggi.

Assiomi e proprietà

ASSIOMI DI KOLMOGOROV (CASO DISCRETO)

Una **distribuzione di probabilità** P su S associa a ogni evento A un numero reale $P(A)$ in modo che

(A1) $P(A) \geq 0$ per ogni evento A ; **(A2)** $P(S) = 1$; **(A3)** se A e B sono mutuamente esclusivi, $P(A \cup B) = P(A) + P(B)$ (negli spazi infiniti si richiede l'additività per ogni successione numerabile di eventi a due a due esclusivi).

Da questi tre assiomi si ricavano tutte le altre proprietà. Le seguenti valgono per eventi qualsiasi A e B .

1. **Complemento.** $P(\text{non } A) = 1 - P(A)$: infatti A e il suo complemento sono esclusivi e la loro unione è S , quindi $P(A) + P(\text{non } A) = P(S) = 1$. In particolare $P(\emptyset) = 1 - P(S) = 0$.
2. **Intervallo.** $0 \leq P(A) \leq 1$, perché $P(A) \geq 0$ per (A1) e $P(\text{non } A) \geq 0$ implica $P(A) \leq 1$.
3. **Monotonia.** Se $A \subseteq B$ allora $P(A) \leq P(B)$: scrivendo B come unione disgiunta di A e di $B \setminus A$ si ha $P(B) = P(A) + P(B \setminus A) \geq P(A)$.
4. **Unione.** $P(A \cup B) = P(A) + P(B) - P(A \cap B)$. Per vederlo, $A \cup B$ è l'unione disgiunta di $A \setminus B$, $A \cap B$ e $B \setminus A$; inoltre $P(A) = P(A \setminus B) + P(A \cap B)$ e $P(B) = P(B \setminus A) + P(A \cap B)$. Sommando le prime due uguaglianze e sottraendo $P(A \cap B)$ si ottiene la formula (è l'analogo probabilistico dell'inclusione ed esclusione del capitolo 18).

NOTA SULLA FONTE

Nelle slide la formula dell'unione compare come terzo assioma. Insieme a $P(\emptyset) = 0$ e a $P(S) = 1$ è una scelta equivalente all'additività per eventi esclusivi (basta prendere $A \cap B = \emptyset$), ma è più naturale presentarla come *teorema*, come abbiamo fatto, e tenere come assioma la forma minima.

Una distribuzione si dice **uniforme** se tutti gli esiti hanno la stessa probabilità. Se S ha n elementi, per (A2) e (A3) ogni esito ha probabilità $1/n$ e un evento A ha probabilità $|A|/n$: si ritrova la definizione classica, e il calcolo delle probabilità si riduce a **contare** casi favorevoli e casi possibili con gli strumenti del capitolo 18.

Probabilità condizionata e indipendenza

Il verificarsi di un evento può cambiare la probabilità di un altro. La probabilità di A **condizionata** a B (con $P(B) > 0$) è

$$P(A | B) = P(A \cap B) / P(B)$$

Intuitivamente, sapere che B si è verificato restringe lo spazio dei campioni a B , e si valuta quale frazione di B cade anche in A . Da qui la **regola del prodotto** $P(A \cap B) = P(A | B) \cdot P(B)$, che si estende alle successioni di eventi:

$P(A_1 \cap \dots \cap A_k) = P(A_1) \cdot P(A_2 | A_1) \cdot \dots \cdot P(A_k | A_1 \cap \dots \cap A_{k-1})$. Per esempio, la probabilità di estrarre tre assi di seguito da un mazzo di 52 carte è $(4/52) \cdot (3/51) \cdot (2/50) = 1/5525$, lo stesso valore che si ottiene come $C(4, 3)/C(52, 3)$ contando i casi favorevoli e possibili.

EVENTI INDIPENDENTI

Due eventi A e B si dicono **indipendenti** se $P(A \cap B) = P(A) \cdot P(B)$. Se $P(B) > 0$ ciò equivale a $P(A | B) = P(A)$: sapere che B è accaduto non cambia la probabilità di A .

Dimenticare il concetto di indipendenza porta a errori gravi. Il più celebre è la **fallacia del giocatore**: chi gioca al lotto pensa che un numero «in ritardo», non uscito da molte estrazioni, abbia più probabilità di uscire alla prossima. È falso: le estrazioni sono eventi indipendenti e la probabilità non cambia. Allo stesso modo, lanciando un dado tre volte la sequenza (2, 1, 6) ha la stessa probabilità di (3, 3, 3): per l'indipendenza dei lanci entrambe valgono $(1/6)^3 = 1/216$.

ESCLUSIVI NON SIGNIFICA INDIPENDENTI

Due eventi mutuamente esclusivi, ciascuno con probabilità positiva, sono sempre *dependenti*: $P(A \cap B) = 0$ mentre $P(A) \cdot P(B) > 0$. Se si sa che A è accaduto, si è certi che B non lo è.

Probabilità totale e regola di Bayes

TEOREMA DELLA PROBABILITÀ TOTALE

Siano $B_1, \dots, B_n$ eventi a due a due mutuamente esclusivi, con $P(B_i) > 0$ e la cui unione è S (si dice che formano una **partizione** di S). Per ogni evento A

$$P(A) = \sum_{i=1}^n P(A | B_i) \cdot P(B_i).$$

Dimostrazione. Gli eventi $A \cap B_i$ sono a due a due esclusivi e la loro unione è A , perché i B_i ricoprono S . Per $(A3)$, $P(A) = \sum P(A \cap B_i)$, e per la regola del prodotto $P(A \cap B_i) = P(A | B_i) \cdot P(B_i)$. ■

Il teorema si usa quando è facile calcolare la probabilità di A *sapendo* in quale caso ci si trova. **Esempio.** Un mazzo di 52 carte è diviso in due mazzi, M_1 con 30 carte tra cui 3 assi e M_2 con 22 carte tra cui il quarto asso. Si sceglie un mazzo a caso e poi una carta a caso in quel mazzo: la probabilità di pescare un asso è

$$P(A) = (3/30) \cdot (1/2) + (1/22) \cdot (1/2) = 1/20 + 1/44 = 4/55 \approx 0,0727$$

REGOLA DI BAYES

Se $P(A) > 0$ e $P(B) > 0$, allora $P(B | A) = P(A | B) \cdot P(B) / P(A)$.

Dimostrazione. Per la regola del prodotto $P(A \cap B) = P(A | B) \cdot P(B) = P(B | A) \cdot P(A)$; dividendo per $P(A)$ si ottiene la tesi. ■

La regola prende il nome da Thomas Bayes, matematico, statistico e pastore presbiteriano inglese, che la usò nella prima metà del Settecento. Ha applicazioni in quasi tutti i campi della scienza e in particolare in informatica e intelligenza artificiale (filtri antispam, sistemi diagnostici, apprendimento automatico). Permette di passare da $P(\text{effetti} | \text{causa})$, spesso noto, a $P(\text{causa} | \text{effetti})$, che è ciò che si vuole sapere nella **diagnosi**. Se $P(E) = 1/10$, $P(S) = 4/10$ e $P(S | E) = 7/10$, allora $P(E | S) = (7/10 \cdot 1/10) / (4/10) = 7/40$. Quando $P(A)$ non è noto lo si calcola con la probabilità totale, e la regola assume la forma più usata, con una partizione $B_1, \dots, B_n$:

$$P(B_j | A) = P(A | B_j) \cdot P(B_j) / \sum_i P(A | B_i) \cdot P(B_i)$$

Un esempio che sorprende (dati inventati a scopo didattico). Una malattia colpisce l'1% delle persone. Un test la rileva nel 99% dei malati ma dà un falso allarme nel 5% dei sani. Se una persona risulta positiva, qual è la probabilità che sia malata? Con M = «malato» e $+$ = «test positivo»: $P(+)$ = $0,99 \cdot 0,01 + 0,05 \cdot 0,99 = 0,0594$, quindi $P(M | +)$ = $0,0099 / 0,0594 = 1/6 \approx 17\%$. Nonostante il test sembri accurato, quasi cinque positivi su sei sono falsi allarmi, perché i sani sono molto più numerosi dei malati. Ignorare la *probabilità a priori* $P(M)$ è un errore frequente.

Problemi d'urna

Gli esperimenti che si possono descrivere come «si estraggono una o più palline numerate da una o più urne» si chiamano **problemi d'urna**: il lancio di dadi, l'estrazione dei numeri del lotto e molti altri. L'ipotesi comune è che le estrazioni non siano truccate e che ciascuna estrazione dipenda dalla precedente solo attraverso il contenuto dell'urna. Si distinguono quattro modelli, secondo due criteri: l'estrazione è ordinata oppure no (l'ordine conta?) e la pallina estratta viene reinserita oppure no. Estruendo k palline da un'urna con n palline, i casi possibili sono quelli della tabella 2 del capitolo 18.

Estrazione di k palline da n	Con reinserimento	Senza reinserimento
Ordinata	n^k	$n!/(n - k)!$
Non ordinata	$C(n + k - 1, k)$	$C(n, k)$

Tabella 1. Numero di estrazioni possibili nei quattro modelli.

Attenzione: nel modello con reinserimento e senza ordine le estrazioni *non* sono equiprobabili (per esempio con due palline e due estrazioni, la coppia {1, 2} si può ottenere in due modi, la coppia {1, 1} in uno solo), quindi le probabilità non si calcolano dividendo per $C(n + k - 1, k)$. Per calcolare le probabilità conviene considerare estrazioni ordinate, che sono equiprobabili, anche quando interessa solo l'insieme estratto.

CODICI PIN

Un ladro tenta di indovinare un PIN di 5 cifre ($10^5 = 100.000$ casi) in 3 tentativi, senza ripetere codici già provati. La probabilità di sbagliare il primo tentativo è $(10^5 - 1)/10^5$, di sbagliare anche il secondo $(10^5 - 2)/(10^5 - 1)$, di sbagliare anche il terzo $(10^5 - 3)/(10^5 - 2)$. Per la regola del prodotto la probabilità di sbagliarli tutti è il prodotto, cioè $(10^5 - 3)/10^5$ (i fattori si semplificano), e la probabilità di indovinare è $1 - (10^5 - 3)/10^5 = 3/10^5 = 0,003\%$. È lo stesso risultato che si ottiene osservando che il PIN è uno dei 100.000 equiprobabili e i codici provati sono 3.

IL LOTTO

In un'urna ci sono 90 palline numerate e se ne estraggono 5. La probabilità che sia estratto il numero 1 è data dal rapporto tra le cinque che lo contengono, $C(89, 4) = 2.441.626$, e tutte le cinque, $C(90, 5) = 43.949.268$: risulta $1/18 \approx 5,6\%$, cioè esattamente $5/90$, come si poteva prevedere (il numero 1 occupa uno qualsiasi dei 5 posti sui 90 possibili). Se si estraessero cinque indipendenti, in media servirebbero 18 estrazioni per vederlo uscire (capitolo 20).

PALLINE DI DUE COLORI

In un'urna ci sono 3 palline bianche e 2 nere; si estrae due volte con reinserimento. Le sequenze possibili sono $5^2 = 25$, di cui $3^2 = 9$ con due bianche e $2^2 = 4$ con due nere: i casi con colori diversi sono $25 - 13 = 12$ e la loro probabilità è $12/25$.

Galileo e i tre dadi

Con tre dadi lo spazio dei campioni contiene le triple (x, y, z) , tutte equiprobabili: $6^3 = 216$. Le somme possibili sono i 16 valori da 3 a 18, ma 16 non divide 216, quindi alcune somme sono più probabili di altre. Per contare in quanti modi si ottiene una somma si osserva che tre numeri uguali danno 1 tripla, due uguali e uno diverso danno 3 triple, tre diversi danno 6 triple. La somma 10 si ottiene con $1 + 3 + 6$, $1 + 4 + 5$, $2 + 3 + 5$ (tre diversi, 18 triple) e con $2 + 2 + 6$, $2 + 4 + 4$, $3 + 3 + 4$ (due uguali, 9 triple): in tutto 27 triple, cioè probabilità $27/216 = 1/8$. La somma 9 si ottiene con $1 + 2 + 6$, $1 + 3 + 5$, $2 + 3 + 4$ (18 triple), con $1 + 4 + 4$, $2 + 2 + 5$ (6 triple) e con $3 + 3 + 3$ (1 tripla): 25 triple, probabilità $25/216$. Per simmetria (la somma s e la somma $21 - s$ hanno lo stesso numero di triple, sostituendo ogni valore v con $7 - v$) la somma 11 ha 27 triple e la 12 ne ha 25.

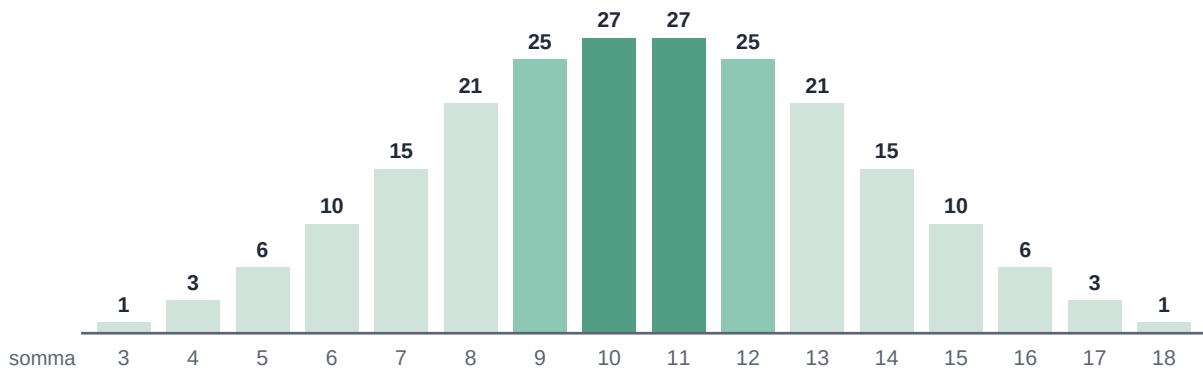


Figura 1. Numero di triple su 216 che danno ciascuna somma con tre dadi: 10 e 11 (27 casi ciascuna) battono 9 e 12 (25 casi ciascuna).

Quindi la probabilità di ottenere 10 o 11 è $54/216 = 1/4$, quella di ottenere 9 o 12 è $50/216 \approx 23\%$: Galileo aveva ragione.

Il problema del compleanno

Se dovessimo scommettere che in un'aula con 20 persone almeno due compiono gli anni lo stesso giorno, conviene scommettere di sì o di no? E con 30, 40, 50 persone? Il problema è noto come **paradosso del compleanno**, non perché porti a una contraddizione logica ma perché la risposta è controintuitiva. Per il principio dei cassetti, con almeno 367 persone la coincidenza è certa (i giorni dell'anno sono al più 366). Ma quando diventa più probabile che improbabile?

Una versione più semplice: i mesi. Quante persone servono perché sia più probabile che due siano nate nello stesso mese? Con 13 persone la coincidenza è certa. Con 3 persone i casi possibili sono $12^3 = 1.728$ e quelli con mesi tutti diversi sono $12 \cdot 11 \cdot 10 = 1.320$: la probabilità di mesi distinti è $1.320/1.728 \approx 0,76$, quindi la coincidenza ha probabilità $\approx 0,24$. Con 4 persone la probabilità di mesi distinti è $(12 \cdot 11 \cdot 10 \cdot 9)/12^4 \approx 0,57$, con 5 è $\approx 0,38$ ($95.040/248.832$): bastano **5 persone** perché la coincidenza sia più probabile del contrario ($\approx 62\%$).

Il compleanno. Il caso generale è analogo. Supponiamo che i giorni dell'anno siano 365 e che le nascite siano equiprobabili. Con p persone la probabilità che i compleanni siano tutti diversi è

$$P_d(p) = (365/365) \cdot (364/365) \cdot \dots \cdot ((365 - p + 1)/365)$$

perché la prima persona può avere un compleanno qualsiasi, la seconda uno dei 364 giorni rimanenti, e così via. Si può calcolare in modo ricorsivo: $P_d(p + 1) = P_d(p) \cdot (365 - p)/365$. La probabilità cercata di almeno una coincidenza è il complemento, $1 - P_d(p)$. Con 366 giorni (anno bisestile) i risultati cambiano pochissimo e la soglia resta la stessa.

PERSONE	COMPLEANNI TUTTI DIVERSI	ALMENO DUE COMPLEANNI UGUALI
10	0,883	0,117
20	0,589	0,411
23	0,493	0,507
30	0,294	0,706
40	0,109	0,891
50	0,030	0,970
70	0,001	0,999

Tabella 2. Probabilità nel problema del compleanno (365 giorni, nascite equiprobabili).

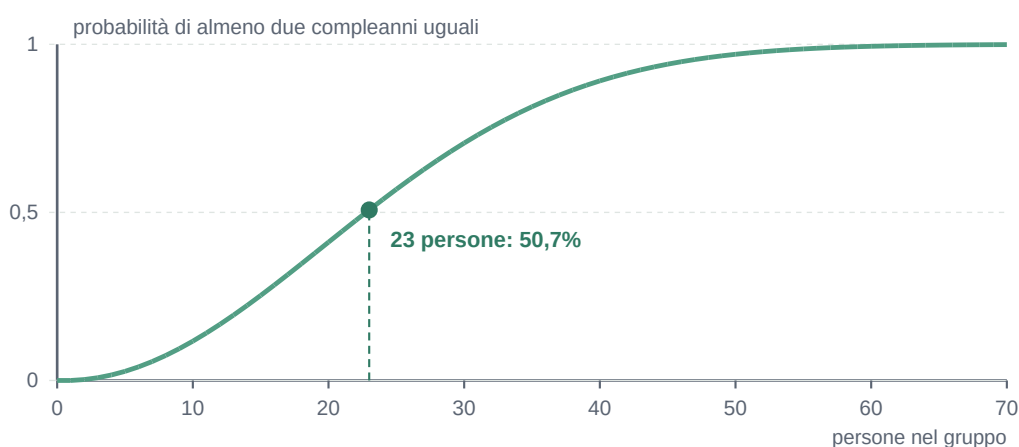


Figura 2. Probabilità di almeno due compleanni uguali in un gruppo di p persone: supera $1/2$ con $p = 23$.

Con 23 persone la probabilità di una coincidenza è circa il 50,7%, con 30 persone il 70%, con 50 persone il 97%, con 70 persone il 99,9%. Perché il risultato sorprende? Perché si pensa a un confronto con la *propria* data di nascita, mentre la coincidenza può avvenire tra qualunque coppia, e le coppie in un gruppo di 23 sono $C(23, 2) = 253$, molte più di 23. Il problema ha applicazioni importanti in informatica: la probabilità di **collisione** tra valori scelti a caso (per esempio le impronte hash) cresce con il numero di coppie, non con il numero di valori (capitolo 16).

CORREZIONE RISPETTO ALLE SLIDE

Nelle slide il calcolo per 23 persone si fa moltiplicando valori arrotondati ($0,58 \cdot 0,83 \approx 0,48$) e si conclude che la probabilità di una coincidenza è circa 0,52. Il valore corretto è 0,507 (con 365 giorni): l'arrotondamento intermedio ha introdotto un errore di circa 1,3 punti percentuali. La conclusione, però, non cambia: da 23 persone in poi conviene scommettere sulla coincidenza.

```

from itertools import islice

def prob_tutti_diversi(p, giorni=365):
    risultato = 1.0
    # i fattori sono giorni/giorni, (giorni meno 1)/giorni, ...
    for restanti in islice(reversed(range(giorni + 1)), p):
        risultato = risultato * restanti / giorni
    return risultato

# la probabilita di almeno una coincidenza e il complemento a 1
print(round(prob_tutti_diversi(23), 4)) # 0.4927

```

Altri problemi risolti

Una moneta contro due. A lancia una moneta una volta, B due volte. Qual è la probabilità che A ottenga più teste di B? Le 8 combinazioni (esito di A, esiti di B) sono equiprobabili. A può superare B solo se A ottiene testa e B non ne ottiene nessuna (CC): una sola combinazione su 8, quindi la probabilità è $1/8$.

Tre carte in ordine. Da dieci carte numerate da 1 a 10 se ne estraggono tre. Qual è la probabilità che escano in ordine crescente? Le tre carte estratte, in qualunque ordine, possono comparire in $3! = 6$ modi, e uno solo è crescente: la probabilità è $1/6$, indipendentemente dal numero delle carte.

UNA MONETA EQUA DA UNA MONETA TRUCCATA

Disponete di una moneta truccata che dà testa con probabilità p e croce con probabilità $1 - p$, con $p \neq 1/2$, e volete simulare una moneta equa. Il procedimento (attribuito a John von Neumann) è questo: si lanciano due volte; se i due esiti sono uguali si ripete, altrimenti si restituisce il primo.

```

import random

def lancio_truccato(p):
    return "T" if random.random() < p else "C"

def moneta_equa(p):
    while True:
        x = lancio_truccato(p)
        y = lancio_truccato(p)
        if x != y:
            return x

```

Perché funziona. Gli esiti (T, C) e (C, T) hanno la stessa probabilità $p(1 - p)$, quindi l'algoritmo restituisce T e C con uguale probabilità. Il ciclo si ferma quando i due lanci sono diversi, evento di probabilità $2p(1 - p)$; il numero medio di cicli è l'inverso, $1/(2p(1 - p))$ (capitolo 20): con $p = 1/5$ è $25/8 \approx 3,1$, con $p = 1/20$ è $200/19 \approx 10,5$.

POKER

Una mano di poker è formata da 5 carte scelte a caso dalle 52 del mazzo: le mani sono $C(52, 5) = 2.598.960$, tutte equiprobabili. Per avere un **poker d'assi servito** servono i 4 assi e una quinta carta qualunque tra le 48 rimaste: la probabilità è $48/2.598.960 = 1/54.145$, cioè circa 18 su un milione. Per avere una **scala colore** (cinque carte consecutive dello stesso seme, comprese le 4 scale reali 10, J, Q, K, A) si osservi che per ogni seme le scale si individuano dalla carta più bassa: dall'asso al 10, cioè 10 possibilità, perché l'asso conta sia come carta più bassa sia come più alta. Le scale colore sono $10 \cdot 4 = 40$ e la probabilità è $40/2.598.960 = 1/64.974$, circa 15 su un milione.

COMBINAZIONE	NUMERO DI MANI	PROBABILITÀ	FREQUENZA
Scala colore (comprese le 4 scale reali)	40	0,0015%	1 su 64.974
Poker	624	0,0240%	1 su 4.165
Full	3.744	0,1441%	1 su 694
Colore	5.108	0,1965%	1 su 509
Scala	10.200	0,3925%	1 su 255
Tris	54.912	2,1128%	1 su 47,3
Doppia coppia	123.552	4,7539%	1 su 21,0
Coppia	1.098.240	42,2569%	1 su 2,4
Carta alta	1.302.540	50,1177%	1 su 2,0

Tabella 3. Le mani di poker a cinque carte (le categorie si escludono a vicenda e sono classificate per esaurimento su tutte le mani).

Le formule di conteggio sono quelle del capitolo 18. Per il **poker** si sceglie il valore (13 modi) e la quinta carta (48 modi): $13 \cdot 48 = 624$. Per il **full** si scelgono il valore del tris (13), i suoi tre semi ($C(4, 3)$), il valore della coppia (12) e i suoi due semi ($C(4, 2)$): $13 \cdot 4 \cdot 12 \cdot 6 = 3.744$. Per il **colore** si scelgono il seme e cinque valori, $4 \cdot C(13, 5)$, togliendo le 40 scale colore: 5.108. Per la **scala** le 10 sequenze di valori hanno 4^5 assegnazioni di semi ciascuna, meno le 40 scale colore: 10.200. Per il **tris**: $13 \cdot C(4, 3) \cdot C(12, 2) \cdot 4^2 = 54.912$. Per la **doppia coppia**: $C(13, 2) \cdot 6^2 \cdot 44 = 123.552$. Per la **coppia**: $13 \cdot C(4, 2) \cdot C(12, 3) \cdot 4^3 = 1.098.240$. Il resto, 1.302.540 mani, è la **carta alta**.

NOTA TERMINOLOGICA

Nel poker italiano «scala reale» indica spesso soltanto la scala colore con l'asso più alto (10, J, Q, K, A); nelle slide, invece, il termine indica qualunque sequenza di cinque carte dello stesso seme. Qui usiamo «scala colore» per la seconda e «scala reale» per la prima. Il numero medio di mani da giocare per avere servito un poker d'assi è 54.145 (non 55 mila, come scritto nelle slide) e per una scala colore è circa 64.974 (non 66 mila).

Esercizi di riepilogo svolti

Ecco una raccolta di esercizi con le relative soluzioni. Quasi tutti si risolvono contando i casi favorevoli e i casi possibili con gli strumenti del capitolo 18, oppure passando al complemento; quando si parla di «estrazione» senza altra indicazione si intende senza reinserimento.

QUESITO	SOLUZIONE	RISULTATO
Urna con 2 rosse, 3 verdi, 2 bianche: 2 estrazioni senza reinserimento, nessuna bianca	$C(5, 2)/C(7, 2) = 10/21$	10/21
Dado con facce 2, 4, 8, 16, 32, 64: valore atteso	$(2 + 4 + 8 + 16 + 32 + 64)/6 = 126/6$	21
Il 10% dei possessori di portatile è informatico, il 5% ha Linux, il 40% degli informatici ha Linux: probabilità che chi ha Linux sia informatico	Bayes: $(0,4 \cdot 0,1)/0,05$	4/5
6 rosse, 5 verdi, 4 bianche: 3 palline senza reinserimento, tutte dello stesso colore	$(C(6, 3) + C(5, 3) + C(4, 3))/C(15, 3) = 34/455$	34/455

QUESITO	SOLUZIONE	RISULTATO
3 rosse, 3 bianche, 4 verdi: 3 palline, almeno due dello stesso colore	Complemento: tutte diverse in $3 \cdot 3 \cdot 4 = 36$ casi su $C(10, 3) = 120$	7/10
15 studenti (8 italiani, 7 stranieri): 3 scelti, almeno uno per tipo	$1 - (C(8, 3) + C(7, 3))/C(15, 3) = 1 - 91/455$	4/5
100 esami: 26 con il voto massimo, 70% ragazzi (20% di voto massimo), 30% ragazze (40%): da un esame con il voto massimo, ragazza o ragazzo?	Probabilità totale e Bayes: $0,7 \cdot 0,2 + 0,3 \cdot 0,4 = 0,26$; ragazza $0,12/0,26$, ragazzo $0,14/0,26$	6/13 e 7/13
2 dadi: somma prima	Somme 2, 3, 5, 7, 11 con $1 + 2 + 4 + 6 + 2 = 15$ casi su 36	5/12
10 palline numerate: 3 estratte, almeno 2 con numero primo (2, 3, 5, 7)	$(C(4, 2) \cdot C(6, 1) + C(4, 3))/C(10, 3) = 40/120$	1/3
12 palline (8 bianche, 3 rosse, 1 verde), 3 estratte: tutte bianche; nessuna bianca	$C(8, 3)/C(12, 3) = 56/220$; $C(4, 3)/C(12, 3) = 4/220$	14/55; 1/55
9 palline numerate: 2 estratte, numeri coprimi	27 coppie coprime su $C(9, 2) = 36$	3/4
12 persone (3 SR, 4 ME, 5 CT): 2 scelte della stessa provincia	$(C(3, 2) + C(4, 2) + C(5, 2))/C(12, 2) = 19/66$	19/66
11 persone (3 mancini, 2 ambidestri, 6 destrimani): 2 con la stessa caratteristica	$(C(3, 2) + C(2, 2) + C(6, 2))/C(11, 2) = 19/55$	19/55
8 palline (2 per ciascuno di 4 colori): 4 estratte, tutte di colore diverso	$2^4/C(8, 4) = 16/70$	8/35
10 carte (2 cuori, 2 quadri, 3 picche, 3 fiori): 2 dello stesso seme	$(1 + 1 + 3 + 3)/C(10, 2) = 8/45$	8/45
3 dadi: stesso valore	6 triple su 216	1/36
9 palline: 2 estratte in ordine (x_1, x_2) , $10x_1 + x_2$ multiplo di 9	Equivale a $x_1 + x_2 = 9$ (resto 0 modulo 9): 8 coppie ordinate su $9 \cdot 8 = 72$	1/9
Metà degli studenti UNICT risiede in provincia di CT e un terzo di questi a Catania: probabilità di essere residente a Catania	$(1/2) \cdot (1/3)$	1/6

Tabella 4. Esercizi di riepilogo con le soluzioni.

Variabili aleatorie e distribuzioni

Variabili casuali, valore atteso e sua linearità, varianza, prove di Bernoulli, distribuzioni binomiale e geometrica, disuguaglianza di Chebyshev e legge dei grandi numeri.

Variabili casuali

Spesso di un esperimento casuale non interessa l'esito in sé ma una quantità numerica che ne dipende: la somma dei punteggi di due dadi, il numero di teste in 10 lanci, il numero di tentativi prima di un successo. Una **variabile casuale** (o aleatoria) è una funzione X dallo spazio dei campioni S ai numeri reali: associa un numero $X(\omega)$ a ogni esito ω . L'evento « X assume il valore x » è l'insieme degli esiti $\{\omega : X(\omega) = x\}$, e si scrive $X = x$; la sua probabilità $P[X = x]$ come funzione di x è la **distribuzione** di X . Le probabilità $P[X = x]$, al variare di x , sommano a 1, perché gli eventi $X = x$ formano una partizione di S (capitolo 19).

Esempio. Sia X la somma dei punteggi di due dadi. Dei 36 esiti equiprobabili, la somma s si ottiene in 1, 2, 3, 4, 5, 6, 5, 4, 3, 2, 1 modi per $s = 2, 3, \dots, 12$:

Somma s	2	3	4	5	6	7	8	9	10	11	12
Casi su 36	1	2	3	4	5	6	5	4	3	2	1

Tabella 1. Distribuzione della somma di due dadi.

Valore atteso

VALORE ATTESO

Il **valore atteso** (o valore medio, o speranza matematica) di una variabile casuale X è

$$E[X] = \sum_x x \cdot P[X = x],$$

dove la somma è estesa a tutti i valori x che X può assumere. Raggruppando gli esiti per valore si ottiene anche

$$E[X] = \sum_{\omega \in S} X(\omega) \cdot p(\omega).$$

È la media dei valori, pesati con le loro probabilità, e rappresenta il valore che si ottiene in media su un grande numero di ripetizioni (si veda la legge dei grandi numeri, più avanti). Per un dado, $E[X] = 1 \cdot 1/6 + 2 \cdot 1/6 + \dots + 6 \cdot 1/6 = 21/6 = 3,5$. Il valore atteso non è necessariamente un valore che la variabile può assumere: con un dado non esce mai 3,5.

LINEARITÀ

LINEARITÀ DEL VALORE ATTESO

Per ogni coppia di variabili casuali X e Y sullo stesso spazio, e per ogni coppia di numeri a e b ,

$$E[X + Y] = E[X] + E[Y] \quad \text{e} \quad E[aX + b] = a \cdot E[X] + b.$$

Dimostrazione. Usando la forma $E[X] = \sum_{\omega} X(\omega) p(\omega)$: $E[X + Y] = \sum_{\omega} (X(\omega) + Y(\omega)) p(\omega) = \sum_{\omega} X(\omega) p(\omega) + \sum_{\omega} Y(\omega) p(\omega)$. La seconda uguaglianza si dimostra allo stesso modo. ■

La proprietà è molto potente perché vale **sempre**, anche quando X e Y sono dipendenti. Lanciando due dadi, $E[X + Y] = 3,5 + 3,5 = 7$, senza dover usare la tabella 1 (la cui somma pesata dà lo stesso risultato).

Il massimo di due dadi. Per m da 1 a 6, i casi su 36 in cui il massimo vale m sono $2m - 1$ (le coppie con massimo 6 sono 11, con 5 sono 9, ..., con 1 solo una). Quindi

$$E[\max] = (6 \cdot 11 + 5 \cdot 9 + 4 \cdot 7 + 3 \cdot 5 + 2 \cdot 3 + 1 \cdot 1)/36 = 161/36 \approx 4,47$$

(il massimo è in media più alto di 3,5). Conviene scommettere che il massimo sia maggiore di 4? Il massimo è 5 o 6 in $9 + 11 = 20$ casi su 36, probabilità $5/9 > 1/2$: sì.

VARIABILI INDICATRICI

La linearità si sfrutta al meglio con le **variabili indicatrici**: per un evento A , la variabile I_A vale 1 se A si verifica e 0 altrimenti, e quindi $E[I_A] = P(A)$. Un conteggio si scrive come somma di indicatrici, e il suo valore atteso come somma di probabilità, senza dover capire la distribuzione complessiva.

Esempio: l'amico segreto. n persone mettono il proprio biglietto in un'urna e ciascuna ne pesca uno a caso (una permutazione casuale). Quante persone pescano in media il proprio nome? Sia I_i l'indicatrice dell'evento «la persona i pesca il proprio biglietto»: $P = 1/n$. Il numero di punti fissi è $X = I_1 + \dots + I_n$ e $E[X] = n \cdot (1/n) = 1$, **qualunque sia** n . Eppure le I_i non sono indipendenti: la linearità non lo richiede.

VALORE ATTESO DI UN PRODOTTO, VARIANZA

Due variabili X e Y sono **indipendenti** se $P[X = x, Y = y] = P[X = x] \cdot P[Y = y]$ per ogni x e y . In questo caso $E[XY] = \sum_{x,y} xy \cdot P[X = x] \cdot P[Y = y] = E[X] \cdot E[Y]$. In generale *non* vale (per esempio $E[X^2] \neq E[X]^2$, come vedremo).

Il valore atteso dice dove si trova il «centro» della distribuzione ma non quanto sono dispersi i valori. La **varianza** misura la dispersione:

$$\text{Var}(X) = E[(X - \mu)^2] = E[X^2] - \mu^2, \text{ con } \mu = E[X]$$

La seconda forma segue sviluppando il quadrato e usando la linearità: $E[X^2 - 2\mu X + \mu^2] = E[X^2] - 2\mu^2 + \mu^2$. La **deviazione standard** è $\sigma = \sqrt{\text{Var}(X)}$, nelle stesse unità di X . Per un dado $E[X^2] = 91/6$ e $\text{Var} = 91/6 - 49/4 = 35/12 \approx 2,92$ ($\sigma \approx 1,71$). Proprietà: $\text{Var}(aX + b) = a^2 \text{Var}(X)$; e se X e Y sono indipendenti, $\text{Var}(X + Y) = \text{Var}(X) + \text{Var}(Y)$, perché il termine misto $2(E[XY] - E[X]E[Y])$ si annulla. Per la somma di due dadi, $\text{Var} = 35/6$.

Prove di Bernoulli

Una **prova di Bernoulli** (da Jacob Bernoulli, matematico svizzero di una celebre famiglia di studiosi, autore dell'*Ars conjectandi*, in cui compare la prima forma della legge dei grandi numeri) è un esperimento con due soli esiti: **successo**, con probabilità p , e **insuccesso**, con probabilità $q = 1 - p$. In una successione di prove **indipendenti** la probabilità di successo resta costante. Lanciare una moneta, tirare un dado osservando se esce 6, controllare se un componente prodotto è difettoso sono prove di Bernoulli.

DISTRIBUZIONE BINOMIALE

Il numero X di successi in n prove indipendenti ha una **distribuzione binomiale**. Una particolare sequenza con k successi e $n - k$ insuccessi ha probabilità $p^k q^{n-k}$ (indipendenza), e le sequenze di questo tipo sono $C(n, k)$: scegliamo le posizioni dei successi. Quindi

$$P[X = k] = C(n, k) \cdot p^k \cdot q^{n-k}, \quad k = 0, 1, \dots, n$$

La somma di queste probabilità è $(p + q)^n = 1$ per il teorema binomiale (capitolo 18): è da qui che viene il nome. Con la linearità si ricava subito il valore atteso: X è la somma di n indicatrici indipendenti, ciascuna con valore atteso p , quindi $E[X] = np$, e la varianza è npq (somma di varianze, per l'indipendenza, ciascuna pq). Ad esempio, in 10 lanci di una moneta equa la probabilità di avere esattamente 5 teste è $C(10, 5)/2^{10} = 252/1.024 \approx 24,6\%$, e tra 4 e 6 teste $672/1.024 \approx 66\%$, e in media si hanno 5 teste, con deviazione standard $\sqrt{2,5} \approx 1,6$.

DISTRIBUZIONE GEOMETRICA: L'ATTESA DEL PRIMO SUCCESSO

Sia X il numero di prove necessarie per ottenere il **primo** successo. Perché sia $X = k$ servono $k - 1$ insuccessi seguiti da un successo: $P[X = k] = q^{k-1} p$, con $k = 1, 2, 3, \dots$ (**distribuzione geometrica**). Il valore atteso è

$$E[X] = 1 \cdot p + 2 \cdot qp + 3 \cdot q^2 p + \dots = \sum_{k \geq 1} k q^{k-1} p = 1/p$$

Dimostrazione. Alla prima prova, con probabilità p si ha successo e ci si ferma (1 prova); con probabilità q la prova è sprecata e si ricomincia da capo: $E = p \cdot 1 + q \cdot (1 + E)$, cioè $E(1 - q) = 1$ e $E = 1/p$. Con le serie: $\sum_{k \geq 1} k q^{k-1}$ è la derivata di $\sum q^k = 1/(1 - q)$ e vale $1/(1 - q)^2 = 1/p^2$; moltiplicando per p si ottiene $1/p$. ■

Quanto minore è la probabilità di successo, tanto maggiore è il numero medio di tentativi, in modo inversamente proporzionale. Esempi:

- per ottenere testa con una moneta equa servono in media $1/(1/2) = 2$ lanci; per ottenere un 6 con un dado, 6 lanci;
- estraendo una carta da un mazzo siciliano (40 carte), rimettendola se non è un asso, servono in media $1/(1/10) = 10$ estrazioni per pescare un asso;
- per estrarre un numero fissato del Lotto, che esce con probabilità $1/18$ a ogni estrazione, servono in media 18 estrazioni;
- per vedere tre assi di seguito (probabilità $1/5525$) servono in media 5.525 tentativi; per un poker d'assi servito ($1/54.145$) in media 54.145 mani (capitolo 19).

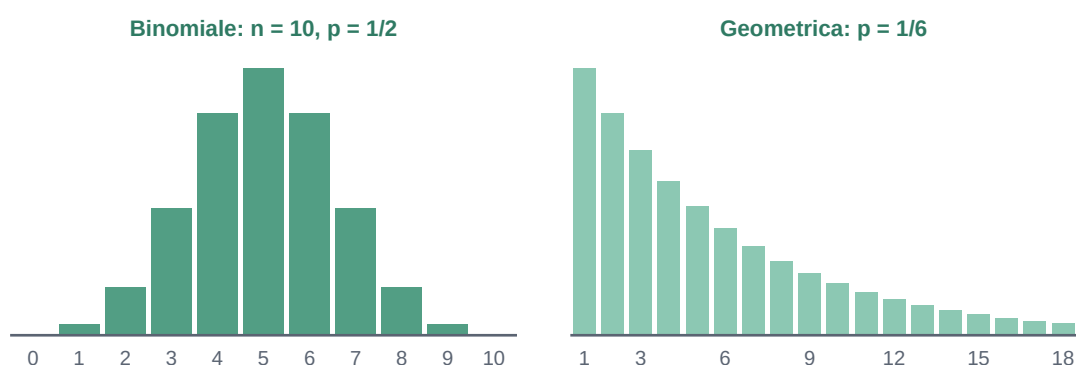


Figura 1. A sinistra, la distribuzione binomiale con $n = 10$ e $p = 1/2$ (simmetrica attorno a 5); a destra, la distribuzione geometrica con $p = 1/6$: ogni valore è meno probabile del precedente.

LA GEOMETRICA NON HA MEMORIA

Per la distribuzione geometrica $P[X > m] = q^m$ (i primi m tentativi falliscono), quindi $P[X > m + n \mid X > m] = q^m \cdot q^n / q^m = q^n = P[X > n]$. Dopo m insuccessi, l'attesa del successo ricomincia come all'inizio: è la versione quantitativa del fatto che «il numero in ritardo» al lotto non ha più probabilità di uscire (capitolo 19).

La moneta equa da una moneta truccata. Nell'algoritmo del capitolo 19 il ciclo termina quando i due lanci sono diversi, con probabilità $2p(1 - p)$ a ogni giro; il numero atteso di giri è quindi $1/(2p(1 - p))$. Per $p = 1/5$ sono $25/8 \approx 3,1$ giri, per $p = 1/20$ sono $200/19 \approx 10,5$. Nel caso migliore, $p = 1/2$, sono 2 giri.

RACCOGLIERE TUTTE LE FIGURINE

Quante volte bisogna lanciare un dado, in media, per vedere tutte e sei le facce? Dopo aver visto k facce diverse, la probabilità che il prossimo lancio ne mostri una nuova è $(6 - k)/6$, e l'attesa di una faccia nuova è geometrica con valore atteso $6/(6 - k)$. Per linearità, il numero totale atteso di lanci è

$$6/6 + 6/5 + 6/4 + 6/3 + 6/2 + 6/1 = 6 \cdot (1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6) = 14,7$$

In generale, per completare un album di n figurine equiprobabili servono in media $n \cdot (1 + 1/2 + \dots + 1/n)$ acquisti, circa $n \ln n$: per $n = 100$ sono circa 519, più di cinque volte il numero delle figurine (è il cosiddetto problema del collezionista).

Legge dei grandi numeri

Come si collega il valore atteso alla frequenza osservata? La **legge dei grandi numeri** (o teorema di Bernoulli, pubblicato postumo nel 1713) afferma che la media dei risultati di molte prove indipendenti si avvicina al valore atteso. Si dimostra con una disuguaglianza dovuta a Pafnuty Chebyshev.

DISUGUAGLIANZA DI CHEBYSHEV

Se X ha valore atteso μ e varianza σ^2 , per ogni $t > 0$ vale $P[|X - \mu| \geq t] \leq \sigma^2/t^2$.

Dimostrazione. $\sigma^2 = \sum_x (x - \mu)^2 P[X = x] \geq \sum_{|x - \mu| \geq t} (x - \mu)^2 P[X = x] \geq t^2 \cdot P[|X - \mu| \geq t]$. ■

LEGGE (DEBOLE) DEI GRANDI NUMERI

Siano $X_1, \dots, X_n$ variabili indipendenti con lo stesso valore atteso μ e la stessa varianza σ^2 , e sia M_n la loro media. Per ogni $\varepsilon > 0$,

$P[|M_n - \mu| \geq \varepsilon] \leq \sigma^2/(n\varepsilon^2)$, che tende a 0 per $n \rightarrow \infty$.

Dimostrazione. Per linearità $E[M_n] = \mu$, e per l'indipendenza $\text{Var}(M_n) = n\sigma^2/n^2 = \sigma^2/n$. Si applica la disuguaglianza di Chebyshev a M_n . ■

Con i lanci di un dado ($\mu = 3,5$, $\sigma^2 = 35/12$), dopo 1.000 lanci la probabilità che la media si discosti da 3,5 di almeno 0,2 è al più $(35/12)/(1.000 \cdot 0,04) \approx 7\%$. Per la moneta il risultato giustifica la definizione frequentista del capitolo 19: la frequenza delle teste si avvicina a $1/2$.

ATTENZIONE

La legge vale per i *grandi* numeri e riguarda le *medie*, non compensa gli scarti passati. Il ragionamento «il 6 non è uscito in 100 lanci, quindi al lancio 101 è più probabile» è sbagliato: i lanci sono indipendenti. Le deviazioni iniziali non vengono «recuperate»: vengono semplicemente diluite dai lanci successivi, perché la media su un numero enorme di prove pesa poco anche uno scarto grande.

Paradossi probabilistici

Quando il calcolo corretto delle probabilità contraddice l'intuizione: i due bambini, le tre carte, i tre prigionieri e il problema di Monty Hall, con un metodo sicuro per non sbagliare.

Il fascino dei problemi controintuitivi

Come già visto con il problema del compleanno (capitolo 19), esistono problemi per i quali il calcolo corretto delle probabilità dà una risposta fortemente contraria all'intuizione. Molti, proposti come giochi, sono diventati celebri per le dispute che hanno generato e per l'ingegno dei loro autori. Il divulgatore più famoso fu il matematico statunitense Martin Gardner, che per oltre vent'anni curò la rubrica «Giochi matematici» (*Mathematical Games*) sulla rivista *Scientific American*. In questo capitolo rivediamo quattro esempi: il paradosso dei due bambini, il paradosso delle tre carte (o delle tre scatole), quello dei tre prigionieri e il problema di Monty Hall.

UN METODO PER NON SBAGLIARE

In tutti questi problemi gli errori nascono dallo stesso punto: si valuta la probabilità *dopo* un'informazione senza chiedersi **come** l'informazione è stata ottenuta. Il metodo sicuro è sempre lo stesso: (1) elencare gli esiti elementari equiprobabili dell'intero esperimento, includendo anche la scelta di chi fornisce l'informazione; (2) eliminare quelli incompatibili con ciò che si è osservato; (3) contare, tra i rimasti, quelli favorevoli. In alternativa, si applica la regola di Bayes (capitolo 19).

Il paradosso dei due bambini

Un professore di probabilità passeggia con il figlio e vi dice: «Ho due figli». La domanda è: qual è la probabilità che anche l'altro figlio sia maschio? La risposta dipende da *come* si è venuti a sapere che c'è un maschio, ed è proprio questo il punto del problema. Indicando con M e F un figlio maschio e femmina, nell'ordine di nascita, ci sono 4 possibilità equiprobabili: MM, MF, FM, FF.

PRIMA LETTURA: «ALMENO UNO DEI DUE È MASCHIO»

Se l'unica informazione è che i figli *non* sono due femmine, FF viene escluso. Restano 3 casi equiprobabili (MM, MF, FM), di cui uno solo con due maschi: la probabilità è **1/3**. Per la regola di Bayes: $P(\text{MM} \mid \text{almeno un maschio}) = (1 \cdot 1/4) / (3/4) = 1/3$.

SECONDA LETTURA: «IL FIGLIO MAGGIORE È MASCHIO»

Se l'informazione riguarda un figlio *specificato in anticipo* (per esempio il primo), restano MM e MF: la probabilità che anche l'altro sia maschio è **1/2**. Il sesso del secondo figlio è indipendente da quello del primo.

TERZA LETTURA: IL PROFESSORE PASSEGgia CON UN FIGLIO, SCELTO A CASO

Se incontriamo il professore con un figlio e sappiamo solo che si tratta di un maschio, dobbiamo considerare anche la scelta di *quale* figlio è con lui. Con MM il figlio visibile è maschio per certo, con MF o FM lo è con probabilità 1/2, con FF mai. Per la regola di Bayes

$$P(\text{MM} \mid \text{visto un maschio}) = (1/4 \cdot 1) / (1/4 \cdot 1 + 2/4 \cdot 1/2 + 1/4 \cdot 0) = (1/4) / (1/2) = 1/2$$

Quindi, con questa seconda procedura di acquisizione dell'informazione, la probabilità è **1/2**. Il fatto che il padre sia accompagnato da un maschio rende più probabile MM rispetto a MF o FM esattamente quanto basta a compensare l'esclusione di FF.

CORREZIONE RISPETTO ALLE SLIDE

Le slide presentano la domanda «il professore passeggia con il figlio, qual è la probabilità che l'altro sia maschio?» come equivalente a «non sono due femmine», concludendo $1/3$. Le due formulazioni non sono equivalenti: il risultato $1/3$ vale soltanto se l'informazione è «almeno un maschio»; se il maschio incontrato è uno dei due figli scelto a caso, la risposta è $1/2$. Il problema, così com'è enunciato, è ambiguo, e va sempre specificato come si è ottenuta l'informazione.

Una variante che sorprende. Se si sa che «almeno uno dei due figli è un maschio nato di martedì», la probabilità che entrambi siano maschi sale a $13/27 \approx 48\%$, quasi $1/2$. Enumerando i $14 \cdot 14 = 196$ casi (sesso e giorno di nascita di ciascun figlio), i casi con almeno un maschio nato di martedì sono 27 e in 13 di essi i figli sono entrambi maschi. Più si precisa l'informazione, più ci si avvicina a $1/2$.

Il paradosso delle tre carte (o delle tre scatole)

Il problema, noto già alla fine dell'Ottocento e riportato dal matematico francese Joseph Bertrand nel 1889 nella versione delle scatole, ha due formulazioni equivalenti.

- **Tre carte.** Una carta, R, è rossa su entrambi i lati; un'altra, B, è bianca su entrambi; la terza, M, è rossa da un lato e bianca dall'altro. Se ne sceglie una a caso e la si pone sul tavolo, su un lato scelto a caso. Se il lato visibile è rosso, qual è la probabilità che anche l'altro lato sia rosso?
- **Tre scatole.** Una scatola contiene due monete d'oro, un'altra due d'argento, la terza una d'oro e una d'argento. Si sceglie una scatola a caso, si estrae a caso una moneta e risulta d'oro: qual è la probabilità che anche l'altra moneta sia d'oro?

L'intuizione dice $1/2$: «la carta è R o M, due casi». Ma i due casi non sono equiprobabili. Elenchiamo i 6 esiti elementari equiprobabili (carta, lato visibile): R con il primo lato visibile, R con il secondo, M con il lato rosso, M con il lato bianco, B con il primo lato, B con il secondo. Il lato visibile è rosso in 3 di questi esiti: i due di R e quello di M. Nei due casi di R anche l'altro lato è rosso, nel caso di M è bianco.

$$P(\text{altro lato rosso} \mid \text{lato visibile rosso}) = 2/3$$

Con le monete è identico: la moneta vista è una delle tre monete d'oro, due delle quali si trovano nella scatola con due monete d'oro. La probabilità è $2/3$. L'errore dell'intuizione sta nel contare le *carte* invece dei *lati*: una carta R fornisce due modi per vedere un lato rosso, la carta M uno solo.

Il paradosso dei tre prigionieri

Il problema, proposto da Martin Gardner nel 1959, è il seguente. Tre condannati a morte, A, B e C, sono in celle separate. Il re ha deciso di graziarne uno, scelto a caso; il carceriere sa chi sarà, ma non può rivelarlo. A chiede al carceriere di dirgli il nome di uno tra B e C che sarà giustiziato: «Se B sarà graziato dimmi C, se C sarà graziato dimmi B, e se sarò io il graziato scegliane uno a caso». Il carceriere risponde che B sarà giustiziato.

A è contento: pensa che ora la grazia sia tra lui e C, e che la sua probabilità sia salita da $1/3$ a $1/2$. Durante l'ora d'aria A comunica la notizia a C, che è ancora più contento: pensa che la probabilità di A sia rimasta $1/3$ e che la sua sia salita a $2/3$. Chi ha ragione?

Soluzione. Prima della risposta ciascuno ha probabilità $1/3$. Il carceriere dice «B sarà giustiziato» in due situazioni: se C è graziato (probabilità $1/3$, e in tal caso risponde B per certo), oppure se A è graziato e il carceriere sceglie B a caso (probabilità $1/3 \cdot 1/2 = 1/6$). La probabilità che dica «B» è dunque $1/3 + 1/6 = 1/2$. Condizionando:

CHI È GRAZIATO	PROBABILITÀ	IL CARCERIERE RISPONDE «B»	PROBABILITÀ CONGIUNTA
A	1/3	con probabilità 1/2	1/6
B	1/3	mai	0
C	1/3	per certo	1/3

Tabella 1. I casi del paradosso dei tre prigionieri.

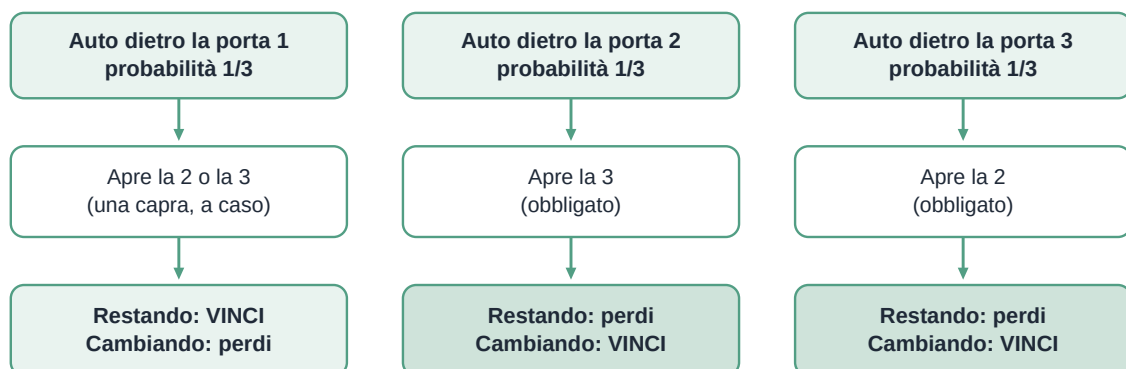
Quindi $P(A \text{ graziato} \mid \text{risposta «B»}) = (1/6)/(1/2) = \mathbf{1/3}$ e $P(C \text{ graziato} \mid \text{risposta «B»}) = (1/3)/(1/2) = \mathbf{2/3}$. Con la regola di Bayes: $P(A \mid b) = P(b \mid A) \cdot P(A)/P(b) = (1/2 \cdot 1/3)/(1/2) = 1/3$. Ha ragione C: la probabilità di A non è cambiata, perché la risposta del carceriere sarebbe stata possibile, con B o con C, in qualunque caso in cui A sia graziato, e dunque non porta nessuna informazione su di lui. L'informazione si è concentrata tutta su C.

Il problema di Monty Hall

Il problema prende il nome da Monty Hall, conduttore di un celebre gioco a premi televisivo statunitense (*Let's Make a Deal*). Fu formulato già nel 1975 da Steve Selvin in una lettera alla rivista *American Statistician*, ma diventò famosissimo all'inizio degli anni Novanta, quando fu posto a Marilyn vos Savant, che teneva una rubrica sulla rivista *Parade*: «In un gioco a premi ci sono tre porte: dietro una c'è un'automobile, dietro le altre due una capra. Scegli la porta 1; il conduttore, che sa che cosa c'è dietro ciascuna porta, ne apre un'altra, per esempio la 3, e mostra una capra. Poi ti chiede: vuoi cambiare e scegliere la 2? Ti conviene?»

La risposta di vos Savant fu: **sì**, conviene cambiare, perché la probabilità che l'automobile sia dietro la porta 2 è 2/3. La risposta scatenò polemiche vivacissime, con molte lettere di lettori, anche matematici di professione, che la ritenevano sbagliata: «restano due porte, quindi 1/2 e 1/2». Il ragionamento corretto è il seguente.

Il giocatore ha scelto la porta 1. Con probabilità 1/3 l'automobile è lì; con probabilità 2/3 è dietro una delle altre due porte. Il conduttore, che sa dov'è l'auto e *apre sempre* una porta con la capra tra le due non scelte, non cambia queste probabilità sulla porta 1: i 2/3 rimangono, interamente, sull'unica porta non scelta e chiusa. Restando si vince quando la scelta iniziale era giusta (1 caso su 3), cambiando si vince quando la scelta iniziale era sbagliata (2 casi su 3).



Il giocatore sceglie la porta 1: restando vince in 1 caso su 3, cambiando in 2 casi su 3

Figura 1. I tre casi del problema di Monty Hall, supponendo che il giocatore scelga la porta 1.

Con la regola di Bayes. Indichiamo con A_i l'evento «l'auto è dietro la porta i », con probabilità 1/3 ciascuno. Il conduttore apre la 3 con probabilità 1/2 se A_1 (può aprire la 2 o la 3), con probabilità 1 se A_2 (non può aprire né la 1 né la 2 che ha l'auto) e con probabilità 0 se A_3 . Quindi $P(\text{apre 3}) = 1/6 + 1/3 + 0 = 1/2$ e $P(A_1 \mid \text{apre 3}) = (1/2 \cdot 1/3)/(1/2) = 1/3$, $P(A_2 \mid \text{apre 3}) = (1 \cdot 1/3)/(1/2) = 2/3$.

L'IPOTESI CHE CONTA

Il fattore decisivo è che il conduttore apre la porta che **di sicuro non contiene l'auto**. Se invece aprisse a caso una delle porte 2 e 3, il discorso cambierebbe: con probabilità $1/3$ aprirebbe la porta con l'auto e il gioco finirebbe. Se, per caso, mostrasse una capra aprendo la 3, la probabilità che l'auto sia dietro la porta 1 sarebbe, con A_3 l'evento «auto dietro la 3»,

$$P(A_1 | \text{non } A_3) = P(\text{non } A_3 | A_1) \cdot P(A_1) / P(\text{non } A_3) = (1 \cdot 1/3) / (2/3) = 1/2$$

e allora restare o cambiare sarebbe indifferente. Il problema è dunque lo stesso del paradosso dei tre prigionieri: ciò che conta è *come* è stata ottenuta l'informazione. Non basta sapere che dietro la porta 3 c'è una capra.

Il metodo più convincente per credere al risultato è provare. La simulazione seguente ripete molte volte il gioco, con la strategia «cambia» e con la strategia «resta»; le frequenze si avvicinano a $2/3$ e a $1/3$ (è una conferma frequentista, capitolo 19).

```
import random

def gioca(cambia):
    porte = [0, 1, 2]
    auto = random.choice(porte)
    scelta = random.choice(porte)
    # il conduttore apre una porta con la capra, diversa dalla scelta
    aperta = random.choice([p for p in porte if p != scelta and p != auto])
    if cambia:
        scelta = [p for p in porte if p != scelta and p != aperta][0]
    return scelta == auto

prove = 100000
for cambia in (False, True):
    vittorie = sum(gioca(cambia) for _ in range(prove))
    print(cambia, vittorie / prove)    # circa 0.333 e 0.667
```

DIECI BUSTE

Una domanda per verificare di aver capito: in un gioco ci sono 10 buste e una sola contiene un assegno da un milione di euro. Voi avete la busta numero 1. Scambiereste la vostra busta con tutte le altre 9? Sì: avreste 9 buste su 10, probabilità $9/10$. E se chi conosce l'assegno aprisse 8 delle altre 9 buste, che certamente non lo contengono, scambiereste la vostra con quella rimasta? Ancora sì, e per lo stesso motivo: la busta rimasta eredita l'intera probabilità $9/10$ delle altre nove, mentre la vostra resta a $1/10$. In generale, con n porte e un conduttore che ne apre $n - 2$ con una capra, cambiare vince con probabilità $(n - 1)/n$. Con $n = 3$ si ritrova $2/3$.

PROBLEMA	RISPOSTA INTUITIVA	RISPOSTA CORRETTA	DOVE SI SBAGLIA
Due bambini, «almeno un maschio»	$1/2$	$1/3$	I casi MF e FM sono due, MM uno solo
Tre carte o tre scatole	$1/2$	$2/3$	Si contano le carte invece dei lati
Tre prigionieri (per A)	$1/2$	$1/3$	La risposta non dà informazione su A
Monty Hall (cambiando)	$1/2$	$2/3$	Il conduttore non apre a caso

Tabella 2. Riepilogo dei problemi di questo capitolo.

Introduzione ai grafi

Dalle strette di mano ai ponti di Königsberg: definizioni di grafo, gradi dei vertici e teorema delle strette di mano, classi di grafi, sottografi, isomorfismi e omeomorfismi.

Un problema per cominciare: le strette di mano

Roberto e la moglie Giulia organizzano una cena e invitano altre 4 coppie sposate. Alcuni dei presenti si salutano stringendosi la mano (ovviamente nessuno la stringe al proprio coniuge, né a sé stesso). Alla fine Roberto chiede a ciascuno degli altri nove a quante persone abbia stretto la mano e riceve **nove risposte tutte diverse**. Quante persone hanno stretto la mano a Roberto? E a Giulia? Hanno stretto la mano alle stesse persone?

Il problema sembra senza dati, ma si risolve con un disegno: ogni persona è un cerchietto e due cerchietti sono uniti da un segmento se le persone si sono strette la mano. Le persone sono 10, e ciascuna può stringere la mano al più a 8 altre (tolti sé stessa e il coniuge). Le nove risposte diverse date a Roberto sono quindi i numeri 0, 1, ..., 8, e possiamo chiamare «persona k » quella che ha stretto k mani.

- La persona 8 ha stretto la mano a tutti tranne il coniuge. Non può averla stretta alla persona 0, che non ha stretto nessuna mano: quindi il coniuge di 8 è 0, e 8 ha stretto la mano a tutti gli altri, compreso Roberto.
- La persona 7 ha stretto la mano a 7 persone, ma non a 0 né a 1 (che ha già stretto la mano solo a 8): quindi il suo coniuge è 1. Allo stesso modo il coniuge di 6 è 2 e quello di 5 è 3.
- Restano Roberto, Giulia e la persona 4, che non può essere sposata con nessuno dei precedenti: è dunque **Giulia** la persona 4.

Giulia ha stretto la mano a 4 persone (le persone 5, 6, 7, 8); Roberto ha stretto la mano alle stesse quattro. La risposta è: **4, 4 e sì**. Una verifica esaustiva (tutti i grafi con le condizioni date) conferma che il disegno è unico.

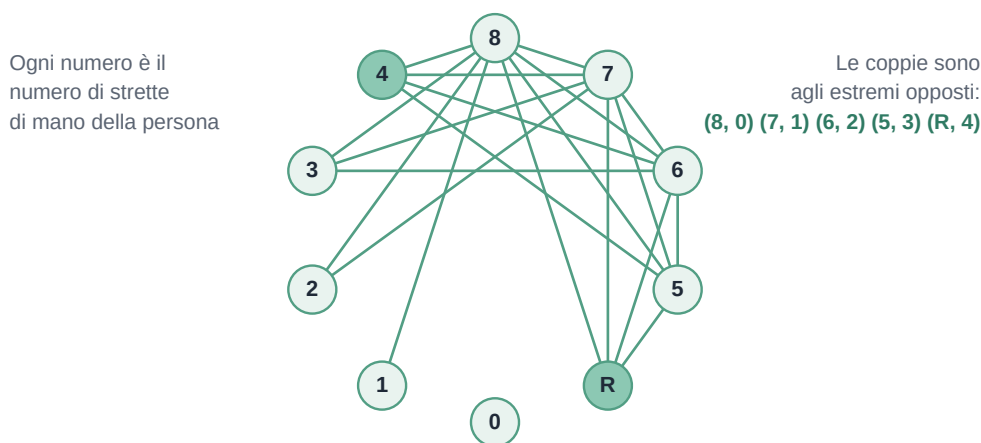


Figura 1. Il grafo del problema delle strette di mano. Le persone sono identificate dal numero di strette di mano; R è Roberto.

Ci sono due lezioni. La prima: strutturare bene l'informazione, con un disegno, permette di rispondere a domande apparentemente impossibili. La seconda: le persone che hanno stretto un numero *dispari* di mani sono quattro (quelle con 1, 3, 5 e 7 strette), cioè un numero pari: non è un caso, e lo spiega il teorema delle strette di mano che dimostreremo tra poco.

VERIFICATE

Le persone che hanno stretto un numero dispari di mani sono 1, 3, 5 e 7: quattro, un numero pari. (Roberto e Giulia ne hanno strette 4, un numero pari.)

I sette ponti di Königsberg

La teoria dei grafi nasce, di fatto, con un problema «reale»: quello dei sette ponti di Königsberg, città prussiana sul Baltico oggi chiamata Kaliningrad (in Russia), dove nacque nel 1724 il filosofo Immanuel Kant. La città è attraversata dal fiume Pregel e comprende due isole che, nel Settecento, erano collegate tra loro e con le due sponde da sette ponti. Gli abitanti si chiedevano se fosse possibile fare una passeggiata che attraversasse ogni ponte **una e una sola volta**.

Nel 1736 il matematico svizzero Leonhard Euler (Eulero), che viveva a San Pietroburgo, venne a conoscenza del problema e ne dimostrò l'impossibilità. (Una versione diffusa della storia lo vuole in visita a Königsberg, ma Eulero non andò mai nella città: il problema gli fu sottoposto per lettera.) Eulero osservò che il percorso all'interno di una zona della città è irrilevante: conta soltanto la *sequenza dei ponti attraversati*. Rappresentò quindi ogni zona con un punto (un **vertice** o nodo) e ogni ponte con una linea (un **arco**) che unisce le due zone collegate. Nasceva così il grafo dei sette ponti, che non è un grafo «semplice» perché due zone sono unite da più ponti (è un *multigrafo*).

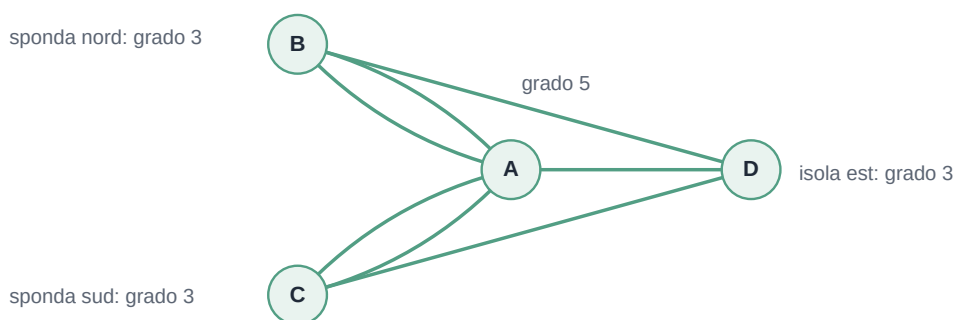


Figura 2. Il multigrafo dei sette ponti di Königsberg: quattro vertici, sette archi, tutti i vertici di grado dispari.

La soluzione completa, che usa i gradi dei vertici, è nel capitolo 24 (cammini euleriani).

Definizioni fondamentali

GRAFO SEMPLICE NON ORIENTATO

Un **grafo semplice non orientato** è una coppia $G = (V, E)$ dove V è un insieme finito non vuoto, i cui elementi sono detti **vertici** o nodi, ed E è un insieme di sottoinsiemi di V di cardinalità 2, detti **archi**: un arco è un insieme $\{i, j\}$, scritto anche (i, j) , con $i \neq j$.

I due vertici che definiscono un arco sono i suoi **estremi** e si dicono **adiacenti**; l'arco si dice **incidente** in ciascuno dei suoi estremi. Un vertice che non è estremo di alcun arco è **isolato**. Il numero dei vertici si indica con $|V|$ e il numero degli archi con $|E|$.

GRAFO ORIENTATO (DIGRAFO)

Un **grafo orientato** o **digrafo** è una coppia $G = (V, E)$ in cui gli archi sono *coppie ordinate* (i, j) di vertici: l'arco va da i a j . Si disegna con una freccia. Un arco della forma (i, i) si chiama **cappio**.

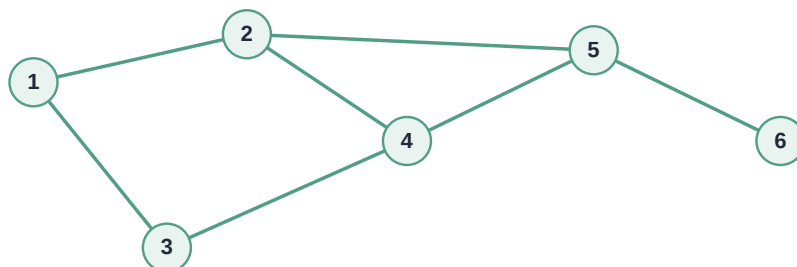
Nel disegno di un grafo conta solo quali vertici sono uniti, non la posizione dei punti né la forma delle linee. Un grafo in cui due vertici possono essere uniti da più archi, o in cui sono ammessi i cappi, è un **multigrafo**: il grafo dei ponti di Königsberg lo è. Per il resto di questa parte, a meno che non sia detto altrimenti, per «grafo» intenderemo un grafo semplice, senza archi multipli né cappi (anche nel caso orientato).

Esempio. Il grafo non orientato G_0 con $V = \{1, \dots, 6\}$ ed $E = \{(1, 2), (1, 3), (2, 4), (2, 5), (3, 4), (4, 5), (5, 6)\}$ ha 6 vertici e 7 archi. Il digrafo D_0 con $V = \{1, \dots, 5\}$ ed $E = \{(1, 2), (1, 3), (2, 3), (2, 4), (4, 3), (5, 2), (5, 4)\}$ ha 5 vertici e 7 archi. Li useremo anche nei capitoli successivi.

Il grado di un vertice e il teorema delle strette di mano

GRADO

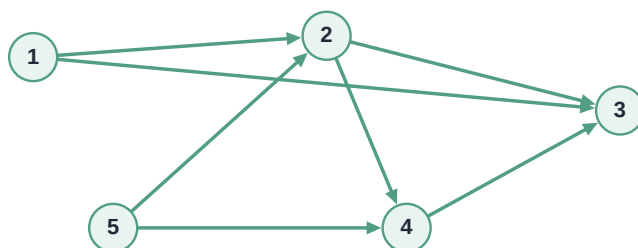
Il **grado** $\delta(v)$ di un vertice v di un grafo non orientato è il numero degli archi incidenti in v , cioè il numero dei vertici adiacenti a v . In un digrafo si distinguono il **grado entrante** $\delta^-(v)$, numero degli archi che entrano in v , e il **grado uscente** $\delta^+(v)$, numero degli archi che escono da v .



$\delta(1) = 2$, $\delta(2) = 3$, $\delta(3) = 2$
 $\delta(4) = 3$, $\delta(5) = 3$, $\delta(6) = 1$

somma dei gradi = 14
= 2 · 7 archi

Figura 3. Il grafo G_0 e i gradi dei suoi vertici.



grado entrante: 0, 2, 3, 2, 0
grado uscente: 2, 2, 0, 1, 2

somme: 7 e 7
= numero degli archi

Figura 4. Il digrafo D_0 e i suoi gradi entranti e uscenti.

Nel grafo G_0 la somma dei gradi è $2 + 3 + 2 + 3 + 3 + 1 = 14$, il doppio del numero degli archi (7). Nel digrafo D_0 la somma dei gradi entranti e la somma dei gradi uscenti sono entrambe 7, il numero degli archi. Non è una coincidenza.

TEOREMA DELLE STRETTE DI MANO (HANDSHAKING)

Se $G = (V, E)$ è un grafo non orientato, la somma dei gradi di tutti i vertici è uguale al doppio del numero degli archi:

$$\sum_{v \in V} \delta(v) = 2 |E|.$$

Dimostrazione. Contiamo in due modi le coppie (v, e) in cui v è un estremo di e . Per ogni vertice v ce ne sono $\delta(v)$, quindi in tutto $\sum \delta(v)$. Per ogni arco e ce ne sono esattamente 2, i suoi estremi, quindi in tutto $2|E|$. ■

Il corollario più utile: **in ogni grafo il numero dei vertici di grado dispari è pari**. Infatti la somma dei gradi è pari; i vertici di grado pari contribuiscono con un numero pari, quindi anche la somma dei gradi dispari deve essere pari, e questo richiede un numero pari di addendi dispari. In una festa, quindi, il numero di persone che hanno stretto un numero dispari di mani è sempre pari. Per i digrafi vale l'analogo: $\sum \delta^-(v) = \sum \delta^+(v) = |E|$, perché ogni arco entra in un vertice ed esce da uno.

UN'APPLICAZIONE DEL PRINCIPIO DEI CASSETTI

In ogni grafo con almeno due vertici ci sono due vertici con lo stesso grado. I gradi possibili sono i valori da 0 a $n - 1$, ma 0 e $n - 1$ non possono comparire insieme (un vertice adiacente a tutti gli altri esclude che esista un vertice isolato): i valori utilizzabili sono al più $n - 1$ per n vertici (si veda il capitolo 18). Per questo, a una festa, ci sono sempre due persone che hanno stretto lo stesso numero di mani.

Alcune classi di grafi

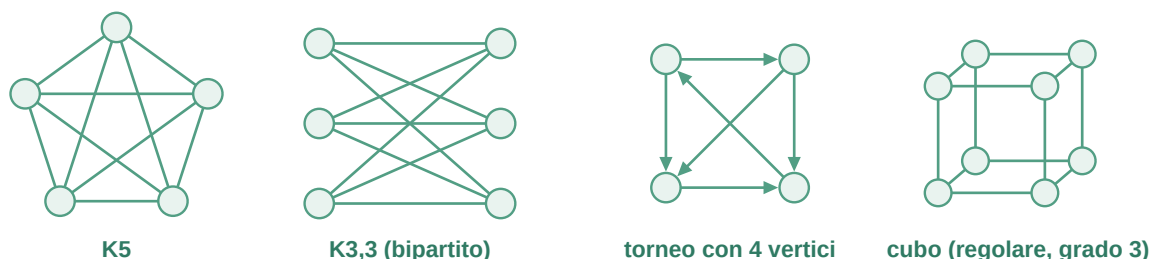


Figura 5. Alcune classi di grafi: il grafo completo K_5 , il bipartito completo $K_{3,3}$, un torneo con 4 vertici e il cubo, regolare di grado 3.

GRAFI REGOLARI

Un grafo è **regolare di grado r** se tutti i suoi vertici hanno grado r . Per il teorema delle strette di mano $r|V| = 2|E|$, quindi $|E| = r|V|/2$. In particolare un grafo regolare di grado dispari ha un numero *pari* di vertici: non esiste, per esempio, un grafo con 5 vertici in cui ogni vertice abbia grado 3.

GRAFI COMPLETI E TORNEI

Un grafo non orientato è **completo** se ogni coppia di vertici è unita da un arco. Il grafo completo con n vertici si indica con K_n (la lettera K richiama il tedesco *komplett*; talvolta si legge che onori Kuratowski, ma l'attribuzione è incerta). Ha tanti archi quante sono le coppie di vertici, cioè $C(n, 2) = n(n - 1)/2$, ed è regolare di grado $n - 1$. Un digrafo è completo se per ogni coppia di vertici i, j esistono entrambi gli archi (i, j) e (j, i) : ne ha $n(n - 1)$.

Un **torneo** è un digrafo ottenuto da un grafo completo assegnando un verso a ciascun arco: rappresenta i risultati di un campionato in cui ogni giocatore incontra ogni altro una volta e il pareggio non è ammesso, con l'arco orientato dal vincitore al perdente. Dato K_n , i tornei possibili sono $2^{C(n, 2)}$: per $n = 4$ sono $2^6 = 64$.

GRAFI BIPARTITI

Un grafo non orientato è **bipartito** se i vertici si possono partizionare in due insiemi V_1 e V_2 in modo che ogni arco abbia un estremo in V_1 e l'altro in V_2 . È **bipartito completo**, indicato con $K_{n,m}$ (con $n = |V_1|$ e $m = |V_2|$), se è presente un arco per ogni coppia formata da un vertice di V_1 e uno di V_2 : ha $n \cdot m$ archi. Per esempio $K_{5,3}$ ha 15 archi, mentre $K_{3,3}$ ne ha 9. Nel capitolo 25 caratterizzeremo i grafi bipartiti con i cicli di lunghezza dispari.

Sottografi

SOTTOGRAFO

$G' = (V', E')$ è un **sottografo** di $G = (V, E)$ se $V' \subseteq V$, $E' \subseteq E$ e ogni arco di E' ha entrambi gli estremi in V' . La stessa definizione vale per i digrafi.

Dato un sottoinsieme $V' \subseteq V$, il **sottografo indotto** da V' è quello che contiene tutti gli archi di G i cui estremi stanno in V' : si ottiene eliminando da G i vertici non appartenenti a V' e tutti gli archi incidenti in almeno uno dei vertici eliminati. Per esempio, il sottografo di G_0 indotto da $\{2, 4, 5\}$ è il triangolo con archi $(2, 4)$, $(2, 5)$, $(4, 5)$.

Isomorfismo di grafi

In che senso due grafi possono essere considerati «uguali»? La proprietà caratteristica di un grafo è il modo in cui i vertici sono collegati dagli archi, non il nome dei vertici né il disegno.

ISOMORFISMO

Due grafi (entrambi orientati o entrambi non orientati) $G_1 = (V_1, E_1)$ e $G_2 = (V_2, E_2)$ sono **isomorfi** se esiste una biezione $f: V_1 \rightarrow V_2$ tale che $(f(u), f(v))$ è un arco di E_2 se e solo se (u, v) è un arco di E_1 . La biezione f è un **isomorfismo**.

Esempio. G_1 ha vertici $\{a, b, c, d\}$ e archi $\{(a, b), (a, d), (b, c), (b, d), (c, d)\}$; G_2 ha vertici $\{t, u, v, w\}$ e archi $\{(t, u), (t, v), (u, v), (u, w), (v, w)\}$. La funzione $f(a) = t, f(b) = v, f(c) = w, f(d) = u$ è un isomorfismo: i cinque archi di G_1 vengono trasformati rispettivamente in $(t, v), (t, u), (v, w), (v, u), (w, u)$, che sono i cinque archi di G_2 . Entrambi sono un K_4 privato di un arco.

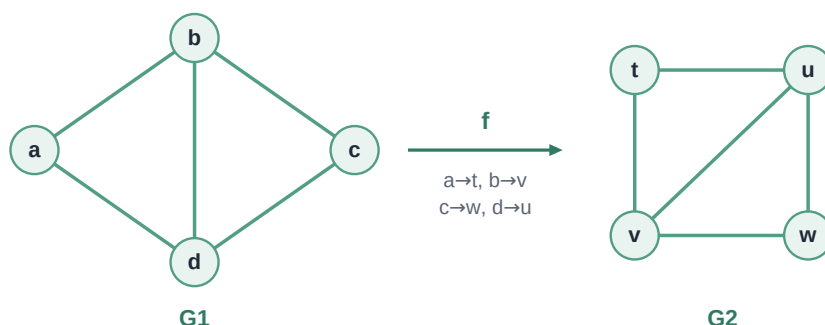


Figura 6. I grafi G_1 e G_2 sono isomorfi: lo stesso grafo disegnato in due modi, con l'isomorfismo f .

Se due grafi sono isomorfi hanno lo stesso numero di vertici e di archi, e i vertici che si corrispondono hanno lo stesso grado (grado entrante e uscente, nel caso orientato). Inoltre a ogni sottografo del primo corrisponde un sottografo isomorfo del secondo. Queste sono condizioni **necessarie**, non sufficienti: servono per dimostrare che due grafi *non* sono isomorfi. Per esempio, il grafo ottenuto da K_4 aggiungendo un vertice collegato a uno solo dei quattro (5 vertici, 7 archi, gradi 4, 3, 3, 3, 1) e il grafo ottenuto da $K_{2,3}$ aggiungendo l'arco tra i due vertici del lato da 2 (5 vertici, 7 archi, gradi 4, 4, 2, 2, 2) non sono isomorfi, perché le sequenze dei gradi sono diverse: nel primo c'è un vertice di grado 1, nel secondo nessuno. Nel caso orientato, due digrafi con lo stesso numero di vertici e archi possono non essere isomorfi perché i gradi uscenti sono diversi.

Non si conosce un algoritmo veloce, cioè polinomiale, per decidere se due grafi sono isomorfi, ma nemmeno si sa se il problema sia difficile: è un caso a parte nella teoria della complessità (capitolo 26). **Quanti grafi?** Sull'insieme di vertici $\{1, \dots, n\}$ si possono scrivere $2^{C(n, 2)}$ grafi diversi (ciascuna delle $C(n, 2)$ coppie è un arco oppure no): 1, 2, 8, 64, 1.024, 32.768 per $n = 1, \dots, 6$. A meno di isomorfismo il numero è molto più piccolo: 1, 2, 4, 11, 34, 156, 1.044 per $n = 1, \dots, 7$.

Omeomorfismo di grafi

Un altro modo in cui due grafi possono avere «la stessa forma» è che si ottengano l'uno dall'altro inserendo vertici lungo gli archi.

SUDDIVISIONE E OMEOMORFISMO

Sia $e = (u, v)$ un arco di G . Una **suddivisione** di e si ottiene introducendo un nuovo vertice w e sostituendo l'arco (u, v) con i due archi (u, w) e (w, v) (nel caso orientato, con gli archi orientati (u, w) e (w, v)). Due grafi G_1 e G_2 sono **omeomorfi** se, con una successione di suddivisioni di archi di G_1 e di G_2 , si ottengono due grafi isomorfi.



Figura 7. La suddivisione di un arco: un nuovo vertice di grado 2 viene inserito lungo l'arco.

Per esempio tutti i cicli sono omeomorfi tra loro: un triangolo, suddividendo un arco, diventa un quadrato (un ciclo con 4 vertici), e così via. L'omeomorfismo è la nozione topologica di «stesso disegno»: due grafi omeomorfi si possono disegnare in modo identico, a meno dei punti inseriti lungo le linee. Sarà il linguaggio del teorema di Kuratowski sui grafi planari (capitolo 25).

Percorsi, connessione e rappresentazione dei grafi

Percorsi, cammini, circuiti e cicli; componenti connesse e connessione forte; matrici e liste di adiacenza; come contare i percorsi con le potenze della matrice e come riconoscere i cicli di un digrafo.

Percorsi, cammini, circuiti e cicli

Un grafo serve a rappresentare «collegamenti», e la prima domanda naturale è: posso andare da un vertice a un altro seguendo gli archi? Per rispondere servono quattro termini, che nella letteratura italiana non sono del tutto uniformi: noi useremo quelli del corso.

PERCORSO

Un **percorso** in un grafo (o in un digrafo) $G = (V, E)$ è una sequenza di vertici $v_1, \dots, v_k$ tale che per ogni i con $1 \leq i < k$ la coppia (v_i, v_{i+1}) è un arco (in un digrafo si percorre ogni arco solo nel suo verso). v_1 è l'**origine**, v_k la **destinazione**, gli altri sono i vertici **intermedi**. La **lunghezza** del percorso è il numero di archi, cioè $k - 1$.

Un percorso può passare più volte per lo stesso vertice e per lo stesso arco. Da questa definizione si ricavano le altre tre:

TERMINE	DEFINIZIONE	ESEMPIO IN G0	LUNGHEZZA
Percorso	sequenza di vertici consecutivamente adiacenti	1, 2, 4, 5, 2, 4, 3	6
Cammino	percorso in cui tutti i vertici sono diversi	1, 2, 5, 6	3
Circuito	percorso chiuso: primo e ultimo vertice coincidono	1, 2, 4, 5, 2, 1	5
Ciclo	cammino chiuso: i vertici sono tutti diversi tranne il primo e l'ultimo	1, 2, 4, 3, 1	4

Tabella 1. I quattro tipi di percorso, con esempi nel grafo G0 del capitolo 22.

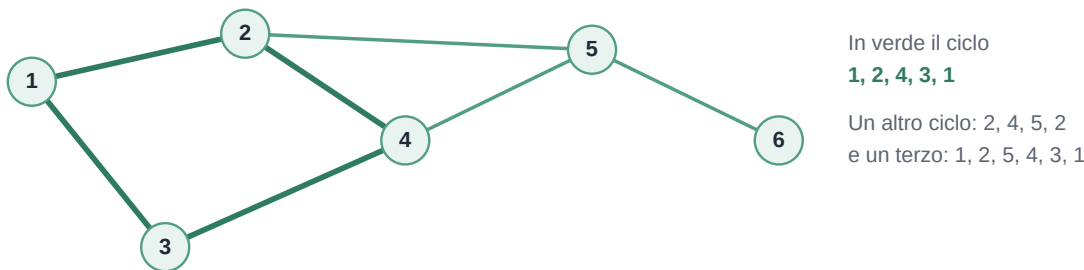


Figura 1. Il grafo G0 con un suo ciclo evidenziato.

NOMI IN ALTRI TESTI

In inglese il percorso è *walk*, il cammino è *path*, il circuito è *closed walk* e il ciclo è *cycle*. Molti testi italiani chiamano «cammino» quello che qui è un percorso e «cammino semplice» quello che qui è un cammino. Controllate sempre la definizione usata dal vostro docente.

Lunghezza minima di un ciclo. In un grafo non orientato (semplice) un ciclo ha almeno 3 vertici: con 2 vertici l'unico «ciclo» sarebbe u, v, u , che percorre due volte lo stesso arco. In un digrafo bastano 2 vertici, perché gli archi (u, v) e (v, u) sono diversi: 1, 3, 1 è un ciclo di lunghezza 2.

DA UN PERCORSO SI RICA VA SEMPRE UN CAMMINO

PERCORSI E CAMMINI

Se esiste un percorso dal vertice v al vertice w , allora esiste un cammino da v a w .

Dimostrazione. Tra tutti i percorsi da v a w scegliamo uno di lunghezza minima: $v_1, \dots, v_k$. Se due vertici coincidessero, $v_i = v_j$ con $i < j$, potremmo eliminare i vertici $v_{i+1}, \dots, v_j$ ottenendo ancora un percorso da v a w , ma più corto: assurdo. Quindi i vertici sono tutti diversi. ■

Il ragionamento vale sia per grafi sia per digrafi. La stessa idea, applicata a un percorso chiuso, dà un ciclo, ma con una precisazione importante.

CORREZIONE: DAL CIRCUITO AL CICLO

Non è vero che da *ogni* circuito si ottiene un ciclo: nel grafo non orientato G_0 il circuito 1, 3, 1 va e torna sullo stesso arco e non contiene alcun ciclo. L'enunciato corretto è: **in un digrafo ogni circuito di lunghezza positiva contiene un ciclo; in un grafo non orientato ogni circuito che non usa due volte lo stesso arco contiene un ciclo.** Dimostrazione: percorrendo il circuito si cerca la prima volta che si arriva in un vertice già visitato, $v_j = v_i$ con $i < j$ e j minimo. I vertici da v_i a v_{j-1} sono tutti diversi, quindi $v_i, \dots, v_j$ è un ciclo. Se il grafo è non orientato e $j = i + 2$, il percorso avrebbe percorso due volte l'arco $\{v_i, v_{i+1}\}$, caso escluso dall'ipotesi.

GRAFI ACICLICI

GRAFO ACICLICO

Un grafo (o digrafo) è **aciclico** se non contiene cicli.

I grafi non orientati aciclici sono le *foreste* e, se connessi, gli *alberi* (capitolo 26). I digrafi aciclici (in inglese *DAG*, *directed acyclic graph*) sono ovunque in informatica: dipendenze tra moduli di un programma, propedeuticità tra esami, ordine delle operazioni di una compilazione. Il digrafo D_0 del capitolo 22 è aciclico: da 1 e da 5, i vertici senza archi entranti, tutti gli archi vanno «avanti» verso il vertice 3, che non ha archi uscenti. Un ordine dei vertici compatibile con tutti gli archi, per esempio 1, 5, 2, 4, 3, si chiama **ordinamento topologico**: esiste per un digrafo se e solo se è aciclico.

Grafi connessi

VERTICI CONNESSI

Due vertici u, v di un grafo G sono **connessi** se esiste un cammino da u a v (o, che è lo stesso, un percorso).

La connessione è una **relazione di equivalenza** sull'insieme dei vertici (capitolo 5): è riflessiva (un vertice è connesso a sé stesso con un cammino di lunghezza 0); è simmetrica (si percorre il cammino al contrario); è transitiva (se u è connesso a v e v a w , si concatenano i due percorsi e si ottiene un percorso da u a w , da cui si ricava un cammino per il risultato precedente). Le classi di equivalenza partizionano V in insiemi $V_1, \dots, V_m$.

COMPONENTI CONNESSE

I sottografi indotti dalle classi $V_1, \dots, V_m$ si chiamano **componenti connesse** di G . Un grafo è **connesso** se ha una sola componente connessa, cioè se due vertici qualsiasi sono connessi.

In un grafo ci sono archi soltanto *dentro* le componenti, mai tra componenti diverse. Un vertice isolato è una componente da solo. Il grafo della figura qui sotto, con 8 vertici, ha tre componenti connesse, di 4, 3 e 1 vertici.

DIGRAFI: CONNESSIONE DEBOLE E FORTE

Per i digrafi le definizioni sono due. Un digrafo è **debolmente connesso** se il grafo non orientato ottenuto dimenticando il verso degli archi (il *grafo sottostante*) è connesso. Due vertici u, v sono **fortemente connessi** se esistono un cammino da u a v e un cammino da v a u . Anche la connessione forte è una relazione di equivalenza (stessa verifica di prima, usando i due versi) e le sue classi danno le **componenti fortemente connesse**; un digrafo è **fortemente connesso** se ne ha una sola.

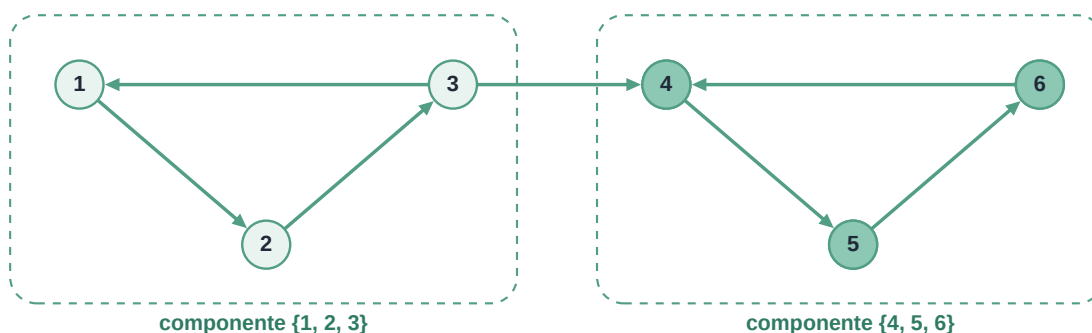


Figura 2. Il digrafo D_1 è debolmente connesso ma non fortemente: ha due componenti fortemente connesse. Aggiungendo l'arco $(6, 1)$ diventerebbe fortemente connesso.

Nel digrafo D_1 i vertici 1, 2, 3 formano il ciclo 1, 2, 3, 1 e quindi sono fortemente connessi tra loro; lo stesso vale per 4, 5, 6 (ciclo 4, 5, 6, 4). Dal vertice 3 si arriva a 4 con l'arco $(3, 4)$, ma da 4 non si torna a 3: le due componenti sono distinte. Ogni digrafo fortemente connesso è debolmente connesso, non viceversa. Inoltre il «grafo delle componenti» (un vertice per componente, un arco da A a B se c'è un arco da un vertice di A a uno di B) è sempre **aciclico**: se avesse un ciclo, tutte le componenti coinvolte sarebbero fortemente connesse tra loro e si fonderebbero in una sola.

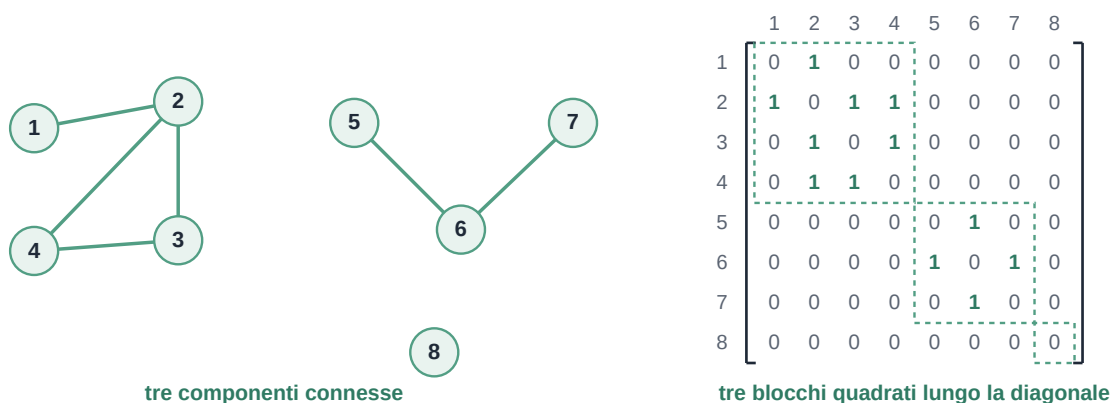


Figura 3. Un grafo con tre componenti connesse e la sua matrice di adiacenza: numerando i vertici componente per componente, la matrice è fatta di blocchi quadrati lungo la diagonale e di zeri altrove.

GRAFI K CONNESSI

Connesso significa «si può andare da ogni vertice a ogni altro», ma non dice quanto è *robusta* la rete: un solo guasto potrebbe spezzarla. Si misura con il numero di percorsi indipendenti.

GRAFO k CONNESSO

Un grafo è **k connesso rispetto agli archi** se per ogni coppia di vertici u, v esistono k cammini da u a v senza archi in comune. È **k connesso rispetto ai vertici** se i k cammini non hanno vertici intermedi in comune.

Se un grafo è k connesso rispetto agli archi, per sconnetterlo bisogna eliminare almeno k archi (ogni arco eliminato interrompe al più uno dei k cammini); analogamente per i vertici. Il teorema di Menger, che qui citiamo senza dimostrazione, dice che vale anche il viceversa: il numero minimo di archi (o di vertici) da eliminare per separare due vertici è uguale al numero massimo di cammini indipendenti tra loro. Alcuni valori: un ciclo C_n è 2 connesso (per andare da u a v si può girare nei due versi); il grafo completo K_n è $(n - 1)$ connesso; il cubo è 3 connesso; un grafo che ha un arco come $(5, 6)$ in G_0 (un **ponte**) o un vertice come 5 che lo sconnette se tolto (un **punto di articolazione**) è soltanto 1 connesso. Per le reti reali, di computer o di strade, avere $k \geq 2$ vuol dire sopravvivere a un singolo guasto.

Rappresentare un grafo al calcolatore

Per usare un grafo come struttura dati servono due scelte classiche: una matrice, oppure un array di liste.

MATRICE DI ADIACENZA

MATRICE DI ADIACENZA

Sia G un grafo con $V = \{1, \dots, n\}$. La **matrice di adiacenza** è la matrice M di dimensione $n \times n$ con $M[i, j] = 1$ se c'è un arco da i a j e $M[i, j] = 0$ altrimenti.

Sia le righe sia le colonne corrispondono ai *vertici* (non agli archi: la matrice che ha i vertici sulle righe e gli archi sulle colonne è un'altra, la matrice di incidenza). Le proprietà da ricordare:

- la matrice ha solo 0 e 1 e la diagonale è fatta di 0, perché non ci sono cappi;
- se il grafo è non orientato la matrice è **simmetrica**, $M[i, j] = M[j, i]$, e la somma degli 1 di una riga (o colonna) è il **grado** del vertice;
- se il grafo è orientato la matrice in generale non è simmetrica: la somma della riga i è il grado **uscente** di i e la somma della colonna i è il grado **entrante**;
- verificare se due vertici sono uniti da un arco richiede **tempo costante**: si legge $M[i, j]$.

	1	2	3	4	5	6	grado
1	0	1	1	0	0	0	2
2	1	0	0	1	1	0	3
3	1	0	0	1	0	0	2
4	0	1	1	0	1	0	3
5	0	1	0	1	0	1	3
6	0	0	0	0	1	0	1

matrice M di G_0

	1	2	3	4	5	uscente
1	0	1	1	0	0	2
2	0	0	1	1	0	2
3	0	0	0	0	0	0
4	0	0	1	0	0	1
5	0	1	0	1	0	2
	0	2	3	2	0	

matrice di D_0

Figura 4. A sinistra la matrice di G_0 (simmetrica, con i gradi a destra); a destra la matrice di D_0 , con i gradi uscenti a destra e quelli entranti sotto.

MATRICE E COMPONENTI CONNESSE

Se i vertici sono numerati componente per componente, la matrice di adiacenza è **a blocchi**: ogni componente con k vertici occupa un blocco quadrato $k \times k$ sulla diagonale, e tutto il resto è fatto di zeri, perché non ci sono archi tra componenti diverse (Figura 3). Se la numerazione è casuale, i blocchi si riconoscono solo dopo aver rinumerato i vertici.

LISTE DI ADIACENZA

La matrice occupa n^2 posizioni qualunque sia il numero di archi, e per un grafo *sperso* (con pochi archi rispetto a n^2) è uno spreco. Alternativa: un array di n elementi, in cui l'elemento i è la lista dei vertici adiacenti a i (per un digrafo, dei successori di i).

VERTICE	LISTA DEI VICINI
1	2, 3
2	1, 4, 5
3	1, 4
4	2, 3, 5
5	2, 4, 6
6	5

Tabella 2. Le liste di adiacenza del grafo G_0 : in tutto $6 + 2 \cdot 7 = 20$ valori, contro i 36 della matrice.

Per un grafo non orientato servono $n + 2|E|$ valori, perché ogni arco compare in due liste; per un digrafo $n + |E|$. Il digrafo D_0 (5 vertici, 7 archi) usa $5 + 7 = 12$ valori contro i 25 della matrice. Il vantaggio cresce con n : per una rete con un milione di vertici e in media 10 archi per vertice (cioè 5.000.000 di archi) la matrice avrebbe 10^{12} posizioni, le liste circa 11.000.000, quasi 91.000 volte meno.

CONFRONTO TRA LE DUE RAPPRESENTAZIONI

OPERAZIONE	MATRICE	LISTE
Memoria occupata	n^2	$n + 2 E $ (non orientato), $n + E $ (orientato)
C'è l'arco (i, j) ?	tempo costante	fino a $\delta(i)$ controlli (la lista di i)
Elencare i vicini di i	scorrere una riga: n controlli	scorrere la lista: $\delta(i)$ passi
Grado di i (non orientato)	somma della riga: n somme	lunghezza della lista
Grado entrante di i (orientato)	somma della colonna: n somme	scorrere tutte le liste
Aggiungere un arco	tempo costante	tempo costante (si aggiunge in coda)

Tabella 3. Matrice e liste di adiacenza a confronto.

Regola pratica: per grafi **densi** o piccoli, o quando si testano spesso archi singoli, conviene la matrice; per grafi **sparsi** e grandi (reti sociali, mappe stradali, il Web) si usano quasi sempre le liste. Il codice seguente costruisce entrambe le rappresentazioni a partire dall'elenco degli archi e conta le componenti connesse con una visita in ampiezza (BFS, *breadth first search*): si parte da un vertice non ancora visitato, si visitano prima i suoi vicini, poi i vicini dei vicini, e così via; ogni visita completa trova una componente. Costa $n + |E|$ passi.

```
from collections import deque

def costruisci(n, archi, orientato=False):
    """Vertici numerati da 0 a n meno 1. Restituisce matrice e liste di adiacenza."""
    matrice = [[0] * n for _ in range(n)]
    liste = [[] for _ in range(n)]
```

```

for i, j in archi:
    matrice[i][j] = 1
    liste[i].append(j)
    if not orientato:
        matrice[j][i] = 1
        liste[j].append(i)
return matrice, liste

def componenti(liste):
    """Visita in ampiezza: numera le componenti connesse (grafo non orientato)."""
    n = len(liste)
    comp = [None] * n
    k = 0
    for s in range(n):
        if comp[s] is None:
            comp[s] = k
            coda = deque([s])
            while coda:
                u = coda.popleft()
                for v in liste[u]:
                    if comp[v] is None:
                        comp[v] = k
                        coda.append(v)
            k += 1
    return comp, k

```

Con gli archi del grafo della Figura 3 (numerati da 0 a 7) il programma restituisce $comp = [0, 0, 0, 0, 1, 1, 1, 2]$ e $k = 3$: tre componenti, come in figura.

Contare i percorsi con le potenze della matrice

La matrice M dice dove c'è un percorso di lunghezza 1. Come trovare quelli più lunghi? Un percorso di lunghezza 2 da i a j è un percorso i, h, j : c'è un arco da i a h e un arco da h a j . Il numero di tali percorsi, al variare di h , è proprio il prodotto riga per colonna:

$$M^2[i, j] = \sum_h M[i, h] \cdot M[h, j].$$

Ogni addendo vale 1 se e solo se h è un vertice intermedio valido, 0 altrimenti. Nel grafo G_0 , per esempio, $M^2[1, 4] = 2$ (1, 2, 4 e 1, 3, 4).

POTENZE DELLA MATRICE DI ADIACENZA

Sia M la matrice di adiacenza di un grafo o digrafo. Per ogni $k \geq 1$ l'elemento $M^k[i, j]$ è il **numero di percorsi di lunghezza k da i a j** .

Dimostrazione. Per induzione su k . Per $k = 1$ è la definizione di M . Supponiamo vero per k . Un percorso di lunghezza $k + 1$ da i a j è un percorso di lunghezza k da i a un vertice h seguito dall'arco (h, j) ; ogni percorso si decompone in un solo modo così. Perciò il loro numero è $\sum_h M^k[i, h] \cdot M[h, j] = M^{k+1}[i, j]$. ■

	1	2	3	4	5	6
1	2	0	0	2	1	0
2	0	3	2	1	1	1
3	0	2	2	0	1	0
4	2	1	0	3	1	1
5	1	1	1	1	3	0
6	0	1	0	1	0	1

M al quadrato (grafo G0)

Elemento (1, 4) = 2:

i percorsi 1, 2, 4 e 1, 3, 4.

Diagonale = gradi: 2, 3, 2, 3, 3, 1,

perché i percorsi chiusi di lunghezza 2

da un vertice sono uno per ogni vicino.

Figura 5. La matrice M al quadrato di G0. Gli elementi evidenziati sono i percorsi di lunghezza 2 da 1 a 4 (e da 4 a 1).

Alcune conseguenze, tutte verificabili sugli esempi:

- **Diagonale di M^2 .** In un grafo non orientato $M^2[i, j] = \delta(i, j)$: i percorsi chiusi di lunghezza 2 da i sono i, h, i , uno per ogni vicino h . Non sono dunque «cicli»: sono andate e ritorni.
- **Triangoli.** La somma della diagonale (la *traccia*) di M^3 vale 6 volte il numero dei triangoli: ogni triangolo dà 6 percorsi chiusi di lunghezza 3 (3 vertici di partenza $\times$ 2 versi). G_0 ha un solo triangolo, $\{2, 4, 5\}$, e infatti la traccia di M^3 è 6.
- **Cicli orientati.** Nel digrafo D_1 il percorso chiuso di lunghezza 3 che parte da 1 è unico (1, 2, 3, 1), e $M^3[1, 1] = 1$.
- **Raggiungibilità.** Il vertice j si raggiunge da i se e solo se esiste un cammino, di lunghezza al più $n - 1$; quindi G è connesso se e solo se la matrice $(I + M)^{n-1}$ non contiene zeri.

Il calcolo diretto di M^k costa k prodotti di matrici, ciascuno con n^3 moltiplicazioni; con il metodo dei quadrati ripetuti ne bastano circa $\log_2 k$. Il codice seguente calcola le potenze di una matrice di interi.

```
def prodotto(A, B):
    n = len(A)
    return [[sum(A[i][h] * B[h][j] for h in range(n)) for j in range(n)]
            for i in range(n)]

def potenza(M, k):
    """M alla k: l'elemento (i, j) conta i percorsi di lunghezza k da i a j."""
    n = len(M)
    R = [[int(i == j) for j in range(n)] for i in range(n)]
    for _ in range(k):
        R = prodotto(R, M)
    return R
```

Riconoscere i cicli in un digrafo

CONDIZIONE SUFFICIENTE PER UN CICLO

Sia $G = (V, E)$ un digrafo senza cappi con n vertici. Se ogni vertice ha grado uscente > 0 , oppure se ogni vertice ha grado entrante > 0 , allora G contiene un ciclo.

Dimostrazione (primo caso; il secondo è identico, percorrendo gli archi all'indietro). Partiamo da un vertice i_0 . Poiché $\delta^+(i_0) > 0$ c'è un arco da i_0 a un vertice i_1 ; poiché anche i_1 ha un arco uscente, c'è un arco verso i_2 , e così via, fino a ottenere un percorso $i_0, i_1, \dots, i_n$ di $n + 1$ vertici. Per il principio dei cassetti (capitolo 18) due di essi coincidono. Prendendo la prima ripetizione, $i_a = i_b$ con b minimo, i vertici $i_a, \dots, i_{b-1}$ sono tutti diversi e $i_a, \dots, i_b$ è un ciclo. ■

La condizione è sufficiente ma **non necessaria**. Il digrafo D_2 della figura ha il ciclo 2, 3, 4, 2, ma il vertice 5 non ha archi uscenti e il vertice 6 non ha archi entranti: non vale né l'una né l'altra ipotesi.

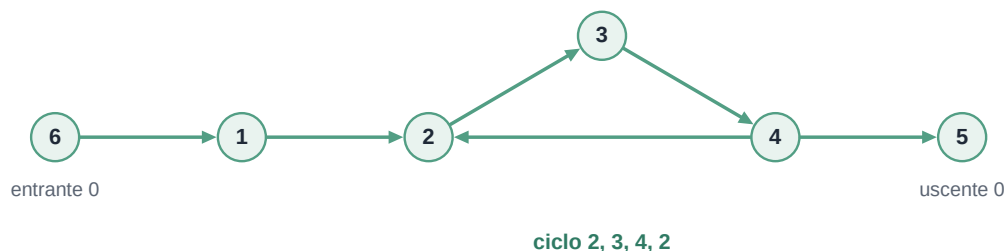


Figura 6. Il digrafo D_2 : contiene il ciclo 2, 3, 4, 2, anche se non tutti i vertici hanno grado uscente positivo né grado entrante positivo.

Diventa però necessaria se la applichiamo a un sottografo: **un digrafo contiene un ciclo se e solo se esiste un sottoinsieme non vuoto di vertici in cui il sottografo indotto ha tutti i vertici con grado uscente positivo, oppure tutti con grado entrante positivo**. (Il «se» è il teorema precedente; per il «solo se» basta prendere i vertici di un ciclo: ognuno ha nel ciclo un arco uscente e uno entrante.) Il teorema suggerisce un algoritmo.

ALGORITMO DI ELIMINAZIONE

Finché esiste un vertice con grado uscente 0 o con grado entrante 0 (calcolato nel grafo rimasto), eliminarlo insieme ai suoi archi. Quando non ne esistono più: se il grafo è vuoto, **G è aciclico**; se resta qualche vertice, in quello che resta ogni vertice ha grado uscente e grado entrante positivi, quindi **G contiene un ciclo**.

Correttezza. Un vertice di un ciclo ha, nel ciclo, un arco entrante e uno uscente, quindi non viene mai eliminato finché il ciclo è intatto: per induzione sui passi, i vertici di un ciclo non vengono mai eliminati. Quindi se il grafo si svuota non c'erano cicli; se resta qualcosa, per il teorema c'è un ciclo.

Applichiamolo a D_2 . Il vertice 6 ha grado entrante 0: si elimina. Ora 1 ha grado entrante 0: si elimina. Il vertice 5 ha grado uscente 0: si elimina. Restano 2, 3, 4 con archi (2, 3), (3, 4), (4, 2): tutti i gradi sono 1, l'algoritmo si ferma e il ciclo 2, 3, 4, 2 è trovato. Se invece applichiamo l'algoritmo al digrafo aciclico D_0 , si eliminano uno dopo l'altro tutti i vertici; l'ordine di eliminazione dei vertici con grado entrante 0 è un ordinamento topologico.

L'implementazione con la matrice, rimuovendo di volta in volta righe e colonne, è semplice ma costa molto: n^2 per vertice eliminato, in tutto fino a n^3 . Con le liste di adiacenza e contando, per ogni vertice, quanti suoi successori e predecessori sono già stati eliminati, si ottiene un algoritmo che costa $n + |E|$ operazioni.

```
def ha_ciclo(n, archi):
    """True se il digrafo (vertici da 0 a n meno 1) contiene un ciclo."""
    succ = [[] for _ in range(n)]
    pred = [[] for _ in range(n)]
    for i, j in archi:
        succ[i].append(j)
        pred[j].append(i)
    uscenti = [len(succ[v]) for v in range(n)]
    entranti = [len(pred[v]) for v in range(n)]
    usc_tolti = [0] * n      # quanti successori sono già stati tolti
    ent_tolti = [0] * n      # quanti predecessori sono già stati tolti
    tolto = [False] * n
    pila = [v for v in range(n) if uscenti[v] == 0 or entranti[v] == 0]
    for v in pila:
        tolto[v] = True
    tolti = 0
    while pila:
        v = pila.pop()
```

```

    tolti += 1
    for w in succ[v]:
        ent_tolti[w] += 1
        if not tolto[w] and ent_tolti[w] == entranti[w]:
            tolto[w] = True
            pila.append(w)
    for u in pred[v]:
        usc_tolti[u] += 1
        if not tolto[u] and usc_tolti[u] == uscenti[u]:
            tolto[u] = True
            pila.append(u)
    return tolti < n          # se resta qualche vertice, c'e un ciclo

```

VERIFICA

Il programma e il teorema sono stati confrontati con un controllo esaustivo su tutti i digrafi senza cappi con 2, 3 e 4 vertici (in tutto $4.096 + 64 + 4$ digrafi), e con 3.000 digrafi casuali con da 5 a 9 vertici: l'algoritmo trova un ciclo esattamente nei digrafi non aciclici, e ogni volta che tutti i gradi uscenti, o tutti i gradi entranti, sono positivi il ciclo c'è.

Grafi euleriani, hamiltoniani e pesati

Percorsi che usano ogni arco una volta sola (Eulero), cammini che toccano ogni vertice una volta sola (Hamilton), grafi con costi sugli archi, cammini di costo minimo e problema del commesso viaggiatore.

Il problema di Eulero: usare ogni arco una sola volta

Torniamo ai ponti di Königsberg. La domanda era: esiste un percorso che attraversi ogni ponte esattamente una volta? Nel linguaggio dei grafi: esiste un percorso che usi **ogni arco una e una sola volta**? Può ripassare per gli stessi vertici (è appunto un percorso, non un cammino) ma non per gli stessi archi.

CIRCUITO E PERCORSO EULERIANO

Un **circuito euleriano** di un grafo connesso G è un circuito che passa per ogni arco di G esattamente una volta.

Un grafo si dice **euleriano** se possiede un circuito euleriano. Un **percorso euleriano** è un percorso, non necessariamente chiuso, che usa ogni arco esattamente una volta.

Nelle dispense del corso il percorso euleriano si chiama anche «cammino euleriano», ma con la terminologia di questo corso (un cammino non ripete vertici) la parola corretta è percorso.

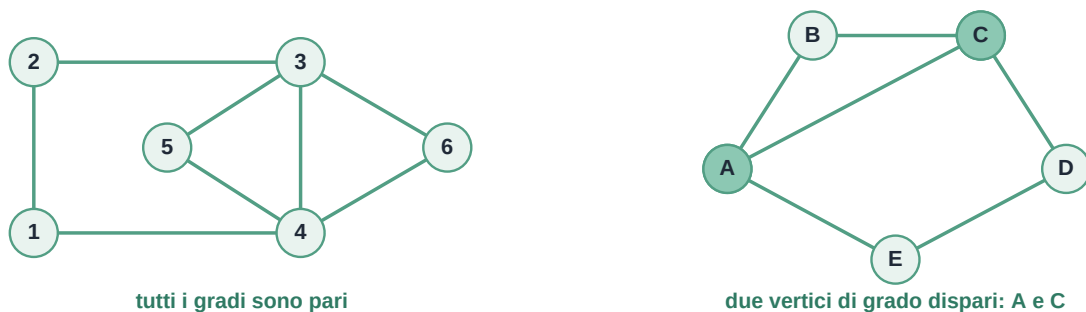


Figura 1. A sinistra un grafo euleriano: il circuito 1, 2, 3, 5, 4, 3, 6, 4, 1 usa ciascuno degli 8 archi una volta. A destra un grafo con un percorso euleriano: A, B, C, D, E, A, C (parte da un vertice dispari e finisce nell'altro).

TEOREMA DI EULERO (CIRCUITO)

Un grafo connesso G è euleriano se e solo se tutti i suoi vertici hanno grado pari.

Dimostrazione. ($\Rightarrow$) Percorrendo un circuito euleriano, ogni volta che si passa per un vertice si entra con un arco e si esce con un altro. Gli archi incidenti in un vertice v si raggruppano quindi in coppie «arco di entrata, arco di uscita», e questo vale anche per il vertice di partenza, dove la prima uscita è compensata dall'entrata finale. Poiché ogni arco viene usato una sola volta, il grado di v è pari.

($\Leftarrow$) Sia G connesso con tutti i gradi pari. Tra i circuiti di G che non usano due volte lo stesso arco scegliamo uno, T , con il maggior numero di archi (esiste, perché gli archi sono finiti; e uno ce n'è: si parte da un vertice e si prosegue finché si può, e come tutti i gradi sono pari ci si può fermare solo tornando al vertice di partenza). Se T non usasse tutti gli archi, per la connessione ci sarebbe un arco non usato incidente in un vertice v di T . Eliminando da G gli archi di T ogni vertice conserva un grado pari (di T ne ha tolti un numero pari). Partendo da v lungo archi non usati, come prima, si può proseguire finché non si torna in v : si ottiene un secondo circuito T' che non ha archi in comune con T . Inserendo T' in T nel punto v si ottiene un circuito più lungo di T : assurdo. Quindi T usa tutti gli archi. ■

Questo spiega la risposta di Königsberg. I gradi dei quattro vertici del multigrafo dei ponti sono 5, 3, 3, 3: tutti dispari, quindi non esiste alcun circuito euleriano, e nemmeno un percorso come vedremo tra poco. Il teorema è anche un algoritmo veloce di decisione: basta calcolare i gradi e controllare la connessione, tempo proporzionale a $n + |E|$.

TEOREMA DI EULERO (PERCORSO)

Un grafo connesso ha un percorso euleriano se e solo se ha 0 oppure 2 vertici di grado dispari. Se ne ha 2, ogni percorso euleriano parte da uno di essi e finisce nell'altro.

Dimostrazione. Se il percorso è chiuso è un circuito euleriano e vale il teorema precedente (0 vertici dispari). Se non è chiuso, con lo stesso ragionamento sulle coppie di archi i vertici intermedi hanno grado pari, mentre il primo e l'ultimo hanno un arco «spaiato» e quindi grado dispari: i vertici dispari sono esattamente 2, l'origine e la destinazione. Viceversa, siano u e v i due vertici dispari. Aggiungiamo un nuovo vertice w e gli archi $\{w, u\}$ e $\{w, v\}$: ora tutti i gradi sono pari e il grafo è ancora connesso, quindi ha un circuito euleriano, che passa per w come u, w, v . Eliminando w si ottiene un percorso euleriano da v a u nel grafo originario. ■

Il grafo a destra nella Figura 1 ha esattamente due vertici di grado dispari, A e C (gradi 3), e il percorso A, B, C, D, E, A, C li collega. Se nei ponti di Königsberg si *eliminasse un ponte qualunque* (cosa che il teorema e una verifica esaustiva confermano), i vertici dispari scenderebbero da 4 a 2 e la passeggiata diventerebbe possibile, ma non più chiusa.

DIGRAFI

Per i digrafi vale un analogo: un digrafo ha un circuito euleriano se e solo se, escludendo i vertici isolati, è debolmente connesso e ogni vertice ha grado entrante uguale al grado uscente. La dimostrazione è la stessa di prima, con «entrare» e «uscire» che si compensano per ogni vertice. L'enunciato è stato verificato su centinaia di digrafi casuali con al più 6 vertici.

La parte « $\Leftarrow$ » della dimostrazione è anche una ricetta per costruire il circuito: si percorre un giro finché si può e poi si «incollano» i giri che restano. Questo è l'algoritmo di Hierholzer, che con strutture dati adeguate costa tempo proporzionale al numero di archi. Il codice seguente lo realizza con una pila: quando un vertice non ha più archi inutilizzati viene scritto nel circuito.

```
def circuito_euleriano(liste, inizio):
    """Grafo non orientato connesso con tutti i gradi pari.
    liste: dizionario che a ogni vertice associa la lista dei vicini."""
    copia = {v: list(vicini) for v, vicini in liste.items()}
    pila = [inizio]
    circuito = []
    while pila:
        v = pila.pop()
        if copia[v]:
            pila.append(v)          # si resta su v: ha ancora archi inutilizzati
            w = copia[v].pop()      # si percorre un arco inutilizzato...
            copia[w].remove(v)     # ...e lo si cancella da entrambe le parti
            pila.append(w)
        else:
            circuito.append(v)      # v non ha più archi: si chiude il giro
    return circuito
```

VERIFICA

Il teorema di Eulero è stato confrontato con una ricerca esaustiva su tutti i grafi connessi con da 2 a 6 vertici (la ricerca prova tutti i modi di percorrere gli archi), e l'algoritmo è stato controllato su grafi casuali con gradi pari.

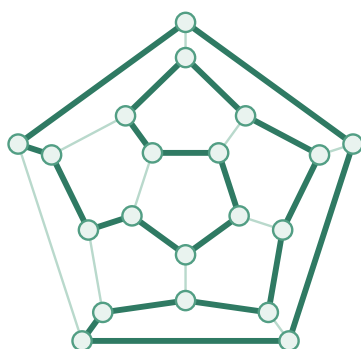
Il problema di Hamilton: toccare ogni vertice una sola volta

La domanda complementare è: esiste un cammino che passi per **ogni vertice** esattamente una volta? Qui si parla proprio di cammino, perché non si possono ripetere vertici.

CAMMINO E CICLO HAMILTONIANO

Sia G un grafo (o digrafo). Un **cammino hamiltoniano** è un cammino che passa una e una sola volta per ciascun vertice di G . Se è chiuso, cioè se è un ciclo, si chiama **ciclo hamiltoniano**. Un grafo è **hamiltoniano** se possiede un ciclo hamiltoniano.

Il nome viene da William Rowan Hamilton, matematico irlandese, che intorno al 1857 propose un rompicapo («icosian game») basato su un dodecaedro regolare, il solido con 12 facce pentagonali, 20 vertici e 30 spigoli: ogni vertice è una città e si deve fare il giro del mondo toccando ciascuna città una volta e tornando al punto di partenza. Il gioco fu poi venduto, nel 1859. Schiacciando il dodecaedro su una sua faccia si ottiene un grafo piano con 20 vertici e 30 archi, e una soluzione è un ciclo hamiltoniano.



Dodecaedro «schiacciato» su una faccia:

20 vertici, 30 spigoli, 12 facce pentagonali.

In verde scuro un ciclo hamiltoniano:

ne esistono esattamente 30 (distinti).

Figura 2. Il grafo del dodecaedro e un suo ciclo hamiltoniano.

Hamilton ed Eulero pongono domande simili ma di difficoltà molto diversa. Per i circuiti euleriani esiste un criterio semplice sui gradi. Per i cicli hamiltoniani **non si conosce alcun criterio semplice**: non esiste una condizione necessaria e sufficiente facile da controllare, e il problema fa parte di una vasta famiglia di problemi per cui non si conoscono algoritmi «veloci», cioè con tempo polinomiale nelle dimensioni del grafo ($|V|$ e $|E|$): li chiameremo NP completi nel capitolo 26. L'unica strategia generale è la ricerca esaustiva con ritorno indietro, qui sotto: prova tutte le sequenze di vertici e abbandona un tentativo non appena è impossibile proseguire.

```
def ciclo_hamiltoniano(liste):
    """liste[v]: vicini di v, vertici da 0 a n meno 1. Restituisce un ciclo o None."""
    n = len(liste)
    percorso = [0]
    usato = [False] * n
    usato[0] = True

    def cerca(u):
        if len(percorso) == n:
            return 0 in liste[u]          # l'ultimo vertice si collega al primo?
        for v in liste[u]:
            if not usato[v]:
                usato[v] = True
                percorso.append(v)
                if cerca(v):
                    return True
                percorso.pop()             # ritorno indietro (backtracking)
                usato[v] = False
        return False

    return percorso if cerca(0) else None
```

Quello che si possiede sono condizioni **necessarie** (se manca una, il ciclo non c'è) e condizioni **sufficienti** (se vale una, il ciclo c'è).

- **Necessarie.** Un grafo hamiltoniano ha tutti i vertici di grado almeno 2 (un ciclo entra ed esce da ogni vertice) e non ha punti di articolazione: se togliendo un vertice il grafo si spezza, il ciclo non può passare da una parte all'altra e tornare indietro. Se il grafo è bipartito con due insiemi V_1 e V_2 , il ciclo alterna i due insiemi, quindi $|V_1| = |V_2|$: per esempio $K_{2,3}$ non è hamiltoniano. Anche un cammino hamiltoniano in un bipartito richiede $|V_1|$ e $|V_2|$ che differiscano al più di 1.
- **Sufficienti.** Più archi ci sono, più è probabile che il ciclo esista. Il risultato più noto è il teorema di Dirac, enunciato qui sotto.
- **Né necessarie né sufficienti sole.** Il grafo di Petersen (10 vertici, regolare di grado 3, 3 connesso) non è hamiltoniano, benché soddisfi tutte le condizioni necessarie elementari; il ciclo C_n è hamiltoniano ma ha solo due archi per vertice.

TEOREMA DI DIRAC (1952)

Sia G un grafo semplice con $n \geq 3$ vertici in cui ogni vertice ha grado almeno $n/2$. Allora G è hamiltoniano.

Dimostrazione. Il grafo è connesso: due vertici non adiacenti x, y hanno ciascuno almeno $n/2$ vicini, tra i $n - 2$ vertici restanti, e $n/2 + n/2 > n - 2$, quindi hanno un vicino in comune. Sia $P = v_1, v_2, \dots, v_k$ un cammino di lunghezza massima. Per la massimalità, tutti i vicini di v_1 e di v_k stanno su P (altrimenti si potrebbe allungare). Consideriamo gli indici i in $\{1, \dots, k - 1\}$ tali che v_1 è adiacente a v_{i+1} : sono almeno $n/2$; e gli indici i in $\{1, \dots, k - 1\}$ tali che v_k è adiacente a v_i : sono almeno $n/2$. I due insiemi sono sottoinsiemi di $\{1, \dots, k - 1\}$, che ha al più $n - 1$ elementi, e la somma delle loro dimensioni è almeno n : si intersecano. Esiste dunque un i con v_1 adiacente a v_{i+1} e v_k adiacente a v_i . Allora $v_1, \dots, v_i, v_k, v_{k-1}, \dots, v_{i+1}, v_1$ è un ciclo che tocca gli stessi vertici di P (Figura 3). Se $k < n$, per la connessione c'è un vertice fuori dal ciclo adiacente a un vertice del ciclo, e partendo da lì si ottiene un cammino più lungo di P : assurdo. Quindi $k = n$ e il ciclo è hamiltoniano. ■

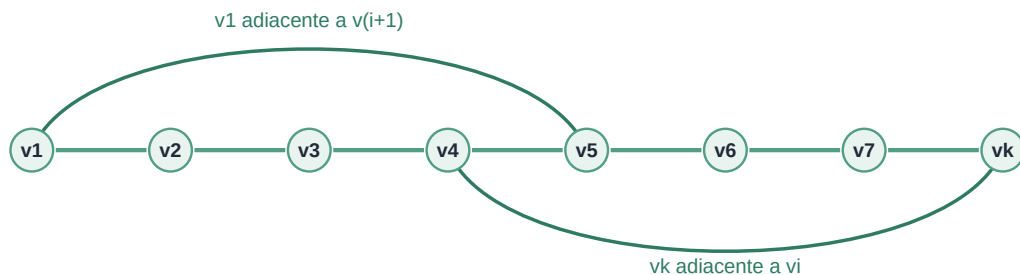


Figura 3. L'idea della dimostrazione di Dirac: se v_1 è adiacente a v_{i+1} e v_k è adiacente a v_i , il cammino si chiude in un ciclo con gli stessi vertici.

Il teorema di Dirac è un caso particolare di un risultato di Ore: se per ogni coppia di vertici *non* adiacenti la somma dei gradi è almeno n , il grafo è hamiltoniano. Entrambe sono condizioni solo sufficienti. Sono state verificate per esaurizione su tutti i grafi con da 3 a 7 vertici; il ciclo C_6 è hamiltoniano ma non le soddisfa (grado 2 contro $n/2 = 3$).

Quanti cicli hamiltoniani ha K_n ? Se tutti i vertici sono collegati tra loro, ogni ordinamento dei vertici è un giro. Fissato il punto di partenza ci sono $(n - 1)!$ ordinamenti dei vertici restanti, e ogni ciclo viene contato due volte, una per ciascun senso di percorrenza: $(n - 1)!/2$ cicli distinti (per $n \geq 3$). Per K_4 sono 3, per K_5 sono 12. Questo numero cresce in modo esplosivo e sarà la chiave del problema del commesso viaggiatore.

Grafi pesati

GRAFO PESATO

Un grafo (o digrafo) $G = (V, E)$ è **pesato** se è data una funzione $c : E \rightarrow \mathbb{R}$ (peso sugli archi) oppure $c : V \rightarrow \mathbb{R}$ (peso sui vertici). Il valore $c(e)$ si chiama peso, costo o lunghezza.

I pesi modellano distanze, tempi, prezzi, capacità. Il **costo di un cammino** $v_1, \dots, v_k$ è la somma dei pesi dei suoi archi, $c(v_1, v_2) + \dots + c(v_{k-1}, v_k)$, oppure la somma dei pesi dei suoi vertici. Un **cammino di costo minimo** (*shortest path*) da v a w è un cammino da v a w di costo minimo; si definisce analogamente il cammino di costo massimo (*longest path*). Con pesi tutti uguali a 1 il cammino di costo minimo è quello con il minor numero di archi.

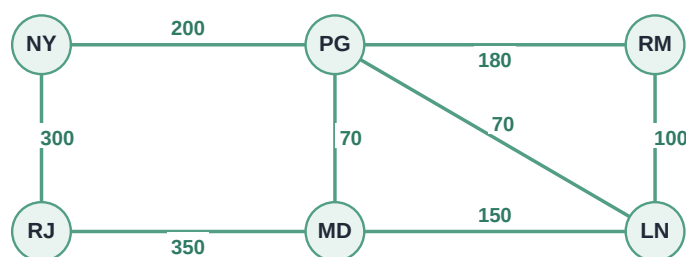
Si parla di *cammini* e non di percorsi perché con pesi negativi un percorso potrebbe ripassare in un ciclo di costo negativo riducendo il costo senza limiti, mentre i cammini sono in numero finito. Il cammino di costo massimo è però un problema difficile in generale (come il commesso viaggiatore), mentre quello di costo minimo con pesi non negativi si risolve in modo efficiente, come vedremo.

RAPPRESENTAZIONE

Con pesi positivi sugli archi, la matrice di adiacenza contiene il peso dell'arco al posto di 1, e 0 per indicare che l'arco manca (se i pesi possono essere 0 o negativi occorre un altro simbolo per «arco assente», per esempio infinito). Con i pesi sui vertici si affianca un vettore di n valori. Nelle liste di adiacenza, ogni elemento della lista è una coppia (vicino, peso), come nel codice di Dijkstra qui sotto.

UN ESEMPIO: I VOLI AEREI

Alcune coppie di città sono collegate da voli di andata e ritorno: Parigi e New York, Parigi e Roma, New York e Rio, Roma e Londra, Parigi e Londra, Rio e Madrid, Madrid e Parigi, Madrid e Londra. Ai voli associamo i prezzi in figura (valori inventati per l'esempio).



Costi dei voli in euro:

RM = Roma, PG = Parigi,
NY = New York, RJ = Rio,
MD = Madrid, LN = Londra.

Figura 4. Il grafo delle rotte aeree con i prezzi dei voli.

Con la teoria vista finora si risponde a molte domande.

- **Minor numero di scali da New York a Roma:** New York, Parigi, Roma (2 voli).
- **Cammino più lungo:** quello della dispensa del corso, New York, Rio, Madrid, Londra, Parigi, Roma, tocca tutte le città (è anche un cammino hamiltoniano) ma non è l'unico di quella lunghezza: anche New York, Rio, Madrid, Parigi, Londra, Roma ha 5 voli.
- **Ciclo hamiltoniano:** Roma, Parigi, New York, Rio, Madrid, Londra, Roma. Per verifica esaustiva è l'unico ciclo hamiltoniano di questo grafo.
- **Circuito euleriano:** non esiste, perché Londra e Madrid hanno grado dispari (3). Esiste invece un percorso euleriano da Londra a Madrid: Londra, Parigi, New York, Rio, Madrid, Parigi, Roma, Londra, Madrid. Eliminando il volo Londra, Madrid i gradi diventano tutti pari e resta il circuito euleriano ottenuto togliendo l'ultimo tratto.
- **Connessione:** il grafo è 2 connesso (sia rispetto agli archi sia ai vertici) e non 3 connesso. Attenzione: il grado minimo 2 *non basta* a concludere che sia 2 connesso in generale; il grado minimo è soltanto un limite superiore per k . Qui la 2 connessione è confermata dal ciclo hamiltoniano, che dà due cammini indipendenti tra ogni coppia di città.

Cammini di costo minimo: l'algoritmo di Dijkstra

Quanto costa andare da Roma a New York? La strada più diretta, Roma, Parigi, New York, costa $180 + 200 = 380$; ma passando per Londra e Parigi (Roma, Londra, Parigi, New York) si spendono $100 + 70 + 200 = 370$. E il costo minimo da Roma a Parigi non è il volo diretto (180) ma quello con scalo a Londra ($100 + 70 = 170$). Il «cammino più breve» in numero di archi non è quello di costo minimo.

L'algoritmo di Dijkstra calcola il costo minimo da un vertice sorgente s a tutti gli altri, **se tutti i pesi sono non negativi**. L'idea: si mantiene per ogni vertice una stima del costo (all'inizio infinito, tranne 0 per s). A ogni passo si sceglie, tra i vertici non ancora definitivi, quello u con la stima più piccola: quel valore è già il costo minimo di u . Si «rilassano» poi gli archi uscenti da u : se passare per u migliora la stima di un vicino v , si aggiorna.

CORRETTEZZA DELL'ALGORITMO DI DIJKSTRA

Con pesi non negativi, quando un vertice u viene dichiarato definitivo la sua stima è il costo minimo da s a u .

Dimostrazione. Per induzione sul numero dei vertici definitivi. Supponiamo che u sia il vertice scelto e che esista un cammino da s a u di costo strettamente minore della stima di u . Questo cammino parte da un vertice definitivo (s) ed esce a un certo punto dall'insieme dei definitivi: sia y il primo vertice non definitivo del cammino, preceduto da un vertice definitivo x . Per ipotesi induttiva la stima di x è corretta, e quando x è diventato definitivo l'arco (x, y) è stato rilassato, quindi la stima di y è al più il costo del tratto del cammino fino a y . Poiché i pesi sono non negativi, quel costo è al più il costo del cammino intero, che per ipotesi è minore della stima di u . Dunque y avrebbe una stima minore di quella di u , e sarebbe stato scelto al posto di u : contraddizione. ■

```

import heapq

def dijkstra(grafo, s):
    """grafo: dizionario vertice: lista di coppie (vicino, peso), pesi >= 0.
    Restituisce i costi minimi da s e il predecessore di ogni vertice."""
    dist = {s: 0}
    padre = {s: None}
    coda = [(0, s)]
    definitivi = set()
    while coda:
        d, u = heapq.heappop(coda)
        if u in definitivi:
            continue
        definitivi.add(u)                # il costo di u e' ormai quello minimo
        for v, peso in grafo[u]:
            nuovo = d + peso
            if v not in dist or nuovo < dist[v]:
                dist[v] = nuovo
                padre[v] = u
                heapq.heappush(coda, (nuovo, v))
    return dist, padre

```

Con una coda con priorità (*heap*) il costo è dell'ordine di $(|V| + |E|) \log |V|$. Con pesi negativi l'algoritmo può sbagliare (anche con pesi negativi, purché non ci siano cicli di costo negativo, si usa l'algoritmo di Bellman e Ford, di costo $|V| \cdot |E|$). La tabella mostra le stime nell'esempio dei voli, partendo da Roma.

PASSO	VERTICE SCELTO	RM	LN	PG	MD	NY	RJ
0	RM (costo 0)	0	100	180	∞	∞	∞
1	LN (100)	0	100	170	250	∞	∞
2	PG (170)	0	100	170	240	370	∞
3	MD (240)	0	100	170	240	370	590
4	NY (370)	0	100	170	240	370	590
5	RJ (590)	0	100	170	240	370	590

Tabella 2. L'algoritmo di Dijkstra con sorgente Roma: stime dei costi dopo ogni passo (RM = Roma, LN = Londra, PG = Parigi, MD = Madrid, NY = New York, RJ = Rio).

I costi minimi da Roma sono 100 (Londra), 170 (Parigi, via Londra), 240 (Madrid, via Londra e Parigi), 370 (New York) e 590 (Rio, via Madrid).

UN ESERCIZIO: IL PRIMO PASSO NON BASTA

Nel digrafo pesato della figura qual è il costo minimo del cammino da 1 a 2, e quello da 2 a 6?

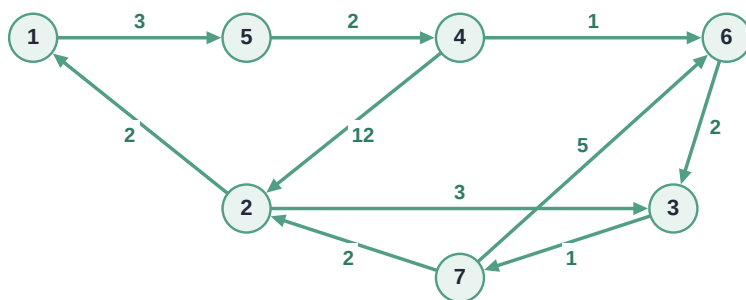


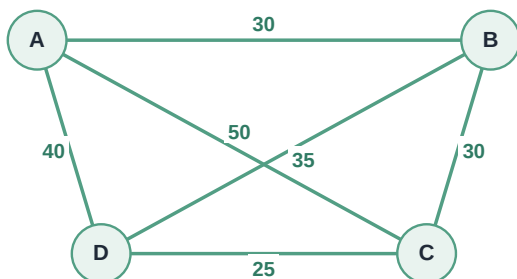
Figura 5. Un digrafo pesato.

Da 1 si può andare solo in 5, poi in 4. Da 4 il percorso più economico al primo passo è l'arco (4, 6) di costo 1, non l'arco diretto (4, 2) di costo 12. Il cammino 1, 5, 4, 6, 3, 7, 2 costa $3 + 2 + 1 + 2 + 1 + 2 = 11$, mentre 1, 5, 4, 2 costa $3 + 2 + 12 = 17$. Da 2 a 6: il cammino 2, 3, 7, 6 costa $3 + 1 + 5 = 9$, ma 2, 1, 5, 4, 6 costa $2 + 3 + 2 + 1 = 8$: la scelta migliore non è quella che inizia con l'arco più economico, né quella con meno archi (qui i due cammini hanno 3 e 4 archi).

Il problema del commesso viaggiatore

Un commesso viaggiatore deve visitare tutte le città di un elenco e tornare al punto di partenza spendendo il meno possibile. Nel linguaggio dei grafi: dato un grafo pesato con pesi positivi, trovare un **ciclo hamiltoniano di costo minimo**. È il **TSP** (*traveling salesman problem*). Per i voli dell'esempio il ciclo hamiltoniano è uno solo e costa $180 + 200 + 300 + 350 + 150 + 100 = 1280$.

Con quattro città A, B, C, D e le distanze della figura, si possono provare tutti i giri partendo da A: sono $3! = 6$ ordinamenti, ma a due a due coincidono (ABCD e ADCBA sono lo stesso ciclo percorso in versi opposti): i giri distinti sono 3.



Distanze in km:

quattro città, sei strade
(il grafo è completo).

Figura 6. Quattro città e le distanze tra loro.

GIRO	CALCOLO	COSTO TOTALE
A, B, C, D, A (e il suo inverso)	$30 + 30 + 25 + 40$	125
A, B, D, C, A (e il suo inverso)	$30 + 35 + 25 + 50$	140
A, C, B, D, A (e il suo inverso)	$50 + 30 + 35 + 40$	155

Tabella 3. I tre giri distinti del TSP con quattro città: il minimo è 125 km.

CORREZIONE

Nelle dispense compaiono sei giri e si dice che «sono 2 i circuiti hamiltoniani di costo minimo» (125 e 125): i sei giri sono i 3 cicli, ciascuno contato due volte (una per verso). Il ciclo di costo minimo è **uno**, di 125 km.

PERCHÉ LA RICERCA ESAUSTIVA NON BASTA

Per n città il numero di giri distinti è $(n - 1)!/2$. Con 30 città, scegliendo il punto di partenza restano 29! ordinamenti, divisi per 2 perché ogni giro è contato due volte ($29!/2 \approx 4,42 \cdot 10^{30}$). Anche ammettendo di esaminare un miliardo di giri al secondo, servirebbero circa $4,42 \cdot 10^{21}$ secondi. Poiché un anno ha circa $3,15 \cdot 10^7$ secondi, sono circa $1,4 \cdot 10^{14}$ anni, cioè circa **140.000 miliardi di anni**: diecimila volte l'età dell'universo (circa 13,8 miliardi di anni).

CITTÀ	GIRI DISTINTI	TEMPO A UN MILIARDO DI GIRI AL SECONDO
5	12	meno di un secondo
10	181.440	meno di un secondo
15	$4,36 \cdot 10^{10}$	circa 44 secondi
20	$6,08 \cdot 10^{16}$	circa 704 giorni
25	$3,10 \cdot 10^{23}$	circa $9,8 \cdot 10^6$ anni
30	$4,42 \cdot 10^{30}$	circa $1,4 \cdot 10^{14}$ anni

Tabella 4. La crescita del numero di giri distinti, $(n - 1)!/2$, del commesso viaggiatore.

CORREZIONE

Nelle dispense il risultato è indicato come «circa 10^{14} , circa diecimila miliardi di anni»: l'ordine di grandezza 10^{14} è giusto, ma 10^{14} anni sono centomila miliardi (e il valore preciso è 1,4 volte tanto), non diecimila miliardi.

Non esistono, a oggi, algoritmi che risolvano il TSP in tempo polinomiale: è un problema NP completo (capitolo 26). Esistono però metodi molto migliori della ricerca esaustiva. La **programmazione dinamica di Held e Karp** (1962) calcola, per ogni sottoinsieme S di città e ogni città j di S , il costo minimo di un cammino che parte dalla città 0, tocca tutte le città di S e finisce in j ; ogni valore si ricava dai valori dei sottoinsiemi più piccoli. Il tempo è dell'ordine di $n^2 \cdot 2^n$: per $n = 30$ sono circa 10^{12} operazioni, una quantità trattabile (minuti o ore), a fronte dei 10^{30} giri della ricerca esaustiva; la memoria richiesta però è grande ($2^n \cdot n$ valori). L'algoritmo del **vicino più vicino** è invece una *euristica* veloce: da ogni città si va alla più vicina tra quelle non ancora visitate. Trova buone soluzioni, ma senza garanzia di ottimalità.

```
from itertools import combinations

def held_karp(d):
    """d: matrice dei costi (n x n). Costo del giro minimo da 0 a 0."""
    n = len(d)
    # costo[(S, j)]: da 0 si toccano tutti i vertici di S e si finisce in j
    costo = {}
    for j in range(1, n):
        costo[(1 << j, j)] = d[0][j]
    for k in range(2, n):
        for sotto in combinations(range(1, n), k):
            S = sum(1 << v for v in sotto)
            for j in sotto:
                senza_j = S ^ (1 << j)
                scelte = [costo[(senza_j, i)] + d[i][j] for i in sotto if i != j]
                costo[(S, j)] = min(scelte)
    tutti = sum(1 << v for v in range(1, n))
    return min(costo[(tutti, j)] + d[j][0] for j in range(1, n))
```

```
def vicino_piu_vicino(d, inizio=0):
    """Euristica: da ogni citta si va alla piu vicina non ancora visitata."""
    u = inizio
    visitati = {inizio}
    giro = [inizio]
    totale = 0
    while len(giro) < len(d):
        v = min((x for x in range(len(d)) if x not in visitati), key=lambda x: d[u][x])
        totale += d[u][v]
        visitati.add(v)
        giro.append(v)
        u = v
    return giro, totale + d[u][inizio]
```

Un esempio in cui il vicino più vicino sbaglia. Con cinque città e le distanze della tabella, partendo dalla città 0 il metodo percorre il giro 0, 4, 2, 1, 3, 0, di costo 17; il giro ottimo costa 11.

DISTANZE	CITTÀ 0	CITTÀ 1	CITTÀ 2	CITTÀ 3	CITTÀ 4
città 0	0	3	7	3	2
città 1	3	0	3	8	3
città 2	7	3	0	3	1
città 3	3	8	3	0	1
città 4	2	3	1	1	0

Tabella 5. Un esempio di cinque città su cui l'euristica del vicino più vicino non trova il giro minimo.

Altre tecniche sono gli algoritmi di approssimazione (per esempio quello di Christofides, che garantisce un costo al più 1,5 volte l'ottimo se le distanze rispettano la disuguaglianza triangolare), i metodi di ricerca locale e quelli *branch and bound*. Con queste tecniche, e con enorme potenza di calcolo, sono state risolte istanze del TSP con decine di migliaia di città: il problema è difficile nel caso peggiore, non necessariamente in ogni istanza. Sono problemi della stessa natura, intrinsecamente difficile, molti altri: li incontreremo nel capitolo 26.

Grafi planari e colorazione

Quando un grafo si può disegnare senza incroci: il teorema di Kuratowski, la formula di Eulero con dimostrazione e le sue conseguenze; poi la colorazione dei vertici, il numero cromatico, il teorema dei quattro colori.

Grafi planari

GRAFO PLANARE

Un grafo non orientato è **planare** se può essere disegnato nel piano in modo che due archi non si intersechino se non negli estremi. Altrimenti è **non planare**.

«Planare» è una proprietà del grafo, non del suo disegno: un grafo planare può anche essere disegnato con gli archi che si incrociano, e il problema è se esista un disegno senza incroci. Il grafo completo K_4 è planare: basta mettere un vertice al centro del triangolo formato dagli altri tre. Anche tutti gli alberi, i cicli, i cubi sono planari. La Figura 1 mostra invece che K_5 e $K_{3,3}$ si disegnano con un solo incrocio, ma non senza: togliendo un solo arco da ciascuno dei due si ottiene un grafo planare.

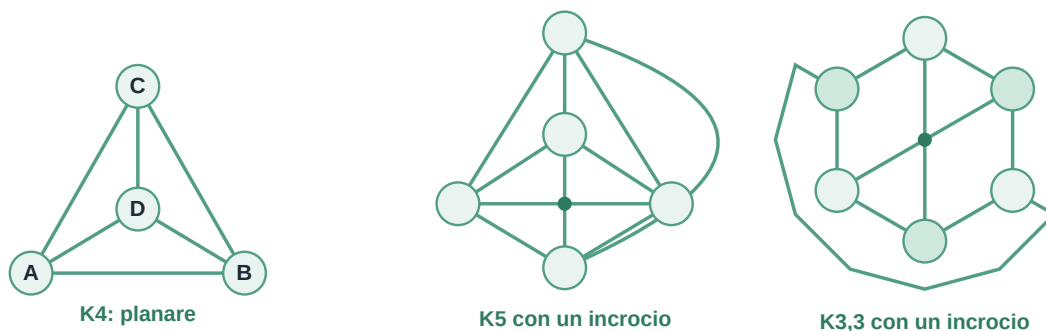


Figura 1. K_4 è planare. Per K_5 e per $K_{3,3}$ si trovano disegni con un solo incrocio (il punto scuro): si possono disegnare senza incroci soltanto togliendo un arco.

TEOREMA DI KURATOWSKI (1930)

Un grafo è planare se e solo se non contiene alcun sottografo omeomorfo a K_5 o a $K_{3,3}$.

Ricordiamo che due grafi sono omeomorfi se si ottengono l'uno dall'altro inserendo vertici di grado 2 lungo gli archi (capitolo 22). K_5 e $K_{3,3}$ sono dunque la «radice» della non planarità: ogni grafo non planare ne contiene una copia, eventualmente con vertici in più sugli archi. Il teorema è citato senza dimostrazione. Applicarlo direttamente richiede però di cercare sottografi, un compito costoso; esistono invece algoritmi molto veloci (tempo proporzionale al numero di vertici, trovati da Hopcroft e Tarjan nel 1974) che decidono la planarità e, quando è planare, producono anche il disegno. Sono però complicati da realizzare.

La formula di Eulero

Un disegno planare divide il piano in **facce**: le regioni delimitate dagli archi, compresa la regione esterna, che è illimitata. Indichiamo con v il numero dei vertici, con e quello degli archi e con f quello delle facce.

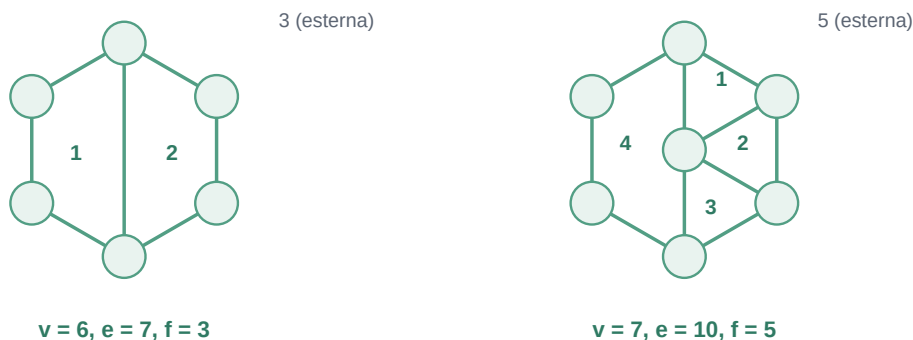


Figura 2. Due grafi planari connessi con le loro facce numerate (la faccia esterna conta). In entrambi $v - e + f = 2$.

FORMULA DI EULERO

Per ogni grafo planare connesso, disegnato nel piano senza incroci, $v - e + f = 2$.

La dimostrazione richiede due lemmi, che servono anche altrove.

LEMMA 1: UN CICLO C'È SEMPRE SE IL GRADO MINIMO È ALMENO 2

Se in un grafo ogni vertice ha grado almeno 2, allora il grafo contiene un ciclo.

Dimostrazione. Consideriamo un cammino $v_1, \dots, v_k$ di lunghezza massima. Il vertice v_k ha almeno due vicini, e tutti stanno sul cammino (altrimenti si potrebbe allungare). Uno di essi è v_{k-1} ; l'altro è un v_j con $j < k - 1$. Allora $v_j, \dots, v_k, v_j$ è un ciclo. ■

LEMMA 2: UN GRAFO CONNESSO E SENZA CICLI HA $n - 1$ ARCHI

Se G è connesso e aciclico con n vertici, allora ha esattamente $n - 1$ archi.

Dimostrazione. Per induzione su n . Con $n = 1$ ci sono 0 archi. Sia $n \geq 2$. Ogni vertice ha grado almeno 1 (connessione); se tutti avessero grado almeno 2, per il Lemma 1 ci sarebbe un ciclo. Dunque esiste un vertice x di grado 1. Eliminiamo x e il suo arco: il grafo rimasto è ancora connesso (un cammino tra due vertici rimasti non può passare per x , che ha un solo vicino e dovrebbe entrarvi e uscirvi da quell'unico arco) e aciclico, con $n - 1$ vertici, quindi per ipotesi induttiva ha $n - 2$ archi. Con l'arco di x sono $n - 1$. ■

DIMOSTRAZIONE DELLA FORMULA DI EULERO

Per induzione sul numero di archi. Se il grafo non ha cicli, è connesso e aciclico: per il Lemma 2 $e = v - 1$ e il disegno ha una sola faccia (la regione esterna), $f = 1$, quindi $v - e + f = v - (v - 1) + 1 = 2$.

Se invece c'è un ciclo, scegliamo un arco a del ciclo. Il ciclo è una curva chiusa nel piano e divide il piano in un interno e un esterno (teorema della curva di Jordan, che accettiamo): i due lati di a appartengono quindi a facce diverse. Eliminando a , queste due facce si fondono in una: il grafo rimane connesso (due vertici collegati attraverso a si collegano girando sul resto del ciclo), e scende di 1, f scende di 1 e $v - e + f$ resta uguale. Ripetendo l'operazione si arriva a un grafo senza cicli, per il quale vale 2. ■

Verifichiamola sui grafi della Figura 2: $6 - 7 + 3 = 2$ e $7 - 10 + 5 = 2$.

NOTA SULLA DIMOSTRAZIONE DEL CORSO

Le dispense scrivono «eliminiamo tutti i cicli dall'albero», ma si parte da un grafo e l'albero è ciò che si ottiene alla fine. Inoltre il Lemma 1 vale per ogni grafo con grado minimo almeno 2: non servono né la connessione né l'ipotesi $|V| \geq 3$ delle dispense (con grado minimo 2 i vertici sono comunque almeno 3).

CONSEGUENZE: LIMITI SUL NUMERO DI ARCHI

Siano G un grafo planare connesso, semplice, con $v \geq 3$ vertici, disegnato senza incroci. Percorrendo il bordo di ciascuna faccia si incontrano gli archi della faccia, e ogni arco viene incontrato due volte in tutto (una per ognuno dei suoi due lati, che possono appartenere alla stessa faccia o a due facce diverse). La somma delle lunghezze dei bordi delle facce è quindi $2e$. Poiché il grafo è semplice e ha almeno 3 vertici, ogni faccia ha bordo lungo almeno 3. Perciò $3f \leq 2e$, cioè $f \leq 2e/3$. Sostituendo in $v - e + f = 2$ si ottiene $2 = v - e + f \leq v - e + 2e/3 = v - e/3$, cioè:

PRIMO LIMITE

Se G è un grafo planare semplice con $v \geq 3$ vertici, allora $e \leq 3v - 6$.

Se inoltre G non ha triangoli, ogni faccia ha bordo lungo almeno 4, quindi $4f \leq 2e$ e con lo stesso calcolo si trova $2 \leq v - e/2$:

SECONDO LIMITE

Se G è un grafo planare semplice con $v \geq 3$ vertici e senza cicli di lunghezza 3, allora $e \leq 2v - 4$.

Più in generale, se il ciclo più corto di G ha lunghezza g (la **maglia** del grafo), ogni faccia ha bordo lungo almeno g e si trova $e \leq g(v - 2)/(g - 2)$. I primi due limiti sono i casi $g = 3$ e $g = 4$. Sono condizioni **necessarie** per la planarità, non sufficienti: servono per dimostrare che un grafo *non* è planare.

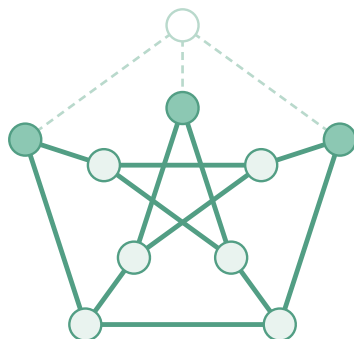
- K_5 ha $v = 5$ ed $e = 10 > 3 \cdot 5 - 6 = 9$: non è planare.
- $K_{3,3}$ ha $v = 6$ ed $e = 9$ e non ha triangoli (è bipartito): $9 > 2 \cdot 6 - 4 = 8$, quindi non è planare.

Questi due fatti, insieme al teorema di Kuratowski, spiegano perché sono proprio K_5 e $K_{3,3}$ i grafi proibiti.

UN ESEMPIO: IL GRAFO DI PETERSEN

Il grafo di Petersen ha 10 vertici e 15 archi, ed è regolare di grado 3. È planare? I primi due limiti non decidono: $15 \leq 3 \cdot 10 - 6 = 24$ e anche, dato che non ha triangoli, $15 \leq 2 \cdot 10 - 4 = 16$. Ma il suo ciclo più corto ha lunghezza 5 (maglia $g = 5$), e il limite generale dà $e \leq 5 \cdot (10 - 2)/3 = 13,33\dots$: 15 archi sono troppi. **Il grafo di Petersen non è planare.**

Si può anche mostrarlo con Kuratowski, trovando un sottografo omeomorfo a $K_{3,3}$. Eliminiamo un vertice qualunque: il grafo che resta ha 9 vertici e 12 archi, e i tre ex vicini hanno grado 2. «Cancellando» questi tre vertici (cioè sostituendo ciascuno con un arco che unisce i suoi due vicini) restano 6 vertici di grado 3 e 9 archi: è esattamente $K_{3,3}$ (verificato con il calcolatore). Il grafo di Petersen privato di un vertice è dunque una suddivisione di $K_{3,3}$.



Grafo di Petersen privato del vertice in alto (tratteggiato).

I tre vertici scuri (ex vicini) hanno grado 2: sono i punti di suddivisione.

Eliminandoli si ottiene un $K_{3,3}$.

Figura 3. Un sottografo del grafo di Petersen omeomorfo a $K_{3,3}$.

GRAFI PLANARI MASSIMALI

Un grafo planare si dice **massimale** (o triangolare) se aggiungendo un qualunque arco tra due vertici non adiacenti diventa non planare. In un grafo planare massimale con $v \geq 3$ vertici ogni faccia, esterna compresa, è un triangolo: se una faccia avesse almeno 4 lati, si potrebbe aggiungere una diagonale al suo interno senza incroci (è un fatto standard, che accettiamo). Allora $3f = 2e$ e dalla formula di Eulero si ricava che ha esattamente **$3v - 6$ archi e $2v - 4$ facce**: il primo limite vale con l'uguaglianza.

GRAFO	VERTICI	ARCHI	FACCE
K_5 meno un arco	5	9	6
Ottaedro	6	12	8
Icosaedro	12	30	20

Tabella 1. Tre grafi planari massimali: archi = $3v - 6$, facce = $2v - 4$ (verificato).

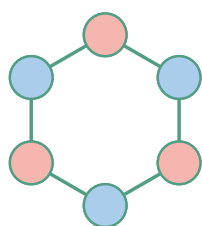
Una conseguenza immediata: in un grafo planare semplice la somma dei gradi è $2e \leq 6v - 12 < 6v$, quindi il grado medio è minore di 6, e **esiste sempre un vertice di grado al più 5**. Questo fatto serve nella dimostrazione del teorema dei sei colori (si veda più avanti). Il limite $e \leq 3v - 6$ vale anche se il grafo non è connesso: si aggiungono archi finché non lo diventa, senza perdere la planarità.

Colorazione di un grafo

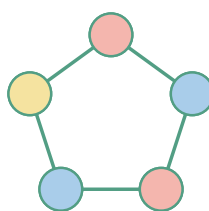
Un problema molto studiato e utile nelle applicazioni è colorare un grafo: assegnare un colore a ciascun vertice in modo che due vertici collegati da un arco abbiano colori diversi. Esempi tipici: assegnare frequenze radio a ripetitori vicini che non devono disturbarsi, assegnare le aule agli esami (due esami con studenti in comune non possono stare nello stesso orario), allocare i registri di una CPU a variabili che vivono nello stesso momento.

COLORAZIONE E NUMERO CROMATICO

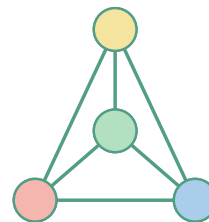
Una **colorazione** (propria) dei vertici di G con k colori è una funzione che a ogni vertice associa uno di k colori in modo che i due estremi di ogni arco abbiano colori diversi. G è **k colorabile** se ha una colorazione con al più k colori. Il **numero cromatico** $\chi(G)$ è il minimo k per cui G è k colorabile; una colorazione con $\chi(G)$ colori si dice **ottimale**.



C6: 2 colori



C5: 3 colori



K4: 4 colori

Figura 4. Colorazioni ottimali di un ciclo pari, di un ciclo dispari e di un grafo completo.

GRAFI COMPLETI, BIPARTITI, CICLI

- **Grafo completo.** Tutti i vertici sono a due a due adiacenti, quindi servono n colori diversi: $\chi(K_n) = n$.
- **Grafo bipartito.** Si colorano con un colore i vertici di V_1 e con un altro quelli di V_2 : $\chi \leq 2$ (e $\chi = 2$ se c'è almeno un arco). Vale anche il viceversa, e c'è una caratterizzazione per i cicli (teorema qui sotto).
- **Ciclo.** C_n ha $\chi = 2$ se n è pari (si alternano due colori) e $\chi = 3$ se n è dispari: con due colori alternati l'ultimo vertice avrebbe lo stesso colore del primo, che gli è adiacente, e quindi ne serve un terzo. In breve $\chi(C_n) = 2 + (n \bmod 2)$.

GRAFI BIPARTITI, DUE COLORI E CICLI DISPARI

Per un grafo G sono equivalenti: (a) G è bipartito; (b) G è 2 colorabile; (c) G non contiene cicli di lunghezza dispari.

Dimostrazione. (a) $\Leftrightarrow$ (b): i due colori danno la partizione, e una partizione bipartita dà i due colori. (a) $\Rightarrow$ (c): in un ciclo i vertici stanno alternativamente in V_1 e in V_2 , quindi la lunghezza è pari. (c) $\Rightarrow$ (a): basta farlo per ogni componente connessa. Fissiamo un vertice r e mettiamo in V_1 i vertici a distanza pari da r e in V_2 quelli a distanza dispari. Se per assurdo un arco $\{x, y\}$ avesse i due estremi nello stesso insieme, le distanze di x e y da r avrebbero la stessa parità: i due cammini minimi da r a x e a y , uniti con l'arco $\{x, y\}$, formano un percorso chiuso di lunghezza dispari. Ora un percorso chiuso di lunghezza dispari contiene sempre un ciclo dispari: se non ripete vertici (tranne il primo e l'ultimo) è già un ciclo; altrimenti lo si spezza nel vertice ripetuto in due percorsi chiusi più corti, la cui lunghezza totale è dispari, e quindi uno dei due è dispari, e si ripete l'argomento. Si ottiene un ciclo dispari: assurdo. ■

LIMITI SUPERIORI: L'ALGORITMO GOLOSO

Calcolare $\chi(G)$ è, come il problema del commesso viaggiatore, un problema difficile: non si conoscono algoritmi veloci (capitolo 26). Si hanno però buoni limiti. Il più semplice usa l'algoritmo **goloso** (*greedy*): si considerano i vertici uno dopo l'altro, in un ordine qualsiasi, e ciascuno riceve il colore più piccolo non usato dai suoi vicini già colorati.

LIMITE $\chi \leq \Delta + 1$

Sia Δ il massimo grado dei vertici di G . Allora $\chi(G) \leq \Delta + 1$.

Dimostrazione. Con l'algoritmo goloso, quando si colora un vertice v al più Δ dei suoi vicini sono già colorati, quindi al più Δ colori sono vietati e tra i primi $\Delta + 1$ colori ce n'è sempre uno libero. ■

Nelle dispense questo limite è chiamato «teorema di Brooks» ed è dimostrato per induzione togliendo il vertice di grado massimo; la dimostrazione con l'algoritmo goloso è equivalente, ma il vero teorema di Brooks è un'altra cosa, più forte.

TEOREMA DI BROOKS (1941)

Se G è connesso e non è né un grafo completo né un ciclo di lunghezza dispari, allora $\chi(G) \leq \Delta$.

I due casi esclusi sono proprio quelli in cui χ vale $\Delta + 1$: K_n ha $\Delta = n - 1$ e $\chi = n$; i cicli dispari hanno $\Delta = 2$ e $\chi = 3$. Il teorema è citato senza dimostrazione; l'abbiamo verificato per esaurimento su tutti i grafi connessi con al più 7 vertici. Si noti che Δ può essere un limite molto largo: il grafo bipartito completo $K_{m,m}$ ha $\Delta = m$ ma $\chi = 2$.

Per un limite *inferiore*, se G contiene un sottografo completo K_k (una *cricca*), servono almeno k colori. Lo useremo per l'Italia.

Mappe geografiche e teorema dei quattro colori

Il problema di colorare una carta geografica, in modo che regioni confinanti abbiano colori diversi, è un caso particolare. Si costruisce un grafo con un vertice per ciascuna regione e un arco tra due vertici se le regioni confinano (cioè hanno in comune un tratto di confine, non solo un punto). Il grafo ottenuto è planare, e viceversa ogni grafo planare è il grafo di una carta.

L'esempio dell'Italia, con le 20 regioni (Trentino Alto Adige come una sola regione), è nella Figura 5: il grafo ha 31 archi, tre componenti connesse (la parte continentale e peninsulare, la Sicilia e la Sardegna, isolate), e contiene un K_4 : Toscana, Marche, Umbria e Lazio confinano tutte a due a due. Servono quindi almeno 4 colori, e una colorazione con 4 esiste, e quindi $\chi = 4$ (anche questo verificato con il calcolatore).

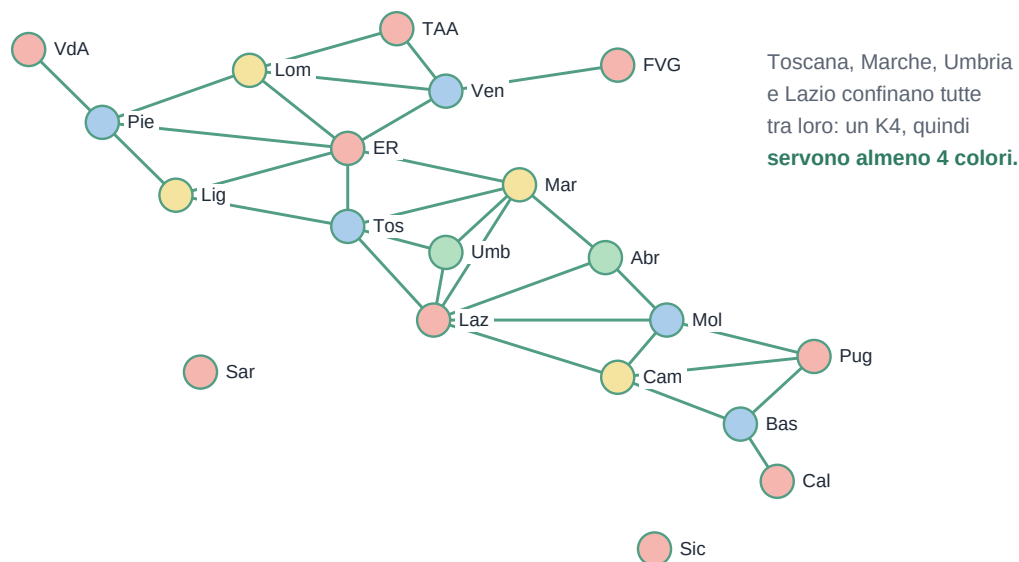


Figura 5. Il grafo delle regioni italiane, con una colorazione ottimale a quattro colori. Il grafo è ricostruito dalla geografia dei confini regionali (non dalle dispense) e le posizioni dei vertici sono schematiche.

TEOREMA DEI QUATTRO COLORI

Ogni grafo planare è 4 colorabile: $\chi(G) \leq 4$.

La storia è celebre. Nel 1852 lo studente Francis Guthrie, colorando la mappa delle contee inglesi, osservò che bastavano quattro colori e si chiese se fosse sempre così (il problema fu poi popolarizzato da De Morgan). Una dimostrazione del 1879 di Kempe, ritenuta valida per oltre dieci anni, fu trovata sbagliata da Heawood nel 1890, il quale ne ricavò però il teorema dei cinque colori. Il teorema dei quattro colori fu dimostrato nel 1976 da Appel e Haken, con un uso essenziale del calcolatore per controllare un grande numero di casi («configurazioni»); nel 1997 Robertson, Sanders, Seymour e Thomas ne diedero una dimostrazione più semplice, sempre con il calcolatore, e nel 2005 Gonthier ne ha fornito una verifica formale con un assistente di dimostrazione. Non si conosce una dimostrazione senza calcolatore.

CORREZIONE

Le dispense collocano la scoperta «alla fine del XIX secolo»: l'osservazione di Guthrie è del 1852 (la dimostrazione, errata, di Kempe è del 1879).

Il teorema dei **sei** colori, invece, si dimostra in poche righe con quanto visto.

TEOREMA DEI SEI COLORI

Ogni grafo planare semplice è 6 colorabile.

Dimostrazione. Per induzione sul numero di vertici v . Se $v \leq 6$ è ovvio. Sia $v > 6$. Per quanto visto sopra, G ha un vertice x di grado al più 5. Il grafo $G - x$ (si elimina x con i suoi archi) è ancora planare, con un vertice in meno, quindi per ipotesi induttiva ha una colorazione con 6 colori. I vicini di x sono al più 5 e usano al più 5 colori: ne resta uno libero, che assegniamo a x . ■

Con un'idea in più (le «catene di Kempe») si dimostra anche il teorema dei cinque colori; il passaggio da 5 a 4 è proprio quello che ha richiesto più di un secolo.

ESERCIZI RISOLTI

GRAFO	PLANARE?	χ	MOTIVO
Ruota con 5 raggi (un vertice collegato a un C_5)	sì	4	il C_5 esterno richiede 3 colori e il centro è adiacente a tutti: 4; è il massimo permesso
Ruota con 6 raggi (centro e C_6)	sì	3	il C_6 si colora con 2 colori, il centro ne prende un terzo
$K_{3,3}$	no	2	è bipartito
Cubo	sì	2	è bipartito
Ottaedro	sì	3	tre coppie di vertici opposti, ciascuna con lo stesso colore
K_5 meno un arco	sì	4	contiene un K_4
Grafo di Petersen	no	3	ha cicli dispari (lunghezza 5), e 3 colori bastano
Icosaedro	sì	4	ogni vertice è adiacente a 5 vertici, che formano un ciclo di 5: servono 3 colori per quel ciclo, più 1 per il vertice

Tabella 2. Planarità e numero cromatico di alcuni grafi (tutti i valori sono stati verificati con il calcolatore).

Un esperimento di programmazione

Per toccare con mano la difficoltà della colorazione si può generare un grafo casuale con 30 vertici, colorarlo e giudicare l'algoritmo. Si usa una matrice di adiacenza simmetrica con la diagonale nulla, in cui ogni coppia di vertici è collegata con probabilità $1/2$.

```
import random

def grafo_casuale(n, seme):
    """Matrice di adiacenza: ogni coppia di vertici e' un arco con probabilita 1/2."""
    rnd = random.Random(seme)
    A = [[0] * n for _ in range(n)]
    for i in range(n):
        for j in range(i + 1, n):
            A[i][j] = A[j][i] = rnd.randint(0, 1)
    return A

def colora(A, ordine):
    """Colorazione golosa: ogni vertice prende il colore minimo non usato dai vicini."""
    colore = {}
    for v in ordine:
        usati = {colore[u] for u in colore if A[v][u]}
        c = 0
        while c in usati:
            c += 1
        colore[v] = c
    return colore
```

Il grafo con seme 0 ha grado massimo 19 e viene colorato dall'algoritmo goloso con 7 colori, nettamente sotto il limite $\Delta + 1$. Su 500 grafi casuali con 30 vertici l'algoritmo goloso usa in media 9,2 colori con l'ordine naturale dei vertici e 8,4 colori se i vertici sono presi in ordine di grado decrescente, mai più di 12. Il valore ottimo χ non è calcolato: si controlla solo che la colorazione sia valida e che non superi $\Delta + 1$. Un esercizio analogo, con pesi casuali da 1 a 100, riguarda il commesso viaggiatore (capitolo 24).

Alberi, complessità e problemi combinatori su grafi

Alberi liberi e radicati e le loro proprietà; polinomiale contro esponenziale, le classi P, NP e i problemi NP completi; colorazione, feedback vertex set, insiemi indipendenti e vertex cover; permutazioni casuali.

Alberi

ALBERO LIBERO

Un **albero libero** (o semplicemente albero) è un grafo connesso e aciclico.

Gli alberi sono i grafi connessi «più economici»: hanno il minimo numero di archi che serve a tenere connessi i vertici. Dal capitolo 25 sappiamo già che un albero con n vertici ha esattamente $n - 1$ archi (Lemma 2). Le caratterizzazioni seguenti sono tutte equivalenti, e ognuna è comoda per un problema diverso.

CARATTERIZZAZIONI DEGLI ALBERI

Per un grafo G con n vertici sono equivalenti: (a) G è un albero; (b) G è connesso e ha $n - 1$ archi; (c) G è aciclico e ha $n - 1$ archi; (d) tra ogni coppia di vertici esiste un *unico* cammino; (e) G è connesso e ogni arco è un ponte (eliminandolo il grafo si sconnette); (f) G è aciclico e aggiungere un arco qualsiasi crea esattamente un ciclo.

Dimostrazione. (a) $\Rightarrow$ (b), (c): Lemma 2 del capitolo 25. (b) $\Rightarrow$ (a): se ci fosse un ciclo, eliminando un suo arco il grafo rimarrebbe connesso; si procede finché non rimane alcun ciclo: si ottiene un grafo connesso e aciclico, quindi un albero con $n - 1$ archi, ma partendo da $n - 1$ archi non se n'è tolto nessuno, quindi non c'erano cicli. (c) $\Rightarrow$ (a): un grafo aciclico con k componenti connesse è unione di k alberi, quindi ha $n - k$ archi; da $n - k = n - 1$ segue $k = 1$, cioè è connesso. (a) $\Rightarrow$ (d): se ci fossero due cammini diversi tra u e v , a partire dal primo punto in cui divergono e fino al punto in cui si ricongiungono si avrebbe un ciclo. (d) $\Rightarrow$ (a): l'esistenza del cammino dà la connessione; se ci fosse un ciclo, due suoi vertici sarebbero uniti da due cammini diversi. (a) $\Rightarrow$ (e): se eliminando un arco $\{u, v\}$ il grafo restasse connesso ci sarebbe un secondo cammino tra u e v , contro (d). (e) $\Rightarrow$ (a): se ci fosse un ciclo, eliminando un suo arco il grafo rimarrebbe connesso, contro (e). (a) $\Rightarrow$ (f): aggiungendo $\{u, v\}$ esso chiude, con l'unico cammino da u a v , un ciclo; e non può chiuderne due perché il cammino è unico. (f) $\Rightarrow$ (a): se G non fosse connesso, aggiungendo un arco tra due componenti diverse non si creerebbe alcun ciclo. ■

FOGLIE E FORESTE

In un albero con almeno 2 vertici i vertici di grado 1 si chiamano **foglie** (o vertici terminali); quelli di grado maggiore di 1 sono **vertici interni**. Un albero con almeno 2 vertici ha **almeno due foglie**: la somma dei gradi è $2(n - 1) = 2n - 2$; se al più una foglia avesse grado 1 e tutti gli altri gradi fossero almeno 2 (nessun vertice ha grado 0, per la connessione), la somma sarebbe almeno $1 + 2(n - 1) = 2n - 1$, troppo grande. Una **foresta** è un grafo aciclico, non necessariamente connesso: ogni sua componente connessa è un albero, e una foresta con k componenti e n vertici ha $n - k$ archi.

Quanti alberi ci sono? Con n vertici *etichettati* (cioè distinguibili) sono n^{n-2} (formula di Cayley, 1889): 1, 1, 3, 16, 125, 1.296 per $n = 1, \dots, 6$ (verificato per enumerazione fino a $n = 7$). Per $n = 3$ sono 3: il vertice centrale può essere uno qualunque dei tre. Se invece non si distinguono i vertici, cioè a meno di isomorfismo, gli alberi con $n = 1, 2, \dots, 8$ vertici sono 1, 1, 1, 2, 3, 6, 11, 23 (sempre verificato al calcolatore).

ALBERI RADICATI

Se in un albero libero si sceglie un vertice, la **radice**, e si immagina di appenderlo a un chiodo in modo che gli altri vertici cadano per gravità, si ottiene un **albero radicato**. Ogni vertice diverso dalla radice ha un unico **genitore** (il vertice adiacente che lo precede sul cammino verso la radice) e i vertici che si trovano subito sotto di lui sono i suoi **figli**; le foglie sono i vertici senza figli. Il **livello** di un vertice è la lunghezza del cammino che lo unisce alla radice; l'**altezza** dell'albero è il massimo livello, cioè la lunghezza del cammino più lungo dalla radice a una foglia; il **fattore di ramificazione** è il massimo numero di figli di un vertice.

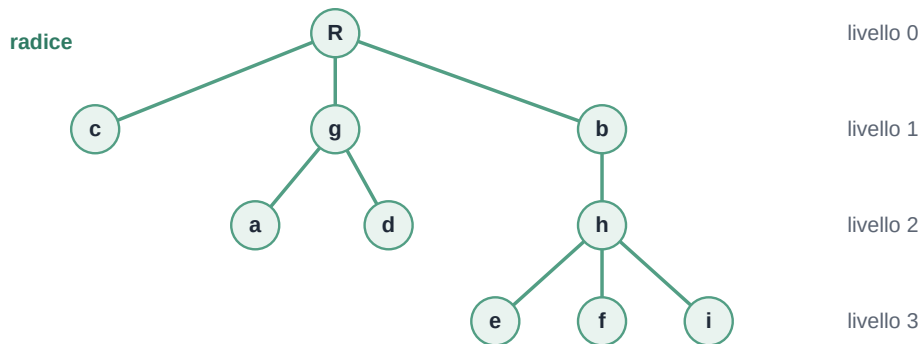
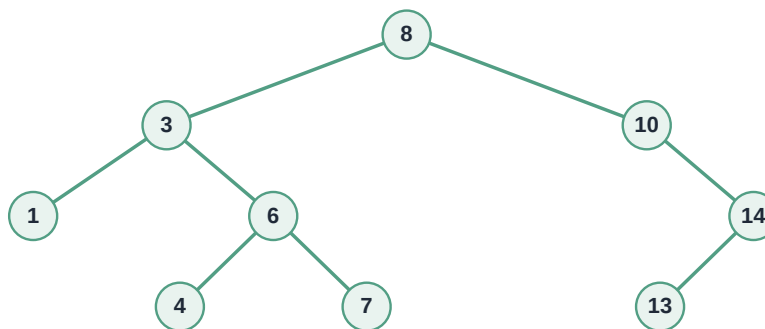


Figura 1. Un albero radicato con 10 vertici: la radice R ha 3 figli, il vertice g ne ha 2, le foglie sono a, c, d, e, f, i. L'altezza è 3 e il fattore di ramificazione è 3.

Un albero con fattore di ramificazione $b \geq 2$ e altezza h ha al più b^i vertici al livello i (si procede per induzione: ogni vertice ha al più b figli), quindi in tutto al più $1 + b + \dots + b^h = (b^{h+1} - 1)/(b - 1)$ vertici e al più b^h foglie. Per $b = 2$: al più $2^{h+1} - 1$ vertici. Ne segue che un albero binario con n vertici ha altezza almeno $\lceil \log_2(n + 1) \rceil - 1$: per questo gli alberi bilanciati sono efficienti, perché l'altezza, e dunque il costo del cammino dalla radice a una foglia, cresce solo come il logaritmo del numero di vertici.

ALBERI BINARI E VISITE

Un **albero binario** è un albero radicato in cui ogni vertice ha al più due figli, distinti come figlio *sinistro* e figlio *destro*. Per visitare tutti i vertici ci sono tre ordini classici, definiti ricorsivamente: nella visita in **preordine** si visita la radice, poi il sottoalbero sinistro, poi il destro; in **ordine simmetrico** (*inorder*) il sinistro, la radice, il destro; in **postordine** il sinistro, il destro, la radice.



un albero binario:
ogni nodo ha al più
due figli, sinistro
e destro.

Figura 2. Un albero binario con 9 vertici (è anche un albero binario di ricerca: ogni valore è maggiore di quelli del suo sottoalbero sinistro e minore di quelli del destro).

```
# un albero binario e' None (vuoto) oppure una terna (valore, sinistro, destro)
albero = (8,
          (3, (1, None, None), (6, (4, None, None), (7, None, None))),
          (10, None, (14, (13, None, None), None)))

def preordine(t):
```

```

    if t is None:
        return []
    valore, sx, dx = t
    return [valore] + preordine(sx) + preordine(dx)

def inordine(t):
    if t is None:
        return []
    valore, sx, dx = t
    return inordine(sx) + [valore] + inordine(dx)

def postordine(t):
    if t is None:
        return []
    valore, sx, dx = t
    return postordine(sx) + postordine(dx) + [valore]

def altezza(t):
    """Lunghezza in archi del cammino piu lungo dalla radice a una foglia."""
    valore, sx, dx = t
    figli = [f for f in (sx, dx) if f is not None]
    if not figli:
        return 0
    return 1 + max(altezza(f) for f in figli)

```

Sull'albero della figura le tre visite danno: preordine 8, 3, 1, 6, 4, 7, 10, 14, 13; ordine simmetrico 1, 3, 4, 6, 7, 8, 10, 13, 14; postordine 1, 4, 7, 6, 3, 13, 14, 10, 8. Nell'albero di ricerca la visita in ordine simmetrico restituisce i valori *in ordine crescente*, e questo è il motivo per cui ha questo nome.

ALBERI DI COPERTURA

Un **albero di copertura** di un grafo connesso G è un sottografo che è un albero e contiene tutti i vertici di G . Esiste sempre: finché c'è un ciclo si elimina uno dei suoi archi (il grafo resta connesso), e alla fine si ottiene un grafo connesso aciclico. Se gli archi hanno un peso, l'**albero di copertura di peso minimo** (la rete più economica che collega tutto) si trova con un algoritmo goloso che, a differenza dei problemi che vedremo tra poco, è sempre ottimo: l'algoritmo di Kruskal considera gli archi in ordine di peso crescente e accetta un arco se non chiude un ciclo con quelli già accettati.

Problemi facili e problemi difficili

Alcuni problemi sui grafi, come decidere se esiste un circuito euleriano, trovare un cammino di costo minimo o riconoscere un grafo planare, hanno algoritmi efficienti. Altri, come la colorazione o il commesso viaggiatore, no: finora nessuno ne ha trovato uno efficiente. Per un informatico «efficiente» ha un significato preciso: il numero di passi è limitato da una funzione **polinomiale** della dimensione dell'input (nei grafi, in n e in $|E|$).

PASSI	$N = 20$	$N = 30$	$N = 50$	$N = 100$
n^2	meno di un secondo	meno di un secondo	meno di un secondo	meno di un secondo
n^3	meno di un secondo	meno di un secondo	meno di un secondo	meno di un secondo
2^n	meno di un secondo	circa 1 secondi	circa 13 giorni	circa $4,0 \cdot 10^{13}$ anni
$n!$	circa 77 anni	circa $8,4 \cdot 10^{15}$ anni	circa $9,6 \cdot 10^{47}$ anni	circa $3,0 \cdot 10^{141}$ anni

Tabella 1. Tempo necessario per eseguire n elevato a 2, n elevato a 3, 2 elevato a n e n fattoriale passi, con un calcolatore che esegue un miliardo di passi al secondo.

La differenza è radicale: un algoritmo con n^3 passi resta praticabile anche con 100 vertici, mentre uno con 2^n o con $n!$ passi diventa irrealizzabile già con 50 o 100 elementi, e nessun miglioramento dei calcolatori cambia la situazione (raddoppiare la velocità permette di aggiungere un solo elemento a un algoritmo con 2^n passi).

LE CLASSI P E NP

La teoria della complessità si occupa soprattutto di problemi di **decisione**, cioè con risposta sì o no. Per esempio: «il grafo G si può colorare con al più k colori?». I problemi di **ottimizzazione** («qual è il numero cromatico di G ?») sono strettamente legati ai primi: se so rispondere velocemente alla domanda con k colori, trovo $\chi(G)$ provando $k = 1, 2, \dots$ (oppure, più in fretta, con una ricerca binaria); viceversa, se conosco $\chi(G)$ rispondo subito alla domanda per ogni k .

P E NP

P è la classe dei problemi di decisione risolvibili da un algoritmo in tempo polinomiale. **NP** è la classe dei problemi di decisione per i quali, quando la risposta è «sì», esiste un *certificato* (una prova) che si può *verificare* in tempo polinomiale.

Esempio: dato un grafo e un numero k , un certificato per « G è k colorabile» è una colorazione, e controllare che sia valida costa $|E|$ confronti. Ogni problema in P è anche in NP (la verifica è la soluzione stessa), ma non si sa se valga l'uguaglianza: «**P = NP?**» è il più celebre problema aperto dell'informatica teorica, uno dei sette problemi del millennio del Clay Mathematics Institute (2000). Quasi tutti gli esperti ritengono che P sia diverso da NP, ma nessuno l'ha dimostrato.

PROBLEMI NP DIFFICILI E NP COMPLETI

Un problema è **NP difficile** (*NP hard*) se è almeno altrettanto difficile di qualunque problema di NP: un algoritmo polinomiale per esso permetterebbe di risolvere in tempo polinomiale tutti i problemi di NP. È **NP completo** se è NP difficile e appartiene a NP.

I problemi NP completi sono i più difficili di NP: se si trovasse un algoritmo polinomiale per anche uno solo di essi, si avrebbe $P = NP$. Il primo problema NP completo, la soddisfacibilità di una formula booleana, fu dimostrato tale da Stephen Cook nel 1971 (e indipendentemente da Leonid Levin); nel 1972 Richard Karp mostrò che altri 21 problemi lo erano, tra cui la colorazione di grafi, il ciclo hamiltoniano, l'insieme indipendente (o la cricca), il vertex cover, il feedback vertex set. Nel corso incontreremo quasi solo problemi di questo tipo. «NP difficile» si dice anche di problemi che non stanno in NP, come la versione di ottimizzazione del commesso viaggiatore, e non va confuso con «richiede tempo esponenziale»: si tratta di una presunzione, non di una dimostrazione.

PROBLEMA SUI GRAFI	COMPLESSITÀ
Componenti connesse, cammini di costo minimo (pesi ≥ 0), albero di copertura minimo	in P
Esistenza di un circuito euleriano	in P (basta controllare i gradi)
Planarità	in P (algoritmi lineari)
Bipartito, ovvero 2 colorabile	in P (visita in ampiezza)
k colorabilità con $k \geq 3$	NP completo (anche per grafi planari con $k = 3$)
Esistenza di un ciclo hamiltoniano	NP completo
Commesso viaggiatore (versione di decisione)	NP completo
Insieme indipendente, cricca, vertex cover	NP completi

Feedback vertex set	NP completo
Isomorfismo di grafi	non si sa se in P o NP completo

Tabella 2. Alcuni problemi sui grafi e la loro complessità.

CORREZIONE

Nelle dispense la colorazione «nella sua versione decisionale» è detta NP difficile senza specificare k . La precisazione importante è che la 2 colorabilità si decide in tempo polinomiale (è la bipartizione), mentre per ogni $k \geq 3$ il problema è NP completo. Inoltre, in un'altra frase, si legge che trovando una soluzione polinomiale per *uno solo* dei problemi NP difficili la si avrebbe per tutti: questo è vero per i problemi NP completi (che stanno in NP); per problemi NP difficili fuori da NP si ottiene comunque $P = NP$, ma non vale il converso.

Colorazione: dall'algorithmo esaustivo all'algorithmo goloso

Dato un grafo G con n vertici, un algorithmo che trova sicuramente la colorazione ottimale esiste: per $k = 1, 2, \dots, n$ si controlla se G è k colorabile e ci si ferma alla prima risposta positiva. Per controllare se G è k colorabile si possono provare tutte le k^n assegnazioni di colori, oppure, equivalentemente, tutti gli $n!$ ordinamenti dei vertici (si veda l'algorithmo goloso qui sotto). Per $n = 100$ le permutazioni sono $100! \approx 9,33 \cdot 10^{157}$ (nelle dispense questo numero compare come «9157», che va letto $9 \cdot 10^{157}$). Con un calcolatore che ne esamina 10 miliardi al secondo servirebbero circa $9,33 \cdot 10^{147}$ secondi, cioè circa $3 \cdot 10^{140}$ anni.

Che fare, quindi? Se il grafo è piccolo si può provare; se è planare sappiamo che bastano 4 colori; in generale ci si accontenta di una colorazione non ottimale ottenuta con un algorithmo di approssimazione. Il più semplice è quello goloso già visto nel capitolo 25: si scorrono i vertici in un certo ordine e ciascuno prende il più piccolo colore non usato dai suoi vicini. L'algorithmo è «goloso» (o avaro, *greedy*) perché a ogni passo fa la scelta localmente migliore, cioè riusa un colore già adoperato, senza guardare al futuro.

```
def colora_ordine(archi, ordine):
    """Colorazione golosa secondo un ordine dei vertici (numero di colori)."""
    vicini = {v: set() for v in ordine}
    for u, v in archi:
        vicini[u].add(v)
        vicini[v].add(u)
    colore = {}
    for v in ordine:
        usati = {colore[u] for u in vicini[v] if u in colore}
        c = 0
        while c in usati:
            c += 1
        colore[v] = c
    return max(colore.values()) + 1
```

La qualità del risultato dipende però dall'**ordine** dei vertici. Il grafo «corona» si ottiene dal grafo bipartito completo $K_{n,n}$ con vertici $a_1, \dots, a_n$ e $b_1, \dots, b_n$ eliminando gli archi $a_i b_i$: è bipartito, quindi 2 colorabile. Se i vertici sono presi nell'ordine $a_1, b_1, a_2, b_2, \dots$ il metodo goloso usa **n colori**: a_1 e b_1 (non adiacenti) ricevono il colore 1, ma a_2 è adiacente a b_1 e ha il colore 2, b_2 è adiacente a a_1 e ha il colore 2, a_3 è adiacente a b_1 e b_2 e ha il colore 3, e così via. Con l'ordine $a_1, \dots, a_n, b_1, \dots, b_n$ si usano invece 2 colori.

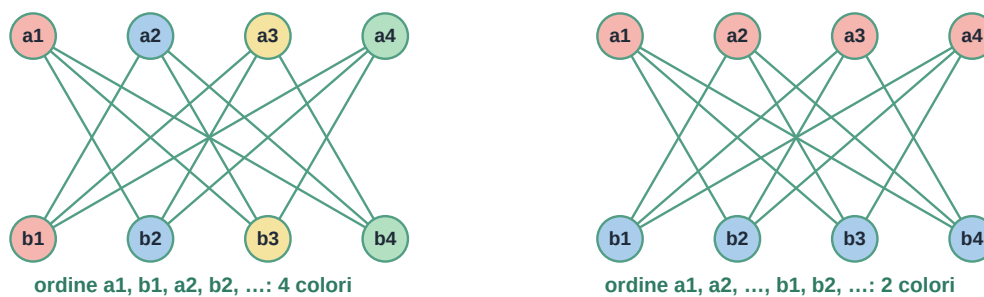


Figura 3. Il grafo corona con 8 vertici ($n = 4$) colorato con l'algoritmo goloso in due ordini diversi: 4 colori contro 2.

Questo mostra che la differenza tra l'ottimo e il risultato goloso può essere arbitrariamente grande. Ma lo stesso esempio dice qualcosa di più: **esiste sempre un ordine che dà una colorazione ottimale**. Dimostrazione: se G ha una colorazione ottimale con classi di colore $C_1, \dots, C_k$ ($k = \chi(G)$), si elencano prima i vertici di C_1 , poi quelli di C_2 , e così via. Un vertice di C_i ha, tra i vertici già colorati, soltanto vicini delle classi $C_1, \dots, C_{i-1}$ (nessun vicino nella propria classe), che per induzione hanno colori al più $i - 1$: quindi il colore i è libero e il vertice riceve un colore al più i . In totale, al più k colori. La difficoltà è che per trovare l'ordine giusto bisognerebbe già conoscere la colorazione ottimale, o provare tutti gli $n!$ ordini: **cercare una colorazione ottimale equivale a cercare una buona permutazione** dell'insieme dei vertici, ed è la stessa difficoltà che si incontra negli altri problemi di questa sezione.

Sul grafo corona con 16 vertici ($n = 8$) abbiamo anche provato 4000 ordini scelti a caso: l'algoritmo goloso ha usato in media 2,15 colori, mai meno di 2 e mai più di 5, e ha trovato i 2 colori ottimi nel 87,1% dei casi.

Rendere aciclico un digrafo: il feedback vertex set

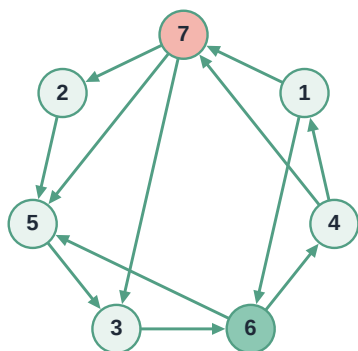
Dato un grafo (o digrafo) con dei cicli, si vogliono eliminare dei vertici per renderlo aciclico. Un insieme di vertici la cui eliminazione elimina tutti i cicli si chiama **feedback vertex set** (FVS). Tutti i vertici tranne uno formano sempre un FVS; l'interesse è per quelli di *cardinalità minima* (MFVS). Il problema ha applicazioni, per esempio, nell'eliminazione dei blocchi reciproci (*deadlock*) tra processi e nella verifica di circuiti elettronici.

Il metodo esaustivo prova tutti gli insiemi di vertici (2^n) o, equivalentemente, tutte le permutazioni: per ogni ordine si tolgono i vertici uno alla volta finché il grafo diventa aciclico. Ogni controllo di aciclicità è rapido (capitolo 23), ma i tentativi sono troppi. Il problema è NP difficile, quindi non possiamo sperare di fare di meglio nel caso peggiore, e si ripiega su un algoritmo goloso: si eliminano a turno i vertici con grado totale massimo, $\delta(v) = \delta^-(v) + \delta^+(v)$, ricalcolando i gradi. Un perfezionamento naturale è eliminare prima, senza contarli, i vertici con grado entrante 0 o grado uscente 0, che non stanno su alcun ciclo (è l'algoritmo di eliminazione del capitolo 23).

Il metodo goloso a volte trova l'ottimo, ma non sempre. Nel digrafo seguente (D con 7 vertici e 12 archi: $1 \rightarrow 6, 1 \rightarrow 7, 2 \rightarrow 5, 3 \rightarrow 6, 4 \rightarrow 1, 4 \rightarrow 7, 5 \rightarrow 3, 6 \rightarrow 4, 6 \rightarrow 5, 7 \rightarrow 2, 7 \rightarrow 3, 7 \rightarrow 5$) i gradi totali sono $\delta(1) = 3, \delta(2) = 2, \delta(3) = 3, \delta(4) = 3, \delta(5) = 4, \delta(6) = 4, \delta(7) = 5$: il vertice di grado massimo è 7, e il metodo lo elimina. Restano però dei cicli, per esempio $1 \rightarrow 6 \rightarrow 4 \rightarrow 1$, quindi bisogna eliminare ancora un vertice (il 6): in tutto **2 vertici**. Ma eliminando il **solo vertice 6** il digrafo diventa aciclico: l'ottimo è 1 (verificato per esaustione).

NOTA

Gli esempi delle dispense (figure delle pagine 165 e 166) non erano ricostruibili dal solo testo: nel secondo il metodo goloso toglie 3 vertici mentre «bastava eliminare 4 e 7». L'esempio di questo paragrafo è invece nostro, con gradi totali tutti distinti nel primo passo e verificato al calcolatore.



Digrafo con 7 vertici e 12 archi.

Gradi totali: 1:3, 2:2, 3:3, 4:3, 5:4, 6:4, 7:5.

Il metodo goloso toglie prima 7 (rosso), poi serve anche 6: 2 vertici.

Basta il solo vertice 6 (verde): il minimo è 1.

Figura 4. Un digrafo in cui il metodo goloso non trova il feedback vertex set minimo.

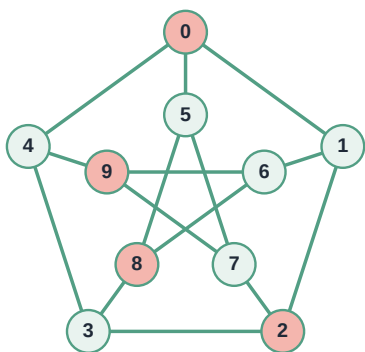
Insiemi indipendenti e vertex cover

Due altri problemi famosi e NP difficili. Un **insieme indipendente** di G è un insieme di vertici a due a due non adiacenti; si cerca quello di cardinalità *massima*, $\alpha(G)$. Un **vertex cover** (copertura dei vertici) è un insieme di vertici che contiene almeno un estremo di ogni arco; si cerca quello di cardinalità *minima*, $\beta(G)$. Sono due facce della stessa medaglia.

INDIPENDENTI E COPERTURE

Un insieme S di vertici è indipendente se e solo se il suo complementare $V - S$ è un vertex cover. Quindi $\alpha(G) + \beta(G) = n$.

Dimostrazione. S è indipendente se e solo se nessun arco ha entrambi gli estremi in S , cioè se e solo se ogni arco ha almeno un estremo fuori da S , cioè in $V - S$. Scegliendo S di cardinalità massima, $V - S$ ha cardinalità minima tra i vertex cover. ■



Grafo di Petersen.

In rosso un insieme indipendente massimo (4 vertici: nessun arco tra loro). Gli altri 6 formano un **vertex cover minimo**.

Figura 5. Nel grafo di Petersen (10 vertici) gli insiemi indipendenti massimi hanno 4 vertici e i vertex cover minimi ne hanno 6: $4 + 6 = 10$.

Nel grafo di Petersen, $\alpha = 4$ e $\beta = 6$ (verificato per esaurizione). Come per la colorazione, anche questi problemi si possono vedere come ricerca di una buona permutazione: l'insieme indipendente massimo si ottiene scorrendo i vertici nell'ordine giusto e prendendo ciascun vertice se non è adiacente a nessuno dei già scelti.

Per il vertex cover esiste un semplice algoritmo di approssimazione: si scorrono gli archi e, ogni volta che l'arco corrente non è ancora coperto, si prendono *entrambi* i suoi estremi.

```
def vertex_cover_2(archi):
    """Copertura dei vertici con al più il doppio dei vertici dell'ottimo."""
    copertura = set()
    for u, v in archi:
        if u not in copertura and v not in copertura:
            copertura.add(u)          # l'arco (u, v) e' scoperto: si prendono
            copertura.add(v)          # entrambi i suoi estremi
    return copertura
```

Il risultato è un vertex cover (ogni arco, quando viene esaminato, ha un estremo nell'insieme o ne riceve due), ed è **al più il doppio dell'ottimo**: gli archi per i quali si sono presi i due estremi non hanno vertici in comune (appena un arco viene scelto, entrambi i suoi estremi entrano nell'insieme e nessun arco successivo che li contenga viene scelto), quindi ogni copertura, per coprire m archi disgiunti, deve contenere almeno m vertici, mentre l'algoritmo ne usa $2m$. La garanzia è stata verificata su tutti i grafi con al più 7 vertici e su 300 grafi casuali.

Permutazioni casuali

Abbiamo visto che molti problemi si riconducono alla ricerca di una permutazione «buona» dei vertici. Un **algoritmo randomizzato** prova a risolverli generando permutazioni a caso e controllando il risultato, fermandosi quando ne trova una soddisfacente. Due problemi si pongono: come generare una permutazione a caso in modo che *tutte* abbiano la stessa probabilità $1/n!$, e come generare tutte le permutazioni, che esistono algoritmi specifici per fare e che per n grande non ha comunque senso (sono troppe). Ci occupiamo solo del primo.

Il procedimento è il **mescolamento di Fisher e Yates** (reso popolare da Knuth): dato l'array $A = [0, 1, \dots, n-1]$, per $i = 0, \dots, n-1$ si sceglie a caso un intero k tra i e $n-1$ compresi e si scambiano $A[i]$ e $A[k]$.

```
import random

def mescola(A):
    """Mescolamento di Fisher e Yates: ogni permutazione ha probabilita 1/n!."""
    n = len(A)
    for i in range(n):
        k = random.randrange(i, n)      # un intero casuale tra i e n meno 1 compresi
        A[i], A[k] = A[k], A[i]
    return A

def mescola_sbagliato(A):
    """Versione sbagliata: k puo essere qualunque posizione."""
    n = len(A)
    for i in range(n):
        k = random.randrange(0, n)
        A[i], A[k] = A[k], A[i]
    return A
```

IL MESCOLAMENTO DI FISHER E YATES È EQUIPROBABILE

Ogni permutazione di n elementi è prodotta con probabilità $1/n!$.

Dimostrazione. Per induzione su n . Per $n = 1$ c'è una sola permutazione. Al passo $i = 0$ ciascuno degli n elementi ha probabilità $1/n$ di finire in posizione 0. Fissato l'elemento x in posizione 0, il resto dell'algoritmo è esattamente lo stesso algoritmo applicato agli altri $n-1$ elementi, e per ipotesi induttiva produce ciascuna delle $(n-1)!$ disposizioni con probabilità $1/(n-1)!$. Quindi una qualsiasi permutazione data ha probabilità $(1/n) \cdot (1/(n-1)!) = 1/n!$. ■

Un altro modo per vederlo: l'algoritmo compie n scelte indipendenti con $n, n-1, \dots, 1$ valori possibili, in tutto $n \cdot (n-1) \cdot \dots \cdot 1 = n!$ sequenze di scelte, tutte con la stessa probabilità, e sequenze di scelte diverse producono

permutazioni diverse; poiché le permutazioni sono proprio $n!$, ciascuna è prodotta da una sola sequenza (per $n \leq 6$ l'abbiamo controllato elencando tutte le sequenze).

CORREZIONE AL RAGIONAMENTO DELLE DISPENSE

Le dispense calcolano la probabilità che il valore j si trovi nella posizione i come prodotto $(n-1)/n \cdot (n-2)/(n-1) \cdot \dots = 1/n$ (il prodotto si semplifica a telescopio, e il calcolo è giusto), e da questo concludono che «tutte le permutazioni sono equiprobabili». L'implicazione però **non è valida**: avere probabilità $1/n$ per ogni coppia (valore, posizione) è necessario, ma non sufficiente. Per esempio, le n rotazioni cicliche dell'array $[0, 1, \dots, n-1]$, scelte con uguale probabilità, danno a ogni valore probabilità $1/n$ in ogni posizione, ma producono solo n delle $n!$ permutazioni. La dimostrazione corretta è quella per induzione data sopra.

Basta una piccola modifica per rovinare tutto. Se nel secondo codice k è scelto fra *tutte* le posizioni da 0 a $n-1$, le sequenze di scelte sono n^n : per $n=3$ sono 27, e 27 non è divisibile per le 6 permutazioni, quindi non possono essere equiprobabili. Elencando le 27 sequenze si trova che tre permutazioni escono 4 volte e le altre tre 5 volte; per $n=4$ le 256 sequenze producono le 24 permutazioni con frequenze tra 8 e 15 volte.

PERMUTAZIONE DELL'ARRAY [0, 1, 2]	NUMERO DI SEQUENZE (SU 27)
[0, 1, 2]	4
[0, 2, 1]	5
[1, 0, 2]	5
[1, 2, 0]	5
[2, 0, 1]	4
[2, 1, 0]	4

Tabella 3. Il mescolamento sbagliato per $n=3$: le permutazioni non sono equiprobabili (con Fisher e Yates sarebbero 1 su 6 ciascuna).