

Giulia Maria Piacentini Cattaneo

# Matematica discreta

e applicazioni

#### L'autore

Giulia Maria Piacentini Cattaneo è professore ordinario di Algebra all'Università di Roma "Tor Vergata".

#### L'opera

La matematica discreta, o dei numeri interi, è la base su cui poggia l'intera tecnologia moderna, dai calcolatori ai sistemi di controllo e di comunicazione.

Comprendere concetti quali induzione e ricorsività, padroneggiare il calcolo combinatorio, le algebre booleane e le tecniche di costruzione dei grafi significa poter affrontare problemi complessi di natura tecnica e applicativa che vanno dall'informatica alla chimica, dalla biologia alla fisica, dalla ricerca operativa alla sociologia.

Il testo è corredata di oltre 400 esercizi, le soluzioni della maggior parte dei quali compaiono al termine del libro.

Ogni capitolo si chiude con alcuni esercizi di programmazione da implementare.

In appendice sono raccolti dei problemi che hanno lo scopo di rinfrescare alcune nozioni apprese nella scuola secondaria.

PIACENTINI-CATTANEO/MATEM DISCRETA

ISBN 978-88-08-08813-2



9 788808 088132  
9 01234567 (60B)

Al pubblico € 35,00\*\*\*

Piacentini Cattaneo

# Matematica discreta

UNIVERSITÀ DI BARI
07/11
1149
A05
DIPARTIMENTO DI

Giulia Maria Piacentini Cattaneo

# Matematica discreta

e applicazioni

ZANICHELLI

#### *Analisi e matematica generale*

Antognini, Barozzi **Matematica e Mathematica**

Barozzi **Primo corso di analisi matematica**

Barozzi, Matarasso **Analisi matematica (volume 1º) N.R.**

Boieri, Chiti **Percorso di matematica**

Bramanti, Pagani, Salsa, **Matematica (2ª edizione)**

Bramanti, Pagani, Salsa **Analisi matematica 1**

Casolari **Integrali** (Masson)

Davis **Il mondo dei grandi numeri**

De Marco **Analisi zero (3ª edizione)**

De Marco **Analisi Uno (2ª edizione - Decibel)**

De Marco **Analisi Due (2ª edizione - Decibel)**

De Marco, Mariconda **Esercizi di analisi due (Decibel)**

De Marco, Mariconda **Esercizi di calcolo in una variabile (Decibel)**

De Marco, Mariconda **Esercizi di calcolo in più variabili (Decibel)**

De Marco **Matematica Uno (Decibel)**

Ghizzetti, Rosati **Analisi matematica (Masson - 2ª edizione)**

Maffei **Migliori Esercizi, appunti e note di Istituzioni matematiche**

Pagani, Salsa **Analisi matematica (Masson - 2 volumi)**

Pagani, Salsa **Matematica (Masson)**

Pagani, Salsa **Serie di funzioni ed equazioni differenziali**

Piacentini Cattaneo **Matematica discreta**

Ritelli, Bergamini, Trifone **Fondamenti di matematica**

Salsa, Squellati **Esercizi di matematica (2 volumi)**

Salsa, Squellati **Esercizi di analisi matematica II (Masson - 3 volumi)**

Thomas Jr., Finney **Elementi di analisi matematica e geometria**

Torrigiani **Ripensare matematica. In preparazione alle facoltà universitarie scientifiche**

#### *Algebra e Geometria*

Abeasis **Complementi di algebra lineare e geometria**

Abeasis **Elementi di algebra lineare e geometria**

Abeasis **Geometria analitica del piano e dello spazio**

Brogli, Fortuna, Luminati **Problemi risolti di algebra lineare (Decibel)**

#### *Geometria, Geometria Calcolata (2 volumi)*

Dedò **Trasformazioni geometriche**

Dedò **Forme**

Enriques **Lezioni di geometria proiettiva (Ristampa anastatica)**

Questioni riguardanti le matematiche elementari 2 voll. a cura di Enriques

Facchini **Algebra** (Decibel)

Jänich **Topologia**

Kosniowski **Introduzione alla topologia algebrica**

Maroscia **Geometria e algebra lineare**

Maroscia **Introduzione alla geometria e all'algebra lineare**

Piacentini Cattaneo **Algebra** (Decibel)

Procesi Ciampi, Rota **Esercizi di geometria e algebra**

Ragusa, Sparacino **Esercizi di algebra. Teoria degli insiemi, teoria dei gruppi, teoria degli anelli**

Salce **Lezioni sulle matrici** (Decibel)

Serafini **Ottimizzazione**

Steinhaus **Matematica per istantanee**

Vaccaro, Carfagna, Piccolella **Lezioni di geometria e algebra lineare** (Masson)

Ventre **Introduzione ai grafi planari**

#### *Analisi numerica e Fisica matematica*

Bagarello **Fisica matematica**

Barozzi **Matematica per l'ingegneria dell'informazione (ristampa aggiornata)**

Bevilacqua, Bini, Capovani, Menchi **Introduzione alla matematica computazionale**

Bevilacqua, Bini, Capovani, Menchi **Metodi numerici**

Bini, Capovani, Menchi **Metodi numerici per l'algebra lineare**

Bordoni **Lezioni di meccanica razionale** (Masson)

Cercignani **Spazio, tempo, movimento. Introduzione alla meccanica razionale**

Codegone **Metodi matematici per l'ingegneria**

Fabrizio **Elementi di meccanica classica**

Finzi **Meccanica razionale (2 volumi)**

Levi-Civita **Caratteristiche dei sistemi differenziali e propagazione ondosa**

Levi-Civita, Amaldi **Compendio di meccanica razionale - volume 1**

Levi-Civita, Amaldi **Lezioni di meccanica razionale (volume 2 parte 2)**

Vivarelli **Appunti di meccanica razionale (2ª edizione ampliata)**



Giulia Maria Piacentini Cattaneo

# **Matematica discreta**

## **e applicazioni**

**ZANICHELLI**

I diritti di elaborazione in qualsiasi forma o opera, di memorizzazione anche digitale su supporti di qualsiasi tipo (inclusi magnetici e ottici), di riproduzione e di adattamento totale o parziale con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche), i diritti di noleggio, di prestito e di traduzione sono riservati per tutti i paesi.  
L'acquisto della presente copia dell'opera non implica il trasferimento dei suddetti diritti né li esaurisce.

Le fotocopie per uso personale (cioè privato e individuale) possono essere effettuate, nei limiti del 15% di ciascun volume, dietro pagamento alla S.I.A.B. del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941 n. 633.  
Tali fotocopie possono essere effettuate negli esercizi commerciali convenzionati S.I.A.E. o con altre modalità indicate da S.I.A.E.

Per le riproduzioni ad uso non personale (ad esempio: professionale, economico o commerciale) l'editore potrà concedere a pagamento l'autorizzazione a riprodurre un numero di pagine non superiore al 15% delle pagine del presente volume.  
Le richieste per tale tipo di riproduzione vanno inviate a:

Associazione Italiana per i Diritti di Riproduzione  
delle Opere dell'Ingegno (ADIRO)  
Corso di Porta Romana, 108  
20122 Milano  
e-mail: segreteria@aidro.org e sito web www.aidro.org

L'editore, per quanto di propria spettanza, considera rare le opere fuori del proprio catalogo editoriale.  
La riproduzione degli esemplari esistenti nelle biblioteche di tali opere è consentita, non essendo concorrentiale  
all'opera. Non possono considerarsi rare le opere di cui esiste, nel catalogo dell'editore, una successiva edizione,  
le opere presenti in cataloghi di altri editori o le opere antologiche.

Maggiori informazioni sul nostro sito: [www.zanichelli.it/f\\_info\\_fotocopie.html](http://www.zanichelli.it/f_info_fotocopie.html)

Impaginazione: Compomat, Configui

Copertina:

- Progetto grafico: Miguel Sal & C., Bologna

- Immagine di copertina: © Harrison Eastwood/Getty Images

Prima edizione: ottobre 2008

Ristampa

5 4 3 2 1      2013    2012    2011    2010    2009

Realizzare un libro è un'operazione complessa, che richiede numerosi controlli:  
sul testo, sulle immagini e sulle relazioni che si stabiliscono tra essi.

L'esperienza suggerisce che è praticamente impossibile pubblicare un libro  
privo di errori. Saremo quindi grati ai lettori che vorranno segnalarceli.

Per segnalazioni o suggerimenti relativi a questo libro l'indirizzo a cui rivolgersi è:

Zanichelli editore S.p.A.

Via Irnerio 34

40126 Bologna

fax 051293322

e-mail: [linea\\_universitaria@zanichelli.it](mailto:linea_universitaria@zanichelli.it)

sito web: [www.zanichelli.it](http://www.zanichelli.it)

Prima di effettuare una segnalazione è possibile verificare se questa sia già stata inviata in precedenza,  
identificando il libro interessato all'interno del nostro catalogo on line ([www.zanichelli.it/f\\_catalog.html](http://www.zanichelli.it/f_catalog.html))  
e selezionando il link ERRATA CORRIGE, dove sono disponibili le eventuali correzioni in formato PDF.

Per comunicazioni di tipo commerciale: [universita@zanichelli.it](mailto:universita@zanichelli.it)

Stampa: Tipografia Babina  
Via Aldo Moro 18, 40068 San Lazzaro di Savena (BO)  
per conto di Zanichelli editore S.p.A.  
Via Irnerio 34, 40126 Bologna



# Indice

## Introduzione

## Indice dei simboli

### 1 Il linguaggio base della matematica

1	Prime nozioni sugli insiemi	1
2	Stringhe bit e sottoinsiemi	8
3	Elementi di logica	9
4	Relazioni	16
5	Funzioni	19
6	Relazioni d'ordine	25
7	Relazioni di equivalenza	28
8	Relazioni di equivalenza e funzioni	34

### 2 Induzione e ricorsività

1	Successioni e stringhe	37
2	Sommatorie	37
2.1	Proprietà della sommatoria	42
2.2	Doppie sommatorie	44
3	I numeri naturali e il principio di induzione matematica	46
4	Ricorsività	52
4.1	I numeri di Fibonacci	58

### 3 Numeri interi e algoritmi

1	Prime proprietà dei numeri interi	65
2	Divisibilità, irriducibili e primi in $\mathbb{Z}$	67
3	La divisione in $\mathbb{Z}$ e l'algoritmo euclideo	69
3.1	L'algoritmo euclideo.	71
4	Rappresentazione degli interi	74
5	Identità di Bézout ed equazioni diofantee	76
6	Il Teorema Fondamentale dell'Aritmetica	81
6.1	Il crivello di Eratostene	83
7	Conseguenze del Teorema Fondamentale dell'Aritmetica	84
7.1	I numeri primi sono infiniti	84
7.2	Irrazionalità di ogni numero della forma $\sqrt[p]{p}$ , $p$ primo.	85
8	Alcune divagazioni sui numeri primi	85

vi

xi

1

1

8

9

16

19

25

28

34

37

37

38

42

44

46

52

58

37

37

38

42

44

46

52

58

65

67

69

71

74

76

81

83

84

84

85

85

<b>4 Calcolo combinatorio</b>	<b>89</b>	<b>9 L'algebra booleana</b>	<b>214</b>
1 Quanti sono?	89	1 Variabili booleane e funzioni booleane	214
2 Calcolo combinatorio	94	2 La forma normale disgiuntiva di una funzione booleana	219
2.1 <i>Permutazioni.</i>	96	3 Forme minimali di un'espressione booleana: il metodo di Karnaugh	223
2.2 <i>Disposizioni e combinazioni semplici</i>	99	4 Porte logiche e circuiti	226
2.3 <i>Disposizioni e combinazioni con ripetizione</i>	102	5 Reticoli	228
3 Il principio di inclusione-esclusione	109	6 Le algebre di Boole	233
<b>5 Dalle congruenze alla crittografia</b>	<b>113</b>	<b>10 Grafi</b>	<b>240</b>
1 Congruenze e loro proprietà	113	1 Motivazioni e prime definizioni	240
2 Il Piccolo Teorema di Fermat e conseguenze	118	2 Grafi euleriani	245
3 Altre applicazioni	119	3 Matrici di adiacenza	250
3.1 <i>Criteri di divisibilità</i>	119	4 Isomorfismi e automorfismi di grafi	254
3.2 <i>La prova del nove</i>	121	5 Alcune classi di grafi	256
4 Risoluzione di congruenze lineari	121	5.1 <i>Grafi bipartiti</i>	256
5 Il Teorema Cinese dei Resti	124	5.2 <i>Alberi e foreste</i>	257
6 La funzione di Eulero	131	5.3 <i>Grafi planari</i>	258
7 Congruenze e test di primalità	135	6 Applicazioni dei grafi	261
8 Fattorizzazione di interi	136	<b>11 Approfondimenti</b>	<b>266</b>
9 Calcolo di potenze modulo $n$	139	1 Le operazioni in $\mathbb{N}$	266
<b>10 Crittografia</b>	<b>140</b>	2 I numeri interi come classi di equivalenza	267
10.1 <i>Il sistema RSA</i>	142	3 I numeri razionali	270
11 L'autenticazione delle firme	146	4 Generalità sugli anelli e alcune classi di anelli	273
<b>6 Polinomi e algoritmi</b>	<b>149</b>	5 Funzioni generatrici	274
1 Prime definizioni relative ai polinomi	149	6 Approfondimenti sui numeri primi	277
2 Interi e polinomi a confronto	154	<b>A Esercizi di elementi di matematica</b>	<b>279</b>
3 Polinomi irriducibili su $\mathbb{C}$ e su $\mathbb{R}$ e loro caratterizzazione	160	<b>Bibliografia</b>	<b>285</b>
4 Riducibilità e irriducibilità di polinomi su $\mathbb{Q}$	162	<b>Soluzioni degli esercizi</b>	<b>286</b>
5 Metodi per studiare la irriducibilità di un polinomio su $\mathbb{Q}$	167	<b>Indice analitico</b>	<b>331</b>
6 Algoritmi a confronto	169		
7 Crescita di funzioni e loro confronto	170		
8 L'ordine di grandezza di una funzione: la notazione $\mathcal{O}$	172		
9 Tipi di complessità	173		
<b>7 Campi finiti</b>	<b>176</b>		
1 Dalla congruenza tra interi alla congruenza tra polinomi	176		
2 Campi finiti	180		
<b>8 Strutture algebriche</b>	<b>185</b>		
1 Gruppoidi, semigruppi, monoidi	185		
2 I gruppi	188		
3 Il gruppo simmetrico $S_n$	197		
4 Altri esempi di gruppi: i gruppi diedrali	206		
5 Anelli	208		

# Introduzione

La domanda di rito quando si scrive un nuovo libro è: perché scriverlo? Dato che il libro in questione è un libro di matematica discreta, la domanda è collegata alla seguente: a cosa serve la matematica discreta? Innanzitutto, che cosa è la matematica discreta? È la matematica del non continuo, in pratica è la matematica basata esclusivamente sull'aritmetica, quindi sui numeri interi. Beh, allora è proprio banale, non c'è bisogno di un libro per studiare l'aritmetica, obietterà qualcuno; in fondo sappiamo tante cose sugli interi, li abbiamo studiati fin dalle scuole elementari. Rispondiamo con la seguente osservazione: la matematica discreta è la base su cui si fonda l'intera tecnologia moderna, dai calcolatori (software e hardware) ai sistemi di controllo e di comunicazione, ecc. Infatti il linguaggio della matematica discreta è il linguaggio dei calcolatori. Si comincia a capire che forse le nozioni che dovranno essere affrontate potrebbero non essere così banali come si pensava. Questo è lo spirito con cui è stato scritto questo libro: *fornire strumenti* che permettano di affrontare importanti problemi attuali: a questo scopo verranno introdotti svariati algoritmi sugli interi e sui polinomi, verranno studiati i campi finiti, verranno date nozioni di combinatoria e sui grafi. In realtà il libro ha anche un obiettivo più ambizioso: fornire allo studente un *modo nuovo di ragionare*, metterlo in condizione di capire qual è la vera essenza di un problema e creare modelli che servano a risolvere non solo quel problema particolare, ma una intera categoria di problemi. Per fare ciò occorre impossessarsi non tanto di nuove nozioni, quanto di una nuova mentalità, che è offerta per l'appunto dalla matematica in generale (non solo dalla matematica del discreto). Con questo obiettivo in mente si sono introdotti anche argomenti che forse vanno al di là di un corso tradizionale di matematica discreta, alcuni dei quali sono inclusi in un capitolo dedicato agli approfondimenti per lo studente più interessato.

Il fatto, come si è detto, che la matematica discreta è la base su cui si fonda gran parte della tecnologia moderna e che fornisce un nuovo modo di affrontare i problemi sembra quindi un motivo sufficiente per giustificare lo studio. A qualcuno questa giustificazione potrebbe non bastare. Basti allora aggiungere che in realtà ci sono motivi più profondi che spingono allo studio di questi argomenti: la matematica discreta, ebbene sì, la matematica cioè che si basa quasi esclusivamente sui numeri interi, costituisce la base per affrontare problemi profondi sia di natura teorica sia di natura applicativa. In questo testo accenneremo solo ad alcuni di tali problemi, come per esempio il sistema crittografico RSA largamente utilizzato, che è basato su (semplici) problemi relativi ai numeri interi e molte altre applicazioni in svariati campi.

Questo libro è frutto di diversi anni di insegnamento del corso di Matematica Discreta presso il Corso di Laurea in Informatica dell'Università di Roma Tor Vergata.

Ritengo che un libro non possa nascere che dopo averne sperimentato i contenuti in classe, di fronte agli studenti, e aver capito quali sono le difficoltà da loro incontrate. A seconda di come viene presentato il materiale lo studente può incontrare maggiore o minore difficoltà: l'averlo sperimentato in classe fornisce quindi la (quasi) garanzia di presentarlo nel modo giusto. Desidero quindi ringraziare gli studenti che mi hanno aiutato in questo difficile compito nel corso degli anni.

Il materiale è distribuito in 11 capitoli più un'appendice.

Nel primo capitolo si introduce il linguaggio base della matematica, con i concetti base, quali gli insiemi e la loro rappresentazione come stringhe bit, alcune nozioni di logica, le funzioni, le relazioni, le relazioni d'ordine, le relazioni di equivalenza.

Nel secondo capitolo, dedicato alla induzione e alla ricorsività, vengono presentate le proprietà fondamentali delle sommatorie, vengono introdotti gli assiomi di Peano, che definiscono i numeri naturali, assiomi sui quali si basa il tipo di dimostrazione per induzione matematica. Il capitolo prosegue con il concetto di definizione ricorsiva che è di fondamentale importanza per l'informatica e la matematica.

Il capitolo 3 riguarda interamente gli interi e gli algoritmi sugli interi. Come si è detto, tutta la matematica discreta è basata su tali strutture, per cui è importante capirne bene tutti i concetti, che tra l'altro verranno ripresi quando nel sesto capitolo si studieranno i polinomi a coefficienti in un campo. Il capitolo si conclude con alcune divagazioni sui numeri primi, che sono i pilastri su cui si fonda l'edificio dei numeri interi, come è espresso dal teorema fondamentale dell'aritmetica.

Nel capitolo 4 si affronta il problema di contare gli elementi di vari insiemi, finiti e infiniti. Gran parte del capitolo è dedicato al calcolo combinatorio e ai relativi concetti di permutazioni, combinazioni e disposizioni, con e senza ripetizioni.

Nel capitolo 5 si parte dagli interi e, definendo una opportuna relazione di equivalenza (la congruenza modulo  $n$ ), si passa dall'insieme infinito degli interi all'insieme finito delle classi resto modulo  $n$ . Vengono presentate diverse applicazioni delle congruenze: queste risulteranno poi fondamentali nella crittografia a chiave pubblica, su cui ci si sofferma nell'ultima parte del capitolo.

Nel capitolo 6, dedicato ai polinomi, si mostra il parallelismo tra gli interi e i polinomi a coefficienti in un campo e si affronta il cruciale problema della riducibilità e irriducibilità dei polinomi su un campo, in particolare quando il campo è complesso, reale o razionale. Si accenna poi al problema della complessità degli algoritmi, confrontando fra loro alcune funzioni fondamentali e introducendo la cosiddetta notazione  $\mathcal{O}$  che permette di fornire l'ordine di grandezza di una data funzione.

Il capitolo 7, conseguenza naturale del capitolo precedente sui polinomi, affronta il problema della costruzione di campi finiti. Queste strutture si rivelano fondamentali in informatica.

Nel corso dei precedenti capitoli si è avuto modo di conoscere varie strutture algebriche, quali gli anelli e i gruppi, soprattutto sotto forma di esempi. Non si è però avuta una visione generale e sistematica. È quanto si conta di fare nel capitolo 8 dove si fornisce una panoramica generale delle principali strutture algebriche, e si raccolgono i principali risultati. Si parte dalle strutture con una sola operazione, quali i gruppoidi, i semigruppi, i monoidi, fino ad arrivare alla struttura algebrica per eccellenza, il gruppo. Vengono forniti i principali esempi di gruppi non abeliani, i gruppi simmetrici e i gruppi diedrali. Si passa poi agli anelli e alle loro principali proprietà.

L'argomento del capitolo 9 riguarda le algebre booleane, delle quali ci interesseranno soprattutto le ricadute applicative. Un circuito elettrico o una proposizione sembrano a priori essere concetti completamente slegati: se però si osserva che un circuito può essere acceso o spento, una proposizione può essere vera o falsa, allora si capisce che tali concetti hanno in comune il fatto di essere *sistemi a due stati*. Le algebre di Boole colgono i tratti comuni e gli aspetti essenziali dei circuiti e delle proposizioni, generalizzandoli.

Il capitolo 10 è dedicato ai grafî: scopo dei grafi è di modellare in maniera schematica una vasta quantità di problemi che vanno dall'informatica e la matematica ai campi più svariati come la chimica, la biologia, la fisica, la ricerca operativa, la sociologia, ecc. L'ultimo paragrafo è dedicato appunto alla presentazione di alcune di queste applicazioni.

Il capitolo 11 è riservato agli studenti più curiosi e interessati, che non si accontentano della presentazione non del tutto precisa che è stata fatta di alcuni argomenti: per motivi didattici nei capitoli precedenti infatti si è preferito, per non appesantire il discorso, tralasciare alcune definizioni assiomatiche, come per esempio gli interi e i razionali, che vengono invece presentate in questo capitolo. Vengono poi studiate alcune classi di anelli che non verificano le proprietà *ovvie* che riteniamo dover sempre essere verificate (quali per esempio la fattorizzazione unica di un intero in numeri primi oppure la possibilità di fare sempre la divisione con resto come avviene per gli interi). Si parla poi di funzioni generatrici e si conclude con alcuni approfondimenti sui numeri primi.

Segue un'appendice in cui sono raccolti alcuni esercizi assegnati durante il corso di Elementi di Matematica per la laurea in Informatica, corso propedeutico ad ogni corso di matematica. Scopo dell'appendice è infatti quello di rinfrescare alcune nozioni che tutti dovrebbero già conoscere dalle scuole superiori, senza pretendere però di esaurire tutte le nozioni di base che uno studente dovrebbe conoscere.

Alcuni dei capitoli sono indipendenti dagli altri, mentre altri sono collegati tra loro. Per esempio i capitoli 1-3 e 5-7 sono tutti collegati, mentre gli altri possono essere studiati indipendentemente senza problema di comprensione. Il nucleo di un corso di Matematica Discreta potrebbe, secondo la mia esperienza, essere costituito dai primi sette capitoli: dopo di che, a seconda delle diverse esigenze, si può scegliere di affrontare uno o più degli altri capitoli.

La maggior parte delle definizioni e dei teoremi è seguita da esempi illustrativi, con lo scopo di chiarire i concetti e motivarne l'introduzione.

Il testo è corredata di innumerevoli esercizi (più di quattrocento), per la maggior parte risolti. Le soluzioni appaiono al termine del libro, proprio per evitare che lo studente guardi la soluzione *prima* di cercare di risolvere da solo l'esercizio: un tale atteggiamento sarebbe assolutamente inutile per la comprensione delle nozioni studiate. Teoria ed esercizi devono andare di pari passo: dopo avere studiato un argomento è indispensabile risolvere degli esercizi sui concetti studiati, e, d'altra parte, a loro volta, gli esercizi stessi aiutano a chiarire la teoria. Molti degli esercizi sono stati assegnati come compito d'esame al corso di Matematica Discreta presso il corso di laurea in Informatica dell'Università di Roma Tor Vergata. Ringrazio pubblicamente il dottor Paolo Lipparini che mi ha affiancato nell'insegnamento del corso in questi anni e che è stato il creatore di moltissimi di questi esercizi.

Ogni capitolo infine si chiude con una serie di proposte di esercizi di programmazione, che lo studente è invitato ad implementare. In tal modo è costretto a rendersi conto di tutti i passi presenti nel procedimento e della necessità di imporre certe condizioni.

Roma, 6 agosto 2008

Giulia Maria Piacentini Cattaneo

# Indice dei simboli

Di seguito si trova un elenco dei principali simboli utilizzati nel testo. Nella prima colonna il simbolo, nella seconda il suo significato e nella terza il numero della pagina dove esso compare la prima volta.

$\mathbb{N}$	insieme dei numeri naturali	2
$\mathbb{Z}$	insieme dei numeri interi	2
$\mathbb{Q}$	insieme dei numeri razionali	2
$\mathbb{R}$	insieme dei numeri reali	2
$\mathbb{C}$	insieme dei numeri complessi	2
$a \in A$	$a$ è un elemento di $A$	2
$a \notin A$	$a$ non è un elemento di $A$	2
$ $	tale che	2
$\emptyset$	insieme vuoto	2
$B \subseteq A$	$B$ è un sottoinsieme di $A$	2
$B \subset A$	$B$ è un sottoinsieme proprio di $A$	2
$B \varsubsetneq A$	$B$ è un sottoinsieme proprio di $A$	2
$B \not\subseteq A$	$B$ non è un sottoinsieme di $A$	2
$A \cap B$	intersezione di $A$ con $B$	4
$A \cup B$	unione di $A$ con $B$	4
$\bigcap_{\alpha \in I} A_\alpha$	intersezione degli $A_\alpha$	5
$\bigcup_{\alpha \in I} A_\alpha$	unione degli $A_\alpha$	5
$U$	insieme universale	5
$\complement A$	complementare di $A$	5
$B \setminus A$	complemento relativo di $A$ in $B$ o insieme differenza	5
$A \times B$	prodotto cartesiano di $A$ e $B$	6
$A_1 \times A_2 \times \dots \times A_n$	prodotto cartesiano di $n$ insiemi $A_i$	6
$\mathcal{P}(A)$	insieme delle parti (o sottoinsiemi) di $A$	6
$\neg p$	negazione della proposizione $p$	9
$\exists$	esiste (quantificatore esistenziale)	10
$\forall$	per ogni (quantificatore universale)	10
$\wedge$	operatore di congiunzione	11
$\vee$	operatore di disgiunzione	11
$p \implies q$	$p$ implica $q$	12
$T$	vero	14
$F$	falso	14
$a \rho b$	$a$ è in relazione con $b$	17
$\rho^{-1}$	relazione inversa della $\rho$	18

$f : A \rightarrow B$	funzione $f$ da $A$ a $B$	19
$[x]$	il più grande intero minore o uguale a $x$	19
$\lceil x \rceil$	il più piccolo intero maggiore o uguale a $x$	20
$f(S)$	immagine dell'insieme $S$ mediante la funzione $f$	21
$\text{Im } f$	immagine della funzione $f$	21
$f^{-1}(T)$	immagine inversa o controimmagine di $T$ mediante la $f$	21
$g \circ f$	funzione composta di $f$ con $g$	22
$f^{-1}$	applicazione inversa della $f$	23
$i_X$	applicazione identica di $X$	23
$\chi_A$	funzione caratteristica di $A$	23
$\preccurlyeq$	relazione d'ordine parziale	26
$(X, \preccurlyeq)$	insieme parzialmente ordinato	26
$[a]$ o $\bar{a}$	classe di equivalenza dell'elemento $a$	28
$A/\varrho$	insieme quoziante rispetto alla relazione di equivalenza $\varrho$	29
$\rho_f$	relazione di equivalenza associata alla funzione $f$	34
$\pi : A \rightarrow A/\varrho$	proiezione canonica sul quoziante	34
$\{a_n\}_{n \in \mathbb{N}}$	successione con termine $n$ -esimo $a_n$	37
$\sum$	successione con termine $n$ -esimo $a_n$	37
$\sum_n a_i$	simbolo di sommatoria (o notazione sigma)	39
$\sum_{i=1}^n a_i$	somma dei termini $a_1, a_2, \dots, a_n$	39
$\mathbb{N}_3$	principio di induzione matematica	47
$M$	principio del minimo o del buon ordinamento	51
$I$	altra forma equivalente del principio di induzione matematica	51
$f_n$	$n$ -esimo numero di Fibonacci	58
$\Phi$	rapporto aureo o proporzione divina	59
$\widehat{\Phi}$	$-\frac{1}{\Phi}$	59
$A(n, m)$	funzione di Ackermann	63
$a b$	$a$ divide $b$	67
$a \nmid b$	$a$ non divide $b$	67
$ a $	valore assoluto di $a$	69
$\text{MCD}(a, b)$ o $(a, b)$	massimo comun divisore di $a$ e $b$	70
$\text{mcm}(a, b)$ o $[a, b]$	minimo comune multiplo di $a$ e $b$	71
$D(a, b)$	numero di divisioni per trovare $\text{MCD}(a, b)$ con algoritmo euclideo	72
$\pi(x)$	numero dei primi minori di $x$	85
$F_n$	$n$ -esimo numero di Fermat	86
$M_k$	$k$ -esimo numero di Mersenne	87
$A \sim B$	$A$ ha la stessa cardinalità di $B$	89
$\text{Card}(A)$	cardinalità o potenza dell'insieme $A$	90
$I_n$	insieme formato dai primi $n$ numeri naturali	90
$ S $	cardinalità dell'insieme finito $S$	90
$\aleph_0$	potenza del numerabile	91
$n!$	$n$ fattoriale	97
$D(n, k)$	numero delle disposizioni semplici di $n$ oggetti di classe $k$	99
$\binom{n}{k}$	numero delle combinazioni semplici di $n$ oggetti di classe $k$	100
$a \equiv b \pmod{n}$	$a$ congruente a $b$ modulo $n$	113

$a \equiv b \pmod{n}$	$a$ congruente a $b$ modulo $n$	113
$\mathbb{Z}_n$	insieme delle classi resto modulo $n$	114
$\varphi(n)$	funzione di Eulero di $n$	132
$U(\mathbb{Z}_n)$	insieme delle classi invertibili di $\mathbb{Z}_n$	133
$(\mathbb{K}[x], +, \cdot)$	anello dei polinomi su $\mathbb{K}$ nell'indeterminata $x$	151
$\deg(f) \circ \partial(f(x))$	grado del polinomio $f(x)$	152
$\Delta$	discriminante di un'equazione di secondo grado	161
$\mathcal{O}$	notazione big-o	172
$\mathcal{O}(n)$	complessità lineare	174
$NP$	classe di problemi	174
$(n)$	ideale generato da $n$	177
$(f(x))$	ideale generato da $f(x)$	177
$(S, *)$	insieme dotato di una operazione	187
$M_{mn}(R)$	matrici su $R$ a $m$ righe e $n$ colonne	189
$M_n(R)$	matrici quadrate di dimensione $n$ su $R$	189
$GL_2(\mathbb{R})$	matrici $2 \times 2$ su $\mathbb{R}$ dotate di inversa	190
$SL_2(\mathbb{R})$	matrici $2 \times 2$ su $\mathbb{R}$ con determinante uguale a 1	190
$H \leq G$	$H$ sottogruppo di $G$	191
$H < G$	$H$ sottogruppo di $G$ e $H \neq G$	191
$\langle X \rangle$	sottogruppo generato dal sottoinsieme $X$	192
$\langle g \rangle$	sottogruppo ciclico generato da $g$	192
$\mathcal{S}(X)$	insieme delle corrispondenze biunivoche di $X$ in sé	197
$\mathcal{S}_n$	$\mathcal{S}(X)$ quando $ X  = n$	197
$\mathcal{O}_\sigma(x)$	orbita dell'elemento $x$ sotto l'azione di $\sigma$	199
$\mathcal{A}_n$	permutazioni pari di $\mathcal{S}_n$	201
$p(n)$	numero di partizioni distinte dell'intero $n$	205
$p_k(n)$	numero di partizioni di $n$ con esattamente $k$ parti	205
$V$	gruppo di Klein	206
$D_n$	gruppo diedrale delle simmetrie di un $n$ -gono regolare	208
$R_1 \oplus R_2$	somma diretta di $R_1$ e $R_2$	210
$I \trianglelefteq R$	$I$ ideale dell'anello $R$	211
$\text{Ker}(\varphi)$	nucleo dell'omomorfismo $\varphi$	211
$\mathbb{Z}[i]$	interi di Gauss	213
	porta NOT	216
	porta AND	216
	porta OR	216
$\inf(B)$	espressione booleana	220
$\sup(B)$	estremo inferiore di $B$	231
$x \wedge y$	estremo superiore di $B$	231
$x \vee y$	estremo inferiore tra $x$ e $y$	231
$(L, \preceq)$	estremo superiore tra $x$ e $y$	231
$V_3^5$	reticolo	232
$V_4^5$	diamante	233
$\mathcal{B}$	pentagono	233
$G = (V, E)$	algebra di Boole	234
$G(n, m)$	grafo con insieme dei vertici $V$ e insieme degli archi $E$ grafo di ordine $n$ e grandezza $m$	243

$N_n$	grafo nullo con $n$ vertici	243
$K_n$	grafo completo su $n$ vertici	244
$(a, a)$	cappio	244
$d(v_i, v_j)$	distanza tra due vertici $v_i$ e $v_j$ di un grafo	245
$\mathcal{A}(G)$	automorfismi di un grafo	256
$K_{n,m}$	grafo bipartito	257
$X$	caratteristica di Eulero	264
$\mathbb{Z}^+$	interi positivi	269
$\mathbb{Z}^-$	interi negativi	269
$\zeta(s)$	funzione zeta	278

# 1

## Il linguaggio base della matematica

*Tutte le cose il Tempo, l'infinito dai giorni innumerabili,  
alla luce dalle tenebre rende e dalla luce le rinasconde in sé.*

Sofocle, AIACE

La matematica, come tutte le discipline, ha un suo linguaggio. È importante quindi impadronirsi il più presto possibile di questo linguaggio, che d'altra parte è la chiave per capire l'intima bellezza della matematica. È quanto contiamo di fare in questo primo capitolo, dove verranno introdotte le prime nozioni che sono alla base di tutta la matematica, e non solo della matematica discreta, quali le nozioni di insieme, i connettivi logici, le relazioni, le funzioni, le relazioni d'ordine, le relazioni di equivalenza, ecc.

### ■ 1 PRIME NOZIONI SUGLI INSIEMI

Non daremo la definizione di insieme, che verrà invece assunta come concetto *primitivo*, cioè non riconducibile a nozioni più elementari. Si tratta di un concetto abbastanza intuitivo: ognuno ha un'idea di tale concetto, che corrisponde all'attività elementare di "raccogliere". Per noi quindi un insieme sarà semplicemente una collezione di oggetti.

Per esempio, sono insiemi i seguenti:

- (a) l'insieme di tutti gli abitanti di Parigi;
- (b) l'insieme di tutti i bambini nati nel 2008;
- (c) l'insieme  $\mathbb{N}$  di tutti i numeri  $0, 1, 2, 3, \dots$ ;
- (d) l'insieme di tutte le rette del piano;
- (e) l'insieme costituito dal numero 3, da un libro, da un triangolo.

Si è soliti indicare un insieme con una lettera maiuscola. Gli oggetti che compongono un insieme  $A$  prendono il nome di *elementi* di  $A$ , e si indicano con una lettera minuscola. Dai primi esempi che abbiamo dato ci si rende conto che gli elementi di un insieme possono essere di natura arbitraria.

Per potere fare esempi concreti di insiemi conviene elencare qui di seguito gli insiemi numerici di cui diamo per scontata la conoscenza:

l'insieme dei numeri naturali  $\mathbb{N} := \{0, 1, 2, 3, 4, \dots\}$ ;

l'insieme dei numeri interi  $\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots\}$ ;

l'insieme dei numeri razionali  $\mathbb{Q} := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$ .

Nel prossimo capitolo daremo una definizione assiomatica dei numeri naturali (assiomi di Peano), mentre la definizione *formale* degli interi e dei razionali verrà sviluppata nel capitolo 11 dedicato proprio agli approfondimenti. Parleremo anche dell'insieme  $\mathbb{R}$  dei numeri reali o dell'insieme  $\mathbb{C}$  dei numeri complessi senza darne però una definizione formale.

Per indicare che un elemento  $a$  appartiene ad un insieme  $A$  si scrive  $a \in A$ . Per indicare che un elemento  $a$  non appartiene ad  $A$  si scrive  $a \notin A$ . L'insieme vuoto, ossia l'insieme che non contiene nessun elemento, si indica con il simbolo  $\emptyset$ .

Un insieme  $A$  si può definire o elencando tra parentesi graffe i suoi elementi, oppure, sempre tra parentesi graffe, specificando una sua proprietà caratteristica. Se indichiamo con  $\mathbb{N}$  l'insieme dei numeri naturali  $0, 1, 2, 3, \dots$ , l'insieme  $A$  costituito dai numeri naturali minori di 20 e maggiori di 5 può scriversi per esempio in uno dei due modi seguenti:

$$A = \{6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19\}$$

oppure

$$A = \{n \in \mathbb{N} \mid 5 < n < 20\}$$

dove il simbolo  $|$  si legge: *tale che*.

Si noti che l'*ordine* con cui sono elencati gli elementi di un insieme non ha importanza: ossia

$$\{1, 3, 5, 7, 8, 9\} = \{8, 9, 3, 5, 7, 1\} = \{1, 3, 8, 9, 5, 7\} = \{9, 7, 1, 3, 5, 8\}.$$

Inoltre si noti che l'insieme  $\{1, 2, 3, 4\}$  coincide con l'insieme  $\{1, 1, 1, 2, 3, 4, 4\}$ : ossia l'aggiunta nella lista degli elementi di un insieme di uno o più dei suoi elementi non altera l'insieme; in altre parole quello che importa è la lista degli elementi *distinti* che appartengono all'insieme.

Un *sottoinsieme* di  $A$  è un insieme  $B$  tale che ogni elemento  $b$  di  $B$  è anche elemento di  $A$ : si scrive

$$B \subseteq A.$$

Per indicare che l'inclusione è propria, ossia che esiste almeno un elemento di  $A$  che non appartiene a  $B$ , si scrive

$$B \subset A \quad \text{oppure} \quad B \varsubsetneq A.$$

Per indicare che un insieme  $B$  non è un sottoinsieme di  $A$  si scrive

$$B \not\subseteq A.$$

L'insieme vuoto è un sottoinsieme di ogni insieme.

Se  $A = \{a_1, a_2, a_3\}$ , i suoi sottoinsiemi sono  $\emptyset, \{a_1\}, \{a_2\}, \{a_3\}, \{a_1, a_2\}, \{a_1, a_3\}, \{a_2, a_3\}, \{a_1, a_2, a_3\}$ .

Si faccia attenzione alla differenza tra il simbolo  $\in$  di *appartenenza* (di un *elemento* ad un insieme) e il simbolo  $\subseteq$  di *essere contenuto* (di un *insieme* in un altro). Nell'esempio precedente,  $a_1 \in A$  (quindi  $a_1$  è un elemento di  $A$ ), mentre  $\{a_1\} \subset A$ , cioè il sottoinsieme che ha  $a_1$  come unico suo elemento, è un sottoinsieme di  $A$ . Un sottoinsieme che contiene un solo elemento  $a$ , ossia l'insieme  $\{a\}$ , si chiama *singleton*.

Due insiemi  $A$  e  $B$  si dicono *uguali* se  $A \subseteq B$  e  $B \subseteq A$ . Per dimostrare che due insiemi sono uguali si deve quindi provare la doppia inclusione.

### Esempio 1.1

Siano  $A = \{x \in \mathbb{N} \mid 2x+1 < 10\}$  e  $B = \{0, 1, 2, 3, 4\}$ . È ovvio che  $B \subseteq A$ : infatti ogni elemento  $x$  di  $B$  (ossia  $0, 1, 2, 3, 4$ ) è un numero naturale che verifica la condizione che  $2x + 1 < 10$  e quindi appartiene ad  $A$ . D'altra parte se  $x$  appartiene ad  $A$ , ossia se è un numero naturale tale che  $2x + 1 < 10$ , allora  $x$  deve essere un numero naturale minore di  $\frac{9}{2}$ , ossia non può che essere  $0, 1, 2, 3, 4$ : quindi  $A \subseteq B$ . Dunque  $A = B$ .

**OSSERVAZIONE** È opportuno a questo punto fare una piccola divagazione. In quanto seguirà parlando di insiemi li penseremo sempre, anche se non lo diremo esplicitamente, contenuti di volta in volta in un *insieme universale* o *universo* che contiene tutti gli insiemi con i quali stiamo lavorando in quel momento. Perché questa scelta? Per evitare paradossi. Presenteremo due esempi significativi, senza però approfondire la questione.

1. Consideriamo l'insieme  $S$  di tutti gli insiemi che non contengono se stessi come elementi, ossia

$$S := \{x \mid x \notin x\}.$$

Tra gli elementi di  $S$  c'è o non c'è  $S$  stesso?

(a) Se  $S \in S$ , allora (per definizione di  $S$ , come l'insieme di tutti gli insiemi che non contengono se stessi come elementi)  $S \notin S$ .

(b) Il non appartenere di  $S$  ad  $S$ , cioè l'essere  $S \notin S$  (cioè l'essere  $S$  un insieme che non contiene se stesso come elemento), implica che  $S$  ha diritto di stare in  $S$ , cioè  $S \in S$ .

In ogni caso si ottiene una *contraddizione*.

2. Un'altra antinomia si ha con il cosiddetto *paradosso del barbiere*, formulato dal filosofo e matematico Bertrand Russell agli inizi del 1900.

In un paese c'è un solo barbiere e questo è sempre ben rasato. Sopra il suo negozio è affissa la seguente insegna:

*Il barbiere rade tutti e soli quelli che non si radono da soli.*

Ma allora: chi rade il barbiere?

La prima risposta che viene in mente è: "il barbiere si rade da solo". Ma sull'insegna c'è scritto che il barbiere rade *solo* quelli che non si radono da soli: quindi

non può radere se stesso e pertanto il barbiere si fa radere da qualcun altro: ma ricordiamoci che sull'insegna c'è scritto che il barbiere rade *tutti* quelli che non si radono da soli: quindi lui (il barbiere) rientrerebbe nella classe di quelli che non si radono da soli, e quindi si dovrebbe radere.

Come la mettiamo?

Queste contraddizioni si possono però evitare restringendo opportunamente la classe degli insiemi, per esempio supponendo, come faremo sempre, che gli insiemi siano contenuti in un universo, ossia un insieme  $U$  contenente tutti gli insiemi che ci interessano.

A partire da due o più insiemi se ne possono costruire altri: diamo qui le principali operazioni che si possono fare con gli insiemi.

### 1. Intersezione di due insiemi

**DEFINIZIONE 1.1** Dati due insiemi  $A$  e  $B$ , si definisce loro *intersezione*, e si indica con  $A \cap B$ , l'insieme di tutti gli elementi che appartengono sia ad  $A$  sia a  $B$ . In simboli,

$$A \cap B \stackrel{\text{def}}{=} \{x \mid x \in A \text{ e } x \in B\}.$$

### 2. Unione di due insiemi

**DEFINIZIONE 1.2** L'*unione* di due insiemi  $A$  e  $B$ , che si indica con  $A \cup B$ , è l'insieme degli elementi che appartengono ad  $A$  o a  $B$ . In simboli,

$$A \cup B \stackrel{\text{def}}{=} \{x \mid x \in A \text{ o } x \in B\}.$$

### Esempio 1.2

Siano  $A = \{1, 2, 3, 5, 8, 9, 10\}$  e  $B = \{2, 4, 6, 8\}$ . Allora

$$A \cap B = \{2, 8\}, \quad A \cup B = \{1, 2, 3, 4, 5, 6, 8, 9, 10\}$$

L'unione è costituita dagli elementi che appartengono ad *almeno* uno dei due insiemi  $A$  e  $B$  (non escludendo che gli elementi appartengano ad entrambi). Nel nostro esempio, 1, 3, 5, 9 e 10 appartengono *soltamente* ad  $A$ , 4 e 6 appartengono *soltamente* a  $B$ , mentre 2 e 8 appartengono sia ad  $A$  sia a  $B$  (infatti  $A \cap B = \{2, 8\}$ ).

### 3. Intersezione e unione di una famiglia di insiemi

Le definizioni di unione e di intersezione di due insiemi si possono generalizzare al caso di una famiglia non vuota, anche infinita,  $\{A_\alpha\}_{\alpha \in I}$ , di insiemi:

$$\bigcap_{\alpha \in I} A_\alpha \stackrel{\text{def}}{=} \{x \in A_\alpha \text{ per ogni } \alpha \in I\}$$

$$\bigcup_{\alpha \in I} A_\alpha \stackrel{\text{def}}{=} \{x \in A_\alpha \text{ per qualche } \alpha \in I\}.$$

### 4. Il complementare di un insieme

Sia ora  $U$  un fissato *universo*, ossia un insieme che contiene tutti gli oggetti che ci possono interessare.

**DEFINIZIONE 1.3** Si definisce *complemento* o *complementare* di un insieme  $A$  (rispetto all'universo  $U$ ) l'insieme di tutti gli elementi di  $U$  che non appartengono ad  $A$ . Esso si indica con  $\complement A$ .

Quindi:

$$\complement A \stackrel{\text{def}}{=} \{x \in U \mid x \notin A\}.$$

**DEFINIZIONE 1.4** Il *complemento relativo* di un insieme  $A$  in un insieme  $B$  è costituito da tutti gli elementi di  $B$  che non stanno in  $A$ . Si indica con  $B \setminus A$  e prende anche il nome di *insieme differenza* di  $B$  ed  $A$ :

$$B \setminus A \stackrel{\text{def}}{=} \{x \in B \mid x \notin A\}.$$

Nella figura 1.1 le definizioni date vengono illustrate con i cosiddetti *diagrammi di Venn*.

### 5. Il prodotto cartesiano di insiemi

Un altro concetto che si può definire a partire da due insiemi  $A$  e  $B$  è il loro prodotto cartesiano.

**DEFINIZIONE 1.5** Si definisce *prodotto cartesiano* di due insiemi  $A$  e  $B$ , e si indica con  $A \times B$ , l'insieme costituito da tutte le *coppie ordinate*  $(a, b)$ , dove il primo elemento varia in  $A$  e il secondo varia in  $B$ :

$$A \times B \stackrel{\text{def}}{=} \{(a, b) \mid a \in A, b \in B\}.$$

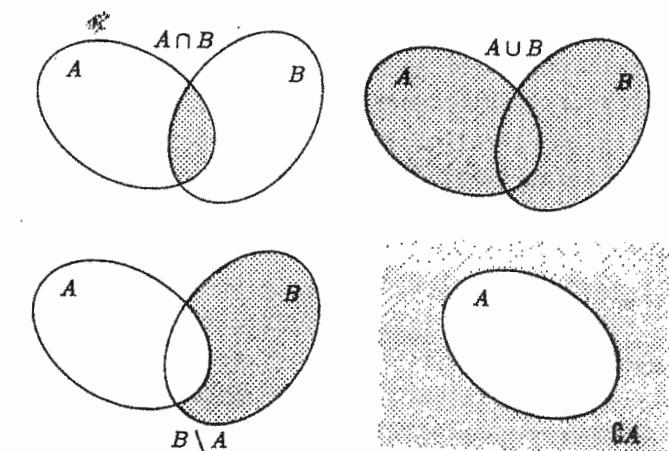


Figura 1.1. Diagrammi di Venn.

Per esempio, se  $A = \{3, 4\}$  e  $B = \{1, 5\}$ , allora

$$A \times B = \{(3, 1), (3, 5), (4, 1), (4, 5)\}.$$

Gli elementi del prodotto cartesiano di due insiemi  $A$  e  $B$  non sono quindi elementi di  $A$  o di  $B$ , ma sono elementi di altra natura: sono *coppie* di elementi di  $A$  e  $B$ .

Ovviamente si può definire il prodotto cartesiano di più di due insiemi.

**DEFINIZIONE 1.6** Si definisce *prodotto cartesiano* di  $n$  insiemi  $A_1, A_2, \dots, A_n$ , e si indica con  $A_1 \times A_2 \times \dots \times A_n$ , l'insieme costituito da tutte le  $n$ -uple *ordinate*  $(a_1, a_2, \dots, a_n)$ , dove il primo elemento varia in  $A_1$ , il secondo varia in  $A_2$ , l' $n$ -esimo varia in  $A_n$ :

$$A_1 \times A_2 \times \dots \times A_n \stackrel{\text{def}}{=} \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i, i = 1, 2, \dots, n\}. \quad \blacksquare$$

#### 6. L'insieme delle parti di un insieme

Terminiamo con un altro importante insieme associato ad un insieme  $A$ : l'insieme delle parti di  $A$ .

**DEFINIZIONE 1.7** Dato un insieme  $A$ , l'*insieme delle parti* (o dei *sottoinsiemi*) di  $A$ , che si indica con  $\mathcal{P}(A)$ , è dato da

$$\mathcal{P}(A) \stackrel{\text{def}}{=} \{B \mid B \subseteq A\}. \quad \blacksquare$$

Si noti che gli *elementi* di  $\mathcal{P}(A)$  sono *sottoinsiemi* (o *parti*) di  $A$ .

Ricordando quanto detto a proposito della differenza tra *essere elemento di* e *essere contenuto in*, se  $A = \{a, b\}$ , allora  $a \in A$ , ma  $a \notin \mathcal{P}(A)$ . Invece,  $\{a\} \in \mathcal{P}(A)$ , e  $\{a\} \subseteq A$ .

Per esempio, se  $A = \{a, b\}$ , sarà

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

#### Esercizi

- Si provi che  $(A \cup B) \cup C = A \cup (B \cup C)$  (proprietà associativa dell'unione).
- Si provi che  $(A \cap B) \cap C = A \cap (B \cap C)$  (proprietà associativa dell'intersezione).
- Si provi che  $A \cup B = A$  se e solo se  $B \subseteq A$ .
- Si provino le seguenti proprietà distributive:

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

(distributività dell'intersezione rispetto all'unione);

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

(distributività dell'unione rispetto all'intersezione).

- Si provi che  $\complement(A \cap B) = \complement A \cup \complement B$  e che  $\complement(A \cup B) = \complement A \cap \complement B$ .

- Si considerino i seguenti insiemi:

$$A = \{n \in \mathbb{N} \mid 10 < n < 16\}, \quad B = \{n \in \mathbb{N} \mid 12 \leq n \leq 17\}, \quad C = \{11, 15\}.$$

Dire se

$$(1.1) \quad A \cap (B \cup C) = (A \cap B) \cup C.$$

- Dire se la relazione (1.1) vale per ogni scelta degli insiemi  $A$ ,  $B$  e  $C$ . In caso positivo, dimostrarlo, altrimenti dare un controsenso.

- Scrivere esplicitamente gli elementi dei seguenti insiemi:

- $A = \{\text{numeri dispari divisibili per } 11 \text{ e minori di } 100\}$ .
- $A = \{x \in \mathbb{R} \mid x^2 + 4x - 5 = 0\}$ .
- $A = \{x \in \mathbb{Z} \mid x = 2h, h \in \mathbb{Z} \text{ e } 0 \leq x < 20\}$ .

- Quali dei seguenti insiemi sono uguali?

$$A = \emptyset, \quad B = \{\emptyset\}, \quad C = \{0\}.$$

- Quali dei seguenti insiemi sono l'insieme vuoto?

$$A = \{x \in \mathbb{R} \mid x^2 = 4, 3x = 5\}, \quad B = \{x \in \mathbb{Z} \mid x + 5 = 5\}, \quad C = \{x \in \mathbb{Z} \mid x^2 = 81, x = 2h, h \in \mathbb{Z}\}, \quad D = \{x \in \mathbb{Z} \mid x^2 < 9, x < 0\}.$$

- Scrivere le relazioni di inclusione relative agli insiemi del punto precedente.

- Determinare  $A \cup B$  e  $A \cap B$  se:

- $A = \{x \in \mathbb{Z} \mid x^2 + 3x - 10 \leq 0\}, \quad B = \{x \in \mathbb{Z} \mid x^2 - x - 6 < 0\}$ .
- $A = \{x \in \mathbb{Z} \mid x^2 - 4x - 5 \leq 0\}, \quad B = \{x \in \mathbb{Z} \text{ divisibili per } 3\}$ .
- $A = \{x \in \mathbb{Q} \mid x^2 = 3\}$  e  $B = \{x \in \mathbb{N} \mid x^2 - x - 6 < 0\}$ .

- Determinare  $\mathcal{P}(A)$  se:

- $A = \{a, b, c\}$ .
- $A = \{x \in \mathbb{Z} \mid x^2 - 2x - 3 < 0\}$ .
- $A = \{-1, 3, 5, 4\}$ .

- Determinare esplicitamente  $A \times A$ ,  $A \times B$ ,  $B \times A$ ,  $B \times B$ ,  $A \times C$ ,  $C \times A$ ,  $C \times C$ ,  $B \times C$ ,  $C \times B$  se  $A = \{t, u, v\}$ ,  $B = \{x \in \mathbb{Z} \mid x^2 - 2x - 3 \leq 0\}$  e  $C = \{x \in \mathbb{N} \mid x < 20, x = 3k, x = 2h, h, k \in \mathbb{Z}\}$ .

## 2 STRINGHE BIT E SOTTOINSIEMI

Abbiamo parlato nel paragrafo precedente di insiemi. Ci poniamo ora il seguente problema, di fondamentale importanza per chi deve risolvere problemi attraverso il calcolatore. Qual è un modo efficiente per rappresentare un insieme? Cioè qual è un modo efficiente per trasmettere al calcolatore l'informazione sulla composizione degli elementi di un insieme finito e sulle operazioni tra insiemi?

Un sistema molto efficiente è il seguente. Si fissa un *universo* finito  $U$  tale che il numero  $n$  dei suoi elementi non ecceda la memoria del calcolatore. Ordinando i suoi elementi in modo arbitrario, si potranno *numerare* i suoi  $n$  elementi da 1 ad  $n$  al modo seguente:

$$U = \{a_1, a_2, a_3, \dots, a_n\}.$$

Ogni sottoinsieme  $A$  di  $U$  si può rappresentare sotto forma di  $n$ -pla  $(i_1, i_2, \dots, i_n)$ , dove  $i_j$  vale 1 o 0 a seconda che il corrispondente elemento  $a_j$  stia o non stia in  $A$ . Per esempio, se

$$U = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\}, \quad A = \{a_2, a_4, a_5, a_{10}\},$$

$A$  si scriverà nella forma:

$$A : (0, 1, 0, 1, 1, 0, 0, 0, 0, 1).$$

Ora, è ben noto che i calcolatori rappresentano le informazioni usando i *bit*. Un bit ha due possibili valori, 0 e 1. Avendo rappresentato gli insiemi come *stringhe bit*, ossia come sequenze di 0 e 1, si capisce che fare unione, intersezione, differenza, ecc., tra insiemi così definiti è semplice per il calcolatore, perché non richiede nessun tipo di ricerca.

Per fare il complementare di un insieme  $A$  descritto come stringa bit, basta cambiare ogni 1 in 0 e ogni 0 in 1.

Per quanto riguarda l'unione di due insiemi  $A$  e  $B$ , il bit nella  $i$ -esima posizione della stringa bit dell'unione è 1 se e solo se uno almeno dei bit nella  $i$ -esima posizione di  $A$  o di  $B$  è 1.

L'intersezione di due insiemi  $A$  e  $B$  avrà 1 nella posizione  $i$ -esima se e solo se i corrispondenti bit di  $A$  e di  $B$  sono entrambi 1.

Per esempio, se  $A$  è l'insieme precedente e  $B$  è l'insieme  $B = \{a_2, a_3, a_4, a_6, a_7, a_9\}$ , per determinare l'unione e l'intersezione di  $A$  e  $B$  si scrive innanzitutto  $B$  nella forma

$$B : (0, 1, 1, 1, 0, 1, 1, 0, 1, 0),$$

e allora

$$A \cup B : (0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$$

e

$$A \cap B : (0, 1, 0, 1, 0, 0, 0, 0, 0, 0).$$

Naturalmente, si può poi passare alla scrittura ordinaria dell'insieme.

Sia  $A = \{n \in \mathbb{N} \mid n \leq 21\}$  e siano  $B$  e  $C$  i due sottoinsiemi

$$B = \{0, 2, 4, 6, 8, 20\}, \quad C = \{1, 2, 3, 4, 5, 6, 21\}.$$

Scrivere sotto forma di stringa bit i sottoinsiemi  $B$ ,  $C$ ,  $B \cap C$ ,  $B \cup C$ ,  $\complement B$  e  $\complement C$ .

## 3 ELEMENTI DI LOGICA

**DEFINIZIONE 1.8** Una *proposizione* è una affermazione che è vera o falsa, ma non può essere contemporaneamente vera e falsa.

I seguenti sono esempi di proposizioni.

1. Londra si trova in Europa.

2. Madrid è la capitale d'Italia.

3.  $3 + 3 = 8$ .

4.  $8 - 4 = 4$ .

Quelle che seguono sono affermazioni che *non* sono proposizioni:

1. Che ore sono?

2. Mostrami quello che hai scritto.

3. Che bella musica!

4.  $x + 6 = 1$  (non è né vera né falsa, perché alla  $x$  non è stato assegnato nessun valore).

Se avessimo scritto: *per ogni*  $x \in \mathbb{R}$   $x + 6 = 1$ , oppure *esiste un*  $x \in \mathbb{R}$  *tale che*  $x + 6 = 1$  avremmo ottenuto due proposizioni (la prima falsa, la seconda vera).

5. Tutti i giorni in estate piove almeno due ore.

Non si hanno gli elementi per dire se questa affermazione è vera o falsa: in certe parti della terra può essere vera, in altre può essere falsa. Se per esempio la trasformassimo nella seguente: *in qualche parte della terra tutti i giorni in estate piove almeno due ore*, allora diventerebbe una proposizione (vera). Oppure la potremmo trasformare nella seguente: *a Roma tutti i giorni in estate piove almeno due ore*, allora diventerebbe una proposizione (falsa).

Le proposizioni si indicano generalmente con lettere quali  $p$ ,  $q$ ,  $r$ ,  $s$ ,  $t$ , ecc.

A partire da una proposizione  $p$  possiamo costruire una nuova proposizione, che indicheremo con  $\neg p$ :

$\neg p$ : Non è vero che  $p$ .

La nuova proposizione è la *negazione della proposizione*  $p$ , e si legge *non*  $p$ .

Essa è vera quando  $p$  è falsa, e falsa quando  $p$  è vera.

### Esempio 1.3

Sia  $p$  la proposizione

*Ieri abbiamo battuto gli avversari.*

La sua negazione è la proposizione

$\neg p$ : *Non è vero che ieri abbiamo battuto gli avversari*

cioè la proposizione

*Ieri non abbiamo battuto gli avversari.*

Negli esempi di affermazioni che *non* sono proposizioni, abbiamo visto che esse possono trasformarsi in proposizioni specificando opportunamente le variabili, per esempio, scrivendo *per ogni*  $x \in \mathbb{R}$   $x + 6 = 1$ , oppure *esiste un*  $x \in \mathbb{R}$  tale che  $x + 6 = 1$ . Espressioni come *esiste* o *per ogni* danno un'idea della quantità degli oggetti per cui un dato enunciato può diventare una proposizione. Per questo motivo si chiamano *quantificatori*.

È opportuno a questo punto introdurre dei simboli matematici che li rappresentino. Se vogliamo scrivere:

per qualche  $x, p(x)$

cioè per qualche valore della variabile  $x$  vale  $p(x)$ , allora useremo il *quantificatore esistenziale*  $\exists$  e scriveremo

$\exists x \mid p(x)$

Se invece vogliamo dire

per ogni  $x, p(x)$ .

cioè che per tutti i valori della variabile  $x$  vale  $p(x)$ , allora useremo il *quantificatore universale*  $\forall$  e scriveremo

$\forall x \mid p(x)$ .

Utilizziamo subito questi simboli per tradurre in linguaggio matematico alcuni enunciati espressi in lingua italiana.

#### Esempio 1.4

Sia  $P(a, b)$  l'affermazione: *a ha ascoltato b*. Usare i quantificatori per esprimere le seguenti proposizioni:

1. *Tutti hanno ascoltato la terza sinfonia di Beethoven.*
2. *Tutti hanno ascoltato qualche sinfonia.*
3. *C'è qualche sinfonia che tutti hanno ascoltato.*

1.  $\forall a \mid \forall b \mid P(a, b)$ .
2.  $\forall a \mid \exists b \mid P(a, b)$ .
3.  $\exists b \mid \forall a \mid P(a, b)$ .

#### Esempio 1.5

Negare le proposizioni dell'esempio precedente, esprimendo tali negazioni sia in forma di linguaggio ordinario, sia con i quantificatori.

1. Non è vero che tutti hanno ascoltato la terza sinfonia di Beethoven, cioè esiste almeno una persona che non ha ascoltato la terza sinfonia di Beethoven, ossia

$\exists a \mid \neg P(a, B)$ .

2. Non è vero che tutti hanno ascoltato qualche sinfonia, ossia esiste una persona che non ha ascoltato nessuna sinfonia.

$\exists a \mid \forall b \mid \neg P(a, b)$ .

3. Non è vero che c'è qualche sinfonia che tutti hanno ascoltato, ossia data comunque una sinfonia, esiste almeno una persona che non l'ha ascoltata.

$\forall b \mid \exists a \mid \neg P(a, b)$ .

**DEFINIZIONE 1.9** Siano  $p$  e  $q$  due proposizioni. La proposizione " $p$  e  $q$ " si denota con  $p \wedge q$  ed è vera quando entrambe  $p$  e  $q$  sono vere, falsa altrimenti, ossia quando una almeno delle due proposizioni è falsa. 

**DEFINIZIONE 1.10** Siano  $p$  e  $q$  due proposizioni. La proposizione " $p$  o  $q$ " si denota con  $p \vee q$  ed è falsa quando entrambe  $p$  e  $q$  sono false, vera altrimenti, ossia quando una almeno delle due proposizioni è vera. 

Gli operatori logici appena definiti prendono i seguenti nomi:

$\wedge$ : operatore di congiunzione

$\vee$ : operatore di disgiunzione.

#### Esempio 1.6

Se  $p$  e  $q$  sono rispettivamente le proposizioni:  $p$ : È domenica e  $q$ : Piove, allora  $p \wedge q$  e  $p \vee q$  sono le proposizioni:

$p \wedge q$  : È domenica e piove e  $p \vee q$  : È domenica o piove.

Osserviamo che

$$\begin{aligned} \neg(p \wedge q) &= \neg(\text{è domenica e piove}) = \\ &= \text{o non è domenica oppure non piove} \end{aligned}$$

cioè esattamente  $\neg p \vee \neg q$ .

Così

$$\begin{aligned} \neg(p \vee q) &= \neg(\text{è domenica o piove}) = \\ &= \text{non è domenica e non piove} = \neg p \wedge \neg q. \end{aligned}$$

In questo esempio abbiamo così visto che

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

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

Faremo vedere fra breve che queste relazioni valgono *in generale*: averle verificate su un esempio non costituisce una dimostrazione!

Diamo ora un'importante nuova proposizione che si può costruire a partire da due proposizioni.

**DEFINIZIONE 1.11** Siano  $p$  e  $q$  due proposizioni. L'*implicazione*

$$p \implies q$$

è una proposizione che è falsa quando  $p$  è vera e  $q$  è falsa, e vera in tutti gli altri casi. 

$p$  prende il nome di *ipotesi*,  $q$  prende il nome di *conclusione* o *tesi*.

Si noti quindi che la  $p \implies q$  è falsa solamente quando  $p$  è vera e  $q$  è falsa. Quindi la  $p \implies q$  è vera anche quando  $p$  è falsa (indipendentemente dal valore di verità della  $q$ ).

#### Esempio 1.7

Sia  $p$  la proposizione *Un cane ha sempre due sole zampe* e  $q$  la proposizione:  $4+12=10$ . Allora la  $p \implies q$  è vera: da una ipotesi falsa si conclude qualunque cosa. In tal modo si sottolinea l'assurdità di una premessa traendo una conclusione ancora più assurda.

Una proposizione del tipo  $p \implies q$  in sostanza dice che se  $p$  è vera, allora è vera anche  $q$  (se  $p$  è falsa, come abbiamo visto, possiamo concludere qualunque cosa).

Modi equivalenti sono i seguenti:

1.  $p$  è condizione sufficiente per  $q$ .
2.  $q$  è condizione necessaria per  $p$ .

#### Esempio 1.8

Sia  $p$  l'affermazione: *la televisione funziona*,  $q$  l'affermazione: *l'impianto elettrico è acceso*. La proposizione  $p \implies q$  può leggersi nei seguenti modi:

1. Se la televisione funziona, allora (si può concludere che) l'impianto elettrico è acceso.
2. Condizione sufficiente per decidere se l'impianto elettrico è acceso è che la televisione funzioni.
3. Condizione necessaria perché la televisione funzioni è che l'impianto elettrico sia acceso.

È chiaro che perché la televisione funzioni non basta che l'impianto elettrico sia acceso: molte altre cose devono funzionare nella televisione.

Osserviamo che la implicazione  $p \implies q$  (cioè che il fatto che la televisione funzioni sia un test per verificare che l'impianto elettrico è acceso) è falsa solo nel caso in cui la  $p$  sia vera e la  $q$  falsa (ossia se la televisione funziona con l'impianto elettrico spento: questo sarebbe davvero anomalo).

#### Esempio 1.9

Siano  $p$  e  $q$  le seguenti affermazioni:

$p$ : Ada ottiene un voto minore di 18 nel primo esonero  
 $q$ : si metterà seriamente a studiare il giorno dopo il primo esonero.

La nuova proposizione  $p \implies q$  (ossia la proposizione che dice che se Ada otterrà un voto minore di 18 nel primo esonero si metterà seriamente a studiare il giorno dopo) rappresenta una specie di promessa o di patto che Ada fa con se stessa. Se succede una certa cosa allora si comporterà in un certo modo.

Quand'è che la  $p \implies q$  è vera? In tutti i casi che non comportano una rottura della promessa. Esaminiamo i vari casi, a seconda del comportamento di Ada il giorno dopo l'esonero.

1. Il giorno dopo l'esonero Ada si mette seriamente a studiare (ossia  $q$  è vera).
  - (a) Se  $p$  è vera, allora la promessa è stata mantenuta e quindi  $p \implies q$  è vera.
  - (b) Se  $p$  è falsa, Ada fa comunque una cosa buona (studiare non può che fare bene), anche se non sarebbe stata obbligata a farlo, perché non c'era nessuna promessa da mantenere. Quindi  $p \implies q$  è vera.
2. Il giorno dopo l'esonero Ada sta tutto il giorno a fare compere e la sera va al cinema (ossia  $q$  è falsa).
  - (a) Se  $p$  è vera, Ada non ha rispettato la promessa, quindi  $p \implies q$  è falsa.
  - (b) Se  $p$  è falsa, non ha rotto nessuna promessa, quindi  $p \implies q$  è vera.

In definitiva, in quali casi è falsa la  $p \implies q$ ? Solamente nel caso in cui  $p$  è vera e  $q$  è falsa.

**OSSERVAZIONE** In molti programmi il *se, allora*, che comunemente si scrive *if, then*, è usato in modo diverso da quello logico che abbiamo appena descritto. Se  $p$  è una proposizione e  $C$  è un comando da eseguire,  $C$  viene eseguito se  $p$  è vera, mentre non viene eseguito se  $p$  è falsa.

#### Esempio 1.10

Supponiamo di avere due variabili,  $t$  e  $x$ , e supponiamo di avere la seguente riga in un programma:

*if t = t<sup>2</sup> - 2, then x := x + 1.*

Se  $x = 0$  prima di incontrare questa affermazione, ci domandiamo qual è il valore della variabile  $x$  dopo una tale affermazione. Tutto dipende da quanto vale la  $t$ . Se per esempio  $t = 2$ , allora la condizione  $t = t^2 - 2$  è verificata, e quindi il valore di  $x$  dal valore 0 passa al valore 1 (il comando viene eseguito). Se invece il valore di  $t$  è 0, allora non è soddisfatta la condizione  $t = t^2 - 2$ , quindi il valore di  $x$ , che era 0, continua a rimanere tale (ossia il comando *non* viene eseguito).

Conviene ora dare la seguente definizione.

**DEFINIZIONE 1.12** Una proposizione si dice *primitiva* se non si può spezzare in proposizioni più semplici mediante connettivi logici. Una proposizione non primitiva si dice *composta*. 

Abbiamo già visto come a partire da due o più proposizioni se ne possano costruire altre, per esempio attraverso i connettivi logici, l'implicazione, ecc. Queste nuove proposizioni non saranno sicuramente primitive.

Per esempio la proposizione  $s$ : *Giovanni è alto e ha vinto la gara* non è una proposizione primitiva, perché si può scrivere come congiunzione delle due proposizioni  $p$ : *Giovanni è alto* e  $q$ : *Giovanni ha vinto la gara*, ossia

$$s : p \wedge q.$$

Invece la proposizione *Giovanni ha studiato* è primitiva.

**DEFINIZIONE 1.13** Una proposizione composta che è sempre vera, indipendentemente dal valore di verità delle proposizioni da cui è composta, prende il nome di *tautologia*.

Una proposizione composta che è sempre falsa prende il nome di *contraddizione*. 

#### Esempio 1.11

La  $p \vee \neg p$  è un esempio di tautologia, dato che, qualunque sia  $p$ , o  $p$  o  $\neg p$  è sicuramente vera, quindi la  $p \vee \neg p$  è sempre vera.

#### Esempio 1.12

La  $p \wedge \neg p$  è un esempio di contraddizione, dato che  $p$  e  $\neg p$  non possono essere contemporaneamente vere, quindi la  $p \wedge \neg p$  è sempre falsa.

**DEFINIZIONE 1.14** Due proposizioni  $p$  e  $q$  si dicono *logicamente equivalenti* se  $p$  è vera (o falsa) se e solo se  $q$  è vera (o falsa). 

Come abbiamo visto dalla definizione, una proposizione può essere vera o falsa (ma non entrambe): quindi ad ogni proposizione possiamo associare un *valore di verità*: vero o falso, che si indicano rispettivamente con i simboli  $T$  (=true) e  $F$ .

Precisamente, il valore di verità della proposizione  $p$  è  $T$  se la proposizione è vera, è  $F$  se la proposizione è falsa.

Si possono quindi costruire le cosiddette *tavole di verità*.

Per esempio, per definizione di negazione  $\neg p$  di una proposizione  $p$ , sappiamo che essa è falsa quando  $p$  è vera e viceversa. Ciò significa che possiamo costruire la seguente tavola di verità:

$p$	$\neg p$
$T$	$F$
$F$	$T$

La tavola di verità corrispondente alle proposizioni di congiunzione  $p \wedge q$  e disgiunzione  $p \vee q$  è la seguente:

$p$	$q$	$p \wedge q$	$p \vee q$
$T$	$T$	$T$	$T$
$T$	$F$	$F$	$T$
$F$	$T$	$F$	$T$
$F$	$F$	$F$	$F$

Dalle tavole di verità si può controllare per esempio se due proposizioni composte sono logicamente equivalenti.

Per verificare per esempio che le due proposizioni

$$\neg(p \wedge q) \quad \text{e} \quad \neg p \vee \neg q$$

sono logicamente equivalenti, basta costruire le corrispondenti tavole di verità:

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

Altre due proposizioni logicamente equivalenti sono le seguenti:

$$(3.1) \quad p \implies q \quad \text{e} \quad (\neg p) \vee q,$$

come si vede dalle corrispondenti tavola di verità:

$p$	$q$	$\neg p$	$p \implies q$	$\neg p \vee q$
$T$	$T$	$F$	$T$	$T$
$T$	$F$	$F$	$F$	$F$
$F$	$T$	$T$	$T$	$T$
$F$	$F$	$T$	$T$	$T$



Negare la seguente proposizione: *esistono giorni in cui piove e c'è il sole*.



Negare la seguente proposizione: *ogni intero è somma di due quadrati*.



Negare la seguente affermazione: *esistono interi  $a$  e  $b$  tali che  $(a+b)(a-2b) = 0$* .



Negare la seguente proposizione: *ogni mese qualche studente legge almeno un libro*.



Negare la seguente proposizione: *ogni studente in quest'aula supererà a febbraio almeno un esame*.



Negare la seguente proposizione: *esistono giorni in cui piove e c'è il sole*.

Sia  $p$  la proposizione: *l'intero  $n$  termina con la cifra 3* e sia  $q$  la proposizione *l'intero  $n$  è dispari*. Eprimere la proposizione  $p \Rightarrow q$  in termini di condizione necessaria e di condizione sufficiente.

Sia  $p$  la proposizione: *Paolo vota* e sia  $q$  la proposizione: *Paolo è maggiorenne*. Eprimere in termini di condizione necessaria e sufficiente la proposizione  $p \Rightarrow q$ .

Sia  $p$ : *R è un quadrato*,  $q$ : *R è un rettangolo*. Eprimere in termini di condizione necessaria e sufficiente la proposizione  $p \Rightarrow q$ .

Provare che la proposizione  $\neg(p \Leftrightarrow q) \Leftrightarrow ((p \vee q) \wedge \neg(p \wedge q))$  è una tautologia.

Sia  $X$  l'insieme degli studenti in aula. Sia  $p(x)$  l'affermazione: *x è nato a Roma* e  $q(x)$  l'affermazione: *x conosce l'inglese*. Eprimere in funzione dei connettivi logici e dei quantificatori le espressioni che seguono:

- C'è uno studente in quest'aula che è nato a Roma e conosce l'inglese.*
- C'è uno studente in quest'aula che è nato a Roma ma non conosce l'inglese.*
- Ogni studente in quest'aula o è nato a Roma o conosce l'inglese.*
- Nessuno studente in quest'aula è nato a Roma o conosce l'inglese.*

Negare tutte le proposizioni dei punti precedenti.

In una classe di prima elementare, la piccola Margherita corre piangendo dalla maestra e dice: "qualcuno ha scarabocchiato con il pennarello il mio disegno". In quel momento in classe ci sono solamente quattro bambini, Antonio, Bruno, Carla e Davide, dato che tutti gli altri sono andati a ginnastica. La maestra comincia a interrogarli, per individuare il colpevole della marachella. Ecco le risposte dei bambini:

Antonio: *È stata Carla a scarabocchiare, l'ho vista.*

Bruno: *Non sono stato io a fare lo scarabocchio.*

Carla: *È Davide il colpevole.*

Davide: *Carla ha mentito quando mi ha incolpato.*

Sapendo che sicuramente *il responsabile è un solo bambino* (dato che lo scarabocchio è stato fatto con un solo pennarello) e che *una sola delle quattro affermazioni precedenti è vera*, la maestra riuscirà ad individuare il colpevole. Perché?

## 4 RELAZIONI

Supponiamo di volere *collegare* o *mettere in relazione* due elementi  $a$  e  $b$ , uno appartenente ad un insieme  $A$  e uno appartenente ad un altro insieme  $B$ . Per esprimere il legame che esiste tra questi due elementi è naturale pensarli rispettivamente come primo e secondo elemento di una stessa *coppia*  $(a, b)$ , che, come sappiamo, appartiene al prodotto cartesiano  $A \times B$ . Il concetto di relazione è quindi legato alla nozione di prodotto cartesiano, introdotta nel primo paragrafo.

**DEFINIZIONE 1.15** Una *relazione*  $\rho$  da un insieme  $A$  ad un insieme  $B$  è un sottoinsieme del prodotto cartesiano  $A \times B$ . Quando  $A = B$ , allora si parla di relazione  $\rho$  definita su  $A$ .

L'insieme  $A$  dicesi *dominio* della relazione  $\rho$ , l'insieme  $B$  *codominio* di  $\rho$ . Invece che scrivere che la coppia  $(a, b)$  sta in  $\rho$  (ossia che  $(a, b) \in \rho$ ), si usa scrivere  $a \rho b$ . Spesso in luogo della scrittura  $a \rho b$  si scrive anche  $b = \rho(a)$ . Un altro modo di rappresentare una relazione consiste nel collegare con una freccia il primo con il secondo elemento di una coppia appartenente ad una relazione  $\rho$ . Quindi

$$(a, b) \in \rho \iff a \rightarrow b.$$

### Esempio 1.13

Esempi di relazioni.

- Sia  $A$  l'insieme di tutte le città italiane e sia  $B = \mathbb{Q}$ , l'insieme di tutti i numeri razionali. Definiamo una relazione tra  $A$  e  $\mathbb{Q}$  mettendo in relazione una città  $a$  appartenente ad  $A$  con un numero razionale  $h$  se esiste un aereo in partenza da  $a$  all'ora  $h$ . Si tratta di una relazione da  $A$  a  $\mathbb{Q}$ , dato che gli orari di partenza di un aereo sono del tipo 15.16 o 18.27, ecc., quindi si tratta di numeri razionali, ossia  $\rho \subseteq A \times \mathbb{Q}$ .
- La relazione  $\leq$ , definita su  $\mathbb{N}$ .
- La relazione di essere *nato a* dall'insieme  $A$  di tutti i residenti in Italia all'insieme  $B$  di tutte le località del mondo. Si tratta di una relazione, in cui *tutti* i residenti in Italia, ossia tutti gli elementi di  $A$ , compaiono come primi elementi di una e una sola coppia appartenente a  $\rho$ , perché ognuno è nato in una e una sola località del mondo.
- Se nell'esempio precedente avessimo preso come insieme  $B$  l'insieme di tutte le località italiane, si sarebbe trattato ancora di una relazione da  $A$  a  $B$  ma in questo caso alcune persone (cioè alcuni elementi di  $A$ , precisamente i residenti in Italia che sono nati all'estero) non avrebbero avuto nessun corrispondente in  $B$ , ossia nel sottoinsieme  $\rho$  di  $A \times B$  non tutti gli elementi di  $A$  sarebbero comparsi come primi elementi di una coppia di  $\rho$ .
- La relazione  $\rho$  costituita da tutte le coppie  $(a, b)$  di  $\mathbb{R} \times \mathbb{R}$  tali che  $a+2b = 3$ : geometricamente, questa relazione coincide con la retta  $x + 2y = 3$  del piano  $\mathbb{R} \times \mathbb{R}$ . Quindi 2 è in relazione con  $\frac{1}{2}$  (cioè la coppia  $(2, \frac{1}{2})$  sta in  $\rho$ ) perché  $2 + 2(\frac{1}{2}) = 3$ , mentre 2 non è in relazione con 3, ossia la coppia  $(2, 3)$  non sta in  $\rho$ , perché  $2 + 2 \cdot 3 = 8 \neq 3$ .
- Sia  $A = B = \mathbb{N}$ . Consideriamo l'insieme delle coppie  $(a, b) \in \mathbb{N} \times \mathbb{N}$  tali che  $a \cdot b = 30$ . Tale insieme, in quanto sottoinsieme di  $\mathbb{N} \times \mathbb{N}$  per definizione, è una relazione da  $\mathbb{N}$  in  $\mathbb{N}$ . Si tratta del sottoinsieme  $\{(1, 30), (30, 1), (2, 15), (15, 2), (3, 10), (10, 3), (5, 6), (6, 5)\}$ .

Sia ora  $A = B = \mathbb{N}$ : supponiamo di volere associare ad ogni  $n \in \mathbb{N}$  il numero  $\frac{n}{2}$ . Dato che  $\frac{n}{2}$  è un numero naturale solo se  $n$  è un numero pari, non si tratta di una relazione da  $\mathbb{N}$  in  $\mathbb{N}$ . Può diventare una relazione da  $\mathbb{N}$  in  $\mathbb{N}$  se si decide di associare ad ogni intero positivo *pari* la sua metà.

Un altro modo di rappresentare una relazione  $\rho$  da  $A$  a  $B$ , utile per essere implementato al calcolatore, è il seguente: si costruisce una *matrice* (ossia una *tavola*) che ha tante righe quanti sono gli elementi di  $A$  e tante colonne quanti sono gli elementi di  $B$ , e che nella posizione  $(a, b)$ , ossia all'incrocio tra la riga che contiene l'elemento  $a \in A$  e la  $b$ -esima colonna, ossia la colonna che contiene l'elemento  $b \in B$ , contiene 1 o 0 a seconda che la coppia  $(a, b)$  appartenga o no a  $\rho$ . Una tale matrice si chiama

*matrice della relazione*  $\varrho$ . Il suo esame ci permette di individuare quali sono gli elementi che sono in relazione. Sia per esempio  $A = \{2, 4, 6, 8\}$  e  $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$  e sia  $\varrho$  la relazione da  $A$  a  $B$  che associa ad ogni elemento di  $A$  la sua metà. Risulta

$$\varrho = \{(2, 1), (4, 2), (6, 3), (8, 4)\} \subset A \times B,$$

quindi si tratta effettivamente di una relazione da  $A$  a  $B$  e la matrice di questa relazione è:

$\varrho$	1	2	3	4	5	6	7	8
2	1	0	0	0	0	0	0	0
4	0	1	0	0	0	0	0	0
6	0	0	1	0	0	0	0	0
8	0	0	0	1	0	0	0	0

Data una relazione  $\varrho$  da  $A$  a  $B$  si può parlare di *relazione inversa*.

**DEFINIZIONE 1.16** Se  $\varrho$  è una relazione da  $A$  a  $B$ , la *relazione inversa*  $\varrho^{-1}$  è la relazione da  $B$  ad  $A$  definita da

$$b\varrho^{-1}a \iff a\varrho b.$$

#### Esempio 1.14

Sia  $\varrho$  la relazione di cui sopra, ossia la relazione da  $A = \{2, 4, 6, 8\}$  a  $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$  data da

$$\varrho = \{(2, 1), (4, 2), (6, 3), (8, 4)\}.$$

La relazione inversa è la relazione da  $B$  ad  $A$  data da

$$\varrho^{-1} = \{(1, 2), (2, 4), (3, 6), (4, 8)\}.$$

**OSSERVAZIONE** Si noti che l'inversa di una relazione è *sempre* una relazione ed esiste sempre. Si tenga presente questa osservazione per il futuro, quando parleremo di funzioni.

La nozione di relazione è troppo generale perché possa essere di qualche utilità. È necessario restringere tale nozione imponendo delle condizioni. Noi studieremo tre tipi di relazioni nei prossimi paragrafi: *funzioni (o applicazioni)*, *relazioni d'ordine* e *relazioni di equivalenza*.

#### Esercizi

Decidere se l'insieme  $\{(a, a^2 - 7) \mid a \in \mathbb{N}\}$  rappresenta o no una relazione di  $\mathbb{N}$  in sé.

Decidere se  $\{|x|, x^3 \mid x \in \mathbb{R}\}$  rappresenta una relazione da  $\mathbb{R}$  in  $\mathbb{R}$ .

## ■ 5. FUNZIONI

Introduremo ora una nozione che tutti hanno senza dubbio già incontrato: la nozione di funzione (o applicazione): essa è un particolare tipo di relazione da  $A$  a  $B$ .

**DEFINIZIONE 1.17** Una *funzione* (o *applicazione*)  $f$  da un insieme  $A$  ad un insieme  $B$  è una relazione da  $A$  a  $B$  nella quale ogni elemento di  $A$  appare una e una sola volta come primo elemento di una coppia ordinata della relazione. ■

Si scrive

$$f: A \longrightarrow B.$$

Trattandosi di una particolare relazione, anche qui l'insieme  $A$  dicesi *dominio* della funzione  $f$ , l'insieme  $B$  *codominio* di  $f$ , e l'elemento  $b = f(a)$  si dice l'*immagine* di  $a$  mediante la  $f$ . Il sottoinsieme  $\{(a, f(a)) \mid a \in A\} \subseteq A \times B$  che definisce la funzione  $f$  prende anche il nome di *grafico* della funzione  $f$ : per essere il grafico di una *funzione* da  $A$  a  $B$  pertanto, un sottoinsieme  $F$  di  $A \times B$  (ossia una relazione da  $A$  a  $B$ ) deve essere tale che *ogni* elemento di  $A$  compaia come primo elemento di *una e una sola* coppia di  $F$ .

Si può pensare ad una funzione  $f$  come ad una *legge* che associa ad *ogni* elemento di  $A$  *uno e un solo* elemento di  $B$ .

Mentre, come si è visto, ogni funzione è una relazione, non ogni relazione è una funzione.

Per esempio, la relazione del punto (a) dell'esempio 1.13 non è una funzione dall'insieme  $A$  di tutte le città italiane a  $\mathbb{Q}$ , perché non tutte le città italiane hanno un aeroporto, quindi non è vero che da ogni città italiana parte un aereo.

Diamo qui di seguito alcuni esempi di funzioni:

1. La funzione da  $\mathbb{R}$  in  $\mathbb{R}$  definita ponendo

$$f(x) = x^4 + 1 \quad \forall x \in \mathbb{R}.$$

Il grafico è il sottoinsieme di  $\mathbb{R} \times \mathbb{R}$   $\{(x, x^4 + 1) \mid x \in \mathbb{R}\}$ .

2. La funzione  $f: \mathbb{R} \longrightarrow \mathbb{Z}$  definita ponendo

$$f(x) = [x] \quad \forall x \in \mathbb{R},$$

dove con  $[x]$  si denota la *parte intera di*  $x$ , ossia  $[x]$  rappresenta il più grande intero minore o uguale a  $x$ . In altre parole,  $[x]$  rappresenta l'intero  $a$  tale che  $a \leq x < a + 1$ . Per esempio  $[2,9] = 2$ ,  $[-8] = -8$ ,  $[-8,4] = -9$ . Il grafico di questa funzione è dato in figura 1.2.

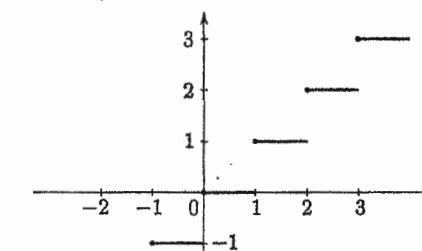


Figura 1.2. La funzione  $[x]$ .

3. La funzione  $f : \mathbb{R} \rightarrow \mathbb{Z}$  definita ponendo

$$f(x) = \lceil x \rceil \quad \forall x \in \mathbb{R},$$

dove con  $\lceil x \rceil$  si denota il più piccolo intero maggiore o uguale a  $x$ .

Quindi  $\lceil 2,9 \rceil = 3$ ,  $\lceil -5,6 \rceil = -5$ , ecc.

Il grafico di questa funzione è dato in figura 1.3.

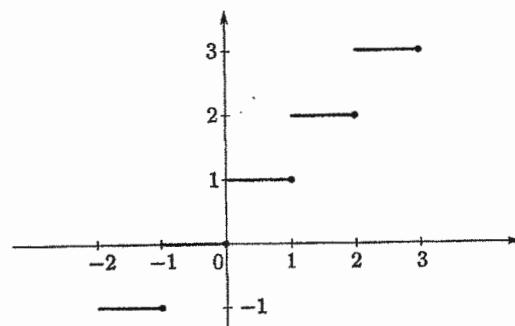


Figura 1.3. La funzione  $\lceil x \rceil$ .

Il grafico di una funzione potrà quindi essere come quello della figura 1.4 ma non come quello della figura 1.5.

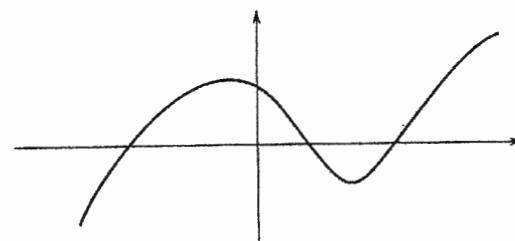


Figura 1.4.

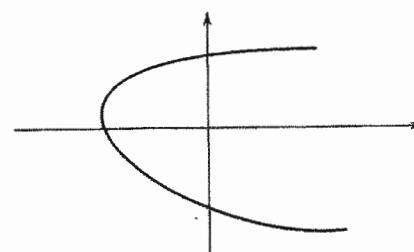


Figura 1.5.

Sia  $f$  una funzione da  $A$  ad  $A'$ , e siano  $S$  e  $T$  due sottoinsiemi di  $A$  e  $A'$  rispettivamente. L'*immagine*  $f(S)$  di  $S$  mediante  $f$  è il sottoinsieme

$$f(S) := \{b \in A' \mid b = f(s) \text{ per qualche } s \in S\}.$$

L'*immagine*  $f(A)$  si indica anche con  $\text{Im } f$ .

L'*immagine inversa* o *controimmagine* di  $T$  mediante la  $f$  è il sottoinsieme

$$f^{-1}(T) := \{a \in A \mid f(a) \in T\}.$$

Nel caso in cui  $T$  sia ridotto ad un solo elemento  $t$ , cioè sia  $T = \{t\}$ , spesso anziché  $f^{-1}(\{t\})$  scriveremo  $f^{-1}(t)$ .

**DEFINIZIONE 1.18** Una funzione  $f$  da  $A$  ad  $A'$  si dice *iniettiva* se elementi distinti di  $A$  hanno immagini distinte in  $A'$ , ossia se

$$\forall a, b \in A \quad a \neq b \implies f(a) \neq f(b)$$

o, in forma equivalente,

$$\forall a, b \in A \quad f(a) = f(b) \implies a = b.$$

In altre parole, un'applicazione iniettiva è tale che la controimmagine di ogni elemento di  $A'$  o è ridotta al sottoinsieme vuoto  $\emptyset$  o ad un solo elemento. In modo espressivo si può dire che un'applicazione è iniettiva quando frecce che partono da punti distinti non colpiscono mai uno stesso bersaglio.

#### Esempio 1.15

La  $f : \mathbb{N} \rightarrow \mathbb{N}$  definita ponendo  $f(x) = 2x + 5 \quad \forall x \in \mathbb{N}$  è iniettiva perché se  $2x_1 + 5 = 2x_2 + 5$ , allora  $2x_1 = 2x_2$ , da cui  $x_1 = x_2$ .

Invece la  $f : \mathbb{R} \rightarrow \mathbb{R}$  data da  $f(x) = x^2$  non è iniettiva, perché per esempio  $f^{-1}(\{3\}) = \{\pm\sqrt{3}\}$ .

**DEFINIZIONE 1.19** Una funzione  $f$  da  $A$  ad  $A'$  si dice *suriettiva* se  $\text{Im } f = A'$ , ossia se per ogni  $a' \in A'$  esiste un  $a \in A$  tale che  $f(a) = a'$ .

Per restare nel linguaggio delle frecce, un'applicazione è suriettiva quando ogni elemento del codominio è colpito da almeno una freccia.

**Esempio 1.16**

La funzione  $f : \mathbb{R} \rightarrow \mathbb{R}$  data  $\forall x \in \mathbb{R}$  da  $f(x) = x^3 - 2$  è suriettiva, perché  $\forall r \in \mathbb{R}$  esiste un  $\bar{x} \in \mathbb{R}$  tale che  $f(\bar{x}) = r$ : basta prendere  $\bar{x} = \sqrt[3]{r+2}$ : infatti  $f(\sqrt[3]{r+2}) = r + 2 - 2 = r$ .

La funzione da  $\mathbb{R}$  in  $\mathbb{R}$  definita da  $f(x) = x^2 \forall x \in \mathbb{R}$  non è suriettiva, perché l'immagine di  $f$  è costituita dai soli reali maggiori o uguali a zero.

**DEFINIZIONE 1.20** Una funzione  $f$  da  $A$  ad  $A'$  si dice *biiettiva* (o *biunivoca*) se è contemporaneamente iniettiva e suriettiva. ■

**DEFINIZIONE 1.21** Date due funzioni  $f : A \rightarrow B$  e  $g : B \rightarrow C$ , si definisce *funzione composta* di  $f$  con  $g$ , e si indica con  $g \circ f$ , la funzione:

$$g \circ f : A \longrightarrow C$$

data da

$$(g \circ f)(a) := g(f(a)) \quad \forall a \in A. \quad \blacksquare$$

**Esempio 1.17**

Siano  $A = B = C = \mathbb{Z}$ . Sia  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  data da  $f(x) = x^2 + 5$ , e sia  $g : \mathbb{Z} \rightarrow \mathbb{Z}$  data da  $g(x) = 2 + 3x$ . Allora

$$(g \circ f)(x) = g(f(x)) = g(x^2 + 5) = 2 + 3(x^2 + 5) = 3x^2 + 17.$$

**OSSERVAZIONE** Se il codominio di  $g$  non coincide con il dominio di  $f$ , non ha senso considerare l'applicazione composta  $f \circ g$ .

Nel nostro caso ha senso calcolare anche  $f \circ g$ :

$$(f \circ g)(x) = f(g(x)) = f(2 + 3x) = (2 + 3x)^2 + 5 = 9x^2 + 12x + 9.$$

da cui risulta che  $g \circ f \neq f \circ g$ : infatti per esempio  $(g \circ f)(0) = 17$  mentre  $(f \circ g)(0) = 9$ .

L'operazione di composizione tra applicazioni non è quindi commutativa: tuttavia è *associativa*, nel senso che se  $f$ ,  $g$  e  $h$  sono applicazioni rispettivamente da  $A$  a  $B$ , da  $B$  a  $C$  e da  $C$  a  $D$ , allora risulta (cfr. eserc. 42)  $h \circ (g \circ f) = (h \circ g) \circ f$ .

**OSSERVAZIONE** Si è visto che *ogni* relazione  $\varrho$  da  $A$  a  $B$  determina una relazione inversa da  $B$  ad  $A$ . Questo non vale per le funzioni, perché la relazione inversa di una funzione in genere non è una funzione. Tuttavia, nel caso in cui  $f$  sia un'applicazione *biiettiva* da  $A$  a  $B$ , allora l'immagine inversa di *ogni* singleton  $\{b\}$  di  $B$ ,  $f^{-1}(\{b\})$ , è un singleton,  $\{a\}$ , dove  $a$  è quell'*unico* elemento tale che  $f(a) = b$ . Ogni applicazione *biiettiva*  $f$  da  $A$  a  $B$  determina quindi una (unica) *applicazione* da  $B$  ad  $A$ , che si indica con  $f^{-1}$ , e che prende il nome di *applicazione inversa* della  $f$ , definita, per ogni  $b \in B$ , da

$$f^{-1}(b) := a$$

dove  $a$  è quell'*unico* elemento  $\in A$  tale che  $f(a) = b$ .

L'applicazione  $i_X$  da  $X$  in  $X$  tale che

$$i_X(x) = x \quad \forall x \in X$$

prende il nome di *applicazione identica* di  $X$ .

Se  $f$  è un'applicazione biiettiva da  $A$  a  $B$ , allora risulta

$$f^{-1} \circ f = i_A, \quad f \circ f^{-1} = i_B.$$

Ricordiamo (cfr. par. 2) come abbiano rappresentato i sottoinsiemi. Tale rappresentazione è strettamente legata alla nozione di funzione, come proviamo ora.

**DEFINIZIONE 1.22** Sia  $A$  un sottoinsieme di  $X$  e sia  $2 := \{0, 1\}$ . Si dice *funzione caratteristica* di  $A$  la funzione  $\chi_A : X \rightarrow 2$  definita: da:

$$\chi_A(x) = \begin{cases} 0 & \text{se } x \in X \setminus A \\ 1 & \text{se } x \in A. \end{cases} \quad \blacksquare$$

Per esempio, se  $X = \{a, b, c, d, e, f, g, h\}$  e  $A = \{d, f, g, h\}$ , allora

$$\begin{aligned} \chi_A : X &\longrightarrow 2 \\ a &\longrightarrow 0 \\ b &\longrightarrow 0 \\ c &\longrightarrow 0 \\ d &\longrightarrow 1 \\ e &\longrightarrow 0 \\ f &\longrightarrow 1 \\ g &\longrightarrow 1 \\ h &\longrightarrow 1. \end{aligned}$$

Viceversa, *ogni* funzione da  $X$  a  $2 := \{0, 1\}$  è la funzione caratteristica di uno e un solo sottoinsieme  $A$  di  $X$ : il sottoinsieme  $A = f^{-1}(\{1\})$ . Nel caso della funzione appena vista, la controimmagine di  $\{1\}$  è esattamente il sottoinsieme  $A = \{d, f, g, h\}$ . In questo senso si parla di funzione *caratteristica* di un sottoinsieme. In definitiva, si ha il seguente risultato.

**TEOREMA 1.1** Sia  $X$  un insieme e sia  $2 := \{0, 1\}$ . Esiste una corrispondenza biunivoca tra  $\mathcal{P}(X)$  e l'insieme  $2^X$  di tutte le funzioni da  $X$  a  $\{0, 1\}$ .

**Esercizi**

● Siano  $A = \{a, b, c\}$ ,  $B = \{0, 1\}$ . Si determinino tutte le funzioni da  $A$  a  $B$  e quelle da  $B$  ad  $A$ . Quali tra queste sono suriettive, quali iniettive, quali biiettive?

● Siano  $f$  e  $g$  due funzioni entrambe iniettive (suriettive) rispettivamente da  $A$  a  $B$  e da  $B$  a  $C$ . Si provi che  $g \circ f$  è anch'essa iniettiva (suriettiva). Se ne deduca che la composizione di due applicazioni biiettive è biiettiva.

Posto  $A = B = \mathbb{Z}$ , si dica quali delle seguenti relazioni sono grafici di applicazioni:

- $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x + y = 3\}$ .
- $\{(x, 6) \mid x \in \mathbb{Z}\}$ .
- $\{(0, y) \mid y \in \mathbb{Z}\}$ .
- $\{(x, (x - 2)^2) \mid x \in \mathbb{Z}\}$ .
- $\{(x, x - 1) \mid x \in \mathbb{Z}\}$ .
- $\{(x, |x|) \mid x \in \mathbb{Z}\}$ .
- $\{|x|, x \mid x \in \mathbb{Z}\}$ .

Di ciascuna delle relazioni precedenti che sono applicazioni si determini l'immagine, e si dica se è iniettiva e/o suriettiva. Nel caso in cui una sia biettiva si determini l'inversa.

Si consideri la funzione da  $\mathbb{R}$  in  $\mathbb{R}$   $f(x) = x^5 + 3x^4 - 2x^3 + x + 1$ . Provare che si tratta di un funzione suriettiva.

Sia  $f$  un'applicazione tra  $A$  e  $A'$ . Indicati con  $X$  e  $Y$  sottoinsiemi di  $A$  e con  $X'$ ,  $Y'$  sottoinsiemi di  $A'$ , si provino le seguenti uguaglianze o inclusioni:

- $f(X \cup Y) = f(X) \cup f(Y)$ .
- $f(X \cap Y) \subseteq f(X) \cap f(Y)$ .
- $f^{-1}(X' \cup Y') = f^{-1}(X') \cup f^{-1}(Y')$ .
- $f^{-1}(X' \cap Y') = f^{-1}(X') \cap f^{-1}(Y')$ .

Si diano esempi che provino che nel punto b. può valere l'inclusione propria.

Si consideri il sottoinsieme  $\{(a, 3(a - 1)^2) \mid a \in \mathbb{Z}\}$  di  $\mathbb{Z} \times \mathbb{Z}$ .

- Decidere se si tratta di una relazione da  $\mathbb{Z}$  in  $\mathbb{N}$ .
- Decidere se si tratta di una funzione da  $\mathbb{Z}$  in  $\mathbb{N}$ .
- Determinare  $f(0)$  e  $f(2)$ .
- Determinare la controimmagine di  $\{0\}$ , la controimmagine di  $\{30\}$  e la controimmagine di  $\{108\}$ .
- Decidere se si tratta di una funzione iniettiva.
- Decidere se è suriettiva.

Si considerino i due insiemi  $A = \{a, b, c, d\}$  e  $B = \{x \in \mathbb{N} \mid x^2 - 3x - 4 < 0\}$ .

Decidere se le seguenti sono funzioni da  $A$  a  $B$ . Per quelle che sono funzioni, decidere se sono iniettive, suriettive o entrambe:

- $\{(a, 0), (b, 0), (c, 2), (d, -1)\}$ .
- $\{(a, 0), (c, 0), (b, 0)\}$ .
- $\{(d, 2), (a, 2), (b, 1), (c, 0)\}$ .

Si considerino gli insiemi  $A = \{1, 2, 3, 4\}$  e  $B = \{3, 4, 5, 6, 7\}$ .

- Quante funzioni esistono da  $A \cap B$  ad  $A \cup B$ ?
- Esiste una funzione iniettiva da  $A \cap B$  ad  $A \cup B$ ? Se sì, determinarne esplicitamente almeno una.
- Esiste una funzione suriettiva da  $A \cap B$  ad  $A \cup B$ ? Se sì, determinarne esplicitamente almeno una.

Sia  $A = \{1, 2, 3, 4, 5\}$ .

Si consideri il sottoinsieme di  $A \times A$   $\{(1, 1), (2, 1), (3, 4), (4, 5), (5, 1)\}$ .

- Decidere se si tratta di una funzione, che indichiamo con  $f$ .
- Determinare  $f(3)$ .
- Determinare la controimmagine di  $\{2\}$  e la controimmagine di  $\{1\}$ , ossia  $f^{-1}(\{2\})$  e  $f^{-1}(\{1\})$ .
- Dire se  $f$  è iniettiva.
- Dire se  $f$  è suriettiva.

Siano  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  e  $g : \mathbb{Z} \rightarrow \mathbb{Z}$  le applicazioni definite da  $f(x) = 2x$  e  $g(x) = x^2$ ; si determinino  $f \circ g$  e  $g \circ f$ .

Siano  $f$ ,  $g$  e  $h$  applicazioni rispettivamente da  $A$  a  $B$ , da  $B$  a  $C$  e da  $C$  a  $D$ . Si provi che  $h \circ (g \circ f) = (h \circ g) \circ f$ .

Quali di queste sono applicazioni suriettive, iniettive, biettive:

$$\begin{array}{lll} \phi_1 : \mathbb{R} \longrightarrow \mathbb{R} & \phi_2 : \mathbb{Z} \longrightarrow \mathbb{Z} & \phi_3 : \mathbb{Q} \longrightarrow \mathbb{Q} \\ x \longrightarrow x^3; & x \longrightarrow 5x; & x \longrightarrow x^3; \\ \phi_4 : \mathbb{Q} \longrightarrow \mathbb{Q} & \phi_5 : \mathbb{R} \longrightarrow \mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\} & \phi_6 : \mathbb{R}_+ \longrightarrow \mathbb{R}_+ \\ x \longrightarrow 5x; & x \longrightarrow x^2; & x \longrightarrow x^2; \\ \phi_7 : \mathbb{R}_+ \longrightarrow \mathbb{R} & & \\ x \longrightarrow x^3. & & \end{array}$$

Decidere se la funzione  $f(x) = [x] \forall x \in \mathbb{R}$ , è iniettiva e/o suriettiva. Si ricorda che  $[x]$  rappresenta il più grande intero minore o uguale a  $x$ .

Provare che, se  $x$  non è un intero, allora  $[x] = [x] + 1$ , mentre se  $x$  è un intero,  $[x] = [x]$  ( $[x]$  rappresenta il più piccolo intero maggiore o uguale a  $x$ ).

## 6 RELAZIONI D'ORDINE

Un importante esempio di relazione è dato dalle relazioni d'ordine.

**DEFINIZIONE 1.23** Una relazione  $\rho$  definita su un insieme  $A$  si dice *relazione d'ordine parziale* se verifica le seguenti proprietà:

- Proprietà riflessiva* :  $\forall a \in A \quad a \rho a$ .
- Proprietà antisimmetrica* :  $\forall a, b \in A \quad [a \rho b \wedge b \rho a] \implies a = b$ .
- Proprietà transitiva* :  $\forall a, b, c \in A \quad [a \rho b \wedge b \rho c] \implies a \rho c$ .

Una relazione d'ordine parziale si indica spesso con il simbolo  $\preccurlyeq$ .

**DEFINIZIONE 1.24** Un insieme non vuoto  $X$  si dice *insieme parzialmente ordinato* se è definita su  $X$  una relazione d'ordine parziale  $\preccurlyeq$ , e si scrive  $(X, \preccurlyeq)$ . ■

L'aggettivo *parziale* nella definizione di relazione d'ordine sta a significare che non si richiede che tutte le coppie  $(a, b)$  di elementi di un insieme  $A$  siano tra loro confrontabili, siano tali cioè che  $a \preccurlyeq b$  o  $b \preccurlyeq a$  per ogni  $a, b \in A$ . Se avviene che *tutte* le coppie sono confrontabili si dice che l'insieme è *totalmente ordinato* o una *catena*.

### Esempio 1.18

Esempi di relazioni di ordine.

(a) Nell'insieme  $\mathcal{P}(X)$  la relazione

$$A \preccurlyeq B \iff A \subseteq B.$$

(b) Nell'insieme  $\mathbb{N}$  l'ordinamento "naturale"  $\leq$ , quello cioè per cui  $a \leq b$  se e solo se esiste un  $c \in \mathbb{N}$  tale che  $b = a + c$ , è una relazione d'ordine.

(c) La relazione definita su  $\mathbb{N}$  che per ogni  $a, b \in \mathbb{N}$  dichiara  $a \preccurlyeq b$  se e solo se  $b$  è un multiplo di  $a$ , ossia se e solo se esiste  $c \in \mathbb{N}$  tale che sia  $b = ac$ .

Si noti che la relazione  $\subseteq$  su  $\mathcal{P}(X)$  è un ordinamento *parziale*, mentre la relazione  $\leq$  è un ordinamento *totale* su  $\mathbb{N}$ .

Nel caso in cui l'insieme  $A$  parzialmente (o totalmente) ordinato sia finito possiamo rappresentarlo graficamente congiungendo fra loro con una linea spezzata due elementi  $a$  e  $b$  dal basso verso l'alto se e solo se risulta  $a \preccurlyeq b$ . Tale linea spezzata si ridurrà ad un segmento di estremi  $a$  e  $b$  se non esistono elementi intermedi  $c$  tali che  $a \preccurlyeq c \preccurlyeq b$ . Per esempio, sia  $A = \mathcal{P}(X)$  dove  $X = \{1, 2, 3\}$  e lo si consideri ordinato rispetto alla relazione  $\subseteq$ . Allora

$$\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

e la sua rappresentazione grafica è data dalla figura 1.6.

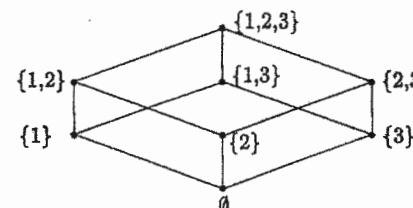


Figura 1.6. L'insieme delle parti di un insieme con 3 elementi.

La rappresentazione grafica di una relazione d'ordine totale è data in figura 1.7.



Figura 1.7. Rappresentazione grafica di una catena.

Da questa figura ci si rende conto facilmente che due insiemi totalmente ordinati finiti con lo stesso numero di elementi  $(X_1, \preccurlyeq_1)$  e  $(X_2, \preccurlyeq_2)$  sono *isomorfi*, ossia esiste una corrispondenza biunivoca  $\varphi$  tra  $X_1$  e  $X_2$  che conserva gli ordinamenti, cioè è tale che

$$\forall x_1, x'_1 \in X_1 \quad x_1 \preccurlyeq_1 x'_1 \implies \varphi(x_1) \preccurlyeq_2 \varphi(x'_1).$$

Torneremo a parlare di relazioni d'ordine nel capitolo 9.

### Esercizi

1) Provare che le relazioni  $\supseteq$  in  $\mathcal{P}(X)$  e  $\geq$  in  $\mathbb{N}$  sono ancora relazioni d'ordine parziale, inverse rispettivamente della  $\subseteq$  e della  $\leq$ .

2) Sia  $\mathcal{P}$  l'insieme costituito da tutti i sottoinsiemi non vuoti di  $\mathbb{N}$  (cioè  $\mathcal{P} = \mathcal{P}(\mathbb{N}) \setminus \emptyset$ ). Si consideri la seguente relazione definita su  $\mathcal{P}$ :

$$A \leq B \iff A = B \text{ oppure } a \leq b \ \forall a \in A, b \in B.$$

- Provare che si tratta di una relazione d'ordine.
- Decidere se si tratta di una relazione d'ordine totale.

3) Trovare esempi di relazioni che *non* sono relazioni d'ordine.

4) Sia  $X = \{1, 2, 3\}$ . Determinare il numero di relazioni d'ordine parziale diverse che si possono definire su  $X$ . Di questi quante sono di ordine totale?

5) Sia  $\varrho$  la relazione su  $\mathbb{Z}$  definita al modo seguente per ogni  $a, b \in \mathbb{Z}$ :

$$a \varrho b \iff \exists c \in \mathbb{Z} \mid b = ac.$$

Si dica se si tratta di una relazione d'ordine.

## 7 RELAZIONI DI EQUIVALENZA

Tra tutte le relazioni definite su di un insieme, quelle che andiamo ora a studiare sono senza dubbio le più importanti.

**DEFINIZIONE 1.25** Una relazione  $\rho$  definita su un insieme  $A$  si dice *relazione di equivalenza* se verifica le seguenti proprietà:

1. *Proprietà riflessiva*:  $\forall a \in A \quad a \rho a$ .
2. *Proprietà simmetrica*:  $\forall a, b \in A \quad a \rho b \implies b \rho a$ .
3. *Proprietà transitiva*:  $\forall a, b, c \in A \quad [a \rho b \wedge b \rho c] \implies a \rho c$ .

Se  $\rho$  è una relazione di equivalenza e  $a \rho b$ , allora si dice che  $a$  è *equivalente a*  $b$ . ■■■

### Esempio 1.19

Esempi di relazioni di equivalenza.

- (a) La relazione di *uguaglianza* definita su un insieme  $A$ .
- (b) La relazione  $\rho$  definita su un insieme  $A$ , che dichiara in relazione tutti gli elementi, ossia  $a \rho b \quad \forall a, b \in A$ .
- (c) La relazione di avere la stessa altezza definita su un insieme  $A$  di persone.
- (d) La relazione di *parallelismo* definita nell'insieme  $A$  di tutte le rette del piano.
- (e) La relazione definita su  $\mathbb{Z}$  che dichiara in relazione due interi  $a$  e  $b$  se e solo se  $a^2 = b^2$ .

Qui di seguito elenchiamo alcuni esempi di relazioni che invece non sono di equivalenza perché non soddisfano tutte le proprietà richieste.

### Esempio 1.20

Esempi di relazioni che non sono di equivalenza.

- (1) La relazione  $\subseteq$  definita su un insieme  $X$ : non vale la proprietà simmetrica.
- (2) La relazione di essere *cugino*, definita su un insieme  $A$  di persone; non vale né la proprietà riflessiva né la proprietà transitiva.
- (3) Se  $A = \{a, b, c, d\}$ , la relazione  $\rho = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, c), (a, c)\}$  non è di equivalenza perché non vale la proprietà simmetrica.
- (4) La relazione di *perpendicolarità* definita sull'insieme  $A$  di tutte le rette del piano. Non vale né la proprietà riflessiva né la transitiva.

**DEFINIZIONE 1.26** Sia  $\rho$  una relazione di equivalenza definita su  $A$ . Si definisce *classe di equivalenza modulo  $\rho$*  di un elemento  $a \in A$ , e si denota con  $[a]$  o con  $\bar{a}$ , l'insieme di tutti gli elementi di  $A$  che sono equivalenti ad  $a$ , ossia

$$[a] \stackrel{\text{def}}{=} \{x \in A \mid x \rho a\}.$$

Riprendendo i cinque esempi di relazioni di equivalenza dati sopra,

- (a) Le classi di equivalenza sono costituite dai *singletons* (cioè dai sottoinsiemi ridotti ad un solo elemento)  $\{a\}$  al variare di  $a \in A$ . In questo esempio (uguaglianza) non identifichiamo nulla: due elementi vengono identificati solo se sono uguali.
- (b) Esiste un'unica classe di equivalenza, data dall'intero insieme  $A$ . Qui stiamo identificando tutto.
- (c) In ogni classe di equivalenza ci sono tutte e sole le persone che hanno la stessa altezza: ogni classe può quindi essere *etichettata* con il numero corrispondente all'altezza comune a tutte le persone che appartengono a quella classe.
- (d) Una classe  $[r]$  è costituita da tutte le rette che sono parallele a  $r$ . In questo caso quello che accomuna tutti gli elementi di una stessa classe è la comune *direzione*.
- (e) Una classe  $[a]$  è costituita da  $\pm a$ : quindi ogni classe possiede due elementi, ad eccezione della classe  $[0]$  che consiste del solo 0.

Sussiste la seguente proposizione:

**PROPOSIZIONE 1.1** Sia  $\rho$  una relazione di equivalenza definita su un insieme  $A$ . Allora,  $[a] = [b] \iff a \rho b$ .

**DIMOSTRAZIONE.** Sia  $[a] = [b]$ . Per la riflessività di  $\rho$ ,  $\forall b \in A \in b \rho b$ , onde  $b \in [b]$ . Essendo per ipotesi  $[a] = [b]$ , segue che  $b \in [a]$ , da cui, per definizione di classe di equivalenza,  $b \rho a$  e, per la simmetria,  $a \rho b$ .

Viceversa, si supponga  $a \rho b$ . Faremo vedere la doppia inclusione  $[a] \subseteq [b]$  e  $[b] \subseteq [a]$ . Sia  $c \in [a]$ . Allora  $a \rho c$ . Quest'ultima relazione, assieme alla  $b \rho a$  implicano (transitività)  $b \rho c$  e quindi (per definizione di  $[b]$ ),  $c \in [b]$ . Abbiamo dimostrato che  $[a] \subseteq [b]$ . La dimostrazione dell'altra inclusione è analoga (scambiando il ruolo di  $a$  e  $b$ ). Quindi  $[a] = [b]$ . ♦

In definitiva, la proposizione precedente mostra come il passaggio dagli *elementi* di  $A$  alle *classi di equivalenza* di  $A$  trasforma la *equivalenza* (tra elementi) in *uguaglianza* (tra classi). Le proprietà di riflessività, simmetria e transitività, proprie delle relazioni di equivalenza, caratterizzano quindi oggetti che *non sono* (necessariamente) uguali, ma che tali possono *venir considerati* limitatamente a particolari scopi.

**OSSERVAZIONE** Si osservi come nella proposizione precedente abbiamo utilizzato *tutte* le proprietà della relazione di equivalenza.

**DEFINIZIONE 1.27** Sia  $\rho$  una relazione di equivalenza definita su un insieme  $A$ . Si definisce *insieme quoziente* di  $A$  rispetto a  $\rho$ , e si indica con  $A/\rho$ , l'insieme di tutte le classi di equivalenza modulo  $\rho$ . In simboli,

$$A/\rho \stackrel{\text{def}}{=} \{[a] \mid a \in A\}.$$

La proposizione precedente dice che elementi  $a$  che erano *equivalenti* in  $A$  si trasformano in un unico elemento,  $[a]$ , di  $A/\rho$ .

La definizione che ora daremo è strettamente legata alla nozione di relazione di equivalenza: anzi, come mostreremo nei due teoremi che seguono, parlare di partizione di un insieme o di relazione di equivalenza sull'insieme è esattamente la stessa cosa.

**DEFINIZIONE 1.28** Dicesi *partizione* di un insieme  $A$  una collezione di parti (o sottoinsiemi)  $A_\alpha$  non vuoti di  $A$  tali che:

1.  $\bigcup_\alpha A_\alpha = A$  (le parti *ricoprono*  $A$ );

2.  $A_\alpha \cap A_\beta \neq \emptyset \iff A_\alpha = A_\beta$  (le parti *o coincidono o sono disgiunte*).  $\blacksquare$

Una partizione di un insieme  $A$  è quindi un insieme  $\mathcal{P}$  di sottoinsiemi non vuoti di  $A$  tali che ogni elemento di  $A$  appartiene ad uno e un solo dei sottoinsiemi dati.

**TEOREMA 1.2** Sia  $\rho$  una relazione di equivalenza in  $A$ . Le classi di equivalenza di  $A$  modulo  $\rho$  costituiscono una partizione di  $A$ .

**DIMOSTRAZIONE.** (1) Ricoprono  $A$ : infatti, essendo  $a\rho a$  per ogni  $a \in A$ , ogni  $a \in A$  appartiene alla sua classe di equivalenza.

(2) Le classi di equivalenza *o coincidono o sono disgiunte*: sia  $x \in [a] \cap [b]$ , cioè siano  $[a]$  e  $[b]$  non disgiunte. Allora  $x\rho a$  e  $x\rho b$ , da cui, per simmetria e transitività,  $a\rho b$ . In base alla Proposizione 1.1,  $[a] = [b]$ , ossia le due classi coincidono.  $\diamond$

**TEOREMA 1.3** Ogni partizione di un insieme  $A$  determina su  $A$  una relazione di equivalenza, per la quale i sottoinsiemi della partizione sono le classi di equivalenza.

**DIMOSTRAZIONE.** Indicati con  $A_\alpha$  i sottoinsiemi della partizione, basta definire la seguente relazione, che si verifica immediatamente essere di equivalenza:  $a\rho b \iff \exists A_\alpha \mid a, b \in A_\alpha$ . Le classi di equivalenza sono le parti  $A_\alpha$ .  $\diamond$

### Esercizi

• Fissato  $n \in \mathbb{N}$ , sia  $\rho$  la seguente relazione definita su  $\mathbb{Z}$ :

$$a\rho b \pmod{n} \iff a - b = kn, k \text{ intero.}$$

Si provi che  $\rho$  è una relazione di equivalenza. Si studino le classi di equivalenza. Tale relazione prende il nome di *congruenza modulo n*, e si indica col simbolo  $\equiv_n$ . Si esamini in dettaglio il caso  $n = 4$ .

• Si provi che le condizioni che definiscono una relazione di equivalenza sono indipendenti, dando

- a. Un esempio di relazione riflessiva e simmetrica, ma non transitiva.
- b. Un esempio di relazione riflessiva e transitiva, ma non simmetrica.
- c. Un esempio di relazione simmetrica e transitiva, ma non riflessiva.

• Dato un insieme  $X$ , si consideri la relazione  $\sim$  in  $\mathcal{P}(X)$  definita da:

$$A \sim B \iff A \text{ e } B \text{ hanno lo stesso numero di elementi.}$$

**N.B.** Come avremo modo di vedere nel paragrafo 1 del capitolo 4, due insiemi "hanno lo stesso numero di elementi" se e solo se esiste tra di loro una corrispondenza biunivoca. In tal caso si dice che i due insiemi *hanno la stessa cardinalità* o la stessa *potenza*.

- a. Dimostrare che si tratta di una relazione di equivalenza e descrivere il quoziente  $\mathcal{P}(X)/\sim$ .
- b. Se  $X$  ha  $n$  elementi, dire quanti elementi ha  $\mathcal{P}(X)/\sim$ .

• Indicato con  $|n|$  il *valore assoluto* dell'intero  $n$ , ossia

$$|n| = \begin{cases} n & \text{se } n \geq 0 \\ -n & \text{se } n < 0 \end{cases}$$

si consideri la relazione  $\rho$  su  $\mathbb{Z}$  definita da

$$m\rho n \iff |m| = |n|.$$

Dimostrare che  $\rho$  è una relazione di equivalenza e determinare  $\mathbb{Z}/\rho$ .

• Si consideri la relazione  $\rho$  su  $\mathbb{R}^2$  definita da:

$$(x, y) \rho (\bar{x}, \bar{y}) \iff x^2 + y^2 = \bar{x}^2 + \bar{y}^2.$$

Dimostrare che  $\rho$  è una relazione di equivalenza e descrivere  $\mathbb{R}^2/\rho$ .

• Sia  $n \in \mathbb{N}$ , e si consideri la relazione  $\equiv_n$  su  $\mathbb{Z}$  definita da

$$m \equiv_n m' \iff \exists k \in \mathbb{Z} \text{ t.c. } m' = m + kn.$$

Dimostrare che  $\equiv_n$  è una relazione di equivalenza e descrivere  $\mathbb{Z}/\equiv_n$ . Quanti elementi ha  $\mathbb{Z}/\equiv_n$ ?

• Si consideri la relazione  $\sim$  su  $\mathbb{R}$  definita nel modo seguente:

$$x \sim y \iff x - y \in \mathbb{Z}.$$

Dimostrare che  $\sim$  è una relazione di equivalenza e descrivere  $\mathbb{R}/\sim$ .

• Sia  $U$  l'insieme degli articoli in vendita in un negozio. Dimostrare che la relazione

$$xpy \iff \text{il prezzo di } x \text{ differisce dal prezzo di } y \text{ per meno di un euro}$$

è una relazione riflessiva, simmetrica ma non transitiva e che quindi non è una relazione di equivalenza.

• Sia  $A = \{1, 2, 3\}$  e  $\mathcal{P}(A)$  l'insieme delle parti di  $A$ ; su  $\mathcal{P}(A)$  definiamo la relazione  $\rho$  nel modo seguente: se  $a, b \in \mathcal{P}(A)$  allora  $a\rho b$  se e solo se  $a \subseteq b$ .

- a. Verificare che  $\rho$  è una relazione d'ordine.
- b. Si descriva in  $\mathcal{P}(A) \times \mathcal{P}(A)$  il sottoinsieme che la individua.

• Sia  $X$  l'insieme delle rette del piano, e sia  $x$  un fissato punto del piano. Dire se le seguenti sono relazioni di equivalenza su  $X$  e, in caso affermativo, descrivere le classi di equivalenza.

- a.  $r \sim s \iff r$  e  $s$  non sono parallele.

- b.  $r \sim s \iff$  la distanza di  $r$  da  $x$  è uguale a quella di  $s$  da  $x$ .

- c.  $r \sim s \iff r \perp s$ .  
d.  $r \sim s \iff$  la distanza di  $r$  da  $x$  è maggiore o uguale a quella di  $s$  da  $x$ .  
e.  $r \sim s \iff$  sia  $r$  che  $s$  passano per  $x$ .

6 Sia  $\sigma$  una relazione definita su un insieme  $E \neq \emptyset$  tale che soddisfi le seguenti condizioni:

- a.  $a\sigma a \forall a \in E$ .  
b.  $a\sigma b, b\sigma c \implies a\sigma c, \forall a, b, c \in E$ .

Provare che la relazione  $\sim$  in  $E$  definita da:

$$a \sim b \iff a\sigma b \wedge b\sigma a, \forall a, b \in E$$

è una relazione di equivalenza in  $E$ .

7 Siano  $S$  e  $T$  i sottoinsiemi di  $\mathbb{Z}$  definiti al modo seguente:

$$S := \{2n \mid n \in \mathbb{Z}\}, \quad T := \{6n \mid n \in \mathbb{Z}\}$$

e siano  $\rho_1$  e  $\rho_2$  le relazioni su  $\mathbb{Z}$  definite al modo seguente:

$$a\rho_1 b \iff a - b \in S, \quad a\rho_2 b \iff a - b \in T.$$

- a. Provare che  $\rho_1$  e  $\rho_2$  sono relazioni di equivalenza.  
b. Provare che se  $a\rho_2 b$ , allora  $a\rho_1 b$ .  
c. Decidere se  $A = \mathbb{Z}/\rho_1$  e  $B = \mathbb{Z}/\rho_2$  hanno un numero infinito o finito di elementi e nel caso in cui il numero sia finito dire quanto vale.

8 Se  $A$  e  $B$  sono gli insiemi quoziente del punto precedente, indicata con  $[x] \in A$  la classe di equivalenza di  $x$  rispetto a  $\rho_1$  e con  $[x] \in B$  la classe di equivalenza di  $x$  rispetto a  $\rho_2$ , dimostrare che la legge che a  $[x]$  associa  $[x]$  è una funzione suriettiva da  $B$  ad  $A$ .

9 Si consideri nell'insieme dei numeri razionali diversi da  $-1$  la seguente relazione

$$a \sim b \iff \frac{1}{(a+1)^2} = \frac{1}{(b+1)^2}.$$

- a. Decidere se si tratta di una relazione di equivalenza.  
b. Studiare l'insieme quoziante.  
c. Nell'insieme  $\mathbb{Z}$  si consideri la relazione  $a \sim b \iff ab > 0$ .  
d. Provare che  $\sim$  non è una relazione di equivalenza.  
e. Determinare un sottoinsieme  $A$  di  $\mathbb{Z}$  sul quale la  $\sim$  sia di equivalenza.  
f. Studiare il quoziante  $A/\sim$ .

10 Sia  $X$  l'insieme di tutte le parole della lingua italiana. Sia  $\rho$  la seguente relazione definita su  $X$ :

$$\forall x, x' \in X \quad x \rho y \iff x \text{ e } x' \text{ cominciano con la stessa lettera.}$$

Provare che si tratta di una relazione di equivalenza. Determinare la cardinalità dell'insieme quoziante.

11 Sull'insieme  $\mathbb{N} = \{0, 1, 2, \dots\}$  dei numeri naturali si definisca la seguente relazione  $\rho$ :  $m \rho n$  se e solo se esiste un numero intero *dispari*  $k \in \mathbb{Z}$  tale che  $m = n2^k$ .

- a. Dire se  $\rho$  è una relazione simmetrica, riflessiva, transitiva, antisimmetrica, d'equivalenza, d'ordine.  
b. Nel caso sia una relazione di equivalenza, dire quali sono le classi di equivalenza che contengono un numero finito di elementi.

12 Sull'insieme  $\mathbb{N} = \{0, 1, 2, \dots\}$  dei numeri naturali si definisca la seguente relazione  $\rho$ :  $m \rho n$  se e solo se esiste un numero intero *pari*  $k \in \mathbb{Z}$  tale che  $m = n2^k$ .

- a. Dire se  $\rho$  è una relazione simmetrica, riflessiva, transitiva, antisimmetrica, d'equivalenza, d'ordine.  
b. Nel caso sia una relazione di equivalenza, dire quali sono le classi di equivalenza che contengono un numero finito di elementi.

13 Sia  $A = \{a, b, c, d, e\}$  e sia  $R \subseteq A \times A$  la relazione su  $A$  definita da

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (b, d), (a, c), (d, b)\}.$$

- a. Dire se  $R$  è riflessiva, simmetrica, antisimmetrica, transitiva su  $A$ .  
b. Verificare che  $R$  non è una relazione di equivalenza su  $A$ .  
c. Verificare che si può ottenere una relazione di equivalenza su  $A$  aggiungendo un unico elemento (cioè una coppia) ad  $R$ .  
d. Sia  $\sigma$  la relazione di equivalenza ottenuta al punto precedente. Quante sono le sue classi di equivalenza? Quanti elementi ha ciascuna classe di equivalenza? Descrivere l'insieme quoziante.

14 Decidere se la seguente relazione  $R$  definita sull'insieme di tutte le stringhe bit

$$xRy \iff x \text{ e } y \text{ contengono lo stesso numero di 1}$$

è una relazione di equivalenza. Nel caso in cui si tratti di una relazione di equivalenza, descrivere la classe della stringa bit 0110111.

15 Su  $\mathbb{Z}$  si definisca la relazione  $\rho$ :  $a\rho b$  se e solo se  $a + b$  è multiplo di 4.

- a.  $\rho$  è transitiva?  
b.  $\rho$  è simmetrica?  
c.  $\rho$  è riflessiva?  
d. Determinare  $\{a \in \mathbb{Z} \mid a\rho 3\}$ . Quanti elementi ha questo insieme?

16 Su  $\mathbb{Z}$  si definisca la relazione  $\rho$ :  $a\rho b$  se e solo se  $a + b$  è multiplo di 6.

- a.  $\rho$  è transitiva?  
b.  $\rho$  è simmetrica?  
c.  $\rho$  è riflessiva?  
d. Determinare  $\{a \in \mathbb{Z} \mid a\rho 3\}$ . Quanti elementi ha questo insieme?

17 Sia  $R$  la relazione su  $\mathbb{N}$  definita da:  $x R y \iff xy = 18$

- a. Descrivere esplicitamente  $R$  come sottoinsieme di  $\mathbb{N} \times \mathbb{N}$ , cioè, descrivere esplicitamente l'insieme  $\{(x, y) \mid x R y\}$ . Si tratta di un insieme finito o infinito?  
b. Dire quali tra le proprietà riflessiva, simmetrica, antisimmetrica o transitiva è verificata.

Sia  $\mathbb{N}^+$  l'insieme dei numeri naturali strettamente positivi, e si definisca  $\rho$  come segue:  $m \rho n$  se e solo se esiste  $k \in \mathbb{Z}$  tale che  $\frac{m}{n} = 2^k$ .

- $\rho$  è una relazione? È una funzione?
- Nel caso  $\rho$  sia una relazione, dire se gode delle proprietà simmetrica, riflessiva, transitiva, antisimmetrica.
- Nel caso  $\rho$  sia una relazione di equivalenza, dire quali classi d'equivalenza sono finite, e quali infinite. Quante sono le classi di equivalenza?

## 8 RELAZIONI DI EQUIVALENZA E FUNZIONI

Chiudiamo questo capitolo facendo un collegamento tra i due importanti concetti introdotti: quello di relazione di equivalenza definita su un insieme  $A$  e il concetto di funzione. Mostriremo come ad ogni funzione  $f$  avente come dominio un insieme  $A$  possiamo associare una relazione di equivalenza  $\rho_f$  definita su  $A$ , detta *relazione di equivalenza associata a f* e viceversa come ad ogni relazione di equivalenza  $\rho$  definita su un insieme  $A$  si può associare una funzione con dominio  $A$  tale che la relazione  $\rho_f$  associata a  $f$  coincida con  $\rho$ .

Sia  $f$  una funzione tra due insiemi  $A$  e  $B$ . Definiamo una relazione  $\rho_f$  in  $A$  al modo seguente:

$$a \rho_f b \iff f(a) = f(b).$$

Chiameremo  $\rho_f$  *relazione associata alla funzione f*. È facile vedere che si tratta di una relazione di equivalenza. Per ogni  $b \in B$  risulta  $f^{-1}(\{b\}) = \emptyset$  se  $b \notin \text{Im } f$ , altrimenti  $f^{-1}(\{b\}) = [a]$ , dove  $a$  è un qualunque elemento di  $A$  tale che  $f(a) = b$ , e  $[a]$  è la classe di equivalenza di  $a$  modulo  $\rho_f$ . Se  $b \in \text{Im } f$ , il sottoinsieme  $f^{-1}(\{b\})$  di  $A$  prende il nome di *fibra* sull'elemento  $b$ . L'insieme delle fibre è pertanto la partizione di  $A$  determinata dalla relazione di equivalenza  $\rho_f$ , cioè le fibre sono gli elementi del quoziente  $A/\rho_f$ .

Se viceversa partiamo da una relazione di equivalenza  $\rho$  definita su un insieme  $A$ , detto  $A/\rho$  l'insieme quoziente, resta individuata un'applicazione (suriettiva)  $\pi$  detta *proiezione canonica* sul quoziente:

$$\begin{aligned}\pi : A &\longrightarrow A/\rho \\ a &\longmapsto [a]\end{aligned}$$

tale che  $\rho_\pi = \rho$ . Questo legame tra applicazioni e relazioni di equivalenza indotte da queste giocherà un ruolo importante in molti teoremi fondamentali.

I seguenti due esempi dovrebbero chiarire questi concetti.

### Esempio 1.21

Si consideri la funzione  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  definita ponendo per ogni  $a \in \mathbb{Z}$

$$f(a) = \text{resto della divisione di } a \text{ per } 4.$$

L'immagine  $\text{Im}(f)$  è l'insieme  $\{0, 1, 2, 3\}$ . Due elementi  $a$  e  $b$  in  $\mathbb{Z}$  hanno la stessa immagine se e solo se divisi per 4 hanno lo stesso resto, quindi se e solo se la loro differenza è un multiplo di 4. La relazione  $\rho_f$  coincide quindi con la congruenza modulo 4.

### Esempio 1.22

Sia  $\mathcal{E}$  un'elica di passo  $t$  che si avvolge su un cilindro circolare retto  $\Sigma$  di raggio 1. Detto  $\alpha$  un piano perpendicolare alle generatrici del cilindro, sia  $\pi$  la proiezione ortogonale sul piano  $\alpha$

$$\begin{aligned}\pi : \mathcal{E} &\longrightarrow \alpha \\ P \in \mathcal{E} &\longmapsto \pi(P) \in \alpha\end{aligned}$$

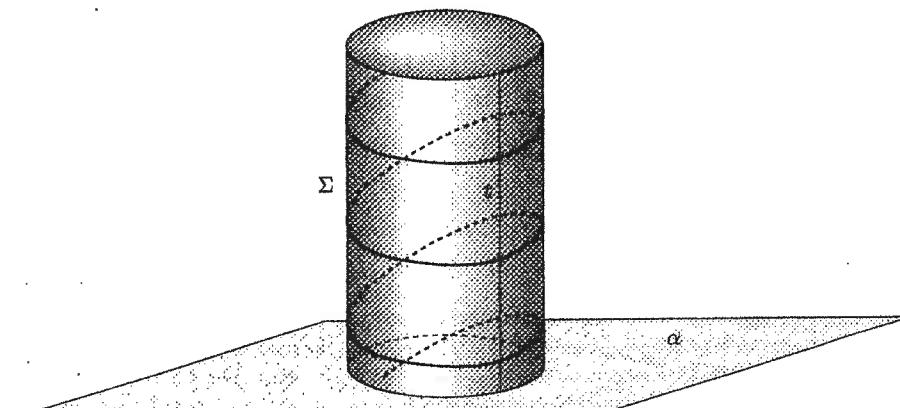


Figura 1.8. Elica.

- Determinare la relazione di equivalenza  $\rho_\pi$  su  $\mathcal{E}$  associata a  $\pi$ .
- Determinare le fibre e la cardinalità di ogni fibra.
- Provare che il quoziente  $\mathcal{E}/\rho_\pi$  è in corrispondenza biunivoca con la circonferenza  $C$  sezione su  $\alpha$  del cilindro.

Spieghiamo i vari punti.

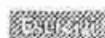
- Dati comunque due punti  $P$  e  $Q$  su  $\mathcal{E}$ ,

$$P \rho_\pi Q \iff \pi(P) = \pi(Q)$$

- Punti di  $\mathcal{E}$  che sono in relazione si trovano su di una stessa generatrice del cilindro. Infatti per ogni  $P \in \mathcal{E}$  la sua classe di equivalenza è costituita dai punti dell'elica che si trovano sulla generatrice passante per  $\pi(P)$  (fig. 1.8). Poiché l'elica ha passo  $t$ , le controimmagini di un punto  $P'$  di  $C$  (ossia i punti della fibra su  $P'$ ) si trovano ad intervalli di lunghezza  $t$ , quindi per ogni  $P \in \mathcal{E}$  la classe di equivalenza di  $P$  ha cardinalità del numerabile (la cardinalità di  $\mathbb{Z}$ ).
- Si noti che l'immagine  $\pi(\mathcal{E})$  di  $\pi$  è costituita dalla circonferenza  $C$  sezione su  $\alpha$  del cilindro. Proveremo ora che tale immagine è in corrispondenza biunivoca con il quoziente  $\mathcal{E}/\rho_\pi$ . Basta definire la seguente applicazione:

$$\begin{aligned}\Psi : \mathcal{E}/\rho_\pi &\longrightarrow C \\ [P] &\longmapsto \pi(P)\end{aligned}$$

Si deve provare che è bene definita, e che è biunivoca (cfr. eserc. 75).



Provare il punto c) dell'esempio 1.22.



Scrivere un programma che determini se una relazione definita su un insieme  $A$  di  $n$  elementi è riflessiva.

Scrivere un programma che determini se una relazione definita su un insieme  $A$  di  $n$  elementi è simmetrica.

Scrivere un programma che determini se una relazione definita su un insieme  $A$  con  $n$  elementi è transitiva.

Scrivere un programma che determini se una relazione definita su un insieme  $A$  con  $n$  elementi è antisimmetrica.

Scrivere un programma che determini se una relazione definita su un insieme  $A$  è una relazione di equivalenza, o se è una relazione d'ordine (e in questo caso riconoscere se si tratta di un ordinamento parziale o totale).

# 2

## Induzione e ricorsività

*Apri la mente a quel ch'io ti paleso  
e fermalvi entro; ché non fa scienza  
senza lo ritenere, avere inteso  
Dante PARADISO V 40-42*

Quando dobbiamo dimostrare che qualche formula dipendente dai numeri naturali è vera per tutti i numeri naturali, c'è un principio fondamentale che ci viene in aiuto, ed è il **principio di induzione matematica**. Legato a questo principio è il concetto di **ricorsività**. Questo sarà l'argomento principale del presente capitolo. Sarà però opportuno premettere alcune considerazioni relative alle successioni e alle sommatorie.

### ■ 1 SUCCESSIONI E STRINGHE

Dato un insieme  $X = \{a, b, c, d\}$ , questo coincide con l'insieme  $\{b, d, a, c\}$  o con l'insieme  $\{b, c, a, d\}$ , ossia non ha importanza l'ordine in cui sono disposti i suoi elementi. Potrebbe invece interessarci disporre gli elementi di un dato insieme secondo un certo ordine: per esempio disporre i nominativi di un elenco in ordine alfabetico, oppure gli studenti di un corso secondo la votazione, ecc. In questo caso, accanto ad ogni nominativo ci sarà una *etichetta*, costituita da un numero naturale, che indica la *posizione* del nominativo all'interno della lista. Questo vale anche per insiemi infiniti.

Ebbene, una successione è una struttura discreta usata per rappresentare una lista *ordinata*. Essa è una *funzione* che ha come dominio  $\mathbb{N}$  o un sottoinsieme di  $\mathbb{N}$  (generalmente  $\{1, 2, 3, \dots\}$ ).

Precisiamo con la seguente definizione.

**DEFINIZIONE 2.1** Una *successione* è una funzione  $f$  dal sottoinsieme  $\{1, 2, 3, 4, \dots\}$  dei numeri naturali  $\mathbb{N}$  o da  $\mathbb{N}$  in un insieme  $S$ .

Si usa in genere la notazione  $a_n$  per indicare l'immagine  $f(n)$  dell'elemento  $n$ . L'elemento  $a_n$  prende il nome di *termine* della successione.

Per descrivere una successione useremo le notazioni  $\{a_n\}_{n \in \mathbb{N}}$  o  $\{a_n\}$ . Si noti che  $a_n$  è il *termine n-esimo* della *successione*  $\{a_n\}$ .

Dato che una successione è una particolare funzione (che ha come dominio i numeri naturali o il sottoinsieme  $\{1, 2, 3, 4, \dots\}$  dei numeri naturali), essa coincide con il

sottoinsieme del prodotto cartesiano  $N \times S$  costituito dalle coppie  $(n, a_n)$ . Il primo elemento della coppia, ossia  $n$ , è l'*etichetta* di cui parlavamo prima.

Descriveremo una successione elencando i termini della successione secondo l'ordine crescente degli indici. Negli esempi che seguono si elencheranno i primi termini delle varie successioni.

#### Esempio 2.1

Sia  $\{a_n\}$  la successione dove  $\forall n a_n = n$ . Allora  $a_1 = 1, a_2 = 2, a_3 = 3, a_4 = 4, \dots$

#### Esempio 2.2

Sia  $\{a_n\}$  la successione dove  $\forall n a_n = \frac{1}{n}$ . Allora:  $a_1 = 1, a_2 = \frac{1}{2}, a_3 = \frac{1}{3}, a_4 = \frac{1}{4}, \dots$

#### Esempio 2.3

Sia  $\{a_n\}$  la successione dove  $\forall n a_n = \frac{1}{4^n}$ . Allora:  $a_1 = \frac{1}{4}, a_2 = \frac{1}{8}, a_3 = \frac{1}{12}, a_4 = \frac{1}{16}, \dots$

#### Esempio 2.4

Sia  $\{a_n\}$  la successione dove  $\forall n a_n = 5^n$ . Allora i primi termini sono  $a_1 = 5, a_2 = 5^2 = 25, a_3 = 5^3 = 125, a_4 = 5^4 = 625, \dots$

**DEFINIZIONE 2.2** Una successione con un numero finito di termini, ossia del tipo  $a_1, a_2, a_3, \dots, a_n$ , prende il nome di *stringa*.

**DEFINIZIONE 2.3** Dicesi *lunghezza* di una stringa il numero di termini che la compongono. La stringa vuota è la stringa che è priva di termini: la sua lunghezza è zero.

#### Esempio 2.5

La lunghezza della stringa *abcde* è 5.

## 2 SOMMATORIE

Sia  $f$  una funzione definita su  $N$  con codominio in  $\mathbb{R}$ . Introdurremo ora un simbolo molto utile per rappresentare le seguenti somme:

$$(2.1) \quad f(1) + f(2) + \dots + f(n)$$

oppure

$$(2.2) \quad f(r) + f(r+1) + f(r+2) + \dots + f(n)$$

In altre parole, pensando agli  $f(1), f(2), f(3), \dots$  come termini della successione  $\{a_n = f(n)\}$ , vogliamo esprimere la somma dei primi  $n$  termini (ossia la (2.1)) o dei termini che partono dal termine  $r$ -esimo e arrivano al termine  $n$ -esimo (ossia la (2.2)).

Ebbene, per indicare  $f(1) + f(2) + \dots + f(n)$  scriveremo

$$\sum_{i=1}^n f(i) \quad \text{ossia} \quad \sum_{i=1}^n a_i.$$

Per indicare invece  $f(r) + f(r+1) + f(r+2) + \dots + f(n)$  scriveremo

$$\sum_{i=r}^n f(i) \quad \text{ossia} \quad \sum_{i=r}^n a_i.$$

Il simbolo  $\sum$  dicesi *simbolo di sommatoria* (o *notazione sigma*), la variabile  $i$  dicesi *indice* di sommatoria. Questa notazione ci dice che dobbiamo includere nella somma esattamente quei termini  $a_i$  il cui indice  $i$  è un intero che si trova tra 1 e  $n$  (limite inferiore e limite superiore rispettivamente della sommatoria). Si osservi che la lettera che rappresenta l'indice di sommatoria non ha importanza: si tratta di un indice cosiddetto *muto*. Si può scrivere

$$\sum_{i=1}^n a_i = \sum_{j=1}^n a_j = \sum_{k=1}^n a_k.$$

Ci sono vari modi equivalenti per indicare la stessa sommatoria:

$$\sum_{i=1}^n a_i = \sum_{i=0}^{n-1} a_{i+1} = \sum_{1 \leq i \leq n} a_i = \sum_{1 \leq i+1 \leq n} a_{i+1}.$$

Diamo alcuni esempi per comprendere il significato di quanto definito.

#### Esempio 2.6

L'addizione dei primi 150 termini della successione  $\{a_n\}$ , dove  $a_n = n$ , ossia  $1+2+3+4+\dots+150$ , si esprime con il simbolo di sommatoria al modo seguente:

$$\sum_{i=1}^{150} i.$$

#### Esempio 2.7

L'addizione dei primi 200 termini della successione  $\{a_n\}$ , dove  $a_n = \frac{1}{n}$ , ossia  $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{200}$  si scrive

$$\sum_{i=1}^{200} \frac{1}{i}.$$

Ci sono altri modi per scrivere una somma di termini di una successione. Per esempio, se dobbiamo scrivere  $3+6+9+12$ , posto  $T = \{3, 6, 9, 12\}$ , scriveremo

$$\sum_{i \in T} i.$$

Così per esempio, se indichiamo con  $T$  il sottoinsieme di  $\mathbb{N}$  costituito dai numeri pari fino a 10, la scrittura

$$(2.3) \quad \sum_{i \in T} i$$

significa  $0 + 2 + 4 + 6 + 8 + 10$ .

Se indichiamo con  $S$  il sottoinsieme di  $\mathbb{N}$  costituito dai numeri dispari minori o uguali a 35, la scrittura

$$(2.4) \quad \sum_{i \in S} \frac{1}{i}$$

equivale a

$$1 + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \dots + \frac{1}{35}.$$

Si osservi che la (2.3) si può anche scrivere al modo seguente

$$\sum_{i=0}^5 2i$$

e la (2.4) si può scrivere

$$\sum_{i=0}^{17} \frac{1}{2i+1}.$$

**OSSERVAZIONE** Il simbolismo di sommatoria adottato ci permette di scrivere in forma compatta l'addizione di un certo numero di termini di una successione, ma *non dice quanto vale tale addizione*. Per saperlo, occorre fare tutte le addizioni.

Poniamoci quindi il problema di determinare effettivamente il *valore* di una certa sommatoria, svolgendo tutte le addizioni coinvolte.

Innanzitutto si osservi che

$$\sum_{i=1}^{100} 1 = 100.$$

Infatti dobbiamo sommare i primi 100 termini della successione costante  $a_n = 1$  per ogni  $n$ .

Supponiamo ora di voler determinare il valore della sommatoria

$$\sum_{i=1}^{100} i.$$

Non è molto agevole calcolare *rapidamente*  $1 + 2 + 3 + 4 + \dots + 100$ .

Però si può fare la seguente osservazione:

$$\sum_{i=1}^{100} i = 1 + 2 + 3 + \dots + 100$$

equivale (per la commutatività dell'addizione) a scrivere

$$\sum_{i=1}^{100} i = 100 + 99 + 98 + \dots + 1.$$

A questo punto, osservando che  $1 + 100 = 2 + 99 = 3 + 98 = \dots$ , ossia il primo + l'ultimo uguaglia il secondo + il penultimo, ecc., addizionando le due sommatorie, si ottiene

$$\begin{aligned} 2 \sum_{i=1}^{100} i &= (1 + 100) + (2 + 99) + (3 + 98) + \dots + (99 + 2) + (100 + 1) = \\ &= \underbrace{(1 + 100) + (1 + 100) + \dots + (1 + 100)}_{100 \text{ addendi di tipo } (1+100)} + (1 + 100) = 100(1 + 100). \end{aligned}$$

Dividendo entrambi i membri per 2

$$(2.5) \quad \sum_{i=1}^{100} i = \frac{100 \cdot 101}{2} = 5050.$$

Con una sola moltiplicazione e una divisione per 2 si riesce a trovare il risultato del problema. Per inciso, questo problema era stato assegnato dalla maestra alla classe in cui si trovava Gauss (a 7 anni) e quest'ultimo riuscì a risolvere il problema facendo per l'appunto le osservazioni che abbiamo fatto.

Si noti la differenza tra il primo membro e il secondo membro della (2.5): nel primo membro ci sono 100 addendi e quindi si devono fare 99 addizioni, nel secondo membro si deve fare solo *una* moltiplicazione tra due numeri e una divisione per due.

### Esempio 2.8

Per calcolare  $\sum_{i=1}^5 (3i - 2)$  dobbiamo sostituire ogni valore intero di  $i$  compreso tra 1 e 5 nell'espressione  $3i - 2$  e poi addizionare i risultati: otterremo quindi

$$(3(1) - 2) + (3(2) - 2) + (3(3) - 2) + (3(4) - 2) + (3(5) - 2) = 1 + 4 + 7 + 10 + 13 = 35.$$

Invece la  $\sum_{i=1}^5 3i - 2$  uguaglia

$$[3(1) + 3(2) + 3(3) + 3(4) + 3(5)] - 2 = (3 + 6 + 9 + 12 + 15) - 2 = 45 - 2 = 43.$$

Anche se le due sommatorie dell'esempio sembrano simili, i risultati sono completamente diversi. Si osservi che la moltiplicazione ha una priorità rispetto alla addizione o differenza, quindi non serve mettere la parentesi attorno al prodotto  $3i$ . Invece, dato che la sottrazione ha la stessa precedenza della addizione, la sottrazione di 2 in quest'ultimo esempio *non* va dentro la sommatoria. In altre parole, occorre stare attenti a mettere le parentesi attorno a una addizione o sottrazione se vogliamo che la sommatoria si applichi a più del primo addendo.

## 2.1 Proprietà della sommatoria

Il vantaggio della notazione di sommatoria è che ci permette di cambiare una sommatoria  $\sum$  in un'altra più semplice o più utile ai nostri scopi. A questo fine è importante conoscere le proprietà di cui gode. Le sommatorie verificano tutte le regole della addizione e moltiplicazione di numeri ordinari.

1.

$$\sum_{k=1}^n ca_k = c \cdot \sum_{k=1}^n a_k.$$

Si noti che  $a_k$  ha un indice  $k$  mentre  $c$  non lo ha. Ciò significa che  $c$  è una costante mentre  $a$  è una funzione di  $k$ . Stiamo sfruttando la proprietà distributiva del prodotto rispetto alla somma, che vale per i numeri reali.

### Esempio 2.9

$$\sum_{i=1}^4 ca_i = ca_1 + ca_2 + ca_3 + ca_4 = c(a_1 + a_2 + a_3 + a_4) = c \cdot \sum_{i=1}^4 a_i.$$

2.

$$\sum_{k=1}^4 (a_k + b_k) = \sum_{k=1}^n a_k + \sum_{k=1}^n b_k.$$

Stiamo sfruttando la proprietà associativa e quella commutativa dell'addizione tra numeri.

### Esempio 2.10

$$\begin{aligned} \sum_{i=1}^4 (a_i + b_i) &= (a_1 + b_1) + (a_2 + b_2) + (a_3 + b_3) + (a_4 + b_4) = \\ &= (a_1 + a_2 + a_3 + a_4) + (b_1 + b_2 + b_3 + b_4) = \sum_{i=1}^4 a_i + \sum_{i=1}^4 b_i. \end{aligned}$$

3.

$$\sum_{k \in K} (a_k - b_k) = \sum_{k \in K} a_k - \sum_{k \in K} b_k.$$

4.

$$\sum_{k=1}^n a_k = \sum_{k=1}^m a_k + \sum_{k=m+1}^n a_k.$$

5.

$$\text{Se } K \cap K' = \emptyset, \quad \sum_{k \in K} a_k + \sum_{k \in K'} a_k = \sum_{k \in K \cup K'} a_k.$$

Tipicamente, utilizziamo queste uguaglianze per unire due sommatorie in un'unica sommatoria o viceversa per staccare un termine della sommatoria dalla sommatoria stessa.

### Esempio 2.11

$$\sum_{i=1}^{t-1} a_i + \sum_{i=t}^n a_i = \sum_{i=1}^n a_i \quad 1 \leq t \leq n$$

oppure (si noti come nel caso seguente il termine  $a_t$  compaia sia nella prima sia nella seconda sommatoria)

$$\sum_{i=1}^t a_i + \sum_{i=t}^n a_i = a_t + \sum_{i=1}^n a_i \quad 1 \leq t \leq n$$

oppure

$$\sum_{i=0}^n a_i = a_0 + \sum_{i=1}^n a_i.$$

### Esempio 2.12

Calcolare  $\sum_{i=1}^{200} 3$ .

Sappiamo che  $\sum_{i=1}^{200} 1 = \underbrace{1 + 1 + 1 + \cdots + 1}_{200 \text{ addendi}} = 200$ . Allora in virtù della (1) si ha

$$\sum_{i=1}^{200} 3 = \sum_{i=1}^{200} 3 \cdot 1 = 3 \sum_{i=1}^{200} 1 = 3 \cdot 200 = 600.$$

Può succedere di avere una sommatoria del seguente tipo:

$$(2.6) \quad \sum_{i=1}^n a_{i,j}.$$

Dato che è l'indice  $i$  ad essere l'indice di sommatoria, si avrà

$$\sum_{i=1}^n a_{i,j} = a_{1,j} + a_{2,j} + \cdots + a_{n,j}.$$

Se avessimo avuto:

$$(2.7) \quad \sum_{j=1}^n a_{i,j}$$

allora il risultato sarebbe stato

$$\sum_{j=1}^n a_{i,j} = a_{i,1} + a_{i,2} + \cdots + a_{i,n}.$$

Possiamo pensare gli elementi  $a_{i,j}$  come elementi di una matrice (per chi non sa cos'è una matrice: si pensi ad una tabella di numeri disposti in un certo numero di righe e un certo numero di colonne) dove il primo indice,  $i$ , sta ad indicare in quale *riga* della matrice si trova l'elemento  $a_{i,j}$  mentre il secondo,  $j$ , sta ad indicare in quale *colonna* si trova l'elemento  $a_{i,j}$ . Quindi la (2.6) ci dice che dobbiamo sommare tutti gli elementi della matrice  $A = (a_{i,j})$  che si trovano sulla colonna  $j$ -esima, mentre la (2.7) ci dice che dobbiamo sommare tutti gli elementi che si trovano sulla riga  $i$ -esima.

## 2.2 Doppie sommatorie

Spesso (per esempio in programmi di informatica) compaiono le *doppie sommatorie*.

### Esempio 2.13

Calcolare la seguente doppia sommatoria:

$$\sum_{i=0}^2 \sum_{j=1}^3 ij.$$

Per valutare una doppia sommatoria, si deve prima espandere la *sommatoria più interna* e poi quella esterna. Avremo quindi

$$\sum_{i=0}^4 \sum_{j=1}^3 ij = \sum_{i=0}^4 (i + 2i + 3i) = \sum_{i=0}^4 6i = 0 + 6 + 12 + 18 + 24 = 60.$$

Una doppia sommatoria si può scrivere usando un solo simbolo di sommatoria, ma due indici. Per esempio la doppia sommatoria

$$\sum_{i=1}^2 \sum_{j=1}^2 a_i b_j$$

si può scrivere

$$\sum_{1 \leq i, j \leq 2} a_i b_j.$$

Sia l'indice  $i$  sia l'indice  $j$  possono variare da 1 a 2 (estremi inclusi). La sommatoria sarà pertanto costituita da 4 addendi:

$$(a_1 b_1 + a_1 b_2) + (a_2 b_1 + a_2 b_2).$$

Se gli estremi di una doppia sommatoria sono indipendenti l'uno dall'altro, i due segni di sommatoria si possono *scambiare*, ossia

$$(2.8) \quad \sum_{i=1}^n \sum_{j=1}^m a_{i,j} = \sum_{j=1}^m \sum_{i=1}^n a_{i,j}.$$

Basta infatti, come si è detto prima, pensare agli elementi  $a_{i,j}$  come elementi della matrice a  $n$  righe e  $m$  colonne

$$\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \dots & a_{1,m} \\ a_{2,1} & a_{2,2} & a_{2,3} & \dots & a_{2,m} \\ a_{3,1} & a_{3,2} & a_{3,3} & \dots & a_{3,m} \\ \dots & \dots & \dots & & \dots \\ a_{n,1} & a_{n,2} & a_{n,3} & \dots & a_{n,m} \end{pmatrix}$$

Allora ciascuna sommatoria della (2.8) corrisponde a fare la somma di *tutti* gli elementi  $a_{i,j}$  che compongono la matrice: la prima sommatoria corrisponde a sommarli per riga (ossia fare la somma di tutti gli elementi della prima riga, a questi sommare tutti gli elementi della seconda riga, ecc.), mentre la seconda somma corrisponde a sommarli per colonna. L'esercizio 3 mostra che effettivamente le due sommatorie della (2.8) sono uguali.

### Esercizi

Scrivere la seguente somma utilizzando il simbolo di sommatoria:  $1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \frac{1}{7} - \frac{1}{8} + \frac{1}{9} - \frac{1}{10}$ .

Calcolare la seguente doppia sommatoria:

$$\sum_{i=1}^2 \sum_{j=1}^3 (i + j).$$

Provare che  $\sum_{i=1}^n \sum_{j=1}^m a_{i,j} = \sum_{j=1}^m \sum_{i=1}^n a_{i,j}$ .

Si considerino le due successioni  $\{a_n\}_{n \in \mathbb{N}}$  e  $\{b_n\}_{n \in \mathbb{N}}$  dove per ogni  $n$

$$a_n = \frac{1}{3+n}, \quad b_n = n^2 + 2.$$

- Determinare  $a_{10}$  e  $b_{10}$ .
- Esprimere con il simbolo di sommatoria  $\Sigma$  (senza calcolare effettivamente la somma) la somma dei primi 15 termini di indice pari della successione  $\{a_n\}_{n \in \mathbb{N}}$ : attenzione, la successione comincia da  $a_0$ .

Si considerino le due successioni  $\{a_n\}_{n \in \mathbb{N}}$  e  $\{b_n\}_{n \in \mathbb{N}}$  dove per ogni  $n$

$$a_n = \frac{1}{n^2 + 1}, \quad b_n = 3n + 5.$$

- Determinare  $a_{10}$  e  $b_{10}$ .
- Esprimere con il simbolo di sommatoria  $\Sigma$  (senza calcolare effettivamente la somma) la somma dei primi 15 termini di indice pari della successione  $\{a_n\}_{n \in \mathbb{N}}$ : attenzione, la successione comincia da  $a_0$ .

Si consideri la seguente sommatoria:

$$\sum_{i=4}^8 a_i \quad \text{dove} \quad a_i = \frac{3^{i+1}}{5^i}$$

che corrisponde ad eseguire le seguenti addizioni:

$$\frac{3^5}{20} + \frac{3^6}{25} + \frac{3^7}{30} + \frac{3^8}{35} + \frac{3^9}{40}$$

Riscrivere tale sommatoria utilizzando un nuovo indice  $j$  in modo che la sommatoria possa essere scritta come

$$\sum_{j=0}^4 b_j.$$

Determinare  $b_j$ .

### 3 I NUMERI NATURALI E IL PRINCIPIO DI INDUZIONE MATEMATICA

Nel paragrafo precedente abbiamo esaminato sommatorie in cui il secondo estremo era un intero positivo fissato. Generalizzando quanto detto nel paragrafo precedente, supponiamo di volere trovare quanto vale la somma dei primi  $n$  numeri interi positivi, dove  $n$  è fissato ma il cui valore non si conosce, ossia

$$\sum_{i=1}^n i.$$

Ragionando come sopra, possiamo *congetturare* che valga la seguente uguaglianza:

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}.$$

Se vogliamo provare che questa formula è vera per ogni  $n$ , dobbiamo dimostrare infiniti teoremi: i primi teoremi sono i seguenti:

$$n = 1 : \quad 1 = \frac{1 \cdot 2}{2} = 1$$

$$n = 2 : \quad 1 + 2 = \frac{2 \cdot 3}{2} = 3$$

$$n = 3 : \quad 1 + 2 + 3 = \frac{3 \cdot 4}{2} = 6$$

... ...

Ogni singolo teorema è vero (con un ragionamento analogo a quello fatto per  $n = 100$ ), ma i puntini stanno ad indicare che dobbiamo andare avanti all'infinito, dobbiamo dimostrare *infiniti* teoremi! Possiamo dire: per  $n = 1$  è vera, per  $n = 2$  è vera, per  $n = 3$  è vera, ... e così via. Ma siamo sicuri? Siamo sicuri che il così via non ci riservi sorprese? Come possiamo procedere? È il momento di esaminare un po' più a fondo i numeri naturali e alcune loro proprietà.

Sia  $U$  un sottoinsieme dell'insieme  $\mathbb{N}$  dei numeri naturali che verifica le seguenti condizioni:

1.  $0 \in U$  (*base dell'induzione*).
2. Per ogni  $k$ , se  $k \in U$  allora  $k + 1 \in U$  (*passo induttivo*).

Allora possiamo concludere che  $U = \mathbb{N}$ .

In altre parole, se  $U$  è un sottoinsieme di  $\mathbb{N}$  che contiene lo zero e, assieme ad ogni elemento, contiene il successivo, allora il sottoinsieme  $U$  coincide con tutto  $\mathbb{N}$ .

Infatti, contenendo lo zero (per ipotesi) conterrà (in base al passo induttivo) 1 (che è il successivo di 0), ma allora (ancora per il passo induttivo) conterrà 2 (che è il successivo di 1), e così via. *Dato che il passo induttivo è vero per ogni  $k$ , siamo sicuri che qualunque numero naturale sta in  $U$  e quindi  $U = \mathbb{N}$ .*

Naturalmente se la base dell'induzione è 1 anziché 0, oppure  $n_0 \in \mathbb{N}$ , il sottoinsieme  $U$  non coinciderà con tutto  $\mathbb{N}$  ma solamente con i numeri naturali maggiori o uguali a 1 o maggiori o uguali a  $n_0$ .

Ebbene, questa proprietà dei numeri naturali (che prende il nome di *principio di induzione matematica*) costituisce uno degli assiomi sui quali si basa la definizione vera e propria dell'insieme  $\mathbb{N}$  dei numeri naturali. Gli assiomi che enunceremo sono i cosiddetti assiomi di Peano.

L'insieme dei numeri naturali è costituito da una terna  $(\mathbb{N}, \sigma, 0)$  dove  $\mathbb{N}$  è un insieme,  $\sigma$  è un'applicazione da  $\mathbb{N}$  in  $\mathbb{N}$  e 0 è un elemento di  $\mathbb{N}$  tali che

$N_1$ :  $\sigma$  è iniettiva;

$N_2$ :  $0 \notin \text{Im} \sigma$ ;

$N_3$ : ogni sottoinsieme  $U$  di  $\mathbb{N}$  tale che

(a)  $0 \in U$ ,

(b)  $\forall k$  fissato, ma arbitrario,  $k \in U \implies \sigma(k) \in U$

coincide con tutto  $\mathbb{N}$ .

Dato un elemento  $n \in \mathbb{N}$ , l'elemento  $\sigma(n)$  si dice il *successivo* di  $n$ . Poniamo  $\sigma(0) := 1$ ,  $\sigma(1) := 2$ , ecc. Resta definita in  $\mathbb{N}$  allora in modo naturale una relazione d'ordine,  $\leq$ . Il postulato  $N_3$  è noto come il *principio di induzione matematica*. Ebbene, i postulati di Peano caratterizzano i numeri naturali. Quello che si deve postulare (cioè accettare senza dimostrazione) è l'esistenza di un insieme  $\mathbb{N}$  verificante gli assiomi di Peano.

Ora, dai soli postulati di Peano è possibile ricavare tutte le proprietà ben note dei numeri naturali (cfr. cap. 11).

Soffermiamoci ora sul principio di induzione matematica,  $N_3$ . Come si è detto, esso sostanzialmente dice che se un sottoinsieme  $U$  di  $\mathbb{N}$  contiene lo zero e, accanto ad ogni elemento, contiene anche il successivo, allora necessariamente  $U$  coincide con tutto  $\mathbb{N}$ . Ora, sarà proprio questo assioma a risolvere il problema del e così via sul quale ci eravamo arenati. Esso ci offre un metodo di dimostrazione, la cosiddet-

ta dimostrazione per induzione, che è di fondamentale importanza in matematica. Vediamo di capire di cosa si tratta.

Supponiamo di dover dimostrare per ogni intero  $n \geq 0$  una proposizione, che chiameremo  $P(n)$ , dipendente da  $n$ .

Prima di procedere in modo rigoroso, pensiamo alla seguente situazione: supponiamo di avere una fila di birilli,  $b_1, b_2, b_3, \dots$ , e che vogliamo far cadere tutti i birilli, ossia supponiamo che la nostra proposizione  $P(n)$  da "dimostrare" sia *far cadere il birillo  $n$ -esimo* e che vogliamo dimostrare questa proposizione per ogni  $n$ , ossia far cadere *tutti* i birilli per ogni  $n$ .

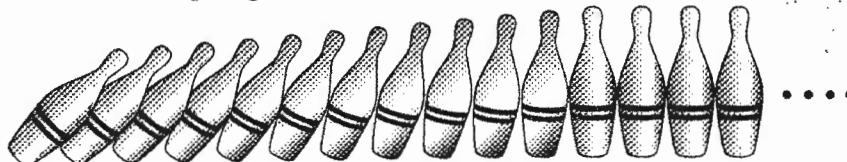


Figura 2.1. I birilli e l'induzione matematica.

Avremo dimostrato che  $P(n)$  è vera per ogni  $n$  se riusciamo a far cadere tutti i birilli. È chiaro che far cadere uno per uno i birilli non porta a nulla, perché i birilli sono infiniti. Si può però ottenere lo stesso risultato finale (di far cadere tutti i birilli) anche procedendo al modo seguente: si fa cadere il primo birillo e poi si ha cura di disporre i birilli allineati e sufficientemente vicini in modo tale che una volta che cade un birillo, allora cade anche quello immediatamente successivo. Allora la caduta del primo porta alla caduta del secondo; la caduta del secondo porta alla caduta del terzo, ecc. Siamo così sicuri di far cadere tutti i birilli, ossia di dimostrare tutte le proposizioni  $P(n)$ .

Avendo in mente questo tipo di situazione, possiamo forse capire meglio in cosa consista il tipo di *dimostrazione per induzione*, che è un metodo molto efficiente di dimostrazione: esso per l'appunto, come nel caso dei birilli, permette di ottenere *infiniti* risultati con due soli passi.

La formalizzazione del metodo è la seguente:

1. *Base dell'induzione: dimostrare che è vera  $P(0)$*
2. *Passo induttivo: dimostrare che per ogni  $k$  dall'essere vera  $P(k)$  segue che è vera  $P(k+1)$ .*

*Allora si può concludere di avere dimostrato che  $P(n)$  è vera per ogni  $n$ .*

Infatti, posto  $U = \{n \in \mathbb{N} \mid P(n) \text{ è vera}\}$ , risulta  $0 \in U$  perché è stato provato che  $P(0)$  è vera. Inoltre, se  $k \in U$ , cioè se  $P(k)$  è vera, allora  $P(k+1)$  è vera (passo induttivo) e quindi  $k+1 \in U$ , da cui segue, in virtù di  $\mathbb{N}_3$ ,  $U = \mathbb{N}$ , ossia  $P(n)$  è vera per ogni  $n$ .

Si noti che se vogliamo dimostrare una proposizione  $P(n)$  non per tutti gli  $n$ , ma per tutti gli  $n \geq n_0$ , basta provare come base dell'induzione  $P(n_0)$  anziché  $P(0)$ .

### Esempio 2.14

Provare per induzione che per ogni  $n$  è vera la proprietà  $P(n)$ , dove  $P(n)$  è la seguente uguaglianza:

$$P(n) : \sum_{i=0}^n i = \frac{n(n+1)}{2}.$$

Dobbiamo fare due passi:

1. Provare la base dell'induzione, ossia che la proprietà è vera per  $n = 0$ , ossia è vera  $P(0)$ : questa si riduce a

$$P(0) : 0 = 0$$

che è ovviamente vera.

2. Provare il passo induttivo. Per ogni  $k$ , dall'essere vera  $P(k)$  proviamo che è vera  $P(k+1)$ .

Supponiamo vera  $P(k)$ , ossia  $0 + 1 + 2 + \dots + k = \frac{k(k+1)}{2}$ .

Aggiungiamo ad entrambi i membri di questa uguaglianza (che è vera per ipotesi) il termine  $k+1$ . Si ottiene allora

$$0 + 1 + 2 + \dots + k + (k+1) = \frac{k(k+1)}{2} + (k+1).$$

Il secondo membro diventa:

$$\frac{k(k+1)}{2} + (k+1) = \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}.$$

Quindi

$$\sum_{i=0}^{k+1} i = 0 + 1 + 2 + \dots + k + (k+1) = \frac{(k+1)(k+2)}{2}$$

che è proprio la  $P(k+1)$  che volevamo dimostrare. Abbiamo così provato che la  $P(n)$  è vera per ogni  $n$ .

Vediamo ora di capire a fondo il principio di induzione matematica.

### Esempio 2.15

Cosa c'è di errato nella seguente *dimostrazione*? Vogliamo provare il seguente teorema (!): ogni numero naturale è uguale al successivo, ossia  $P(n) : n = n+1 \forall n$ .

Assumiamo il risultato vero per  $n = k$ , ossia assumiamo vero il teorema  $P(k) : k = k+1$  e dimostriamo che è vero  $P(k+1)$ , ossia  $k+1 = k+2$ . Ovvivamente basta aggiungere alla uguaglianza  $k = k+1$  (che stiamo supponendo vera) 1 ad entrambi i membri, per ottenere la  $P(k+1)$ .

Quindi (siamo sicuri?) possiamo concludere che la  $P(n)$  è vera per ogni  $n$ , ossia  $n = n+1$  è vera per ogni  $n$ .

Dove sta l'errore nella dimostrazione?

Una dimostrazione per induzione consiste di *due* parti: la base dell'induzione e il passo induttivo: *entrambe* vanno dimostrate. Noi abbiamo provato solamente la seconda (il passo induttivo). La prima (la base dell'induzione) è :

$$P(0) : 0 = 1$$

che chiaramente è falsa. Quindi il teorema (ovviamente) non è vero. Perciò occorre fare attenzione: quando si prova qualcosa per induzione occorre provare entrambi i passi: sono entrambi

essenziali. Spesso lo studente pensa che la base sia trascurabile, perché spesso è semplice da verificare, ma, come mostra questo esempio, non è detto che sia vera, e quindi a nulla serve dimostrare il passo induttivo se il passo base è falso.

Così se si dimostra la base dell'induzione, ma non si prova che per ogni  $k$  è vera l'implicazione  $P_k \Rightarrow P_{k+1}$ , non si riesce a provare nulla (cfr. eserc. 16)

E come se nella fila dei birilli questi fossero attaccati fino ad un certo punto e poi ci fossero due birilli troppo distanziati perché il birillo faccia cadere il successivo. La catena di montaggio si fermerebbe.

**OSSERVAZIONE** Spesso alcuni studenti incontrano difficoltà nel capire il passo induttivo del principio di induzione. La frase *per ogni  $k$ , supposto vero  $P(k)$  dimostriamo  $P(k+1)$*  viene letta al modo seguente: supposta vera  $P(k)$  per ogni  $k$  si dimostra  $P(k+1)$ . Letto così possono ben a ragione dire: bella forza! Se suppongo vera  $P(k)$  per ogni  $k$  è chiaro che è vera  $P(n)$  per ogni  $n$ . Attenzione! Non è questo il passo induttivo. Il passo induttivo è:

Per ogni  $k$  dimostriamo che dall'essere vera  $P(k)$  segue che è vera  $P(k+1)$

Quello che deve essere vero (cioè che dobbiamo dimostrare) per ogni  $k$  non è la  $P(k)$  ma l'*implicazione  $P(k) \Rightarrow P(k+1)$* , una volta che si supponga vera la  $P(k)$ . Quindi

$$[P(1) \wedge (\forall k (P(k) \Rightarrow P(k+1)))] \Rightarrow \forall n P(n)$$

ossia base dell'induzione e passo induttivo implicano che la proposizione  $P(n)$  è vera per ogni  $n$ .

**OSSERVAZIONE** È importante sottolineare che le proposizioni che si possono dimostrare per induzione sono esclusivamente quelle che dipendono dai numeri *naturali*  $n$ .

**OSSERVAZIONE** Si osservi che il metodo di dimostrazione per induzione *non determina la formula o il risultato* da dimostrare: permette di dimostrare una formula nel caso in cui questa sia stata congetturata. Individuare la formula è compito del matematico che la individuerà dall'esame dei *casi bassi*, ossia esaminando i primi valori di  $n$  e cercando di individuare uno schema generale dall'esame di alcuni casi particolari.

Un'altra proprietà fondamentale dei numeri naturali è la seguente. Se prendiamo in  $\mathbb{N}$  un qualunque sottoinsieme  $T$  non vuoto, in  $T$  c'è certamente un numero che è più piccolo di tutti gli elementi di  $T$ , ossia c'è un *minimo*  $m$  in  $T$ , ossia esiste un elemento  $m \in T$  tale che  $m \leq t$  per ogni  $t \in T$ . La stessa cosa non accade né in  $\mathbb{Z}$ , né in  $\mathbb{Q}$ , né in  $\mathbb{R}$ ; infatti per esempio in  $\mathbb{Z}$  il sottoinsieme  $T = \{z \in \mathbb{Z} \mid z \leq 5\}$  chiaramente non possiede minimo; così in  $\mathbb{Q}$  per esempio l'insieme  $T = \{q \in \mathbb{Q} \mid q > 0\}$  non possiede minimo. Cioè in  $\mathbb{Z}$ ,  $\mathbb{Q}$  e  $\mathbb{R}$  ci sono sottoinsiemi non vuoti che non possiedono minimo. Questa proprietà dei numeri naturali, che cioè

**M**: ogni sottoinsieme non vuoto di  $\mathbb{N}$  possiede minimo

è comunemente chiamata *Principio del minimo o del buon ordinamento* e si indica con la lettera **M**. Essa è un'altra delle proprietà fondamentali dei numeri naturali: anzi si dimostra che è equivalente al principio di induzione matematica.

Un'ulteriore formulazione del principio di induzione è la seguente:

I Ogni sottoinsieme  $V$  di  $\mathbb{N}$  tale che

- (a)  $0 \in V$ ,
- (b)  $n \in V$  ogniqualvolta  $k \in V \quad \forall k$  tale che  $0 \leq k < n$

coincide con tutto  $\mathbb{N}$ .

Abbiamo così dato tre formulazioni, che si possono dimostrare essere equivalenti, del principio di induzione matematica. A seconda dei casi, può essere conveniente utilizzare una formulazione invece di un'altra.

Un insieme parzialmente ordinato  $X$  si dice *bene ordinato* se ogni sottoinsieme non vuoto di  $X$  ha un elemento minimo. In questa terminologia **M** afferma che l'insieme  $\mathbb{N}$  dei numeri naturali è bene ordinato.



Si provi che un insieme bene ordinato è totalmente ordinato.

Provare che per ogni intero positivo  $n$  la somma dei cubi dei primi  $n$  numeri pari è data da

$$(3.1) \quad \underbrace{2^3 + 4^3 + 6^3 + \cdots + (2n)^3}_{n \text{ addendi}} = 2n^2(n+1)^2$$

Utilizzando **M**, provare che non esiste alcun intero  $a$  compreso tra 0 e 1.

Si provi per induzione che, per ogni intero  $n$ , risulta

$$\sum_{k=0}^n (4k+1) = (2n+1)(n+1).$$

Si provi per induzione che, per ogni intero positivo  $n$ , risulta

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Dimostrare che per ogni intero  $n \geq 0$  vale

$$1 + 5 + 5^2 + 5^3 + \cdots + 5^n = \frac{5^{n+1} - 1}{4}.$$

Dimostrare per induzione su  $n \geq 1$  che

$$1 + 4 + 7 + \cdots + (3(n-1) + 1) + (3n+1) = \frac{3n^2 + 5n + 2}{2}.$$

Dimostrare per induzione su  $n \geq 1$  che

$$2 + 5 + 8 + \cdots + (3(n-1) + 2) + (3n+2) = \frac{3n^2 + 7n + 4}{2}.$$

Si provi per induzione che, per ogni intero positivo  $n$ , l'insieme delle parti  $\mathcal{P}(X)$  di un insieme finito  $X$  con  $n$  elementi ha  $2^n$  elementi.

Vogliamo provare il seguente "teorema": *Tutti gli studenti hanno lo stesso colore degli occhi.* Dimostriamo questo fatto per induzione sul numero  $n$  di studenti. Se  $n = 1$  è ovvio che uno studente ha lo stesso colore dei propri occhi. Siano  $1, \dots, n$  gli studenti: in virtù dell'induzione, gli  $n - 1$  studenti  $1, \dots, n - 1$  hanno tutti gli occhi dello stesso colore, e così anche gli  $n - 1$  studenti  $2, \dots, n$ . Ma allora gli studenti che si trovano a metà, ossia quelli dal numero 2 al numero  $n - 1$ , appartenendo sia al primo gruppo di studenti, sia al secondo gruppo, avranno lo stesso colore di occhi degli studenti del primo gruppo e anche lo stesso colore di occhi degli studenti del secondo gruppo. Quindi tutti gli  $n$  studenti hanno lo stesso colore e degli occhi.

Dove fa acqua questo ragionamento?

Si provi che è possibile colorare le regioni formate da un qualunque numero di rette del piano (anche in posizione particolare, e non generica) con solo due colori. Si noti che per *colorare* si intende assegnare dei colori alle regioni in modo tale che regioni *confinanti* (ossia che hanno un *lato* in comune) abbiano colori diversi.

Siano  $a, b \in \mathbb{N}$ ,  $b \neq 0$ . Provare, sfruttando l'assioma M del buon ordinamento, che esistono due numeri naturali  $q, r$  tali che  $a = bq + r$ ,  $0 \leq r < b$ .

- a. Ad una lotteria vengono messi in vendita 100 biglietti numerati da 1 a 100. Ogni biglietto costa tanti euro quanto è il valore del suo numero, cioè il biglietto numero 1 costa un euro, il biglietto numero 2 costa 2 euro, e così via fino al centesimo biglietto che costa 100 euro. Sapendo che tutti i biglietti vengono venduti, quale è l'incasso totale?
- b. Ad un'altra lotteria i biglietti costano come nel punto precedente, con l'unica differenza che i biglietti con numero multiplo di 5 sono gratis. Quale è l'incasso in questo caso?

## 4 RICORSIVITÀ

Ricordiamo (cfr. par. 1) che una *successione*  $\{a_n\}_{n \in \mathbb{N}}$  è una funzione definita sull'insieme  $\mathbb{N}$  dei numeri naturali: con  $a_n$  si intende l'immagine di  $n$ , ossia  $a_n := a(n)$ . Gli  $a_n$  prendono il nome di *termini* della successione.

Consideriamo la successione così definita:

$$a_n = 7^n.$$

Risulta ovviamente  $a_0 = 1$ ,  $a_1 = 7$ ,  $a_2 = 7^2$ ,  $a_3 = 7^3$ , ecc. Tale successione si può tuttavia definire anche al modo seguente, ponendo

$$(4.1) \quad a_0 = 1, \quad a_n = 7 \cdot a_{n-1} = 7 \cdot 7^{n-1}.$$

Abbiamo cioè assegnato un *valore iniziale* e una *legge per calcolare un termine della successione in funzione del termine che lo precede*. Una tale definizione prende il nome di definizione *ricorsiva* o *induttiva*. È ovvio che le due relazioni della (4.1) permettono di calcolare i termini della successione: per esempio

$$\begin{cases} a_1 = 7 \cdot a^0 = 7 \cdot 1 = 7 \\ a_2 = 7 \cdot a^1 = 7 \cdot 7 = 49 \\ a_3 = 7 \cdot a^2 = 7 \cdot 49 = 343 \\ \dots \end{cases}$$

Abbiamo utilizzato anche il termine *induttivo* per designare una successione definita *ricorsivamente*: infatti la nozione di ricorsività è strettamente legata al principio di induzione matematica che abbiamo appena studiato, come possiamo subito vedere.

Supponiamo di conoscere i valori iniziali  $a_0, a_1, a_2, \dots, a_{n_0-1}$  di una successione e di sapere determinare  $a_n$  per ogni  $n \geq n_0$  una volta che siano noti i termini che lo precedono. Allora possiamo calcolare  $a_n$  per ogni  $n$ : infatti, indicato con  $U$  l'insieme di tutti gli  $n$  per i quali possiamo calcolare  $a_n$ ,  $U$  verifica le due proprietà del principio di induzione  $N_3$ , quindi, per ogni  $n \geq n_0$ ,  $n \in U$ , e, per quanto riguarda i primi  $n_0$  termini,  $a_0, a_1, \dots, a_{n_0-1}$ , essi stanno in  $U$  per ipotesi.

Diamo la definizione generale di definizione ricorsiva.

**DEFINIZIONE 2.4** Una successione si dice definita *ricorsivamente* o *induttivamente* se

- (*Passo base*): si definiscono i valori della successione nei primi  $k \geq 1$  interi non negativi (valori iniziali);
- (*Passo induttivo*): si dà una regola per determinare il valore della successione a partire dai valori di tutti o parte dei precedenti  $k$  interi.

### Esempio 2.16

La somma  $s_n$  dei primi  $n$  interi positivi si può definire ricorsivamente al modo seguente:

$$(4.2) \quad s_1 = 1, \quad s_n = s_{n-1} + n.$$

Le definizioni ricorsive permettono di creare i cosiddetti *algoritmi ricorsivi*.

Il termine "algoritmo" deriva dal nome del matematico arabo del nono secolo al-Khowarizmi. Ricordiamo che un *algoritmo* è un processo che permette di risolvere un problema in un numero finito di passi. Avremo modo di studiare molti algoritmi definiti sugli interi più avanti.

**DEFINIZIONE 2.5** Un algoritmo si dice *ricorsivo* se risolve un problema riducendolo ad un sottoproblema dello stesso tipo, con un input più piccolo. 

Cerchiamo di chiarire con un esempio.

#### Esempio 2.17

Supponiamo di essere stati incaricati della raccolta di firme nel quartiere per una petizione popolare allo scopo di ottenere l'apertura di un asilo nido. Le firme necessarie sono mille e la raccolta deve avvenire entro una settimana: come procedere? È inverosimile che possiamo, nei tempi richiesti, contattare direttamente 1000 persone. Quello che conviene fare è contattare dieci amici, affidare loro l'incarico di raccogliere 100 firme ciascuno. Ancora, non è detto che ciascuno dei nostri amici abbia il tempo di contattare 100 amici: quello che ciascuno di loro può fare è contattare dieci amici e affidare loro l'incarico di ottenere 10 firme. A questo punto il compito è agevole, e questi ultimi riusciranno, entro i tempi richiesti, a ottenere le 10 firme ciascuno. Alla fine i vari delegati torneranno dai loro capifila e consegneranno le firme ottenute, e arriveremo così alle 1000 firme necessarie. Questo è il tipico procedimento ricorsivo. Il problema originario è la raccolta di 1000 firme. I sottoproblemi diventano via via più semplici: raccolta di 100 firme e poi raccolta di 10 firme. La strategia adottata è comunemente nota con il termine *divide et impera*.

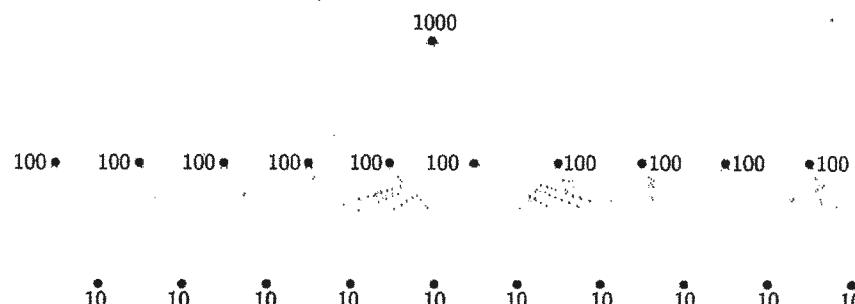


Figura 2.2.

Questo metodo ricorsivo è molto generale e comunemente utilizzato in informatica. Un procedimento ricorsivo, detto in termini semplici, è un processo che permette di risolvere un problema complesso riducendolo ad uno o più sottoproblemi che verificano le seguenti due condizioni:

- hanno la stessa struttura del problema originario
- sono più semplici da risolvere.

In altri termini, un algoritmo ricorsivo *richiama se stesso* per risolvere una situazione più piccola di un dato problema iniziale.

Dato che il problema in questo modo viene via via semplificato, pur rimanendo "uguale" in struttura al problema originario, alla fine si perverrà ad un problema semplice che sapremo risolvere. Dopo di che bisognerà ricomporre i pezzi per ottenere la soluzione del nostro problema originario.

Abbiamo visto che una definizione ricorsiva di una successione richiede un certo numero di termini iniziali e una legge per determinare i termini successivi dai termini precedenti. Tale legge prende il nome di *relazione ricorsiva*. Diamo qui di seguito la definizione precisa.

**DEFINIZIONE 2.6** Data una successione  $\{a_n\}_{n \in \mathbb{N}}$ , una *relazione ricorsiva o alle differenze finite* è una formula che esprime  $a_n$  in termini di uno o più termini precedenti per ogni  $n \geq n_0$ ,  $n_0$  essendo un intero non negativo. Una successione si dice *soluzione* della relazione ricorsiva se i suoi termini soddisfano la relazione stessa. 

#### Esempio 2.18

Le relazioni

$$(4.3) \quad a_1 = a, \quad a_n = a_{n-1} + d \quad \forall n > 1$$

definiscono una *progressione aritmetica*  $a_1, a_2, a_3, \dots$  in cui la differenza tra un termine e il precedente è  $d$ .

Le condizioni  $a_1 = a$  nella (4.3) o la  $a_1 = 1$  nella (4.2) costituiscono le cosiddette *condizioni iniziali*.

Nell'esempio precedente il termine  $n$ -esimo dipende esclusivamente dal precedente (e da una costante), ma vedremo esempi di successioni ricorsive in cui un termine dipende da due o più termini che lo precedono. In generale le condizioni iniziali specificano i termini che precedono il primo termine a partire dal quale la relazione di ricorrenza ha inizio. La relazione di ricorrenza e le condizioni iniziali *determinano univocamente* la successione: il motivo di questa affermazione è che la relazione di ricorrenza e le condizioni iniziali offrono una *definizione ricorsiva* della successione.

Anche se una relazione ricorsiva permette di calcolare il valore del termine  $n$ -esimo  $a_n$  per ogni  $n$ , tuttavia essa dà solo una informazione *locale*, perché il termine  $n$ -esimo si calcola in funzione dei precedenti, questi ultimi in funzione dei precedenti, e così via, fino ad arrivare ai termini iniziali. È importante quindi riuscire a trovare una cosiddetta *formula chiusa*, ossia una formula che esprima *direttamente*  $a_n$  in termini di un numero di operazioni ben note di  $n$  e non in termini dei precedenti elementi della successione. Una tale espressione permette di capire esattamente il valore di ogni  $a_n$ .

Una tale formula per il caso della progressione aritmetica (4.3) è data, come è immediato provare, da

$$a_n = a + (n - 1)d.$$

Il metodo di dimostrazione per induzione può venire in aiuto per trovare una tale formula. Si consideri per esempio la seguente relazione ricorsiva:

$$(4.4) \quad a_0 = 0, \quad a_n = 2a_{n-1} + 1.$$

Cerchiamo di "indovinare" la soluzione. Dall'esame dei primi casi

$$\begin{aligned} a_1 &= 1, \\ a_2 &= 2 \cdot 1 + 1 = 3, \\ a_3 &= 2 \cdot 3 + 1 = 7, \\ a_4 &= 2 \cdot 7 + 1 = 15, \\ &\dots \end{aligned}$$

sembra che la soluzione possa essere

$$(4.5) \quad a_n = 2^n - 1.$$

Occorre ora provare che è effettivamente soluzione per ogni  $n$ . Procediamo per induzione. Per  $n = 0$ ,  $a_0 = 0 = 2^0 - 1$ , e la base dell'induzione è verificata. Supposta vera la  $a_{n-1} = 2^{n-1} - 1$ , si tratta di provare che vale la (4.5). Infatti

$$(4.6) \quad a_n = 2a_{n-1} + 1 = 2(2^{n-1} - 1) + 1 = 2^n - 1,$$

e la dimostrazione è conclusa. Questa successione "modella" il numero di mosse per risolvere il cosiddetto *gioco della Torre di Hanoi* (cfr. es. 2.22).

Non è sempre facile risolvere una relazione ricorsiva, anzi a volte la risoluzione può essere molto complicata. Esistono casi però per i quali la risoluzione è molto semplice e per i quali si hanno delle tecniche sistematiche per trovare una formula chiusa. Tali sono per esempio le relazioni ricorsive *lineari*. Su queste ci concentreremo.

**DEFINIZIONE 2.7** Data una successione  $\{a_n\}_{n \in \mathbb{N}}$ , una *relazione ricorsiva lineare di grado  $k$ , a coefficienti costanti*, è una relazione ricorsiva della forma

$$(4.7) \quad a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k} + \alpha,$$

con  $\alpha_i$ ,  $\alpha$  numeri reali e  $\alpha_k \neq 0$ .

Se  $\alpha = 0$ , allora la relazione si dice *omogenea* (di grado  $k$ ). ■

Cominciamo ad esaminare il caso *omogeneo*, ossia una relazione ricorsiva del tipo:

$$(4.8) \quad a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k}.$$

Cerchiamo una soluzione della (4.8) della forma  $a_n = r^n$ ,  $r$  costante. Ora,  $r^n$  sarà soluzione della (4.8) se e solo se

$$r^n - \alpha_1 r^{n-1} - \alpha_2 r^{n-2} - \cdots - \alpha_k r^{n-k} = 0.$$

Dividendo ambo i membri di tale equazione per  $r^{n-k}$ , otterremo:

$$(4.9) \quad r^k - \alpha_1 r^{k-1} - \alpha_2 r^{k-2} - \cdots - \alpha_k = 0.$$

Ciò significa che  $a_n = r^n$  è soluzione della (4.8) se e solo se  $r$  è soluzione della (4.9). Quest'ultima prende il nome di *equazione caratteristica della relazione ricorsiva*. Le sue radici si chiamano *radici caratteristiche della relazione ricorsiva*. Ebbene, le radici caratteristiche ci permetteranno di trovare una formula esplicita per tutte le soluzioni della relazione ricorsiva, come risulta dalla proposizione che segue della quale non forniamo la dimostrazione.

**PROPOSIZIONE 2.1** Sia data una relazione ricorsiva lineare omogenea di grado  $k$ , ossia del tipo:

$$a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k}, \quad \alpha_i \in \mathbb{R}, \alpha_k \neq 0$$

e si supponga che l'*equazione caratteristica* di tale relazione,

$$r^k - \alpha_1 r^{k-1} - \alpha_2 r^{k-2} - \cdots - \alpha_k = 0,$$

abbia tutte radici distinte  $r_1, r_2, \dots, r_k$ . Allora una successione  $\{a_n\}$  è soluzione di tale relazione ricorsiva se e solo se, per  $n = 0, 1, 2, \dots$ ,

$$a_n = c_1 r_1^n + c_2 r_2^n + \cdots + c_k r_k^n, \quad c_1, c_2, \dots, c_k \text{ costanti.}$$

I coefficienti  $c_1, c_2, \dots, c_k$ , si determinano dai valori iniziali noti  $a_1, a_2, \dots, a_k$ .

### Esempio 2.19

Risolvere la relazione  $a_n = 2a_{n-1}$  per  $n \geq 1$ , con la condizione iniziale  $a_0 = 5$ .

L'*equazione caratteristica* (di grado  $k = 1$  e ha, banalmente, radici distinte) è  $r - 2 = 0$ : per determinare  $c_1$  ricordiamo che  $a_0 = 5$ . Quindi  $5 = c_1$  da cui  $a_n = 5 \cdot 2^n$  è la soluzione della relazione ricorsiva data.

### Esempio 2.20

Determinare il termine  $n$ -esimo della successione definita ricorsivamente al modo seguente:

$$a_n = 5a_{n-1} + 6a_{n-2}, \quad n \geq 2, \quad a_0 = 1, a_1 = 3.$$

L'*equazione caratteristica* (di grado  $k = 2$ ) è  $r^2 - 5r - 6 = 0$ , le cui radici sono  $r_1 = 6$  e  $r_2 = -1$  (distinte!). Quindi

$$a_n = c_1 6^n + c_2 (-1)^n.$$

Dalle  $a_0 = 1$  e  $a_1 = 3$ , si hanno le relazioni:

$$\begin{cases} 1 = c_1 + c_2 \\ 3 = c_1 \cdot 6 - c_2 \end{cases}$$

da cui si ottiene  $c_1 = \frac{4}{7}$ ,  $c_2 = \frac{3}{7}$  e quindi

$$a_n = \frac{4}{7} 6^n + \frac{3}{7} (-1)^n, \quad n \geq 0.$$

#### 4.1 I numeri di Fibonacci

Diamo ora, come esempio di relazione ricorsiva lineare e omogenea, un'importante successione, la *successione dei numeri di Fibonacci*. Si tratta di una successione definita ricorsivamente al modo seguente:

$$f_0 = 0, \quad f_1 = 1, \quad f_n = f_{n-1} + f_{n-2}.$$

Ogni termine è somma dei due termini che lo precedono. I primi termini della successione sono i seguenti:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \dots$$

I numeri di Fibonacci sorgono in molte situazioni e compaiono spesso in natura (per esempio nei petali di certi fiori o in qualche specie di pigna). Sono stati introdotti da Leonardo Fibonacci come soluzione del problema delle *coppie di conigli*. Il problema era quello di modellare la crescita di una popolazione di conigli. Più precisamente, supponiamo che ogni coppia di conigli impieghi un mese per diventare adulta e un secondo mese per procreare un'altra coppia. Se al primo mese si ha una sola coppia e se si fa l'ipotesi ulteriore che nessun animale muoia, quante coppie si avranno dopo  $n$  mesi? Indicando con  $\circ$  una coppia non ancora adulta e con  $\bullet$  una coppia capace di procreare, e con  $f_n$  il numero di coppie dopo  $n$  mesi, la situazione che si presenta è illustrata nella figura 2.3.

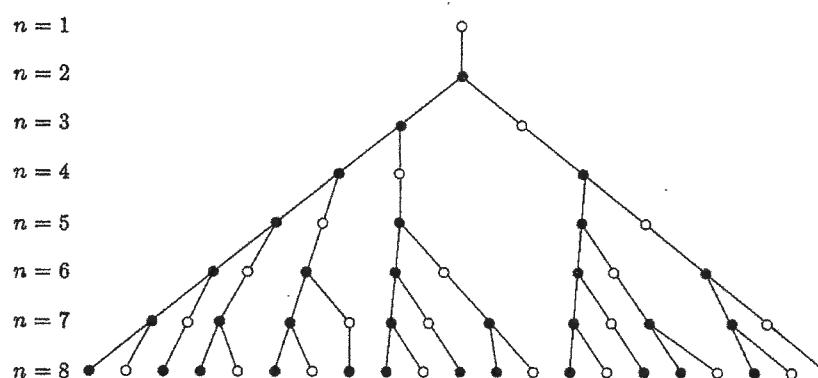


Figura 2.3. La successione di Fibonacci.

Dallo schema si deduce quanto segue:

- a) I *maturi* del mese  $n$ -esimo sono tanti quante tutte le coppie presenti nel mese  $n-1$ -esimo (perché nessuno muore).
- b) Quelli *immaturi* del mese  $n$ -esimo sono tanti quanti i maturi del mese  $n-1$ -esimo e questi, a loro volta, per il punto precedente, sono tanti quanti le coppie del mese  $n-2$ -esimo. Quindi risulta

$$f_n = f_{n-1} + f_{n-2}, \quad f_0 = 0, \quad f_1 = 1.$$

Vogliamo ora trovare una "soluzione" della relazione ricorsiva che definisce i numeri di Fibonacci, cioè la relazione

$$f_n = f_{n-1} + f_{n-2}$$

con le condizioni iniziali  $f_0 = 0, f_1 = 1$ .

L'equazione caratteristica della relazione ricorsiva è

$$(4.10) \quad r^2 - r - 1 = 0$$

le cui radici sono  $r_1 = \frac{1+\sqrt{5}}{2}, r_2 = \frac{1-\sqrt{5}}{2}$ . Esse sono distinte, quindi le soluzioni dell'equazione ricorsiva iniziale sono del tipo

$$(4.11) \quad f_n = c_1 r_1^n + c_2 r_2^n.$$

Le condizioni iniziali impongono che sia verificato il seguente sistema nelle incognite  $c_1$  e  $c_2$ :

$$\begin{cases} 0 = c_1 + c_2 \\ 1 = c_1 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + c_2 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n \end{cases}$$

Si trovano le soluzioni  $c_1 = 1/\sqrt{5}$  e  $c_2 = -c_1 = -1/\sqrt{5}$ , che, sostituiti nella (4.11), danno la forma chiusa dell' $n$ -esimo numero di Fibonacci:

$$(4.12) \quad f_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right]$$

**OSSERVAZIONE** Il numero  $\frac{1+\sqrt{5}}{2}$ , radice dell'equazione caratteristica (4.10), prende il nome di *rapporto aureo* o *proporzione divina*: si indica comunemente con la lettera  $\Phi$ , in omaggio all'artista greco Fidia, che nelle sue sculture utilizzò spesso questo rapporto.

Il nome "proporzione divina" deriva dal fatto che il rapporto più armonioso tra due lunghezze  $a$  e  $b$  era considerato dai Greci quello tale che  $\frac{a}{b} = \frac{a+b}{a}$ , tanto che la facciata del Partenone è stata inscritta in un rettangolo di queste proporzioni. Risolvendo la proporzione, si ottiene

$$\frac{a}{b} = \frac{1+\sqrt{5}}{2} \approx 1,61803.$$

Anche l'altra radice della (4.10),  $\frac{1-\sqrt{5}}{2} = -\frac{1}{\Phi} \approx -0,61803$  gode di molte proprietà di  $\Phi$ , e spesso si indica con  $\bar{\Phi}$ .

Passiamo ora a studiare il caso in cui l'equazione caratteristica abbia radici multiple, ossia radici  $r$  tali che  $(x - r)^m$  sia un fattore dell'equazione caratteristica (con  $m \geq 2$ ). In tale caso vale il seguente risultato.

**PROPOSIZIONE 2.2** Sia data una relazione ricorsiva lineare omogenea di grado  $k$ , ossia del tipo:

$$a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k}, \quad \alpha_i \in \mathbb{R}, \alpha_k \neq 0$$

e si supponga che l'equazione caratteristica di tale relazione,

$$r^k - \alpha_1 r^{k-1} - \alpha_2 r^{k-2} - \cdots - \alpha_k = 0,$$

abbia  $s (\leq k)$  radici distinte  $r_1, r_2, \dots, r_s$  di molteplicità rispettive  $m_1, m_2, \dots, m_s$ ,  $m_i \geq 1, i = 1, \dots, s$ ,  $m_1 + m_2 + \cdots + m_s = k$ . Allora una successione  $\{a_n\}$  è soluzione di tale relazione ricorsiva se e solo se, per  $n = 0, 1, 2, \dots$ ,

$$\begin{aligned} a_n = & (c_{1,0} + c_{1,1}n + \cdots + c_{1,m_1-1}n^{m_1-1})r_1^n + \\ & (c_{2,0} + c_{2,1}n + \cdots + c_{2,m_2-1}n^{m_2-1})r_2^n + \\ & \cdots \cdots \cdots \\ & (c_{s,0} + c_{s,1}n + \cdots + c_{s,m_s-1}n^{m_s-1})r_s^n, \end{aligned}$$

$n = 0, 1, 2, \dots$ ,  $c_{i,j}$  costanti reali per  $1 \leq i \leq s$ ,  $0 \leq j \leq m_i - 1$ . I coefficienti  $c_{i,j}$  si determinano dai valori iniziali noti  $a_1, a_2, \dots, a_k$ .

Chiariamo subito la formula con un esempio.

### Esempio 2.21

Supponiamo di sapere che le radici  $r_i$  dell'equazione caratteristica di una relazione ricorsiva lineare omogenea siano:  $3, -1, -1, 8, 3, -1, 3, 3$ , ossia

$$r_1 = 3 \text{ con molteplicità } m_1 = 4,$$

$$r_2 = -1 \text{ con molteplicità } m_2 = 3,$$

$$r_3 = 8 \text{ con molteplicità } m_3 = 1.$$

Allora la soluzione generale della relazione ricorsiva sarà

$$a_n = (c_{1,0} + c_{1,1}n + c_{1,2}n^2 + c_{1,3}n^3)3^n + (c_{2,0} + c_{2,1}n + c_{2,2}n^2)(-1)^n + c_{3,0}8^n.$$

Concludiamo il paragrafo dando lo schema riassuntivo dell'algoritmo per la risoluzione di una relazione ricorsiva lineare omogenea di grado  $k$ , a coefficienti costanti:

$$a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k}, \quad \alpha_i \in \mathbb{R}, \alpha_k \neq 0.$$

1. Trasportare a primo membro tutto il secondo membro, ottenendo

$$a_n - \alpha_1 a_{n-1} - \alpha_2 a_{n-2} - \cdots - \alpha_k a_{n-k} = 0.$$

2. Determinare l'equazione caratteristica:

$$r^k - \alpha_1 r^{k-1} - \alpha_2 r^{k-2} - \cdots - \alpha_k = 0.$$

3. Determinare le radici  $r_1, r_2, \dots, r_k$  di questa equazione:

a) se le radici sono tutte distinte, la soluzione generale della relazione ricorsiva è

$$a_n = c_1 r_1^n + c_2 r_2^n + \cdots + c_k r_k^n, \quad c_1, c_2, \dots, c_k \text{ costanti.}$$

Per determinare i coefficienti  $c_1, c_2, \dots, c_k$  basta impostare le condizioni iniziali (i primi  $k$  valori  $a_0, a_1, \dots, a_{k-1}$  della successione sono noti) ottenendo

$$\left\{ \begin{array}{l} a_0 = c_1 r_1^0 + c_2 r_2^0 + \cdots + c_k r_k^0 \\ a_1 = c_1 r_1^1 + c_2 r_2^1 + \cdots + c_k r_k^1 \\ a_2 = c_1 r_1^2 + c_2 r_2^2 + \cdots + c_k r_k^2 \\ \cdots \cdots \cdots \\ a_{k-1} = c_1 r_1^{k-1} + c_2 r_2^{k-1} + \cdots + c_k r_k^{k-1} \end{array} \right.$$

b) se ci sono  $s \leq k$  radici distinte  $r_1, r_2, \dots, r_s$  di molteplicità rispettive  $m_1, m_2, \dots, m_s$ ,  $m_i \geq 1, i = 1, \dots, s$ ,  $m_1 + m_2 + \cdots + m_s = k$ , allora

$$\begin{aligned} a_n = & (c_{1,0} + c_{1,1}n + \cdots + c_{1,m_1-1}n^{m_1-1})r_1^n + \\ & (c_{2,0} + c_{2,1}n + \cdots + c_{2,m_2-1}n^{m_2-1})r_2^n + \\ & \cdots \cdots \cdots \\ & (c_{s,0} + c_{s,1}n + \cdots + c_{s,m_s-1}n^{m_s-1})r_s^n, \end{aligned}$$

$n = 0, 1, 2, \dots$ ,  $c_{i,j}$  costanti reali per  $1 \leq i \leq s$ ,  $0 \leq j \leq m_i - 1$ .

I coefficienti  $c_{i,j}$  si determinano dai valori iniziali noti  $a_1, a_2, \dots, a_k$ .

**OSSERVAZIONE** Si noti che il punto a) è un caso particolare del punto b), corrispondente al caso in cui sia  $s = k$  e  $m_i = 1 \forall i = 1, \dots, k$ .

Sappiamo ormai risolvere le relazioni ricorsive lineari omogenee, dato che ne abbiamo fornito esplicitamente la soluzione. Proviamo ora a studiare le relazioni ricorsive lineari non omogenee, ossia del tipo:

$$a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k} + f(n),$$

$\alpha_i \in \mathbb{R}, \alpha_k \neq 0$ ,  $f(n)$  non identicamente nulla, dipendente da  $n$ .

Partiamo da un esempio concreto.

### Esempio 2.22. Il gioco della Torre di Hanoi

Si tratta di un gioco inventato dal matematico E. Lucas nel 1883. La Torre di Hanoi consiste di  $n$  dischi circolari infilati in un'asticella verticale  $A$ , con diametri decrescenti dal basso verso l'alto. Scopo del gioco è di trasferire tutti i dischi, nello stesso ordine di prima (ossia con diametri decrescenti dal basso verso l'alto), su di un'altra asticella  $C$ , seguendo le seguenti regole:

- a) i dischi devono essere trasferiti uno alla volta, utilizzando un'asticella intermedia  $B$ ;
- b) in nessun momento del gioco un disco di diametro maggiore può trovarsi su di un disco di diametro minore.

Pare che il gioco abbia la seguente origine. I sacerdoti del tempio di Brahma avevano il compito di fare in continuazione questi trasferimenti partendo da 64 dischi d'oro posti su tre aste d'oro poggiante su basi di diamante. La leggenda vuole che nell'istante stesso in cui il trasferimento fosse avvenuto il mondo sarebbe terminato!

- a) Si trovi una relazione ricorsiva per il minimo numero  $a_n$  di mosse necessario per trasferire  $n$  dischi;
- b) si trovi una formula chiusa, che esprima tale numero  $a_n$  in funzione di  $n$ ;
- c) si deduca il numero di mosse nel caso  $n = 64$  dei sacerdoti, e si veda quanto lontana era la fine del mondo!

Per individuare una formula ricorsiva procederemo per induzione su  $n$ . Per  $n = 1$  è chiaro che il numero  $a_1$  di mosse per operare il trasferimento è 1. Supponiamo di conoscere il numero  $a_{n-1}$  di mosse necessarie per trasferire  $n - 1$  dischi, e calcoliamo  $a_n$ . Procediamo al modo seguente: trasferiamo dall'asticella A all'asticella B gli  $n - 1$  dischi superiori: ci serviranno  $a_{n-1}$  mosse. Trasferiamo ora sull'asticella C in una mossa il disco rimasto (quello di diametro più largo). Trasferiamo infine sull'asticella C dall'asticella B (in  $a_{n-1}$  mosse) gli  $n - 1$  dischi che avevamo trasferito. Il numero di trasferimenti che abbiamo fatto è

$$a_n = 2a_{n-1} + 1.$$

Si tratta di una relazione ricorsiva lineare *non omogenea di grado 1* che abbiamo già incontrato (cfr. (4.4)), la cui soluzione (con la condizione iniziale  $a_0 = 0$ ) è (cfr. (4.6))

$$a_n = 2^n - 1.$$

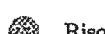
Supponendo che i sacerdoti facciano un trasferimento al secondo, mancano circa  $10^{14}$  anni per la fine del mondo!

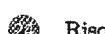
-  Si provi per induzione che per ogni  $n \geq 1$  risulta

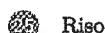
$$f_n > \left(\frac{1+\sqrt{5}}{2}\right)^{n-2}.$$

 Risolvere la relazione ricorsiva  $a_{n+2} = 2a_n + a_{n+1}$  con le condizioni iniziali  $a_0 = -4$ ,  $a_1 = 7$ . Calcolare  $a_8$  e  $a_9$ .

 Risolvere la relazione ricorsiva  $a_{n+2} = 2a_n - a_{n+1}$  con le condizioni iniziali  $a_0 = 5$ ,  $a_1 = 2$ . Calcolare  $a_8$  e  $a_9$ .

 Risolvere la relazione ricorsiva  $a_{n+2} = 2a_n + a_{n+1}$  con le condizioni iniziali  $a_0 = -3$ ,  $a_1 = 6$ . Calcolare  $a_8$  e  $a_9$ .

 Risolvere la relazione ricorsiva  $a_{n+2} = 2a_n - a_{n+1}$  con le condizioni iniziali  $a_0 = 6$ ,  $a_1 = 3$ . Calcolare  $a_8$  e  $a_9$ .

 Risolvere la relazione ricorsiva:  $a_n = -8a_{n-2} + 6a_{n-1}$  con le condizioni iniziali:  $a_0 = 0$ ,  $a_1 = 1$ .

 Risolvere la relazione ricorsiva:  $a_n = 15a_{n-2} - 2a_{n-1}$  con le condizioni iniziali:  $a_0 = 0$ ,  $a_1 = 1$ .

 Risolvere la relazione ricorsiva:  $a_n = 9a_{n-1} - 20a_{n-2}$ ,  $a_0 = a_1 = 1$ .

 Sia  $a_n$  la successione definita, per  $n \in \mathbb{N}$ ,  $n \geq 2$ , da  $a_2 = 17$ ,  $a_3 = 11$  e  $a_{n+1} = a_n + 6a_{n-1}$  per  $n \geq 3$ .

a. Calcolare  $a_4$ .

b. Determinare una formula chiusa per la successione  $a_n$ .

 In ciascuno dei seguenti casi, dire se e quante successioni  $a_n$ ,  $n \in \mathbb{N}$  esistono che soddisfano le condizioni:

a.  $a_{n+2} = -a_{n+1} + 6a_n$ ;  $a_0 = 1$ .

b.  $a_{n+2} = -a_{n+1} + 6a_n$ ;  $a_0 = 1$ ;  $a_1 = 12$ .

c.  $a_{n+2} = -a_{n+1} + 6a_n$ ;  $a_0 = 1$ ;  $a_1 = 12$ ;  $a_4 = -114$ .

d.  $a_{n+2} = -a_{n+1} + 6a_n$ ;  $a_0 = 1$ ;  $a_1 = 12$ ;  $a_4 = 210$ .

Nei casi in cui esiste un'unica successione che soddisfa le condizioni date, determinarne una formula chiusa.

 Si consideri la funzione  $A(n, m)$  (detta *funzione di Ackermann*) da  $\mathbb{N} \times \mathbb{N}$  in  $\mathbb{N}$ , definita risorsivamente al modo seguente:

$$\begin{cases} A(0, n) = n + 1 & \forall n \geq 0 \\ A(m, 0) = A(m - 1, 1), & \forall m > 0 \\ A(m, n) = A(m - 1, f(m, n - 1)) & \forall m, n > 0. \end{cases}$$

a. Calcolare  $A(1, 4)$ .

b. Calcolare  $A(2, 2)$ .

c. Calcolare  $A(3, 2)$ .

d. Provare che  $A(1, n) = n + 2 \quad \forall n$ .

e. Provare che  $A(2, n) = 2n + 3 \quad \forall n$ .

N.B. Sembra una funzione innocua: in realtà questa funzione cresce più rapidamente di una funzione esponenziale: per esempio

$$A(3, n) = 2^{n+3} - 3, \quad A(4, n) = 2^{2^{n+3}-3} - 3$$

dove  $2^{2^{n+3}-3}$  è costituito da  $n + 3$  esponentiazioni: per esempio  $2^{2^{2^2}-3} = 65\,536$ .

La funzione di Ackermann è una delle funzioni più importanti in informatica e gioca un ruolo essenziale nella teoria della complessità.

 Siano date due successioni  $a_n$  e  $b_n$  che rappresentano i rendimenti in euro di due tipi di azioni al variare dei mesi. Supponiamo che la legge di sviluppo sia data, in funzione dei mesi  $n \geq 0$ , dalle equazioni ricorsive (non omogenee):  $a_{n+1} = 5a_n + 2$ , con  $a_0 = 2$  euro e  $b_{n+1} = b_n + 1$  con  $b_0 = 2$  euro.

1. Scrivere la soluzione generale di entrambe le equazioni.

2. Dopo quanti mesi le azioni  $a_n$ , (rispettivamente  $b_n$ ) raggiungono il valore di 1562 euro?

■ Data la relazione ricorsiva  $a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \dots + \alpha_k a_{n-k} + \alpha$ , con  $\alpha_i, \alpha$  numeri reali e  $\alpha_k \neq 0$  e le condizioni iniziali  $a_1 = t_1, a_2 = t_2, \dots, a_r = t_r$ , si scriva un programma che calcoli il termine  $a_n$ .

■ Si scriva un programma che determini l' $n$ -esimo numero di Fibonacci.

■ Si scriva un programma che calcoli il numero  $a_n$  di mosse necessario per risolvere il gioco della torre di Hanoi con  $n$  dischi. Si confrontino i tempi di calcolo rispetto ad un programma che utilizzi la formula chiusa.

■ Si scriva un programma che calcoli la funzione di Ackermann (cfr. eserc. 30)  $A(n, m)$  per vari valori di  $n$  e  $m$ .

# 3

## Numeri interi e algoritmi

*Così solo, numeri di perduta bene  
mi narravo, e giorni,  
e, splendenti in remote aure,  
acque di selve ed erbe.*

Salvatore Quasimodo, In luce di cieli, da ED È SUBITO SERA

Uno dei principali temi della matematica discreta è rappresentato dai numeri interi. Questo capitolo è quindi dedicato alle proprietà fondamentali di tali numeri e alla presentazione di alcuni importanti algoritmi. Vengono inoltre introdotti i "mattoni" su cui sono fondati i numeri naturali, cioè i numeri primi.

### ■ 1 PRIME PROPRIETÀ DEI NUMERI INTERI

L'introduzione dei numeri interi si rende necessaria nel momento in cui si chiede di risolvere un'equazione del tipo

$$x + n = 0, \quad n \in \mathbb{N}, n \neq 0.$$

Chiaramente una tale equazione non ammette soluzioni in  $\mathbb{N}$  e occorre ampliare l'insieme dei numeri naturali con l'introduzione dei numeri *negativi*, pervenendo all'insieme

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

dei numeri interi. Questo modo di introdurre i numeri interi non è tuttavia molto soddisfacente: nel cap. 11 vedremo, per chi è interessato, una definizione rigorosa di tali numeri.

L'insieme  $\mathbb{Z}$ , rispetto alle due ordinarie operazioni di addizione e moltiplicazione gode delle seguenti proprietà:

- (i)  $a + b = b + a, \forall a, b \in \mathbb{Z}$   
(proprietà commutativa dell'addizione);

- (ii)  $(a+b)+c = a+(b+c)$ ,  $\forall a, b, c \in \mathbb{Z}$   
(proprietà associativa dell'addizione);
- (iii) esiste un unico elemento  $0 \in \mathbb{Z}$  tale che  $a+0=0+a=a$ ,  $\forall a \in \mathbb{Z}$   
(esistenza dell'elemento neutro rispetto all'addizione);
- (iv) per ogni  $a \in \mathbb{Z}$  esiste un unico elemento,  $-a$ , tale che  $a+(-a)=(-a)+a=0$   
(esistenza dell'opposto);
- (v)  $a \cdot b = b \cdot a$ ,  $\forall a, b \in \mathbb{Z}$   
(proprietà commutativa della moltiplicazione);
- (vi)  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ ,  $\forall a, b, c \in \mathbb{Z}$   
(proprietà associativa della moltiplicazione);
- (vii) esiste in  $\mathbb{Z}$  un unico elemento,  $1$ , tale che  $a \cdot 1 = 1 \cdot a = a$ ,  $\forall a \in \mathbb{Z}$   
(esistenza dell'elemento neutro rispetto alla moltiplicazione);
- (viii)  $a \cdot (b+c) = a \cdot b + a \cdot c$ ,  $(a+b) \cdot c = a \cdot c + b \cdot c$ ,  $\forall a, b, c \in \mathbb{Z}$   
(distributività della moltiplicazione rispetto all'addizione).

Vedremo nel cap. 8 che un insieme dotato di due operazioni che verificano le precedenti proprietà prende il nome di *anello commutativo con unità*. Dunque gli interi, rispetto alle operazioni definite, costituiscono un anello commutativo con unità.

Inoltre sono verificate anche le seguenti proprietà che, essendo conseguenza degli assiomi sopra riportati, valgono in un qualunque anello:

**PROPOSIZIONE 3.1** Per ogni  $a, b \in \mathbb{Z}$

$$1) a \cdot 0 = 0 \cdot a = 0, \quad 2) (-a) \cdot b = -(a \cdot b), \quad 3) (-a)(-b) = ab.$$

**DIMOStrAZIONE.** Sono semplici conseguenze degli assiomi di anello. Infatti, dalle  $0 + (a \cdot 0) = a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$  segue che  $a \cdot 0 = 0$ . Pur essendo una dimostrazione molto semplice, è istruttivo rendersi conto di quali proprietà ci si è via via serviti. Nelle prime due uguaglianze si è sfruttata l'esistenza dell'elemento neutro rispetto all'addizione; nella terza le proprietà distributive della moltiplicazione rispetto all'addizione e infine l'implicazione derivante dalla  $a \cdot 0 = a \cdot 0 + a \cdot 0$  è conseguenza dell'esistenza dell'opposto di ogni elemento.

I due punti 2) e 3) sono conseguenza di 1) (cfr. eserc. 1)  $\diamond$

**DEFINIZIONE 3.1** Un elemento non nullo  $a$  di un anello commutativo si dice *divisore dello zero* se esiste un elemento  $b$  non nullo tale che  $ab = 0$ .  $\blacksquare$

Un anello commutativo che non possiede divisori dello zero ha un nome: viene detto *dominio di integrità*.

La proposizione che segue mostra come l'anello  $\mathbb{Z}$  degli interi sia un dominio di integrità.

**PROPOSIZIONE 3.2** L'anello degli interi è un dominio di integrità.

**DIMOStrAZIONE.** Dobbiamo provare che se  $a$  e  $b$  sono due numeri interi, allora  $ab = 0$  se e solo se  $a = 0$  o  $b = 0$ , ossia in  $\mathbb{Z}$  non ci sono divisori dello zero. Si osservi innanzitutto che se  $a$  e  $b$  sono entrambi positivi o entrambi negativi, il loro prodotto è sempre positivo (se sono entrambi positivi, si veda la definizione 11.2 di prodotto in  $\mathbb{N}$ ), se sono entrambi negativi basta ricordare (3) della proposizione 3.1. Se invece è  $a > 0$  e  $b < 0$ , allora  $-b$  è positivo, quindi  $a(-b) = -ab$  è positivo, per cui  $ab$  è negativo. Quindi se  $ab = 0$  uno dei due fattori  $a$  o  $b$  deve necessariamente essere uguale a zero.  $\diamond$

**OSSERVAZIONE** Abbiamo appena dimostrato che in  $\mathbb{Z}$ , dotato delle ordinarie operazioni di addizione e moltiplicazione, non ci sono divisori dello zero. Si noti tuttavia che questa proprietà non è conseguenza degli assiomi di anello. Esistono anelli che possiedono divisori dello zero: l'insieme  $\mathbb{Z}$  stesso per esempio, dotato di altre operazioni, viene a possedere divisori dello zero (cfr. eserc. 2). Più in avanti vedremo una vasta e importante classe di anelli che possiedono divisori dello zero: gli anelli  $\mathbb{Z}_n$  delle classi resto modulo un intero non primo  $n$  (cfr. cap. 5).

### ESERCIZI

■ Provare che per ogni  $a, b \in \mathbb{Z}$   $(-a) \cdot b = -(a \cdot b)$  e  $(-a)(-b) = ab$ .

■ Si consideri l'insieme  $\mathbb{Z}$  degli interi: sia + l'ordinaria addizione di interi e si definisca la seguente ulteriore operazione:

$$a \circ b := 0 \quad \forall a, b \in \mathbb{Z}.$$

- Provare che  $(\mathbb{Z}, +, \circ)$  è un anello commutativo privo di unità.
- Provare che possiede divisori dello zero, e che quindi  $\mathbb{Z}$  con queste due operazioni non è un dominio di integrità.
- Determinare tutti i divisori dello zero.

## ■ 2 DIVISIBILITÀ, IRRIDUCIBILI E PRIMI IN $\mathbb{Z}$

Partiamo da alcune definizioni.

**DEFINIZIONE 3.2** Siano  $a$  e  $b$  due interi. Si dice che  $a$  divide  $b$ , e si scrive  $a|b$ , se esiste un intero  $c$  tale che  $b = ac$ . Se  $a$  non divide  $b$  si scrive  $a \nmid b$ .  $\blacksquare$

Se  $a|b$  si dice anche che  $a$  è un divisore di  $b$  (e  $b$  è un multiplo di  $a$ ).

Per esempio,  $5|(-30)$ ,  $9|0$ , ma  $8 \nmid 9$ ,  $0 \nmid 4$ .

**DEFINIZIONE 3.3** Si chiama *divisore comune* degli elementi  $a$  e  $b$  di  $\mathbb{Z}$  un elemento  $c \in \mathbb{Z}$  tale che  $c | a$  e  $c | b$ .  $\blacksquare$

**LEMMA 3.1** Se  $c$  è un divisore comune di  $a$  e  $b$ , allora  $c$  divide ogni intero della forma  $sa + tb$ , con  $s$  e  $t$  in  $\mathbb{Z}$ , cioè  $c | a$  e  $c | b \Rightarrow c | sa + tb \forall s, t \in \mathbb{Z}$ .

**DIMOSTRAZIONE.**  $c \mid a \implies a = ch$  per qualche  $h \in \mathbb{Z}$ ;  $c \mid b \implies b = ck$  per qualche  $k \in \mathbb{Z}$ . Allora, per ogni  $s, t \in \mathbb{Z}$ ,  $sa + tb = s(ch) + t(ck) = c(sh + tk)$ , da cui  $c \mid sa + tb$ .  $\diamond$

**DEFINIZIONE 3.4** Un elemento  $u \in \mathbb{Z}$  che divide 1 si dice una *unità* (o elemento *invertibile*) di  $\mathbb{Z}$ .

È immediato riconoscere che le sole unità di  $\mathbb{Z}$  sono 1 e  $-1$ .

**DEFINIZIONE 3.5** Due elementi  $a$  e  $b$  di  $\mathbb{Z}$  tali che  $a \mid b$  e  $b \mid a$  si dicono *associati*.

Dalla definizione è immediato vedere che due elementi  $a$  e  $b$  sono associati se e solo se  $a = bu$ , dove  $u$  è un'unità (o elemento invertibile). Quindi, in  $\mathbb{Z}$  due elementi sono associati se e solo se differiscono per il segno. La relazione di "essere associati" è una relazione di equivalenza. Ogni classe di equivalenza di un elemento non nullo è costituita da due soli interi, mentre la classe di equivalenza dello zero è costituita dal solo zero.

**DEFINIZIONE 3.6** Un elemento  $a \in \mathbb{Z}$  che sia diverso da zero e non sia una unità si dice *irriducibile* se ognivolta  $a$  si scrive come prodotto  $a = bc$  con  $b, c \in \mathbb{Z}$  allora  $b$  o  $c$  sono delle unità.

**DEFINIZIONE 3.7** Un elemento  $a \in \mathbb{Z}$  che non sia lo zero e non sia una unità si dice *primo* se ogni volta che  $a$  divide un prodotto  $bc$ , con  $b, c \in \mathbb{Z}$ , allora  $a$  divide almeno uno dei due fattori.

**OSSERVAZIONE** In realtà la definizione che abbiamo appena dato di elemento irriducibile corrisponde alla definizione che comunemente si attribuisce ai *numeri primi* in  $\mathbb{Z}$ : infatti si dice normalmente che i numeri primi sono quegli interi positivi che non hanno altri divisori all'infuori di se stessi e l'unità. Si noti tuttavia che in questo caso si parla di *numeri primi* e non di *elementi primi*. Tuttavia non dobbiamo preoccuparci troppo di questa possibilità di confusione in  $\mathbb{Z}$ , perché vedremo comunque che le due nozioni di elemento irriducibile ed elemento primo coincidono in  $\mathbb{Z}$ ; in questo senso sembra futile dare due definizioni diverse quando in  $\mathbb{Z}$  questi due concetti coincidono, ma, lo ripetiamo, questa non sarà la situazione generale (cfr. es. 8.12).

Con i mezzi che abbiamo a disposizione, siamo in grado immediatamente di provare che un elemento primo è necessariamente irriducibile. Per provare che in  $\mathbb{Z}$  anche ogni elemento irriducibile (ossia un ordinario numero primo) è primo occorrerà aspettare la proposizione 3.8.

**PROPOSIZIONE 3.3** *Ogni elemento primo in  $\mathbb{Z}$  è un elemento irriducibile.*

**DIMOSTRAZIONE.** Sia  $a$  un elemento primo in  $\mathbb{Z}$ . Per provare che esso è irriducibile, dobbiamo provare che dall'essere  $a = bc$  con  $b, c \in \mathbb{Z}$  segue che  $b$  o  $c$  sono delle unità. Sia dunque  $a = bc$ ; in particolare  $a \mid bc$ . Allora (essendo  $a$  primo per ipotesi)  $a \mid b$  oppure  $a \mid c$ , cioè  $b = ah$  o  $c = ak$ , con  $h, k \in \mathbb{Z}$ ; ma allora la  $a = bc$ , assieme ad una di queste relazioni comportano che  $b$  o  $c$  sono delle unità.  $\diamond$

### Esercizi

• Sia  $p$  un elemento primo in  $\mathbb{Z}$ . Si provi che se  $p$  divide un prodotto di  $n$  fattori  $a_1 a_2 a_3 \dots a_n$ , allora  $p$  divide almeno uno dei fattori.

## ■ 3 LA DIVISIONE IN $\mathbb{Z}$ E L'ALGORITMO EUCLIDEO

Come abbiamo visto nel paragrafo precedente, dati due interi positivi  $a$  e  $b$ , non è detto che  $a$  sia un multiplo di  $b$  (ossia non è detto che  $b$  divida  $a$ ). Per esempio, 18 non divide 100, perché non esiste nessun intero  $c$  tale che 100 si possa scrivere come  $18 \cdot c$ : questo equivale a dire che facendo la divisione di 100 con 18 il risultato non è un intero. Quello però che possiamo fare è dividere 100 per 18, ottenendo un certo resto: precisamente, dividendo  $a = 100$  per  $b = 18$  si ottiene 5 con resto di 10 e si scrive

$$100 = 18 \cdot 5 + 10.$$

Il numero 5 prende il nome di *quoziente* e il numero 10 di *resto*.

Il fatto che siamo abituati fin dalle scuole elementari a fare questo tipo di operazioni non ci garantisce però che il risultato sia vero *in generale*.

La seguente proposizione mostra invece che questo risultato è vero in generale in  $\mathbb{Z}$ , cioè che, dati *comunque* due interi  $a$  e  $b$  con l'unica condizione che  $b$  sia diverso da zero, si può dividere  $a$  per  $b$  ottenendo un resto e che, con opportune limitazioni sul resto, quoziente e resto sono univocamente associati alla coppia di interi  $a$  e  $b$  ( $b \neq 0$ ).

Riprendiamo la nozione di valore assoluto di un intero, che abbiamo già visto nell'esercizio 54 del capitolo 1.

**DEFINIZIONE 3.8** Si definisce *valore assoluto* di un intero  $a$  il numero intero positivo

$$|a| = \begin{cases} a & \text{se } a \geq 0 \\ -a & \text{se } a < 0. \end{cases}$$

Quindi  $| -7 | = 7$ ,  $| 7 | = 7$ .

**PROPOSIZIONE 3.4 (DIVISIONE IN  $\mathbb{Z}$ )** *Siano  $a$  e  $b$  interi,  $b \neq 0$ . Allora esistono e sono univocamente individuati due interi  $q$  (quoziente) ed  $r$  (resto) tali che*

$$a = bq + r, \quad 0 \leq r < |b|.$$

**DIMOSTRAZIONE. Esistenza:** Esaminiamo separatamente i due casi che si possono presentare, cioè  $a \geq 0$  oppure  $a < 0$ .

•  $a \geq 0$ : Sia  $S$  l'insieme di tutti gli interi non negativi della forma  $a - mb$ ,  $m \in \mathbb{Z}$ : quindi l'insieme

$$S = \{n \in \mathbb{N} \mid n = a - mb, m \in \mathbb{Z}\}$$

è un sottoinsieme non vuoto di  $\mathbb{N}$ , dato che  $a \in S$ . Per il principio del minimo (cfr. par. 3 del cap. 2),  $S$  conterrà un minimo elemento, chiamiamolo  $r$ . Quindi  $r = a - qb$  per qualche  $q \in \mathbb{Z}$ . Supponiamo per assurdo che non sia  $r < |b|$ : allora sarà  $r \geq |b|$  e dalle

$$r = a - qb = a - qb - |b| + |b| = a - (q \pm 1)b + |b|,$$

si avrebbe

$$a - (q+1)b = r - |b| \in S.$$

Questo contraddice la minimalità di  $r$  in  $S$ .

**$a < 0$** : In questo caso  $-a > 0$ , quindi, per quanto appena visto, esistono due interi  $\bar{q}$  e  $\bar{r}$  tali che  $-a = b\bar{q} + \bar{r}$ , con  $0 \leq \bar{r} < b$ . Se  $\bar{r} = 0$ , allora  $a = b(-\bar{q})$ , per cui basta porre  $q = -\bar{q}$  e  $r = 0$ . Se è  $\bar{r} > 0$ , allora  $a = b(-\bar{q}) + (-\bar{r}) = b(-\bar{q}) - |b| + |b| - \bar{r} = b(-\bar{q} + 1) + (|b| - \bar{r})$  con  $0 < |b| - \bar{r} < |b|$ . In ogni caso (cioè a seconda che sia  $b > 0$  o  $b < 0$ ) si riescono a trovare due interi  $q$  ed  $r$  che risolvono il problema.

**Unicità**: Sia  $a = bq + r = bq' + r'$ ,  $0 \leq r, r' < |b|$ . Supponiamo per esempio  $r' \geq r$ . Allora  $0 \leq r' - r = b(q - q')$ , da cui, passando ai valori assoluti,

$$|b| |q - q'| = |b(q - q')| = r' - r \leq r' < |b|.$$

Ciò è possibile solo se  $|q - q'| < 1$  e cioè  $|q - q'| = 0$ , da cui  $q = q'$  e  $r = r'$ .  $\diamond$

### Esempio 3.1

$$\begin{aligned} a = 47, b = 6 & : 47 = 6 \cdot 7 + 5, \\ a = 47, b = -6 & : 47 = (-6) \cdot (-7) + 5, \\ a = -47, b = 6 & : -47 = 6 \cdot (-7) - 5 = 6 \cdot (-7 - 1) + 6 - 5 = 6 \cdot (-8) + 1, \\ a = -47, b = -6 & : -47 = (-6) \cdot 7 - 5 = (-6) \cdot (7 + 1) + 6 - 5 = (-6) \cdot 8 + 1 \end{aligned}$$

.....

**DEFINIZIONE 3.9** Siano  $a, b \in \mathbb{Z}$ . Un elemento  $d \in \mathbb{Z}$  si dice un *massimo comun divisore* tra  $a$  e  $b$  se

(i)  $d | a, d | b$ ;

(ii) se  $d' | a, d' | b$ , allora  $d' | d$ .  $\diamond$

**OSSERVAZIONE** Si parla di *un* massimo comun divisore e non *del* massimo comun divisore tra due elementi, perché se  $d$  gode delle proprietà (i) e (ii), anche ogni associato di  $d$  (e quindi  $\pm d$  nel caso di  $\mathbb{Z}$ ) gode delle stesse proprietà. In generale, quando si parla *del* massimo comun divisore in  $\mathbb{Z}$ , si intende il massimo comun divisore *positivo*. Esso si indica indifferentemente nei seguenti modi:

$$\text{MCD}(a, b), \quad \text{oppure} \quad (a, b).$$

Per esempio,  $\text{MCD}(3, -10) = 1$ ,  $\text{MCD}(a, b) = \text{MCD}(b, a) = \text{MCD}(|a|, |b|)$ ,  $\text{MCD}(ab, ac) = |a| \text{MCD}(b, c)$ ,  $\text{MCD}(0, a) = |a| \forall a \in \mathbb{Z}, a \neq 0$ . Non è invece definito il  $\text{MCD}(0, 0)$ , in quanto ogni  $x \in \mathbb{Z}$  divide lo zero, per cui non esiste un divisore *massimo*.

**DEFINIZIONE 3.10** Due interi  $a$  e  $b$  tali che  $\text{MCD}(a, b) = 1$  si dicono *coprimi* o *relativamente primi*.  $\diamond$

**DEFINIZIONE 3.11** Si definisce *minimo comune multiplo* tra due interi  $a$  e  $b$  un intero  $m$  tale che

1.  $a|m, b|m$ .

2. Dato comunque un intero  $m'$  tale che  $a|m'$  e  $b|m'$ , allora  $m|m'$ .  $\blacksquare$

Anche il minimo comune multiplo tra due interi  $a$  e  $b$ , come il massimo comun divisore, è definito a meno del segno. Normalmente il minimo comune multiplo *positivo* si denota con il simbolo

$$\text{mcm}(a, b) \quad \text{oppure} \quad [a, b].$$

Il legame tra MCD e mcm è dato dalla seguente uguaglianza

$$(3.1) \quad \text{mcm}(a, b) = \frac{|ab|}{\text{MCD}(a, b)}.$$

Abbiamo dato la *definizione* di massimo comun divisore tra due interi, ma nessuno ci garantisce che un tale elemento *esista* per ogni coppia di interi.

Una risposta a questo problema è conseguenza del teorema che abbiamo appena provato (divisione tra interi) che ci offrirà un algoritmo per il calcolo del MCD tra due interi. L'algoritmo che presenteremo è noto come *algoritmo di Euclide* o *algoritmo euclideo delle divisioni successive*: tale algoritmo risale per l'appunto ad Euclide, che lo ha descritto nel libro 7 dei suoi *Elementi*. Esso offre un metodo per il calcolo effettivo del massimo comun divisore di due interi  $a$  e  $b$ . Una dimostrazione teorica e non algoritmica dell'esistenza del MCD tra due interi viene presentata negli esercizi (cfr. eserc. 4).

Si osservi che se vogliamo determinare il  $\text{MCD}(a, b)$ , possiamo senz'altro supporre  $a \geq b > 0$ .

### 3.1 L'algoritmo euclideo.

In quel che segue sottolineiamo gli elementi che dovranno essere divisi nella divisione successiva, in modo da evidenziarli: essi verranno quindi spostati a sinistra nella divisione successiva. Siano dunque  $a, b \in \mathbb{Z}$  e sia  $a \geq b > 0$ . Operiamo le seguenti divisioni:

$$\begin{aligned} (1) \quad a &= bq_1 + r_1 & 0 < r_1 < b \\ (2) \quad b &= r_1 q_2 + r_2 & 0 < r_2 < r_1 \\ (3) \quad r_1 &= r_2 q_3 + r_3 & 0 < r_3 < r_2 \\ &\dots & \\ (i+2) \quad r_i &= r_{i+1} q_{i+2} + r_{i+2} & 0 < r_{i+2} < r_{i+1} \\ &\dots & \\ (n-1) \quad r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} & 0 < r_{n-1} < r_{n-2} \\ (n) \quad r_{n-2} &= r_{n-1} q_n + \boxed{r_n} & 0 < r_n < r_{n-1} \\ (n+1) \quad r_{n-1} &= r_n q_{n+1} + 0. & \end{aligned}$$

Allora

$$\text{MCD}(a, b) = r_n \quad (= \text{ultimo resto con nulla})$$

Il procedimento si deve certamente fermare (in meno di  $b$  passi), dato che  $b > r_1 > r_2 > r_3 \dots$  è una successione strettamente decrescente di *intervi positivi*. Ora, dall'ultima divisione  $(n+1)$ , si vede che  $r_n$  divide  $r_{n-1}$ , per cui  $\text{MCD}(r_n, r_{n-1}) = r_n$ . Inoltre, andando dal basso all'alto, dalla divisione  $n$ -esima si vede che  $r_n$  divide  $r_{n-2}$ , e inoltre, un intero  $c$  divide  $r_n$  e  $r_{n-1}$  se e solo se  $c$  divide  $r_{n-1}$  e  $r_{n-2}$ . Quindi  $\text{MCD}(r_{n-1}, r_{n-2}) = \text{MCD}(r_n, r_{n-1}) = r_n$ . Proseguendo verso l'alto, si ha  $r_n = \text{MCD}(a, b)$ .

Il numero di divisioni per giungere al calcolo del MCD tra  $a$  e  $b$  è limitato superiormente, come si è appena visto, da  $b$ : tuttavia questa non è una buona stima: esistono stime molto migliori sul numero di divisioni, legate ai numeri di Fibonacci, come mostra il seguente teorema.

**TEOREMA 3.2 (TEOREMA DI LAMÉ)** *Siano  $a$  e  $b$  due interi positivi, con  $a \geq b$ . Allora il numero  $D(a, b)$  di divisioni necessarie per trovare il  $\text{MCD}(a, b)$  con l'algoritmo euclideo delle divisioni successive è minore o uguale a  $5k$ , essendo  $k$  il numero di cifre decimali di  $b$ .*

**DIMOSTRAZIONE.** Supponiamo che il numero  $D(a, b)$  di divisioni necessarie per trovare il  $\text{MCD}(a, b)$  con l'algoritmo euclideo sia  $n+1$ .

Per ogni  $i = 1, \dots, n-1$  i quozienti  $q_i$  trovati con l'algoritmo euclideo sono  $\geq 1$ , mentre la  $(n+1)$ -esima divisione ci dice che  $q_{n+1} \geq 2$ , dato che  $r_n < r_{n-1}$ . Ma allora si avranno le seguenti diseguaglianze che collegano i resti con la successione  $\{f_n\}$  dei numeri di Fibonacci:

$$\begin{aligned} r_n &\geq 1 = f_2 \\ r_{n-1} &\geq 2r_n \geq 2f_2 = f_3 \\ r_{n-2} &\geq r_{n-1} + r_n \geq f_3 + f_2 = f_4 \\ &\dots \\ r_i &\geq r_{i+1} + r_{i+2} \geq f_{n-i+1} + f_{n-i} = f_{n-i+2} \\ &\dots \\ r_1 &\geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1} \\ b &\geq r_1 + r_2 \geq f_{n+1} + f_n = f_{n+2} \end{aligned}$$

Dunque  $b \geq f_{n+2}$ . Dato che, per  $\Phi = \frac{1+\sqrt{5}}{2}$ ,  $\forall n > 2$  è  $f_n > \Phi^{n-2}$  (cfr. eserc. 20 cap. 2), allora si avrà  $b \geq f_{n+2} > \Phi^n$ . Ora,  $\log_{10} \Phi$  vale circa 0,208 che è una quantità maggiore di  $\frac{1}{5}$ . Quindi

$$\log_{10} b > \log_{10} \Phi^n = n \log_{10} \Phi > \frac{n}{5},$$

da cui  $n < 5 \log_{10} b$ . Supposto che  $b$  abbia  $k$  cifre decimali (ossia  $b < 10^k$ ), allora  $\log_{10} b < k$ . Ne segue che  $n < 5k$ , per cui  $D(a, b) = n+1 \leq 5k$ .  $\diamond$

### Esempio 3.2

Sia  $a = 897$ ,  $b = 350$ . Il Teorema di Lamé dice che il numero di divisioni necessarie per determinare con l'algoritmo euclideo il  $\text{MCD}(a, b)$  è minore o uguale a  $5 \cdot 3 = 15$ . In realtà ne servono molto meno: si controlli. Tuttavia la stima di 15 è ben migliore della prima stima  $b = 350$ .

**OSSERVAZIONE** Si noti che il numero di divisioni nell'algoritmo euclideo può essere ridotto se, anziché scegliere come resto il più piccolo resto *positivo*, si scelgono i resti soggetti alla condizione

$$-\frac{1}{2} r_{i-1} \leq r_i \leq \frac{1}{2} r_{i-1}.$$

**OSSERVAZIONE** Nelle scuole medie eravamo abituati a calcolare il MCD tra due interi in un altro modo: per esempio, per calcolare il  $\text{MCD}(36, 40)$  procedevamo al modo seguente: fattorizzavamo in primi i due numeri, e il MCD era costituito dai fattori comuni con il più piccolo esponente. Nel nostro caso

$$36 = 2^2 \cdot 3^2, \quad 40 = 2^3 \cdot 5 \implies \text{MCD}(36, 40) = 2^2.$$

È chiaro che se di due interi *conosciamo* la fattorizzazione in primi, il metodo che eravamo soliti usare è senz'altro il più conveniente. Per esempio, se ci viene chiesto di trovare il  $\text{MCD}(a, b)$  con

$$a = 2^4 \cdot 5^6 \cdot 7^2 \cdot 11^3 \cdot 13, \quad b = 2 \cdot 3^5 \cdot 5 \cdot 11^6$$

si trova senza colpo ferire che  $\text{MCD}(a, b) = 2 \cdot 5 \cdot 11^3$ .

Ci sono però due problemi:

- Non abbiamo ancora provato quello che noi diamo per scontato, cioè che *ogni* intero si può fattorizzare in primi, e quindi non siamo sicuri di potere utilizzare questo metodo per ogni coppia di interi: in realtà il risultato è vero, e costituisce uno dei pilastri delle proprietà degli interi: lo proveremo nel Teorema 3.3 (Teorema Fondamentale dell'Aritmetica).
- Il vero problema tuttavia è che, mentre per interi piccoli il metodo delle scuole medie funziona egregiamente, invece, come avremo modo di affermare a più riprese, il problema della fattorizzazione di interi grandi è un problema dal punto di vista computazionale molto complesso. Quindi per interi grandi l'algoritmo euclideo delle divisioni successive è più efficace dal punto di vista computazionale proprio perché non richiede la conoscenza della scomposizione dei numeri in fattori primi.

Si noti che conoscendo la scomposizione in fattori primi anche di uno solo (non necessariamente di entrambi) dei due numeri, allora per trovare il MCD basta dividere il secondo numero per i fattori primi del primo e ancora prendere come MCD i fattori primi comuni con il più piccolo esponente.

### Esempio 3.3

Trovare  $\text{MCD}(2^2 \cdot 3^4 \cdot 13 \cdot 17, 6760)$ .

Basta dividere 6760 per 2, ottenendo 3380, poi dividere 3380 ancora per 2, ottenendo 1690, poi dividere 1690 per 3 (ma non è divisibile), poi dividere 1690 per 13: si ottiene 130. Poi dividere 130 per 17 (ma non è divisibile). In definitiva il  $\text{MCD}(2^2 \cdot 3^4 \cdot 13 \cdot 17, 6760) = 2^2 \cdot 13 = 52$ .

L'algoritmo euclideo delle divisioni successive fornisce un metodo efficiente non solo per il calcolo del MCD tra due interi, ma, stante la (3.1), anche per il calcolo del mcm.

### BALLOON

(Dimostrazione teorica dell'esistenza del MCD) Provare che, dati comunque  $a, b \in \mathbb{Z}$  e non entrambi nulli, esiste il loro massimo comun divisore  $d = \text{MCD}(a, b)$ . Inoltre si possono trovare due interi  $s$  e  $t$  in  $\mathbb{Z}$  tali che  $d = sa + tb$  (identità di Bézout).

Sappiamo che il prodotto di due interi  $a$  e  $b$  è  $ab = 2^5 \cdot 3^4 \cdot 7^2 \cdot 11^4 \cdot 13^2$  e che il loro minimo comune multiplo è  $2^3 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13^2$ . Determinare il MCD( $a, b$ ).

Provare che, dato comunque un  $n > 0$  esistono due interi positivi  $a$  e  $b$  tali che nel calcolo del MCD( $a, b$ ) con l'algoritmo euclideo, il numero delle divisioni necessarie è esattamente  $n$ .

Determinare il MCD tra le seguenti coppie di numeri mediante l'algoritmo euclideo delle divisioni successive:

- (1338, 750);
- (10 285, 8993);
- (2299, 5083).

## 4 RAPPRESENTAZIONE DEGLI INTERI

Approfittiamo del fatto che abbiamo studiato la divisione in  $\mathbb{Z}$  per aprire una breve parentesi sul modo di rappresentare gli interi. Quando scriviamo 2476 diamo per scontato che con ciò intendiamo parlare del numero  $2 \cdot 10^3 + 4 \cdot 10^2 + 7 \cdot 10 + 6$ . Si tratta della ordinaria *scrittura posizionale in base 10* dei numeri, che comunemente adottiamo. Ogni numero intero ha quindi una sua rappresentazione in base 10: le cifre che lo compongono sono interi positivi maggiori o uguali a 0 e minori o uguali a 9 e ogni cifra ha un significato diverso a seconda della posizione che occupa: parliamo di unità, decine, centinaia, ecc. Il numero 2476 ha 6 unità, 7 decine, 4 centinaia, 2 migliaia. Dovremmo scrivere  $(2476)_{10}$  anziché 2476, tuttavia ormai si dà per scontato che gli interi si scrivono in genere in base 10. Tuttavia la base 10 non ha in teoria nulla di speciale: può benissimo essere sostituita da un altro qualunque intero positivo  $b$  maggiore di 1. La possibilità di rappresentare gli interi in basi diverse è offerta dalla seguente proposizione.

**PROPOSIZIONE 3.5** *Sia  $b$  un intero positivo maggiore di 1. Ogni intero positivo  $a$  può essere rappresentato in modo unico nella forma*

$$a = r_k b^k + r_{k-1} b^{k-1} + \cdots + r_1 b + r_0,$$

con  $k$  intero non negativo,  $r_i \in \mathbb{N}$  e minori di  $b$ ,  $r_k \neq 0$ .

**DIMOSTRAZIONE.** Procediamo per induzione su  $a$ . Per  $a = 0$  non c'è niente da dimostrare. Supponiamo quindi di avere dimostrato il risultato per ogni intero minore di  $a$  e dimostriamolo per  $a$ . Dividendo  $a$  per  $b$  si ha:

$$a = b \cdot q + r_0, \quad 0 \leq r_0 < b.$$

Il quoziente  $q$  è ovviamente minore di  $a$ , e quindi, in virtù dell'ipotesi induttiva,  $q$  si può rappresentare in modo unico al modo seguente:

$$q = r_k b^{k-1} + r_{k-1} b^{k-2} + \cdots + r_2 b + r_1, \quad 0 \leq r_i < b \forall i.$$

Ne segue che  $a = bq + r_0 = r_k b^k + r_{k-1} b^{k-1} + \cdots + r_1 b + r_0$ . L'unicità della scrittura deriva dalla unicità di quoziente e resto della prima divisione e dal fatto che per induzione la scrittura di  $q$  è unica.  $\diamond$

Per esempio il 6 (rappresentante le unità del numero 2476) altro non è che il resto della divisione di 2476 per 10:

$$2476 = 10 \cdot 247 + 6.$$

Il 7 (rappresentante le decine di 2476 e le unità del quoziente 247 della divisione precedente) altro non è che il resto della divisione per 10 di 247:

$$247 = 10 \cdot 24 + 7.$$

Andando avanti, il 4 altro non è che il resto della divisione per 10 di 24

$$24 = 10 \cdot 2 + 4$$

e infine il 2 è il resto della divisione di 2 per 10:

$$2 = 10 \cdot 0 + 2.$$

Le basi più comunemente usate sono la base 2, la base 8 e la base 16, soprattutto quando si ha a che fare con i calcolatori. Da quanto ora detto è quindi chiaro come dovremo scrivere in base 2 il numero intero che in base 10 si scrive 2476. Basta fare via via le divisioni per 2 e poi prendere i resti dal basso verso l'alto.

$$\begin{array}{rcl} 2476 & = & 2 \cdot 1238 + 0 \\ 1238 & = & 2 \cdot 619 + 0 \\ 619 & = & 2 \cdot 309 + 1 \\ 309 & = & 2 \cdot 154 + 1 \\ 154 & = & 2 \cdot 77 + 0 \\ 77 & = & 2 \cdot 38 + 1 \\ 38 & = & 2 \cdot 19 + 0 \\ 19 & = & 2 \cdot 9 + 1 \\ 9 & = & 2 \cdot 4 + 1 \\ 4 & = & 2 \cdot 2 + 0 \\ 2 & = & 2 \cdot 1 + 0 \\ 1 & = & 2 \cdot 0 + 1 \end{array}$$

Il numero 2476 si scrive quindi in base 2 al modo seguente:  $(100110101100)_2$ . Si noti come le cifre che lo compongono siano costituite da soli 0 e 1 e che nel fare le divisioni ci siamo fermati quando abbiamo raggiunto *quoziente* nullo.

La scrittura di un numero in base 2 è quella che comunemente si utilizza con i calcolatori.

Per fare le operazioni tra interi in base 10 sappiamo che dobbiamo conoscere le tabelline, ossia le addizioni e moltiplicazioni dei numeri da 0 a 9 (ossia le cifre della scrittura decimale del numero). Ebbene, fissata una qualunque base  $b$ , per operare in base  $b$  occorre conoscere le tabelline relative a quella base, ossia le addizioni e moltiplicazioni dei numeri tra 0 e  $b-1$ . In particolare in base 2 le tabelline sono le seguenti:

+	0	1
0	0	1
1	1	10

*	0	1
0	0	0
1	0	1

In base 3 sono:

+	0	1	2
0	0	1	2
1	1	2	10
2	2	10	11

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	11

Si osservi come la scrittura in base  $b$  del numero  $b$  è sempre 10, cioè  $b = (10)_b$ .

### Esercizi

- Ⓐ Scrivere in base 2 il numero 12345.
- Ⓑ Scrivere in base 3 il numero 12345.
- Ⓒ Addizionare e moltiplicare tra loro i due numeri  $(100001)_2$  e  $(101110)_2$ .
- Ⓓ Passare dalla scrittura in base 2 alla scrittura in base 10 i numeri dell'esercizio precedente.

## 5 IDENTITÀ DI BÉZOUT ED EQUAZIONI DIOFANTEE

Nel corso della dimostrazione dell'esercizio 4 abbiamo visto che il  $\text{MCD}(a, b)$  si può scrivere come combinazione lineare a coefficienti interi di  $a$  e  $b$ , ossia esistono due interi  $s$  e  $t$  tali che  $d = sa + tb$ : una tale relazione prende il nome di *identità di Bézout*. Quella dimostrazione non offriva però un metodo per determinare tali interi  $s$  e  $t$ . L'algoritmo euclideo delle divisioni successive ci permetterà invece di determinare una coppia  $(s, t)$  che risolve il problema.

A partire dall'algoritmo euclideo delle divisioni successive, per ottenere una tale relazione, basta provare che tutti i resti delle divisioni si possono scrivere come combinazioni lineari di  $a$  e  $b$ . Esplicitando i resti si ottiene

$$r_1 = \underline{a} - \underline{b}q_1$$

$$r_2 = \underline{b} - r_1q_2$$

...

$$r_{i+2} = r_i - r_{i+1}q_{i+2}$$

...

da cui

$$r_2 = \underline{b} - r_1q_2 = \underline{b} - (\underline{a} - \underline{b}q_1)q_2 = (-q_2)\underline{a} + (1 + q_1q_2)\underline{b}$$

cioè i primi due resti  $r_1$  e  $r_2$  si scrivono come combinazione di  $a$  e  $b$ . Supposto allora che  $r_i$  e  $r_{i+1}$  si possano scrivere come combinazione di  $a$  e  $b$ , allora  $r_{i+2}$  si può scrivere come combinazione di  $a$  e  $b$ . Ma allora ogni resto si può scrivere nel modo richiesto, e in particolare  $r_n$  che è il massimo comun divisore.

Introduciamo ora, attraverso un esempio, una notazione che facilita i conti e che si presta ad essere programmata.

Supponiamo di voler determinare una identità di Bézout per il  $\text{MCD}(2016, 35)$ . Allora,  $a = 2016$ ,  $b = 35$ . Con l'algoritmo euclideo delle divisioni successive si ricava il MCD:

$$2016 = 35 \cdot 57 + 21$$

$$35 = 21 \cdot 1 + 14$$

$$21 = 14 \cdot 1 + 7$$

$$14 = 7 \cdot 2 + 0$$

da cui  $\text{MCD}(2016, 35) = 7$ . Se vogliamo ora esprimere 7 nella forma  $\alpha\underline{a} + \beta\underline{b}$  il problema che avevamo incontrato era che nel corso dei vari passaggi per distinguere i resti dai coefficienti dei resti (entrambi sono degli interi) avevamo *sottolineato* i resti. Il seguente accorgimento risolve questa difficoltà.

Introduciamo la seguente notazione per rappresentare una combinazione lineare di  $a$  e  $b$ :

$$\alpha\underline{a} + \beta\underline{b} \equiv (\alpha, \beta) :$$

dimentichiamo cioè  $\underline{a}$  e  $\underline{b}$  e scriviamo solo i coefficienti  $\alpha$  e  $\beta$  della combinazione lineare all'interno della coppia. All'elemento  $\underline{a}$  resterà associata la coppia  $(1, 0)$ , mentre a  $\underline{b}$  resterà associata la coppia  $(0, 1)$ . Date due combinazioni lineari  $\alpha\underline{a} + \beta\underline{b}$  e  $\alpha'\underline{a} + \beta'\underline{b}$ , alla loro somma

$$(\alpha\underline{a} + \beta\underline{b}) + (\alpha'\underline{a} + \beta'\underline{b}) = (\alpha + \alpha')\underline{a} + (\beta + \beta')\underline{b}$$

corrisponde ovviamente la coppia  $(\alpha + \alpha', \beta + \beta')$ . Al prodotto di un intero  $\gamma$  per una combinazione lineare  $\alpha\underline{a} + \beta\underline{b}$

$$\gamma(\alpha\underline{a} + \beta\underline{b}) = (\gamma \cdot \alpha\underline{a} + \gamma \cdot \beta\underline{b})$$

corrisponde la coppia  $(\gamma\alpha, \gamma\beta)$ . Definendo quindi l'addizione tra coppie e la moltiplicazione di un intero per una coppia al modo seguente

$$(\alpha, \beta) + (\alpha', \beta') \stackrel{\text{def}}{=} (\alpha + \alpha', \beta + \beta'), \quad \gamma(\alpha, \beta) \stackrel{\text{def}}{=} (\gamma\alpha, \gamma\beta)$$



$\forall \alpha, \beta, \gamma, \alpha', \beta' \in \mathbb{Z}$ , le operazioni che portano alla identità di Bézout si possono riassumere così:

$$\begin{aligned} r_1 &= 21 = \underline{a} + \underline{b} \cdot (-57) \equiv (1, 0) + (0, 1)(-57) = (1, -57) \\ r_2 &= 14 = \underline{b} + \underline{21} \cdot (-1) \equiv (0, 1) + (1, -57)(-1) = (-1, 58) \\ r_3 &= 7 = \underline{21} + \underline{14} \cdot (-1) \equiv (1, -57) + (-1, 58)(-1) = (2, -115) \end{aligned}$$

Quindi

$$7 \equiv (2, -115)$$

da cui  $\alpha = 2$ ,  $\beta = -115$  e l'identità di Bézout cercata è

$$7 = 2 \cdot 2016 + (-115) \cdot 35.$$

La determinazione di una identità di Bézout per il MCD tra due interi risulta fondamentale per trovare delle soluzioni *interne* di equazioni lineari del tipo:

$$ax + by = c, \quad a, b, c \in \mathbb{Z}.$$

Formalizziamo con una definizione questo tipo di equazioni.

**DEFINIZIONE 3.12** Se  $a, b$  e  $c$  sono interi, una equazione della forma  $ax + by = c$ , della quale cerchiamo soluzioni intere prende il nome di *equazione diofantea*.  $\blacksquare$

Geometricamente l'equazione  $ax + by = c$  rappresenta una retta, della quale stiamo cercando punti a coordinate intere. Per esempio, la  $4x + 5y = 1$  è rappresentata dalla figura 3.1.

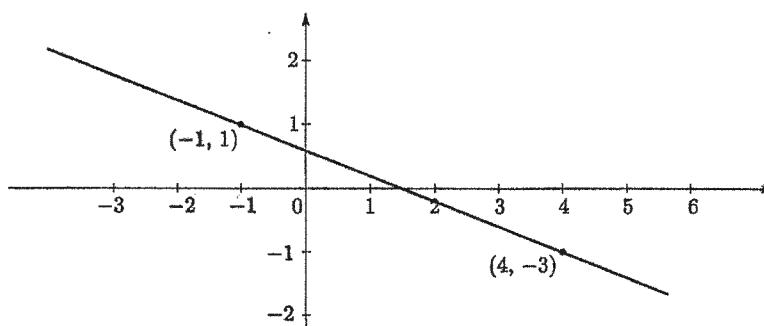


Figura 3.1. La retta  $4x + 5y = 1$ .

Non è difficile vedere che una soluzione intera di questa equazione è per esempio  $(-1, 1)$ . Se invece volessimo trovare soluzioni intere della seguente equazione diofantea

$$3x + 15y = 8,$$

non ci riusciremmo. Perché la prima equazione ammette soluzioni mentre la seconda no? La spiegazione della differenza di comportamento delle due equazioni risiede nella seguente proposizione che offre una condizione necessaria e sufficiente perché un'equazione  $ax + by = c$  con  $a, b, c \in \mathbb{Z}$  ammetta soluzioni intere.

**PROPOSIZIONE 3.6** L'equazione  $ax + by = c$ ,  $a, b, c \in \mathbb{Z}$ , possiede una soluzione intera  $(x, y)$  se e solo se  $\text{MCD}(a, b) = d$  divide  $c$ .

**DIMOSTRAZIONE.** Sia  $(\bar{x}, \bar{y})$  una soluzione intera dell'equazione. Allora il  $\text{MCD}(a, b)$ , dividendo  $a$  e  $b$ , dividerà anche tutto il primo membro dell'equazione e quindi anche  $c$ .

Viceversa, supponiamo che  $d$  divida  $c$ . Scriviamo  $d$  nella forma  $d = \alpha a + \beta b$ . Allora, essendo  $c = d \cdot h$ , sarà  $c = \alpha ha + \beta hb$  cioè  $(\bar{x} = ah, \bar{y} = bh)$  rappresenta una soluzione intera dell'equazione.  $\diamond$

#### Esempio 3.4

L'equazione

$$(5.1),$$

$$3x + 7y = 2$$

è risolubile in  $\mathbb{Z}$ , perché  $(3, 7) = 1$  e 1 divide 2. Allora, essendo  $1 = (-2)\underline{3} + (1)\underline{7}$ , si ha  $2 = (-4)\underline{3} + (2)\underline{7}$ . Una soluzione intera della (5.1) è quindi  $(-4, 2)$ . Si osservi che tale soluzione non è unica. Per esempio, un'altra soluzione intera della (5.1) è  $(10, -4)$ .

**OSSERVAZIONE** La proposizione 3.6 ci offre un metodo per determinare una soluzione  $(\bar{x}, \bar{y})$  della  $ax + by = c$ : basta esprimere il  $\text{MCD}(a, b) = d$  come  $\alpha a + \beta b$  e una soluzione è data da  $\bar{x} = ah$ ,  $\bar{y} = bh$ , essendo  $h$  tale che  $c = dh$ . Naturalmente a volte si riesce a determinare una soluzione della  $ax + by = c$  senza dover ricorrere a questo metodo: in tal caso siamo fortunati, perché ce la caviamo senza fatica. Per esempio, se dobbiamo trovare una soluzione dell'equazione

$$5687x + 5657y = 30$$

si vede immediatamente che una soluzione è data da  $(1, -1)$ , dato che  $5687 - 5657 = 30$ : in questo caso *senza dovere calcolare il MCD(5687, 5657)*, sappiamo che l'equazione ammette soluzioni, e che quindi, in virtù della proposizione 3.6, il MCD sarà necessariamente un divisore di 30.

Ci poniamo ora il problema di determinare *tutte* le soluzioni di un'equazione diofantea che possieda una soluzione.

**PROPOSIZIONE 3.7** Siano  $a, b, c \in \mathbb{Z}$  e sia  $(\bar{x}, \bar{y})$  una soluzione intera della

$$(5.2)$$

$$ax + by = c.$$

Allora tutte e sole le soluzioni intere di tale equazione si ottengono aggiungendo alla  $(\bar{x}, \bar{y})$  la soluzione generale dell'equazione omogenea associata  $ax + by = 0$ , ossia tutte e sole le soluzioni intere della (5.2) sono del tipo  $(x', y')$ , dove

$$x' = \bar{x} - \frac{b}{d}t, \quad y' = \bar{y} + \frac{a}{d}t \quad \text{al variare di } t \in \mathbb{Z},$$

essendo  $d = \text{MCD}(a, b)$ .

**DIMOSTRAZIONE.** La somma di una soluzione della (5.2) e di una soluzione  $(x_0, y_0)$  dell'equazione omogenea associata è ancora soluzione della (5.2). Infatti

$$a(\bar{x} + x_0) + b(\bar{y} + y_0) = \underbrace{a\bar{x} + b\bar{y}}_{=c} + \underbrace{ax_0 + by_0}_{=0} = c.$$

Viceversa, siano  $(\bar{x}, \bar{y})$  e  $(x', y')$  due soluzioni della  $ax + by = c$ . Allora

$$a(\bar{x} - x') + b(\bar{y} - y') = a\bar{x} + b\bar{y} - ax' - by' = c - c = 0,$$

cioè  $(x', y')$  differisce da  $(\bar{x}, \bar{y})$  per una soluzione dell'equazione omogenea, ossia ogni soluzione della (5.2) è somma di una fissata soluzione  $(\bar{x}, \bar{y})$  di (5.2) e di una soluzione dell'equazione omogenea associata. Ma chi è la soluzione generale dell'equazione omogenea associata  $ax + by = 0$ ? Indicato con  $d$  il  $\text{MCD}(a, b)$ , dividiamo primo e secondo membro di questa equazione per  $d$ : siano  $a', b'$  tali che  $a = da'$ ,  $b = db'$ . Allora la  $ax + by = 0$  diventa  $a'x + b'y = 0$ , con  $\text{MCD}(a', b') = 1$ . Ora, come è immediato controllare, tutte e sole le soluzioni  $(x_0, y_0)$  della  $a'x + b'y = 0$  sono  $x_0 = -b't$ ,  $y_0 = a't$ ,  $t \in \mathbb{Z}$ . Quindi in definitiva tutte e sole le soluzioni della  $ax + by = 0$  sono del tipo

$$\left( -\frac{b}{d}t, \frac{a}{d}t \right) \quad \text{al variare di } t \in \mathbb{Z}.$$

In definitiva, tutte e sole le soluzioni della (5.2) sono del tipo  $(x', y')$ , dove

$$x' = \bar{x} - \frac{b}{d}t, \quad y' = \bar{y} + \frac{a}{d}t. \quad \text{al variare di } t \in \mathbb{Z},$$

essendo  $d = \text{MCD}(a, b)$ .

**OSSERVAZIONE** Il teorema appena dimostrato ci mostra come, avendo a disposizione una sola soluzione  $(\bar{x}, \bar{y})$  dell'equazione  $ax + by = c$ , si riescono a determinare tutte le soluzioni. Si osservi che se per caso siamo riusciti a trovare una soluzione  $(\bar{x}, \bar{y})$  della  $ax + by = c$  senza dover calcolare il  $\text{MCD}(a, b)$ , per determinare tutte le soluzioni, che sono del tipo  $(\bar{x} - \frac{b}{d}t, \bar{y} + \frac{a}{d}t)$  al variare di  $t \in \mathbb{Z}$ , il MCD siamo costretti a calcolarlo.

### Esercizi

Decidere se le seguenti equazioni diofantee ammettono soluzioni intere e, in caso positivo, determinare tutte le soluzioni.

a)  $385x + 33y = 143$ ,      b)  $385x + 33y = 105$ .

Trovare tutte le soluzioni intere (se esistono) di ciascuna delle seguenti due equazioni:

a)  $153x + 45y = 18$ ,      b)  $45x + 153y = 10$ .

Dire se esistono  $x, y \in \mathbb{Z}$  tali che

a)  $819x + 221y = 26$ ,      b)  $819x + 221y = 28$ .

In caso affermativo, determinare tutte e sole le soluzioni  $x, y \in \mathbb{Z}$  che soddisfano l'equazione.

Si determinino tutte e sole le soluzioni (se esistono) delle seguenti equazioni diofantee:

a)  $85x + 51y = 78$ ,      b)  $85x + 51y = 68$ .

Provare, senza calcolarlo esplicitamente, che  $\text{MCD}(8747, 8717)$  è un divisore di 120.

## ■ 6 EQUIVALENZA DI IRRIDUCIBILI E PRIMI IN $\mathbb{Z}$ E IL TEOREMA FONDAMENTALE DELL'ARITMETICA

Avendo a disposizione i risultati del paragrafo precedente, siamo finalmente in grado di provare l'*equivalenza* in  $\mathbb{Z}$  delle nozioni di elemento irriducibile ed elemento primo (cfr. definizioni 3.6 e 3.7, con relativi commenti a proposito della nozione di numero primo.) Abbiamo già provato (proposizione 3.3) che ogni elemento primo in  $\mathbb{Z}$  è irriducibile. Proveremo ora che ogni elemento irriducibile in  $\mathbb{Z}$  è primo.

**PROPOSIZIONE 3.8** *Ogni elemento irriducibile in  $\mathbb{Z}$  è primo.*

**DIMOSTRAZIONE.** Sia  $p$  un elemento irriducibile in  $\mathbb{Z}$ . Per provare che  $p$  è primo, dobbiamo provare che se  $p$  divide un prodotto  $ab$ , allora  $p$  divide  $a$  o  $b$ . Sia dunque  $p|ab$ , cioè  $ab = ph$  ( $h \in \mathbb{Z}$ ) e supponiamo che  $p$  non divida  $a$ . Allora, dato che l'unico divisore di  $p$  che divide  $a$  è 1, segue che  $\text{MCD}(a, p) = 1$ . Ma allora (identità di Bézout) esistono  $s, t \in \mathbb{Z}$  tali che  $1 = sa + tp$ . Moltiplicando per  $b$  entrambi i membri, si ottiene  $b = sab + tpb$ ; dato che  $p | ab$  e  $p | p$ , si conclude che  $p | b$ .

Questa equivalenza tra le nozioni di elemento primo e elemento irriducibile in  $\mathbb{Z}$  sarà la base per la dimostrazione di quel risultato che ben a ragione viene chiamato **Teorema Fondamentale dell'Aritmetica**.

**TEOREMA 3.3 (TEOREMA FONDAMENTALE DELL'ARITMETICA)** *Sia  $n$  un intero  $> 1$ . Allora  $n$  si può fattorizzare nel prodotto di un numero finito di elementi irriducibili (o numeri primi)  $p_j > 1$ :*

$$n = p_1^{h_1} p_2^{h_2} p_3^{h_3} \cdots p_s^{h_s}$$

dove i  $p_j$ ,  $j = 1, \dots, s$ , sono tutti distinti, gli esponenti  $h_j$  sono positivi e  $s \geq 1$ . Inoltre tale fattorizzazione è unica, nel senso che se  $n$  può essere fattorizzato anche al modo seguente

$$n = q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t}$$

con i  $q_i$  elementi irriducibili distinti maggiori di 1, allora il numero dei fattori nella prima fattorizzazione uguaglia il numero dei fattori della seconda e i  $q_i$  coincidono a meno dell'ordine con i  $p_j$ .

**DIMOSTRAZIONE. Esistenza della fattorizzazione.** Procederemo per induzione sull'intero  $n$  da fattorizzare, utilizzando il principio di induzione I (cfr. par. 3 del cap. 2). Se  $n = 2$ ,  $2 = 2$  è una fattorizzazione in elementi irriducibili  $> 1$ . Supponiamo allora di avere provato l'esistenza di una tale fattorizzazione per ogni intero positivo  $k < n$ ,  $k \geq 2$  e dimostriamolo per  $n$ . Se  $n$  è irriducibile, non c'è nulla da dimostrare. Sia quindi  $n$  riducibile, e sia  $n = ab$  una fattorizzazione propria, nel senso che  $a$  e  $b$  sono entrambi  $\geq 2$  e  $< n$ . Allora, per l'ipotesi induttiva,  $a$  e  $b$  sono fattorizzabili in un prodotto di irriducibili maggiori di 1:  $a = p_1 p_2 \cdots p_r$ ,  $b = \bar{p}_1 \bar{p}_2 \cdots \bar{p}_s$ . Quindi  $n = p_1 p_2 \cdots p_r \bar{p}_1 \bar{p}_2 \cdots \bar{p}_s$  e, per il principio di induzione I, ogni intero positivo si può fattorizzare in un prodotto di irriducibili maggiori di 1. Basta poi raggruppare fra loro i numeri primi fra loro uguali nella fattorizzazione per ottenere il risultato nella forma voluta.

**Unicità della fattorizzazione.** Per dimostrare l'unicità della fattorizzazione per ogni intero positivo  $n$ , procederemo per induzione sul numero  $m$  di fattori irriducibili di una fattorizzazione di lunghezza minima. Se  $m = 1$ , significa che il numero  $n$  che ha quella come fattorizzazione è un irriducibile (quindi primo)  $p > 1$ : supponiamo che  $n = p$  abbia un'altra

fattorizzazione  $q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t}$ ; allora

$$p = q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t}, \quad q_i > 1.$$

Essendo  $p$  un primo che divide il secondo membro,  $p$  dividerà uno dei fattori del secondo membro; sia  $p \mid q_i$ . Anche  $q_i$  è irriducibile, quindi non ha fattori propri, da cui  $p = q_i$ . Per la legge di cancellazione, valida in  $\mathbb{Z}$ , si ottiene

$$1 = q_1^{k_1} q_2^{k_2} \cdots q_i^{k_i-1} \cdots q_t^{k_t}.$$

Questa relazione implica che tutti gli esponenti a secondo membro sono nulli, altrimenti avremmo un prodotto di interi maggiori di 1 il cui prodotto dà 1. Allora il secondo membro si riduce a  $q_i$  e quindi  $p = q_i$  è l'unica fattorizzazione di  $n$ . Abbiamo così provato la base dell'induzione. Supponiamo ora che la unicità della fattorizzazione sia stata provata per ogni fattorizzazione in  $m-1$  fattori irriducibili. Sia  $n$  un intero che ha una fattorizzazione in  $m$  fattori irriducibili. Siano allora

$$n = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s} = q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t} \quad p_i, q_j > 1$$

due fattorizzazioni di  $n$  in fattori irriducibili, la fattorizzazione di sinistra avendo  $m$  fattori irriducibili, cioè  $h_1 + h_2 + \cdots + h_s = m$ . Ora,  $p_1$  è un primo che divide il secondo membro, quindi dividerà un  $q_j$ . Come prima, risulta  $p_1 = q_j$ , onde si possono cancellare da ambo i membri. Ma allora si resta con

$$p_1^{h_1-1} p_2^{h_2} \cdots p_s^{h_s} = q_1^{k_1} q_2^{k_2} \cdots q_i^{k_i-1} \cdots q_t^{k_t}$$

dove a primo membro il numero di fattori irriducibili è  $m-1$ . Per l'ipotesi induttiva vale in questo caso la unicità della fattorizzazione, onde i  $q_j$  coincidono con i  $p_i$ , a meno dell'ordine. Ma allora anche la fattorizzazione di  $n$  è unica.  $\diamond$

**OSSERVAZIONE** Si noti come nel corso della dimostrazione sia risultata fondamentale l'equivalenza in  $\mathbb{Z}$  tra l'essere primo e l'essere irriducibile.

Il Teorema Fondamentale dell'Aritmetica dice sostanzialmente che i numeri primi (o elementi irriducibili) positivi di  $\mathbb{Z}$  sono i mattoni con i quali, attraverso la moltiplicazione, si costruiscono tutti i numeri naturali. Vale la pena di elencare i numeri primi minori di 1000.

2	3	5	7	9	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89	97
101	103	107	109	113	127	131	137	139	149	151	157	163
167	173	179	181	191	193	197	199	211	223	227	229	233
239	241	251	257	263	269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359	367	373	379	383	389
397	401	409	419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541	547	557	563
569	571	577	587	593	599	601	607	613	617	619	631	641
643	647	653	659	661	673	677	683	691	701	709	719	727
733	739	743	751	757	761	769	773	787	797	809	811	821
823	827	829	839	853	857	859	863	877	881	883	887	907
911	919	929	937	941	947	953	967	971	977	983	991	997

Come abbiamo fatto a creare questa tabella? In altre parole, fissato un intero  $n$ , come si trovano tutti i primi minori o uguali a  $n$ ? Con il seguente algoritmo, detto *crivello di Eratostene*.

## 6.1 Il crivello di Eratostene

Il metodo consiste nei punti seguenti: si scrivono tutti i numeri  $\leq n$ , a partire da 2, che viene sottolineato; poi si cancellano tutti i multipli di 2. Si sottolinea poi il primo numero non cancellato (ossia 3) e si cancellano tutti i multipli di 3, e così via, finché non ci siano numeri non cancellati  $\leq \sqrt{n}$ . Ebbene, tutti i numeri sottolineati, assieme a tutti quelli che non sono stati cancellati, forniscono la lista completa di tutti i numeri primi  $\leq n$ . Perché è stato sufficiente fermarsi a  $\sqrt{n}$ , anziché procedere fino ad  $n$ ? perché se un intero  $n$  non è divisibile per nessun primo  $\leq \sqrt{n}$ , allora  $n$  è primo (cfr. eserc. 18). Questo porta a un notevole vantaggio computazionale. Per esempio, se vogliamo calcolare tutti i primi minori di 100, basta operare come detto sopra solamente fino a  $\sqrt{100} = 10$ . Tutti i numeri sottolineati, assieme ai numeri che non sono stati cancellati rappresentano i primi minori di 100.

Il Teorema Fondamentale dell'Aritmetica garantisce che ogni intero si scrive come prodotto di primi. Questo fatto è molto importante per capire gli interi e dimostrare fatti sugli interi. In particolare, come abbiamo già detto nell'Osservazione 3.1, se di due interi si conosce effettivamente (e non solo in teoria) la fattorizzazione in primi, per il calcolo del loro MCD possiamo utilizzare il metodo che usavamo a scuola: si prendono i fattori primi comuni con il più piccolo esponente. Ma, come abbiamo detto, il problema di trovare effettivamente la fattorizzazione di interi grandi è un problema computazionalmente complesso.

Il Teorema Fondamentale dell'Aritmetica vale anche per interi arbitrari e non solo per numeri naturali.

**PROPOSIZIONE 3.9** Preso comunque un intero  $z$  diverso da zero e da  $\pm 1$ , esso ha una unica scrittura della forma

$$z = \pm p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}, \quad p_i \text{ irriducibili} > 1.$$

Abbiamo già osservato che nella dimostrazione dell'unicità della fattorizzazione del Teorema Fondamentale dell'Aritmetica ha giocato in modo essenziale il fatto che in  $\mathbb{Z}$  le due nozioni di elemento irriducibile e elemento primo coincidono. Ci poniamo questo problema: esistono casi (ovviamente non in  $\mathbb{Z}$ ) in cui la nozione di elemento irriducibile e quella di elemento primo non coincidono? Cosa possiamo allora dire sulla unicità della fattorizzazione in irriducibili? È quanto racconteremo nel capitolo 11 relativo agli Approfondimenti. Qui accenniamo solamente al fatto che questo problema è legato all'Ultimo Teorema di Fermat, di cui forse molti hanno sentito parlare. Si consideri l'equazione

$$x^n + y^n = z^n.$$

Se  $n = 2$  è facile trovare soluzioni intere di questa equazione: per esempio  $x = 3, y = 4, z = 5$ , oppure  $x = 12, y = 5, z = 13$ : terne di questo tipo prendono il nome di *terne pitagoriche* e ce ne sono infinite. Nella prima metà del 1600 il matematico francese P. Fermat, sotto forma di una nota scritta sul margine della sua copia dell'Aritmetica di Diofanto, scrisse di avere trovato una soluzione davvero meravigliosa del fatto che l'equazione diofantea  $x^n + y^n = z^n$  non ammette nessuna soluzione intera diversa dalla soluzione  $(0, 0, 0)$  per  $n > 2$ , ma che non aveva lo spazio per scriverla. Dall'epoca di Fermat molti hanno cercato di provare questo *Ultimo Teorema di Fermat*, senza

riuscirci, tanto che il problema è diventato noto come la *Conggettura di Fermat*. Nel 1995 il *Teorema* di Fermat fu completamente dimostrato dal matematico Andrew Wiles.



- ➊ Fattorizzare in primi l'intero  $2^{14} - 1$ .
- ➋ Si provi che se un numero  $n$  non è primo, allora possiede un divisore primo  $\leq \sqrt{n}$ .
- ➌ Determinare la fattorizzazione in primi di 10!.

## 7 CONSEGUENZE DEL TEOREMA FONDAMENTALE DELL'ARITMETICA

Il Teorema Fondamentale dell'Aritmetica, che è un risultato squisitamente teorico perché nulla dice riguardo alla determinazione effettiva dei primi della fattorizzazione, ha però alcune importanti conseguenze.

### 7.1 I numeri primi sono infiniti

Supponiamo i numeri primi siano in numero finito e siano  $p_1, p_2, \dots, p_N$ . L'intero  $n = p_1 \cdot p_2 \cdots p_N + 1$  è maggiore di 1, per cui, in virtù del Teorema Fondamentale dell'Aritmetica, ammetterà una fattorizzazione in primi. Tuttavia non esiste *nessun* numero primo che lo divida, perché  $n$  diviso per *qualsiasi* primo, ossia per ogni  $p_i$ ,  $i = 1, \dots, N$  dà come resto 1. Questo assurdo ci assicura che i numeri primi sono necessariamente infiniti.

**OSSERVAZIONE** Si noti che il risultato era già noto ad Euclide, che lo aveva enunciato al modo seguente:

Esistono [sempre] numeri primi in numero maggiore di quanti numeri primi si voglia proporre [cioè la serie dei numeri primi è illimitata].

La classica dimostrazione secondo Euclide è la seguente.

Siano dati i numeri primi  $a, b, c$ . Allora esiste almeno un quarto numero primo. Infatti, posto  $d = abc + 1$ , se  $d$  è primo, abbiamo concluso. Altrimenti (ossia se  $d$  non è primo) esso ammette un divisore primo  $p$  (*Elementi VII, 31*). Asseriamo che  $p$  è diverso da  $a, b, c$ , e quindi che esso è il quarto numero primo del quale si voleva appunto dimostrare l'esistenza.

Se, infatti, il numero  $p$  fosse uguale ad uno dei tre numeri  $a, b, c$ , esso dividerebbe il prodotto  $abc$ . Ma si è supposto che  $p$  divida anche  $abc + 1$ , quindi  $p$  dividerebbe pure la differenza tra  $(abc + 1)$  e  $abc$ , ossia l'unità: cosa assurda.

I due grandi matematici Hardy e Dieudonné hanno detto che il teorema dell'infinità dei numeri primi è forse il più bel teorema della matematica greca. Di questo teorema sono state fornite tantissime dimostrazioni.

### 7.2 Irrazionalità di ogni numero della forma $\sqrt{p}$ , $p$ primo.

I numeri reali che non sono razionali si dicono *irrazionali*. Sappiamo che i decimali che compongono il loro sviluppo in forma decimale sono infiniti e non periodici.

Supponiamo che  $\sqrt{p}$  sia razionale: allora esistono due interi  $n, m, m \neq 0$  tali che  $pn^2 = m^2$ .

Ora, a sinistra il fattore (irriducibile)  $p$  compare un numero dispari di volte, mentre a destra compare un numero pari di volte. Questo contraddice la unicità della fattorizzazione in  $\mathbb{Z}$ .

Quindi  $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}$ , ecc. sono tutti numeri irrazionali.

## 8 ALCUNE DIVAGAZIONI SUI NUMERI PRIMI

È forse questo il momento giusto di fare alcune considerazioni sui *mattoni*, ossia i numeri primi, con i quali si costruiscono tutti i numeri interi. Su questo argomento ritroneremo poi anche in seguito, sia quando discuteremo di crittografia al cap. 5 sia negli approfondimenti (cap. 11).

### 1. Distribuzione dei primi

Gauss a 15 anni fece alcune osservazioni sul numero  $\pi(x)$  di primi minori di un dato intero  $x$ , osservando che  $\pi(x)$  dovesse avere un andamento asintotico come quello della funzione  $\frac{x}{\log x}$ . Questa osservazione è giustificata dalla seguente tabella (cfr. [http://wikipedia.org/wiki/Teorema\\_dei\\_numeri\\_primi](http://wikipedia.org/wiki/Teorema_dei_numeri_primi))

$x$	$\pi(x)$	$\frac{\pi(x)}{x/\log x}$
$10$	$4$	$0,921$
$10^2$	$25$	$1,151$
$10^3$	$168$	$1,161$
$10^4$	$1229$	$1,132$
$10^5$	$9592$	$1,104$
$10^6$	$78\,498$	$1,048$
$10^7$	$664\,579$	$1,071$
$10^8$	$5\,761\,455$	$1,061$
$10^9$	$50\,847\,534$	$1,054$
$10^{10}$	$455\,052\,511$	$1,048$
$10^{11}$	$4\,118\,054\,813$	$1,043$
$10^{12}$	$37\,607\,912\,018$	$1,039$
$10^{13}$	$346\,065\,536\,839$	$1,034$
$10^{14}$	$3\,204\,941\,750\,802$	$1,033$
$10^{15}$	$29\,844\,570\,422\,669$	$1,031$

Tuttavia a quell'epoca non c'erano strumenti matematici tali da permettergli di dimostrare la sua supposizione. Per fare ciò bisogna attendere il 1896, quando Hadamard e de la Vallée Poussin, utilizzando i risultati di Riemann sulla funzione  $\zeta$ , dimostrarono il cosiddetto *Teorema dei Numeri Primi* che descrive per l'appunto l'andamento asintotico dei numeri primi.

**TEOREMA 3.4 (TEOREMA DEI NUMERI PRIMI)** Per ogni numero reale  $x > 0$ , posto  $\pi(x) := \text{numero dei primi} \leq x$  si ha

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Questo teorema ci dice sostanzialmente che per numeri  $n$  grandi, il numero  $\pi(n)$  dei numeri primi minori di  $n$  è dell'ordine di  $n/\log n$ . La probabilità quindi che un numero dell'ordine di grandezza di  $n$  sia primo è  $1/\log n$ . Con circa  $\log n$  tentativi si potrà quindi ottenere un numero primo. Dovremo tenere presente questo fatto quando parleremo di crittografia a chiave pubblica.

## 2. I primi di Fermat

Consideriamo i numeri della forma  $2^k + 1$ . Se si chiede ad un numero di questa forma di essere un primo, l'esponente  $k$  non può contenere *nessun fattore dispari*: se infatti contenesse un fattore dispari  $d = 2h + 1$  si avrebbe

$$\begin{aligned} 2^k + 1 &= 2^{dr} + 1 = (2^r)^d + 1 \\ &= (2^r + 1)((2^r)^{2h} - (2^r)^{2h-1} + \cdots + (2^r)^2 - 2^r + 1) \end{aligned}$$

ossia il numero avrebbe una fattorizzazione propria. Quindi, se vogliamo che un numero della forma  $2^k + 1$  sia primo, l'esponente  $k$  deve avere la forma  $2^n$ . Ebbene, si dà la seguente definizione.

**DEFINIZIONE 3.13** Un numero di Fermat è un intero della forma

$$F_n = 2^{2^n} + 1$$

I numeri di Fermat corrispondenti ai primi valori di  $n$  sono

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65\,537.$$

Non è difficile verificare che tutti questi cinque numeri sono numeri primi. Era convinzione di Fermat che *tutti* i numeri della forma  $2^{2^n} + 1$  fossero primi. La sua congettura fu confutata da Eulero, che provò che il successivo numero di Fermat,  $F_5$ , non è primo, esibendo la fattorizzazione

$$F_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417.$$

Il più grande numero di Fermat *primo* conosciuto è  $F_4$ . Il più grande numero di Fermat *non primo* conosciuto è  $F_{23471}$ . Si conoscono le fattorizzazioni di  $F_5$ ,  $F_6$ ,  $F_7$ ,  $F_8$ ,  $F_9$  e  $F_{11}$ . Si sa che  $F_{10}$  non è primo, ma non se ne conosce la fattorizzazione completa.

**OSSERVAZIONE** I numeri primi di Fermat sono legati alla costruzione con soli riga e compasso di poligoni regolari. Si dimostra che un  $n$ -gono regolare si può costruire con riga e compasso se e solo se nella fattorizzazione di  $n$  compare  $2^h$  ( $h \geq 0$ ) per un prodotto (eventualmente vuoto) di primi di Fermat distinti. Quindi un pentagono regolare si può costruire (con soli riga e compasso) mentre per esempio un ennagono (9 lati) non si può costruire, così come non si può costruire un 19-gono, ecc.

## 3. I primi di Mersenne

I numeri di Mersenne sono interi della forma  $2^k - 1$  ( $k \geq 2$ , e si denotano con  $M_k$ ).

Quindi  $M_2 = 3$ ,  $M_3 = 7$ ,  $M_4 = 15$ ,  $M_5 = 31$ ,  $M_6 = 63$ ,  $M_7 = 127$ ,  $M_8 = 255$ ,  $M_9 = 511$ , ecc.

Come per il caso dei numeri di Fermat, poniamoci il problema di scoprire quando un numero di Mersenne è primo. Dalla lista sopra riportata, si vede che  $M_2$ ,  $M_3$ ,  $M_5$ ,  $M_7$  sono primi, mentre  $M_4$ ,  $M_6$ ,  $M_8$ ,  $M_9$  non lo sono. Sembra potersi congetturare (congettura un po' azzardata, dato che sono pochissimi i valori su cui ci basiamo) che un numero di Mersenne  $M_k$  è primo se solo se  $k$  è primo. Questa congettura è subito confutata da  $M_{11} = 2047 = 23 \cdot 89$ . In realtà resta in piedi un parte della congettura: è vero che se  $M_k$  è primo, allora  $k$  deve essere primo. Basta provare che se  $k$  non è primo, allora  $M_k$  non è primo. Sia infatti  $k = ab$ : allora

$$\begin{aligned} 2^k - 1 &= 2^{ab} - 1 = \\ &= (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1). \end{aligned}$$

Vale il seguente risultato che risponde al nostro problema:

**PROPOSIZIONE 3.10 (LUCAS)** Sia  $p$  un numero primo maggiore di 2. Il numero di Mersenne  $2^p - 1$  è un numero primo se e solo se  $M_p$  divide  $S_p$ , dove  $S_h$  è definito ricorsivamente da:

$$S_2 = 4, \quad S_h = S_{h-1}^2 - 2.$$

Per esempio,  $S_3 = S_2^2 - 2 = 16 - 2 = 14$ ,  $S_4 = S_3^2 - 2 = 196 - 2 = 194$ ,  $S_5 = S_4^2 - 2 = 37\,636 - 2 = 37\,634$ ,  $S_6 = S_5^2 - 2 = 1\,416\,317\,954$ .

Di conseguenza,  $M_3 = 7$  è primo, perché divide  $S_3 = 14$ ,  $M_5 = 31$  è primo perché divide  $S_5 = 31 \cdot 1214$ , ecc.

■ ■ ■ Scrivere un programma che calcoli il MCD( $a, b$ ) utilizzando l'algoritmo euclideo delle divisioni successive.

■ ■ ■ Scrivere un programma che esprima il MCD( $a, b$ ) nella forma  $sa + tb$  per opportuni  $s$  e  $t$  in  $\mathbb{Z}$  (identità di Bézout), esprimendo ogni resto trovato nelle divisioni dell'algoritmo euclideo come combinazione di  $a$  e  $b$ .

■ ■ ■ Scrivere un programma che dica se una data equazione  $ax + by = c$ ,  $a, b, c \in \mathbb{Z}$  ammette soluzioni in  $\mathbb{Z}$ , e che in caso positivo ne calcoli una.

■ ■ ■ Fare un programma che faccia passare dalla scrittura decimale alla scrittura binaria (base 2) di un intero  $n$  e viceversa.

■ ■ ■ Fare un programma che trasformi un intero da una base ad un'altra per varie basi.

■ ■ ■ Fare un programma che addizioni e moltiplichi fra loro due numeri scritti in base arbitraria.

- Fare un programma che implementi l'algoritmo del crivello di Eratostene.
- Fare un programma che scriva i primi numeri di Fermat.
- Fare un programma che verifichi se un dato intero è un numero di Fermat.
- Fare un programma che scriva i primi numeri di Mersenne.

# 4

## Calcolo combinatorio

*Forse s'avessi'io l'ale  
da volar su le nubi,  
E neverar le stelle ad una ad una,  
O come il tuono errar di giogo in giogo,  
Più felice sarei, dolce mia greggia,  
Più felice sarei, candida luna.*

G.Leopardi, Canti, da CANTO NOTTURNO DI UN PASTORE ERRANTE DELL'ASIA

Questo capitolo si propone di *contare* gli elementi di vari insiemi, finiti e infiniti.

### ■ 1 QUANTI SONO?

Supponiamo di voler contare quanti sono gli abitanti di un paese o i libri di una biblioteca. Il procedimento che presenteremo è indipendente dalla nozione di numero e dalla capacità di contare. Si tratta del metodo utilizzato dagli uomini primitivi: essi, pur essendo incapaci di contare, erano però capaci di decidere se due insiemi avevano lo stesso numero di elementi: per scoprire se le pecore di un gregge erano rientrate tutte, tenevano in un recipiente tanti bastoncini quante erano le pecore, e al momento del rientro, per ogni pecora che rientrava, prendevano dal recipiente un bastoncino: se alla fine (cioè quando non c'erano più pecore) nel recipiente non rimanevano bastoncini, voleva dire che le pecore erano rientrate tutte, se invece restavano nel recipiente dei bastoncini, voleva dire che c'era qualche pecora ancora in giro. Come ben sappiamo, dietro questa operazione degli uomini primitivi, c'è il concetto di corrispondenza biunivoca (tra bastoncini e pecore). Ebbene, proprio il concetto di corrispondenza biunivoca ci permetterà di contare anche elementi di insiemi infiniti, anzi, di dare la definizione precisa di insieme infinito.

**DEFINIZIONE 4.1** Si dice che due insiemi  $A$  e  $B$  hanno la stessa *cardinalità* o *potenza* o sono *equipotenti* se è possibile stabilire tra di essi una corrispondenza biunivoca. ■

La relazione di avere la stessa cardinalità (o di equipotenza) è una relazione di equivalenza tra insiemi. Due insiemi equipotenti verranno indicati con

$$A \sim B .$$

**DEFINIZIONE 4.2** Si definisce *cardinalità* o *numero cardinale* o *potenza* di un insieme  $A$  la classe di equipotenza a cui  $A$  appartiene. Si indica con  $\text{Card}(A)$ .

Il numero cardinale è quindi ciò che accomuna tutti gli insiemi che sono tra loro in corrispondenza biunivoca, è l'etichetta che si può attaccare ad ogni classe di equipotenza.

Introduciamo ora la seguente famiglia di insiemi, dipendenti da un intero  $n \in \mathbb{N}$

$$I_n := \{0, 1, 2, \dots, n-1\}.$$

Per ogni fissato  $n$  l'insieme  $I_n$  è formato dai primi  $n$  numeri naturali. Risulta per esempio

$$I_1 = \{0\}, I_2 = \{0, 1\}, I_3 = \{0, 1, 2\}.$$

Ora, non è difficile verificare che ognuno di questi insiemi  $I_n$  gode della proprietà di non avere sottoinsiemi propri equipotenti ad esso.

Ebbene, questi insiemi ci permetteranno di dare una definizione *precisa* di insieme finito (e quindi anche di insieme infinito).

**DEFINIZIONE 4.3** Un insieme  $A$  diverso dall'insieme vuoto (che è ovviamente finito) si dice *finito* se per qualche  $n \in \mathbb{N}$ ,  $n \neq 0$ ,  $A$  è equipotente ad  $I_n = \{0, 1, 2, \dots, n-1\}$ . Un insieme che non è finito si dice *infinito*.

Per gli insiemi *finiti*  $S$  la nozione di cardinalità coincide con la nozione di *numero di elementi* dell'insieme e si indica con  $|S|$ . La cardinalità di  $I_n$  viene chiamata  $n$ . In altre parole, ogni numero naturale  $0, 1, 2, \dots$  diventa numero cardinale (finito):  $0$  è il numero cardinale dell'insieme vuoto  $\emptyset$ ,  $1$  è il numero cardinale di  $\{\emptyset\}$  (e di qualunque altro insieme appartenente alla stessa classe di equipotenza),  $2$  è il numero cardinale di  $\{\emptyset, \{\emptyset\}\}$  (e di qualunque altro insieme della stessa classe),  $3$  è il numero cardinale di  $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ , e così via. In conclusione, ogni numero naturale non è altro che una particolare cardinalità.

Da quanto detto in precedenza sulle proprietà degli insiemi  $I_n$ , si può concludere che un insieme è finito se e solo se non si può mettere in corrispondenza biunivoca con un suo sottoinsieme proprio. Quindi un insieme è infinito se e solo se esiste un suo sottoinsieme proprio che si può mettere in corrispondenza biunivoca con l'insieme stesso. Questa che abbiamo dato è una *caratterizzazione* degli insiemi infiniti. Vediamo di utilizzarla per provare che l'insieme  $\mathbb{N}$  dei numeri naturali è infinito. Dal punto di vista intuitivo è chiaro che si tratta di un insieme infinito, ma in matematica l'intuito non basta. Proveremo quindi che  $\mathbb{N}$  è infinito provando che esiste un suo sottoinsieme proprio equipotente a  $\mathbb{N}$ . Basta prendere per esempio il sottoinsieme dei numeri dispari

$$D = \{1, 3, 5, 7, 9, \dots\}$$

e definire la seguente applicazione  $f$  da  $\mathbb{N}$  a  $D$  ponendo  $f(n) = 2n+1$  per ogni  $n \in \mathbb{N}$ .

Si tratta di una applicazione iniettiva, perché se  $f(n) = f(m)$ , allora  $n = m$ : infatti  $f(n) = f(m)$  significa che  $2n+1 = 2m+1$ , il che comporta, per le note proprietà dei numeri naturali,  $n = m$ . Inoltre la  $f$  è suriettiva perché l'immagine di  $f$  è costituita esattamente dai numeri dispari. Quindi il sottoinsieme (proprio!) dei numeri naturali dispari è in corrispondenza biunivoca con tutti i numeri naturali. Se

0	1	2	3	4	5
↓	↓	↓	↓	↓	↓
1	3	5	7	9	11

Figura 4.1. Corrispondenza biunivoca tra i numeri naturali e i numeri dispari.

ne deduce un fatto sorprendente: i numeri naturali dispari sono tanti quanti tutti i numeri naturali! Possiamo andare oltre. I multipli di 10 sono tanti quanti tutti i numeri naturali. Ancora, i numeri naturali sono tanti quanti i numeri interi, i numeri naturali sono tanti quanti i numeri razionali (cfr. eserc. 2).

L'insieme dei naturali dispari, l'insieme dei multipli di 10, l'insieme dei numeri pari sono tutti in corrispondenza biunivoca con l'insieme  $\mathbb{N}$  dei numeri naturali. Appare quindi naturale attribuire alla cardinalità di  $\mathbb{N}$  un nome speciale. La potenza dell'insieme  $\mathbb{N}$  di tutti i numeri naturali prende il nome di  $\aleph_0$  (che si legge alef-zero) e dicesi la potenza del *numerabile*. Quindi si ha la seguente definizione:

**DEFINIZIONE 4.4** Un insieme si dice avere la *potenza del numerabile* (o che è *numerabile*) se si può porre in corrispondenza biunivoca con  $\mathbb{N}$ .

Questo significa che un insieme numerabile  $S$  si potrà scrivere al modo seguente:

$$S = \{a_1, a_2, a_3, \dots, a_i, \dots\}$$

ossia i suoi elementi si possono per l'appunto *numerare* con gli indici  $0, 1, 2, \dots$  oppure  $1, 2, 3, \dots$

Il seguente teorema ci offre la possibilità di trovare molti insiemi numerabili.

**TEOREMA 4.1** L'unione di un numero finito o di una infinità numerabile di insiemi numerabili ha la potenza del numerabile.

**DIMOSTRAZIONE.** Dimostreremo il teorema nel caso di una infinità numerabile di insiemi numerabili a due a due disgiunti: gli altri casi sono conseguenza di questo. Sia  $A_1, A_2, \dots, A_j, \dots$  una infinità numerabile di insiemi numerabili a due a due disgiunti. Gli elementi di  $A_j$  saranno pertanto

$$a_{j,1}, a_{j,2}, a_{j,3}, \dots, a_{j,i}, \dots$$

Si tratta ora di *numerare* anche gli elementi dell'insieme  $A = A_1 \cup A_2 \cup A_3 \cup \dots$ . Per far ciò, disponiamo gli elementi di tale unione in una tabella dove sulla riga  $j$ -esima vengono disposti gli elementi  $a_{j,i}$  dell'insieme  $A_j$ .

$A_1$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$\dots$	$a_{1,i}$	$\dots$
$A_2$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$\dots$	$a_{2,i}$	$\dots$
$A_3$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$\dots$	$a_{3,i}$	$\dots$
$\dots$						
$A_j$	$a_{j,1}$	$a_{j,2}$	$a_{j,3}$	$\dots$	$a_{j,i}$	$\dots$



Per quanto ora visto, la potenza del continuo è *strettamente maggiore* della potenza del numerabile. Essa coincide con la potenza dell'insieme  $\mathbb{R}$  dei numeri reali. Sorge ora un problema: esistono cardinalità *intermedie* tra la potenza del numerabile e la potenza del continuo? La cosiddetta *ipotesi del continuo* afferma che non esistono *potenze intermedie* tra la potenza del numerabile e quella del continuo. È stato provato che l'ipotesi del continuo è indipendente dagli altri postulati sui quali si basa la teoria degli insiemi, il che significa che a partire dagli assiomi ordinari della teoria degli insiemi non si riuscirà né a dimostrare che la congettura è vera né a dimostrare che è falsa. L'insieme delle parti di un insieme che abbia la potenza del continuo è un insieme che ha una potenza strettamente superiore a quella del continuo. Con successivi passi si possono costruire insiemi di potenza via via crescente. Analogamente l'*ipotesi generalizzata del continuo* afferma che per ogni insieme infinito  $X$  non esistono insiemi di potenza *intermedia* tra quella di  $X$  e quella di  $\mathcal{P}(X)$ .



- Si provi che un insieme numerabile possiede sottoinsiemi *propri* numerabili.
- Si provi che l'insieme  $\mathbb{Q}$  dei numeri razionali è numerabile.
- In  $\mathbb{R}$  si definisca la seguente relazione:  $x \sim y \iff x - y \in \mathbb{Q}$ .
  - a. Si provi che si tratta di una relazione di equivalenza;
  - b. si dica se il quoziente  $\mathbb{R}/\sim$  è numerabile.

## 2 CALCOLO COMBINATORIO

Abbandoniamo ora l'infinito e passiamo al finito.

Spesso ci si trova di fronte a problemi del tipo: *in quanti modi diversi può accadere qualcosa?*

### Esempio 4.1

In quanti modi diversi si può formare una squadra di calcio se si hanno a disposizione 25 giocatori?

Vedremo che matematicamente questo tipo di problema si può ridurre spesso a determinare la cardinalità di un insieme finito.

Conviene avere quindi un metodo *sistematico* che permetta di elencare e contare tutti gli elementi di un insieme finito.

Ci sono due regole fondamentali a questo proposito.

#### a. La regola della somma.

Siano  $A_1, A_2, \dots, A_s$  insiemi *a due a due disgiunti*, e sia  $|A_i| = n_i$ ,  $\forall i = 1, \dots, s$ . Posto  $A = A_1 \cup A_2 \cup \dots \cup A_s$ , allora

$$|A| = |A_1| + |A_2| + \dots + |A_s| = n_1 + n_2 + \dots + n_s.$$

### Esempio 4.2

In una biblioteca ci sono 120 testi di matematica, 300 romanzi stranieri e 500 romanzi italiani. Quanti libri ci sono in tutto?

Problemi di questo tipo abbiamo imparato a risolverli fin dalle scuole elementari. Tuttavia è importante fare una osservazione. I testi di matematica non sono romanzi, e i romanzi italiani non sono ovviamente stranieri: quindi ci sono  $120+300+500=920$  libri in tutto.

Si può riformulare il problema dicendo: se si può prendere in prestito un solo libro per volta, quante sono le possibilità di scelta? Saranno esattamente 920.

Ora, questo esempio, per semplice che sia, è però importante per capire meglio quanto segue. Si osservi infatti l'importanza del fatto che gli insiemi siano *a due a due disgiunti*. Diversa infatti sarebbe la situazione seguente:

### Esempio 4.3

In una biblioteca ci sono 300 romanzi stranieri diversi e in un'altra biblioteca ci sono 220 romanzi stranieri diversi. Quanti romanzi distinti ci sono tra le due biblioteche?

Per riformulare come prima la domanda, si può chiedere: *se si può scegliere un solo libro tra le due biblioteche, quante scelte avremo a disposizione?*

Ovviamente questa volta il numero totale di libri distinti (e quindi il numero totale di scelte) non è dato dalla somma dei libri della prima biblioteca con quelli della seconda biblioteca, perché potrebbe addirittura darsi il caso che i 220 libri della seconda biblioteca siano tutti presenti anche nella prima, e quindi il numero di scelte possibili sarebbe solo 300. Vedremo tra breve (cfr. par. 3) come si generalizza la regola della somma nel caso in cui gli insiemi non siano a due a due disgiunti.

Per concludere, la regola della somma, riformulata in modo diverso (e non con gli insiemi) si può enunciare al modo seguente:

Supponiamo che ci siano  $n_1$  modi per fare qualcosa e  $n_2$  modi per fare un'altra cosa *distinta dalla prima*, e che vogliamo fare solo una delle due, allora ci sono esattamente  $n_1 + n_2$  cose che possiamo fare.

#### b. La regola del prodotto.

La seconda regola è data dalla cosiddetta *regola del prodotto* che dice quanto segue: se si può fare una scelta in  $n$  modi e se per ciascuna di queste scelte si può fare una seconda scelta in  $m$  modi, allora il numero totale di modi in cui si possono fare entrambe le scelte è  $n \cdot m$ .

### Esempio 4.4

Supponiamo di avere tre poltrone di tre colori diversi e 4 tavoli di forme diverse. In quanti modi si possono combinare *poltrona-tavolo*, ottenendo tanti arredamenti diversi?

Le possibili scelte per le poltrone sono tre, e in corrispondenza ad ogni scelta della poltrona ci sono 4 possibili scelte dei tavoli. Quindi in tutto si hanno 12 possibili arredamenti.

La regola del prodotto si può leggere nel linguaggio della teoria degli insiemi: se indichiamo con  $A$  l'insieme costituito dalle poltrone, e con  $B$  l'insieme costituito dai tavoli, il nostro problema corrisponde a determinare la cardinalità del prodotto cartesiano  $A \times B$ , che sappiamo essere  $|A| \cdot |B|$ .

La regola del prodotto si può estendere ovviamente a più di due scelte (ossia al prodotto cartesiano di più di due insiemi). Facciamo un esempio.

#### Esempio 4.5

Un ristorante ha un menu al prezzo fisso di 15 euro, dove si ha la possibilità di scegliere un primo tra quattro scelte (bucatini all'amatriciana, minestrone, risotto, tagliatelli al sugo), un secondo tra tre scelte (bistecca, pollo, salsicce) e un dessert con due scelte (gelato e torta di mele). Quante sono le possibili scelte totali (dove per scelta totale si intende una terna, in cui il primo elemento è un "primo", il secondo elemento è un "secondo" e il terzo elemento è un dessert)?

Il primo elemento della terna (cioè il "primo") può essere scelto in 4 modi; fatta la scelta per il primo, il "secondo" può essere scelto in 3 modi, e per ogni scelta di un primo e di un secondo il dessert può essere scelto in due modi. In tutto quindi il numero totale di scelte possibili è  $4 \cdot 3 \cdot 2 = 24$ .

Possiamo visualizzare la situazione mediante il diagramma ad albero della figura 4.2, per mostrare quali sono le scelte possibili ad ogni stadio:  $P_i$ , ( $i = 1, \dots, 4$ ) indica i primi,  $S_j$ , ( $j = 1, 2, 3$ ) indica i secondi e  $D_k$ , ( $k = 1, 2$ ) indica i desserts.

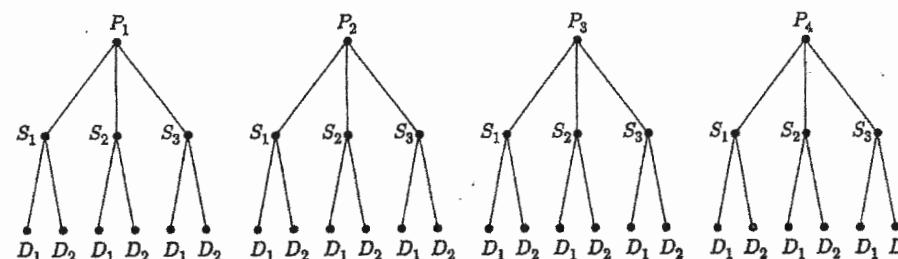


Figura 4.2.

La regola del prodotto sostanzialmente dice che se  $A$  è un insieme di  $k$ -ple  $(x_1, x_2, \dots, x_k)$ , e se, per ogni  $j$ ,  $x_j$  può assumere  $n_j$  valori (indipendentemente dai valori delle coordinate che lo precedono), allora la cardinalità di  $A$  è  $n_1 \cdot n_2 \cdots n_k$ .

Prima di procedere con altri esempi, conviene introdurre alcune nozioni basilari.

#### 2.1 Permutazioni.

**DEFINIZIONE 4.7** Dicesi *permutazione* di  $n$  oggetti  $a_1, a_2, \dots, a_n$  una corrispondenza biunivoca di  $A = \{a_1, a_2, \dots, a_n\}$  in sé. In altre parole, una permutazione di  $n$  oggetti è un ordinamento degli  $n$  oggetti. ■■■

Sia  $A = \{1, 2, 3, 4, 5\}$ . Due permutazioni degli elementi 1, 2, 3, 4, 5 sono per esempio 2, 1, 5, 4, 3 oppure 5, 3, 4, 1, 2.

Dato un insieme con  $n$  elementi, in quanti modi si possono ordinare i suoi elementi? Equivalentemente, quante sono le permutazioni di un insieme con  $n$  elementi?

Pensiamo di avere  $n$  caselle, nelle quali dobbiamo inserire gli  $n$  elementi: nella prima casella possiamo sistemare uno qualunque degli  $n$  elementi, quindi la prima casella può essere riempita in  $n$  modi diversi. La seconda casella può essere riempita con uno qualunque degli  $n - 1$  elementi rimasti, la terza con uno qualunque degli  $n - 2$  elementi rimasti, e così via, fino ad arrivare all'ultima casella che può essere riempita con l'unico elemento rimasto. In tutto le permutazioni di  $n$  oggetti sono pertanto, in base alla regola del prodotto,  $n \cdot (n - 1) \cdot (n - 2) \cdots 3 \cdot 2 \cdot 1$ .

#### Esempio 4.6

Una saletta cinematografica contiene 50 posti a sedere. In quanti modi 50 spettatori si possono disporre?

In  $50 \cdot 49 \cdot 48 \cdot 47 \cdots 4 \cdot 3 \cdot 2 \cdot 1$  modi.

.....

Già da questo esempio appare chiaro che è conveniente introdurre alcune notazioni.

Dato un intero positivo  $n$ , si indica con  $n!$ , e si legge *n fattoriale*, il seguente intero:

$$n! \stackrel{\text{def}}{=} n \cdot (n - 1) \cdot (n - 2) \cdots 3 \cdot 2 \cdot 1, \quad 0! \stackrel{\text{def}}{=} 1.$$

Per esempio,  $8! = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 40\,320$ .

Le permutazioni di un insieme con  $n$  elementi sono quindi  $n!$ .

Dati due insiemi  $A$  e  $B$  (anche non coincidenti) con  $n$  elementi ciascuno, il numero di corrispondenze biunivoche tra  $A$  e  $B$  è precisamente  $n!$ . Infatti, per individuare un'applicazione  $f$  basta assegnare i valori  $f(x_1), f(x_2), \dots, f(x_n)$ , dove  $x_1, x_2, \dots, x_n$  sono gli  $n$  elementi di  $A$ . Data quindi un'applicazione biiettiva arbitraria  $f$  da  $A$  a  $B$ ,  $f(x_1)$  può essere uno qualunque degli  $n$  elementi di  $B$ , cioè può assumere  $n$  valori,  $f(x_2)$  può coincidere con uno qualunque degli elementi di  $B$ , purché diverso da  $f(x_1)$  (per l'iniettività), quindi può assumere  $n - 1$  valori, e così via. Si possono fare quindi in tutto  $n \cdot (n - 1) \cdot (n - 2) \cdots 2 \cdot 1 = n!$  scelte (si ricordi la regola del prodotto), e scelte diverse danno luogo ad applicazioni biunivoche diverse tra  $A$  e  $B$ .

Nel caso in cui sia  $A = B$ , le corrispondenze biunivoche di  $A$  in sé sono precisamente le *permutazioni*. L'insieme di tutte le permutazioni di un insieme  $X$  si indica con  $\mathcal{S}(X)$ . Se si prende in considerazione la composizione di applicazioni, la composizione di elementi di  $\mathcal{S}(X)$  è ancora un elemento di  $\mathcal{S}(X)$ . Inoltre tale composizione è associativa, esiste un elemento  $i_X$  neutro rispetto alla composizione, tale cioè che  $i_X \circ f = f \circ i_X = f$  per ogni  $f \in \mathcal{S}(X)$ . Inoltre, dato comunque un elemento  $f \in \mathcal{S}(X)$  (cioè una corrispondenza biunivoca di  $X$ ), esiste l'applicazione inversa  $f^{-1}$  che è la funzione definita ponendo  $f^{-1}(y) =$  quell'unico elemento  $x \in X$  tale che  $y = f(x)$ . L'importante è osservare che anche la  $f^{-1}$  è biunivoca, e pertanto sta ancora in  $\mathcal{S}(X)$ . Per definizione di inversa, essa è tale che  $f \circ f^{-1} = f^{-1} \circ f = i_X$ . L'insieme  $\mathcal{S}(X)$  rispetto alla composizione di applicazioni ha una *struttura algebrica* che prende il nome di *gruppo*. Parleremo più avanti (cfr. cap. 8) di tali strutture algebriche.

La funzione fattoriale  $f(n) = n!$  si può definire ricorsivamente al modo seguente:

- (*Passo base*): si pone  $f(0) = 1$ , cioè  $0! = 1$ ;
- (*Passo induttivo*): si dà la seguente regola per determinare il valore di  $n!$  a partire dal valore del precedente:

$$n! = n \cdot (n - 1)!.$$

Nei calcoli, quando si ha a che fare per esempio con quozienti di fattoriali, conviene procedere alla loro cancellazione, utilizzando la  $n! = n \cdot (n - 1)!$ . Per esempio, se si deve dividere  $250!$  per  $248!$  conviene scrivere

$$\frac{250!}{248!} = \frac{250 \cdot 249 \cdot 248!}{248!} = 250 \cdot 249 = 62\,250.$$

Concludiamo questo paragrafo sulle permutazioni con un'osservazione.

Tutti sappiamo cosa significhi *anagrammare* una parola: significa permutarne le lettere (o i numeri che corrispondono alla posizione delle lettere nella parola). In genere nei quesiti enigmistici si chiede che il risultato dia una parola che abbia ancora un senso. Noi non chiediamo questo. Il risultato può essere una sequenza di lettere priva di significato. Per esempio, se partiamo dalla parola di quattro lettere *ALTO*, alcune delle parole che si ottengono anagrammandola sono per esempio *LATO*, *ATLO*, *OTLA*, *TALO*, ecc. Pensando all'anagramma come permutazione delle *posizioni* occupate dalle lettere della parola, la permutazione corrispondente alla parola *ALTO* è la permutazione identica, mentre per esempio la permutazione corrispondente alla parola *LATO* è la permutazione che scambia tra loro la prima e la seconda posizione, e lascia fissa la terza e la quarta. In tutto gli anagrammi della parola *ALTO* sono tanti quante le permutazioni delle quattro lettere *A*, *L*, *T*, *O*, o dei quattro numeri 1, 2, 3, 4, ossia sono in tutto  $4! = 24$ . Quindi l'insieme degli anagrammi della parola *ALTO* coincide con l'insieme di tutte le permutazioni di quattro numeri. Ma è sempre così? Cioè possiamo sempre dire che, partendo da una parola di  $n$  lettere, gli anagrammi sono esattamente le permutazioni di  $n$  numeri? Che legame c'è tra le permutazioni e gli anagrammi? È certamente vero che, data una parola con  $n$  lettere, ad ogni permutazione di  $n$  elementi corrisponde un anagramma della parola stessa, ma siamo sicuri che permutazioni diverse diano luogo ad anagrammi diversi (ossia che la corrispondenza che associa ad ogni permutazione l'anagramma corrispondente sia iniettiva)? Nell'esempio appena fatto così sembrava. Partiamo però dalla parola *MAMMA*. Gli anagrammi di questa parola sono permutazioni di cinque lettere, ma vediamo subito che per esempio la permutazione che scambia la prima con la terza posizione o la permutazione che scambia la terza con la quarta *non modificano la parola*: quindi ci sono permutazioni diverse che corrispondono ad uno stesso anagramma, per cui la corrispondenza permutazione → anagramma non è iniettiva. Non è difficile rendersi conto che questo dipende dal fatto che nella parola ci sono lettere ripetute. I possibili anagrammi distinti della parola *MAMMA* sono pertanto

$$\frac{5!}{3!2!}.$$

Infatti tutte le  $3! = 6$  permutazioni che permutano la prima, la terza e la quarta posizione, dove si trovano lettere uguali (ossia la *M*) o quelle che permutano la seconda

e la quinta posizione (dove si trovano due lettere uguali, *A*) non contribuiscono a nuovi anagrammi.

Questo tipo di discorso verrà ripreso fra breve.

## 2.2 Disposizioni e combinazioni semplici

Poniamoci ora un altro problema.

Dato un insieme con  $n$  elementi, in quanti modi si possono *scegliere  $k$  elementi (tutti distinti, ossia senza ripetizioni)* tra questi  $n$ ? Naturalmente il problema ha senso solo se  $k \leq n$ . Dobbiamo distinguere due casi: il primo caso è quando è *importante l'ordine* con cui si scelgono gli oggetti, il secondo caso è quando l'ordine con cui vengono scelti gli oggetti è *irrilevante*. Nel primo caso parleremo di *disposizioni semplici di  $n$  oggetti di classe  $k$* , nel secondo di *combinazioni semplici di  $n$  oggetti di classe  $k$* . L'aggettivo *semplice* sta a significare che non sono ammesse ripetizioni di oggetti, cioè tutti i  $k$  elementi che si scelgono sono distinti.

Esaminiamo il primo caso, ossia vediamo di contare quante sono le *disposizioni semplici di  $n$  oggetti di classe  $k$* , ossia quanti sono i modi di scegliere  $k$  oggetti distinti da un insieme con  $n$  oggetti, tenendo presente che l'ordine con cui viene effettuata la scelta è importante. Tale numero si indica con  $D(n, k)$ .

Il primo elemento può essere scelto tra tutti gli  $n$  elementi dell'insieme, quindi in  $n$  modi, il secondo può essere scelto tra tutti gli  $n - 1$  elementi rimanenti (dato che i  $k$  oggetti devono essere distinti), il terzo tra tutti gli  $n - 2$  rimanenti, e così via fino al  $k$ -esimo oggetto che può essere scelto tra i rimanenti  $n - (k - 1) = n - k + 1$ . In definitiva il numero di disposizioni semplici di  $n$  oggetti di classe  $k$  è

$$D(n, k) = n \cdot (n - 1) \cdot (n - 2) \cdots (n - k + 1).$$

Se  $k = n$ , in quanti modi si possono scegliere  $n$  elementi tra  $n$  elementi? In tanti modi quanti sono i possibili ordinamenti degli  $n$  elementi. Quindi

$$D(n, n) = n!.$$

Se  $k = 1$ , in quanti modi si può scegliere un elemento tra  $n$  elementi? Ovviamente in  $n$  modi, come d'altra parte risulta dalla formula generale di  $D(n, k)$ :

$$D(n, 1) = n.$$

### Esempio 4.7

Ad una gara di atletica hanno partecipato 30 atleti. Il primo riceverà una medaglia d'oro, il secondo una medaglia d'argento e il terzo una medaglia di bronzo. Quanti sono i possibili modi in cui possono essere assegnate le medaglie?

Il problema equivale a determinare quante possono essere le terne *ordinate* di vincitori (tali cioè che il primo elemento della terna sia quello che riceve la medaglia d'oro, il secondo quello che riceve la medaglia d'argento e il terzo quello che riceve la medaglia di bronzo). È chiaro che la terna costituita da Alberto, Bruno e Carlo (con ciò intendendo che Alberto è vincitore, Bruno al secondo posto e Carlo al terzo) è diversa dalla terna Bruno, Alberto, Carlo (si tratta di assegnazioni diverse delle medaglie, anche se sul podio salgono le stesse tre persone). I possibili

vincitori sono 30, i possibili secondi posti sono 29 e i possibili terzi posti sono 28. Quindi i possibili modi in cui possono essere assegnate le medaglie sono in numero di

$$D(30, 3) = 30 \cdot 29 \cdot 28 = 24360,$$

tante quante le *disposizioni semplici* di 30 elementi di classe 3.

Diverso è il caso seguente.

#### Esempio 4.8

Ad una gara di atletica hanno partecipato 30 atleti. Quante sono le possibili terne di vincitori, cioè quante sono le terne di atleti che saliranno sul podio?

In questo caso non ci importa la qualifica primo, secondo o terzo classificato: la terna (Alberto (primo), Bruno (secondo), Carlo (terzo)) o la terna (Bruno, Alberto, Carlo) sono da considerarsi uguali. Ciò significa che vogliamo considerare uguali tutte le terne di "premiati", indipendentemente dal tipo di medaglia. Fissati tre atleti premiati,  $A$ ,  $B$  e  $C$ , in quanti modi diversi possono essere premiati? In tanti modi quanti possono essere le permutazioni di tre elementi, ossia  $3! = 6$ . Quindi la risposta a quest'ultimo problema è

$$\frac{24360}{6} = 4060.$$

Tale numero rappresenta il numero di *combinazioni semplici* di 30 oggetti di classe 3.

Riassumendo, il numero di disposizioni semplici di  $n$  elementi di classe  $k$  rappresenta il numero di  $k$ -ple *ordinate* di  $k$  elementi distinti presi in un insieme di  $n$  elementi, mentre il numero di combinazioni semplici di  $n$  elementi di classe  $k$ , che si indica con il simbolo  $\binom{n}{k}$ , rappresenta il numero di *sottoinsiemi* di  $k$  elementi in un insieme con  $n$  elementi.

Per contare quanti sono i sottoinsiemi con  $k$  elementi di un insieme  $A$  con  $n$  elementi ( $k \leq n$ ), basta osservare che ogni sottoinsieme di  $A$  con  $k$  elementi ha esattamente  $k!$  ordinamenti, quindi corrisponde a  $k!$   $k$ -ple distinte. Se si vuole pertanto il numero di *sottoinsiemi* di  $A$  con  $k$  elementi, si deve dividere per  $k!$  il numero totale di  $k$ -ple ordinate. In conclusione, il numero di sottoinsiemi con  $k$  elementi di un insieme con  $n$  elementi è dato da

$$\frac{n(n-1)\cdots(n-k+1)}{k!}.$$

In altre parole, il numero  $\binom{n}{k}$  di combinazioni semplici di  $n$  oggetti di classe  $k$  si determina dividendo per  $k!$  il numero  $D(n, k)$  di disposizioni semplici di  $n$  elementi di classe  $k$ , ossia

$$\binom{n}{k} = \frac{D(n, k)}{k!} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}{k!} = \frac{n!}{k! \cdot (n-k)!}$$

Riassumendo, si ha la seguente proposizione.

**PROPOSIZIONE 4.1** Sia  $n$  un intero positivo, e sia  $k$  un intero tale che  $0 \leq k \leq n$ . Allora

- il numero  $D(n, k)$  di disposizioni semplici di  $n$  elementi di classe  $k$  è dato da

$$D(n, k) = n \cdot (n-1) \cdot (n-2) \cdots (n-k+1);$$

- il numero  $\binom{n}{k}$  di combinazioni semplici di  $n$  elementi di classe  $k$  è dato da

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

Dalla definizione e dal significato di  $\binom{n}{k}$  appare chiaro che

$$\binom{n}{0} = 1, \quad \binom{n}{1} = n, \quad \binom{n}{n} = 1$$

e che

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

Vale inoltre la seguente utile relazione (cfr. eserc. 16)

$$(2.1) \quad \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Tale formula ci permette di calcolare  $\binom{n+1}{k}$  a partire dai valori  $\binom{n}{k}$  e  $\binom{n}{k-1}$ . Si può così costruire il cosiddetto *triangolo di Tartaglia* (o di Pascal) dove ogni intero che vi compare è somma degli interi che si trovano sulla riga precedente sopra e a sinistra.

$n$	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
7	1	7	21	35	35	21	7	1

Gli interi  $\binom{n}{k}$  prendono anche il nome di *coefficienti binomiali*: il motivo di tale denominazione è che essi compaiono come coefficienti nella formula che dà lo sviluppo della potenza di un binomio  $(x+y)^n$ :

$$(2.2) \quad (x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k.$$

Esaminiamo i primi valori di  $n$ :

$$\begin{aligned}(x+y)^0 &= 1x^0y^0 \\(x+y)^1 &= 1x^1y^0 + 1x^0y^1 \\(x+y)^2 &= 1x^2y^0 + 2x^1y^1 + 1x^0y^2 \\(x+y)^3 &= 1x^3y^0 + 3x^2y^1 + 3x^1y^2 + 1x^0y^3.\end{aligned}$$

In generale, lo sviluppo della potenza

$$(x+y)^n = \underbrace{(x+y)(x+y) \cdots (x+y)}_{n \text{ fattori}}$$

è costituito da una somma di termini, ciascuno dei quali è un prodotto di  $n$  fattori ciascuno dei quali è  $x$  o  $y$ . Se, all'interno di un fattore,  $y$  compare  $k$  volte, allora in quello stesso fattore  $x$  comparirà  $n - k$  volte. Il numero di fattori in cui  $y$  è ripetuto  $k$  volte (e quindi  $x$  è ripetuto  $n - k$  volte) sarà il coefficiente di  $x^{n-k}y^k$ , e tale numero è precisamente il numero di modi di scegliere  $k$  degli  $n$  binomi  $(x+y)$ , ossia  $\binom{n}{k}$ .

### 2.3 Disposizioni e combinazioni con ripetizione

Finora abbiamo studiato il caso di scelte di  $k$  elementi tutti diversi tra loro da un insieme con  $n$  elementi, ossia abbiamo trattato le disposizioni e combinazioni semplici. Passiamo ora a studiare il caso in cui gli elementi da scegliere possano coincidere, ci siano cioè delle ripetizioni. Il problema è quindi il seguente: *in quanti modi si possono scegliere  $k$  elementi (anche coincidenti) in un insieme con  $n$  elementi?* Cioè quante sono le  $k$ -ple con elementi eventualmente coincidenti presi da un insieme con  $n$  elementi?

Anche in questo caso dovremo distinguere il caso in cui siamo interessati all'ordine e il caso in cui invece l'ordine è irrilevante: parleremo allora rispettivamente di *disposizioni con ripetizione di  $n$  elementi di classe  $k$*  e di *combinazioni con ripetizione di  $n$  elementi di classe  $k$* .

- *Calcolo delle disposizioni con ripetizione di  $n$  elementi di classe  $k$ .*

Il primo elemento può essere scelto in  $n$  modi, il secondo ancora in  $n$  modi (dato che ci possono essere ripetizioni), il terzo ancora in  $n$  modi, e così infine il  $k$ -esimo. I possibili modi sono quindi

$$\underbrace{n \cdot n \cdot n \cdots n}_k = n^k.$$

Facciamo un esempio:

#### Esempio 4.9

Quante targhe costituite da 7 cifre si possono formare?

Il problema è: *in quanti modi si possono scegliere 7 elementi (anche coincidenti) nell'insieme (costituito da 10 elementi)  $\{0, 1, 2, \dots, 9\}$ , ossia quante sono le 7-ple di elementi presi dall'insieme  $\{0, 1, 2, \dots, 9\}$ ?*

Ovviamente il primo elemento della 7-pla può essere scelto in 10 modi, così il secondo (dato che possono coincidere) e così via. In tutto quindi le possibili targhe sono

$$\underbrace{10 \cdot 10 \cdot 10 \cdots 10}_7 = 10^7.$$

- *Calcolo delle combinazioni con ripetizione di  $n$  elementi di classe  $k$ .*

Questo è un conteggio un po' più delicato. Si tratta di contare le  $k$ -ple (non ordinate) con eventuali ripetizioni da un insieme con  $n$  elementi. Per fare questo calcolo, procederemo al modo seguente. Indicati con  $a_1, a_2, \dots, a_n$  gli  $n$  elementi da disporre (con eventuali ripetizioni) nelle  $k$ -ple, dato che l'ordine con cui compaiono gli  $a_i$  è irrilevante, ossia dato che considereremo uguali due  $k$ -ple che differiscano solo per l'ordine con cui sono disposti gli elementi  $a_1, a_2, \dots, a_n$ , non è restrittivo limitarci a considerare  $k$ -ple nelle quali elementi uguali siano raggruppati, ossia  $k$ -ple del tipo

$$\underbrace{(a_i, a_i, \dots, a_i)}_{n_i}, \underbrace{(a_j, a_j, a_j, a_j)}_{n_j}, \dots, \underbrace{(a_r, a_r, a_r, a_r)}_{n_r}$$

con  $n_i + n_j + \dots + n_r = k$ . Ora, possiamo visualizzare tali  $k$ -ple in un altro modo, che ci permetterà di contare più agevolmente. Per capire meglio conviene fare un esempio concreto. Sia per esempio  $k = 10$  e  $n = 3$ . Consideriamo la seguente 10-pla:

$$(a_1, a_1, a_2, a_2, a_2, a_3, a_3, a_3, a_3, a_3).$$

Possiamo identificarla con il seguente schema:

$$xx|xxxx|xxxx.$$

Le barre verticali sono in numero di  $n - 1$ , cioè 2 in questo caso. La loro funzione è la seguente: la prima barra verticale, dopo la serie di due  $x$  sta a significare che ci sono due  $a_1$  nella  $k$ -pla, la seconda dopo quattro  $x$ , sta a significare che ci sono 4  $a_2$ : poi ci dovranno essere necessariamente 4  $a_3$  per arrivare a quota 10. In altre parole, la barra verticale sta a significare che si passa ad un altro elemento.

Per esempio, consideriamo la seguente situazione (sempre con  $k = 10$  e  $n = 3$ ):

$$||xxxxxx|xxxxx.$$

A sinistra della prima barra verticale non c'è nessuna  $x$ : questo significa che nella 10-pla non compare nessun  $a_1$ . A sinistra della seconda barra verticale non c'è nessuna  $x$ , quindi significa che non c'è nessun  $a_2$ . Allora la 10-pla corrispondente è la seguente:

$$(a_3, a_3, a_3, a_3, a_3, a_3, a_3, a_3, a_3, a_3).$$

Ancora, la

$$|xx|xxxxxxxx$$

corrisponde invece alla

$$(a_2, a_2, a_3, a_3, a_3, a_3, a_3, a_3, a_3, a_3).$$

Abbiamo stabilito una corrispondenza biunivoca (dando due modi equivalenti di scrivere le  $k$ -ple) tra questi insiemi. Ora il secondo modo ha il vantaggio che, così rappresentate, siamo in grado di determinarne il numero. Infatti dobbiamo contare in quanti modi possiamo sistemare i  $12 = 10 + 2$  elementi che consistono di dieci  $x$  e due barre verticali: in definitiva ci sono due soli simboli:  $x$  e  $|$  e il simbolo  $x$  è ripetuto 10 volte, mentre il simbolo  $|$  è ripetuto 2 volte. Il numero che cerchiamo è dato da tutte le permutazioni di 12 elementi divisi per  $10! \cdot 2!$ : infatti si deve tener conto del fatto che 10 elementi (le  $x$ ) sono uguali tra loro e così 2 elementi (le barre verticali). In definitiva sono in numero di

$$\frac{12!}{10!2!} = \binom{12}{10} = 66.$$

Si noti che  $12 = 10 + 3 - 1 = k + n - 1$ , quindi il discorso fatto in questo caso particolare si generalizza a  $k$  ed  $n$  arbitrari. Per contare le combinazioni con ripetizione di  $n$  elementi di classe  $k$  dovremo contare quante sono le liste con  $k$  elementi  $x$  ripetuti intermezzati da  $n - 1$  barre verticali. Tali liste sono in numero di

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

Quindi questo numero rappresenta il numero totale di combinazioni *con ripetizioni* di  $n$  elementi di classe  $k$ . Tale numero uguaglia il numero di combinazioni *semplici* di  $n+k-1$  elementi di classe  $k$  che sappiamo essere

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

Infatti

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

Concludendo, abbiamo provato la seguente proposizione:

**PROPOSIZIONE 4.2** Il numero di disposizioni con ripetizione di  $n$  elementi di classe  $k$  è  $n^k$ .

Il numero di combinazioni con ripetizione di  $n$  elementi di classe  $k$  uguaglia il numero di combinazioni semplici di  $n+k-1$  elementi di classe  $k$ , ossia

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

Terminiamo con due esempi.

#### Esempio 4.10

Un negozio di dischi ha lanciato un'offerta speciale: sono scontati due tipi di CD: i CD con le musiche di Respighi, che indicheremo con la lettera  $r$ , e i CD con musiche di Schubert, che indicheremo con la lettera  $s$ . Quattro amici, Alberto, Bruno, Carlo e Dario, decidono di acquistarne uno ciascuno. Quanti sono i possibili modi in cui i 4 amici possono fare gli acquisti? Dobbiamo contare tutte le possibili quaterne costituite da due elementi ( $r$  e  $s$ ) eventualmente ripetuti. Si noti che siamo interessati a sapere chi ha comperato *che cosa*.

Si tratta delle disposizioni con ripetizione di  $n = 2$  elementi di classe  $k = 4$ , che sappiamo essere  $n^k = 2^4$ .

Le 16 quaterne sono le seguenti (la colonna  $i$ -esima ( $i = 1, 2, 3, 4$ ) rappresenta l'acquisto fatto dall' $i$ -esimo acquirente):

$r$	$r$	$r$	$r$
$r$	$r$	$r$	$s$
$r$	$r$	$s$	$r$
$r$	$s$	$r$	$r$
$s$	$r$	$r$	$r$
$r$	$r$	$s$	$s$
$r$	$s$	$r$	$s$
$s$	$r$	$r$	$s$
$r$	$s$	$s$	$r$
$s$	$r$	$s$	$r$
$s$	$s$	$r$	$r$
$s$	$s$	$s$	$r$
$s$	$r$	$s$	$s$
$r$	$s$	$s$	$s$
$s$	$s$	$s$	$s$

Facciamo ora una variante al precedente esercizio.

#### Esempio 4.11

Un negozio di dischi ha lanciato un'offerta speciale: sono scontati due tipi di CD: i CD con le musiche di Respighi, che indicheremo con la lettera  $r$ , e i CD con musiche di Schubert, che indicheremo con la lettera  $s$ . Quattro amici, Alberto, Bruno, Carlo e Dario decidono di acquistarne uno ciascuno. Quanti possibili acquisti è possibile fare?

Questa volta che non ci importa *chi* ha fatto l'acquisto, ci interessa solamente quanti tipi di CD (quali quaterne di CD) sono state acquistate dai quattro amici. Quindi considereremo uguali per esempio la quaterna  $rrrs$  e la quaterna  $rsrr$ , dove il primo elemento della quaterna indica che è stato acquistato da  $A$ , il secondo che è stato acquistato da  $B$ , ecc.

Si tratta di contare le combinazioni con ripetizione di  $n = 2$  elementi di classe  $k = 4$  e sappiamo che queste uguagliono il numero di combinazioni semplici di  $n+k-1 = 5$  elementi di classe 4, ossia

$$\binom{n+k-1}{k} = \binom{5}{4} = 5.$$

Sono le seguenti (diamo le due rappresentazioni):

$r$	$r$	$r$	$r$	$x$	$x$	$x$	$x$	$ $	$x$
$r$	$r$	$r$	$s$	$x$	$x$	$x$	$ $	$x$	$x$
$r$	$r$	$s$	$s$	$x$	$x$	$ $	$x$	$x$	$x$
$r$	$s$	$s$	$s$	$x$	$ $	$x$	$x$	$x$	$x$
$s$	$s$	$s$	$s$	$ $	$x$	$x$	$x$	$x$	$x$

Si noti che, come si è visto in questi esempi, se si ammettono ripetizioni, non si deve supporre  $k \leq n$ .



Uno studente vuole usare durante i cinque giorni di lezione settimanali cinque penne diverse, senza mai riutilizzare la stessa penna. Quanti sono i possibili modi con cui può utilizzare le sue penne?

Quante targhe si possono formare utilizzando quattro cifre seguite da tre lettere (scelte tra 26)?

Quante sono le parole (anche senza significato) di cinque lettere che si possono fare con un alfabeto di 26 lettere, che abbiano al secondo posto una *A* e al terzo posto una *S*?

Se  $A = \{a_1, a_2, a_3\}$  e  $B = \{b_1, b_2\}$ , determinare il numero di funzioni tra  $A$  e  $B$ .

Generalizzazione dell'esercizio precedente. Dati due insiemi  $A$  e  $B$  di  $n$  e  $m$  elementi rispettivamente, determinare il numero di funzioni tra  $A$  e  $B$ .

Quanti sono i sottoinsiemi di un insieme con 12 elementi?

Determinare il numero di modi in cui cinque ragazzi e cinque ragazze si possono sedere in una stessa fila uno accanto all'altro, in modo che ragazzi e ragazze si alternino (nel senso che mai due ragazze o due ragazzi siano seduti vicino).

Ad una gara partecipano 7 atleti. Quanti sono tutti i possibili ordini di arrivo?

Si contano tutte le applicazioni *iniettive* tra due insiemi  $A$  e  $B$  con  $n$  elementi ciascuno.

E quelle *suriettive* quante sono?

Siano  $A$  e  $B$  due insiemi con  $n$  e  $m$  elementi rispettivamente. Se è  $n \leq m$  (perché questa condizione?), si contano tutte le applicazioni iniettive di  $A$  in  $B$ .

Determinare il numero di sottoinsiemi con 4 elementi di un insieme con 9 elementi.

Siano  $n, k$  interi positivi tali che  $n \geq k$ . Si provi che

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

Otto persone, *A*, *B*, *C*, *D*, *E*, *F*, *G* e *H* devono sedersi attorno ad un tavolo circolare. Quanti sono i modi in cui si possono disporre, se vengono considerate uguali disposizioni ottenute l'una dall'altra mediante una rotazione (ossia la disposizione *ABCDEFGH* è identificata con la disposizione *DEFGHABC*: infatti attorno ad un tavolo circolare non c'è un capotavola, ossia non ci sono posizioni privilegiate).

Calcolare il coefficiente di  $x^4y^8$  nell'espansione di

$$(x-y)^{12}.$$

Determinare il numero di modi in cui 6 motociclette rosse e 6 motociclette blu si possono disporre sulla linea di partenza di un circuito in modo che mai due motociclette dello stesso colore siano affiancate.

Si considerino gli insiemi  $A = \{a_1, a_2, a_3, a_4, a_5\}$  e  $B = \{b_1, b_2, b_3\}$ . Quante sono le funzioni  $f$  da  $A$  in  $B$  soggette alla condizione  $f(a_3) = b_2$ ?

Una ditta di informatica decide di assumere 7 laureati. Si presentano 10 candidati. In quanti modi la ditta può effettuare la scelta?

Sei studenti hanno svolto un compito seduti sulla stessa fila e ciascuno di essi ha ottenuto una votazione compresa fra 28 e 30 (inclusi). Si sa inoltre che ogni studente ha ottenuto un voto differente da quello del vicino (o dei vicini). In quanti modi possono essere stati attribuiti i voti?

In quanti modi possono essere stati attribuiti i voti dell'esercizio precedente se si suppone inoltre che almeno uno studente abbia ottenuto 28, almeno uno studente abbia ottenuto 29, almeno uno studente abbia ottenuto 30?

Dire quanti anagrammi distinti si possono fare (considerando anche parole senza senso) con la parola

### M A T E M A T I C A

a. Giovanna ha con sé 20 euro e si trova davanti ad un negozio di musica che offre alcuni *CD* al prezzo scontato di 5 euro l'uno. Giovanna può scegliere fra 7 *CD*, ed ha deciso di spendere in quel negozio esattamente tutti i 20 euro che ha con sé. In quanti modi può effettuare la sua scelta?

b. Il giorno successivo, Giovanna torna allo stesso negozio di musica, ed ha sempre con sé 20 euro. Questa volta, ci sono 8 *CD* in offerta a 4 euro l'uno, e 7 *CD* in offerta a 5 euro l'uno. Giovanna ha deciso di spendere in quel negozio esattamente tutti i 20 euro che ha con sé. In quanti modi può effettuare la sua scelta?

Cinque amici decidono di entrare in un negozio di abbigliamento specializzato in pantaloni e camicie e di acquistare ciascuno di loro esattamente una camicia o un paio di pantaloni. Quanti sono i possibili modi in cui possono fare gli acquisti? N.B. siamo interessati a chi compera che cosa.

E se nell'esercizio precedente avessimo chiesto quanti possibili acquisti è possibile fare? (ossia non ci importa chi ha fatto l'acquisto, ma solo il tipo di acquisto che è stato fatto).

Un insieme  $A$  ha 4 elementi e si sa che il numero di funzioni iniettive da  $A$  a un insieme  $B$  è 840. Determinare la cardinalità di  $B$ . Se invece si sapesse che il numero delle funzioni iniettive da  $A$  a  $B$  è 1680, quale sarebbe la cardinalità di  $B$ ?

Quanti sono i numeri naturali minori di 500, composti da tre cifre tutte pari e diverse fra loro?

Quante sono le quaterne  $(a, b, c, d)$  di interi positivi tali che  $a+b+c+d=50$ ?

Ad una competizione elettorale partecipano 6 liste, ciascuna delle quali ha presentato 10 candidati. L'elettore vota scegliendo una fra le liste e può esprimere la preferenza per un certo numero di candidati appartenenti alla lista prescelta, fino ad un massimo di 3 preferenze.

- Aldo ha deciso di votare, ed ha deciso che esprimerà tutte e tre le preferenze consentite. In quanti modi potrà esprimere il suo voto?
- Anche Giovanni ha deciso che voterà, ma non sa se e quante preferenze esprimerà. In quanti modi potrà esprimere il suo voto?
- Risolvere gli esercizi precedenti nel caso in cui 4 delle 6 liste abbiano presentato solo 8 candidati, mentre le altre 2 liste abbiano presentato 10 candidati.

In quanti modi si può fattorizzare come prodotto di *due* soli fattori (diversi da 1 e da se stesso) il numero 210? N.B. Si considerano uguali due fattorizzazioni che differiscono solo per l'ordine.

In una certa nazione le targhe delle automobili sono costituite o da tre lettere seguite da due cifre, oppure da 4 lettere seguite da 1 cifra. Quante sono le possibili targhe?

Quanti numeri interi di 4 cifre hanno almeno una cifra dispari?

Si considerino gli insiemi  $A = \{3, 4, 5\}$  e  $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ . Quante sono le funzioni  $f : A \rightarrow B$  tali che  $f(a) > a$ , per ogni  $a \in A$ ?

Si considerino gli insiemi  $A = \{3, 4, 5, 6\}$  e  $B = \{1, 2, 3, 4, 5, 6, 7\}$ . Quante sono le funzioni  $f : A \rightarrow B$  tali che  $f(a) \geq a$ , per ogni  $a \in A$ ?

a. Da un mazzo di 40 carte si prendono 2 carte. In quanti modi questo può essere fatto (indipendentemente dall'ordine in cui si prendono le carte)?  
b. Il mazzo di 40 carte ha quattro semi, e le carte di ogni seme sono numerate con valori da 1 a 10 (con esattamente un valore per ogni seme). In quanti modi si possono prendere 2 carte con uno stesso valore dal mazzo?

a. Da un mazzo di 40 carte si prendono 3 carte. In quanti modi questo può essere fatto (indipendentemente dall'ordine in cui si prendono le carte)?  
b. Il mazzo di 40 carte ha quattro semi, e le carte di ogni seme sono numerate con valori da 1 a 10 (con esattamente un valore per ogni seme). In quanti modi si possono prendere 3 carte con uno stesso valore dal mazzo?

Si considerino gli insiemi  $A = \{3, 4, 5, 6\}$ ,  $B = \{5, 6\}$ ,  $C = \{3, 4, 5, 6\} \cap \{x \in \mathbb{N} | x < 5\}$ . Quante sono le funzioni  $f : A \times B \rightarrow C$ ?

Si considerino gli insiemi  $A = \{4, 5, 6\}$ ,  $B = \{5, 6\}$ ,  $C = \{3, 4, 5, 6\} \cap \{x \in \mathbb{N} | x \geq 5\}$ . Quante sono le funzioni  $f : A \rightarrow B \times C$ ?

Si considerino gli insiemi  $A = \{4, 5, 6\}$ ,  $B = \{5, 6, 7\}$ ,  $C = \{3, 4, 5, 6\} \cap \{x \in \mathbb{N} | x < 5\}$ . Quante sono le funzioni  $f : A \times B \rightarrow C$ ?

Si considerino gli insiemi  $A = \{4, 5, 6\}$ ,  $B = \{5, 6, 7\}$ ,  $C = \{3, 4, 5, 6\} \cap \{x \in \mathbb{N} | x \geq 5\}$ . Quante sono le funzioni  $f : A \rightarrow B \times C$ ?

- Da un mazzo di 32 carte si prendono 5 carte. In quanti modi questo può essere fatto (indipendentemente dall'ordine in cui si prendono le carte)?
- Il mazzo di 32 carte ha quattro semi, con 8 carte per ciascun seme. In quanti modi si possono prendere 5 carte dello stesso seme dal mazzo?
- Da un mazzo di 28 carte si prendono 5 carte. In quanti modi questo può essere fatto (indipendentemente dall'ordine in cui si prendono le carte)?
- Il mazzo di 28 carte ha quattro semi, con 7 carte per ciascun seme. In quanti modi si possono prendere 5 carte dello stesso seme dal mazzo?
- Quanti sono i numeri interi  $> 0$  che, fattorizzati in primi, hanno tutti i fattori contenuti nell'insieme  $\{3, 5, 7, 11\}$ , con ciascuno di questi fattori elevato a un esponente strettamente minore di 10?
- Quanti fra i numeri precedenti sono tali che gli esponenti a cui sono elevati 3, 5, 7, 11 sono tutti distinti?
- Quanti sono i numeri interi, sia positivi che negativi, che soddisfano alle condizioni delle due domande precedenti?
- Uno studente sta svolgendo un test e deve rispondere a 9 domande su 12: l'ordine con cui risponde alle domande non ha importanza. In quanti modi può scegliere le domande a cui rispondere?
- Se deve rispondere a 4 domande scegliendole tra le prime 6 e 5 domande tra le ultime 6, in quanti modi può fare la sua scelta?

### 3 IL PRINCIPIO DI INCLUSIONE-ESCLUSIONE

Ci siamo già imbattuti nel problema di contare gli elementi che si trovano nell'unione di due insiemi finiti  $A$  e  $B$ , ossia calcolare  $|A \cup B|$ . Ovviamente, come abbiamo visto quando abbiamo parlato della regola della somma, se i due insiemi sono disgiunti, la cardinalità dell'unione non è altro che la somma delle cardinalità dei singoli insiemi. Così partendo da un numero  $s$  di insiemi a due a due disgiunti, la cardinalità dell'unione è la somma delle cardinalità degli  $s$  insiemi. Se però si parte da due insiemi  $A$  e  $B$  non disgiunti, la situazione cambia: in questo caso

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

Infatti il numero  $|A| + |B|$  conta (cfr. fig. 4.3)

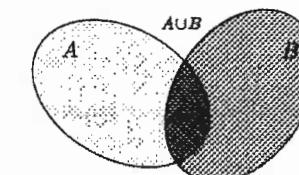


Figura 4.3.

una volta ogni elemento che si trova in esattamente uno dei due insiemi  $A$ ,  $B$ , due volte ogni elemento che si trova nell'intersezione  $A \cap B$  (una volta considerandolo come elemento di  $A$  e un'altra volta come elemento di  $B$ ).

Quindi dal numero  $|A| + |B|$  dobbiamo togliere  $|A \cap B|$ .

Vediamo alcune applicazioni.

#### Esempio 4.12

Quanti sono i numeri minori o uguali di 50 che sono divisibili per 3 o per 5?

Posto  $A := \{n \leq 50 \mid n \text{ divisibile per } 3\}$ ,  $B := \{n \leq 50 \mid n \text{ divisibile per } 5\}$ , allora  $A \cap B = \{n \leq 50 \mid n \text{ divisibile per } 3 \text{ e per } 5\}$ . Ora,

$$|A| = \left[ \frac{50}{3} \right] = \text{parte intera di } \frac{50}{3} = 16,$$

$$|B| = \left[ \frac{50}{5} \right] = \text{parte intera di } \frac{50}{5} = 10.$$

Dato che 3 e 5 non hanno fattori comuni,

$$|A \cap B| = \left[ \frac{50}{15} \right] = \text{parte intera di } \frac{50}{15} = 3.$$

Ne segue che  $|A \cup B| = 16 + 10 - 3 = 23$ .

Verifichiamolo.

$$A = \{3, 6, 9, 12, \underline{15}, 18, 21, 24, 27, \underline{30}, 33, 36, 39, 42, \underline{45}, 48\}$$

$$B = \{5, 10, \underline{15}, 20, 25, \underline{30}, 35, 40, \underline{45}, 50\}$$

$$A \cap B = \{15, 30, 45\}$$

Ora, si vede che i tre numeri 15, 30 e 45 sono contati sia come elementi di  $A$  sia come elementi di  $B$ , quindi da  $|A| + |B|$  va tolto 3.

Passiamo ora al caso di tre insiemi. Vogliamo calcolare  $|A \cup B \cup C|$ . Il numero  $|A| + |B| + |C|$  conta (cfr. fig. 4.4)

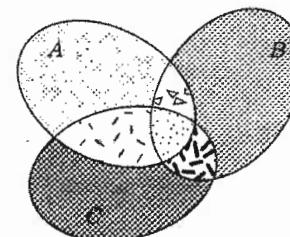


Figura 4.4.

una volta ogni elemento che si trova in esattamente uno dei tre insiemi  $A, B, C$   
due volte ogni elemento che si trova nell'intersezione di due degli insiemi  $A, B, C$   
tre volte ogni elemento che si trova nell'intersezione di tre degli insiemi  $A, B, C$ , cioè che si trova in  $A \cap B \cap C$ .

Proviamo quindi a togliere ad  $|A| + |B| + |C|$  il numero  $|A \cap B| + |A \cap C| + |B \cap C|$ : ora

$$|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C|$$

conta

- una volta ogni elemento che si trova in esattamente uno dei tre insiemi  $A, B, C$ ,
- una volta ogni elemento che si trova nell'intersezione di due degli insiemi  $A, B, C$ , ma
- zero volte ogni elemento che si trova nell'intersezione di tre degli insiemi  $A, B, C$  ossia che si trova in  $A \cap B \cap C$ .

Per rimediare a questo, si deve aggiustare la formula al modo seguente:

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

Non è difficile quindi capire che la formula generale per contare gli elementi che si trovano nell'unione di  $n$  insiemi finiti è la seguente *formula generale per il principio di inclusione-esclusione*:

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \\ &+ \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|. \end{aligned}$$

Vediamo come possiamo servirci di queste formule per risolvere vari problemi.

#### Esempio 4.13

Ad una manifestazione sportiva in cui si svolgono 3 gare partecipano 19 atleti. Se si indicano rispettivamente con  $A, B, C$  gli insiemi degli atleti che partecipano alla prima, alla seconda e alla terza gara, si considerino le seguenti possibilità:

1.

$$|A| = 10, |B| = 12, |C| = 9, |A \cap B| = 3, |A \cap C| = 5, |B \cap C| = 4$$

2.

$$|A| = 10, |B| = 12, |C| = 9, |A \cap B| = 3, |A \cap C| = 6, |B \cap C| = 4$$

Solo una delle possibilità (1), (2) precedenti può verificarsi. Quale? Perché? Quanti sono gli atleti che partecipano a tutte e tre le gare?

3. Potrebbe verificarsi la seguente possibilità?

$$|A| = 10, |B| = 12, |C| = 9, |A \cap B| = 2, |A \cap C| = 0, |B \cap C| = 10?$$

Poiché tutti i 19 atleti partecipano ad almeno una gara,  $|A \cup B \cup C| = 19$ . Quindi,  $19 = |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| = 10 + 12 + 9 - 2 - 0 - 10 + |A \cap B \cap C|$ , da cui si ricava  $|A \cap B \cap C| = 0$ , quindi nessun atleta partecipa a tutte le tre gare.

Allo stesso modo, si ricava  $|A \cap B \cap C| = -1$ , che è impossibile.

L'ultima possibilità è impossibile, poiché non può essere  $|C| < |B \cap C|$ .

## 5

# Dalle congruenze alla crittografia

Provare che per ogni  $n \in \mathbb{N}$ , detti  $A_1, A_2, \dots, A_n$   $n$  insiemi arbitrari, si ha  $|A_1 \cup A_2 \cup \dots \cup A_n| \leq |A_1| + |A_2| + \dots + |A_n|$ .

Al primo anno di Informatica ci sono 100 studenti. I maschi sono 80, gli studenti biondi sono 20 e i maschi biondi sono 9. Quante sono le ragazze brune? Ammettiamo che i capelli possano essere solo biondi o bruni, che cioè non ci siano sfumature intermedie.

Beatrice entra in un negozio per comperare una gonna. È molto esigente, e su 25 gonne che ha visto, 8 sono troppo scure, 6 sono troppo chiare, 12 sono troppo strette, 6 sono troppo scure e troppo strette, 5 sono troppo strette e troppo chiare. In definitiva, quante sono le gonne di suo gradimento?

## Esercizi di programmazione

Scrivere un programma che calcoli  $n!$  per ogni intero non negativo  $n$ .

Scrivere un programma che, dato  $n$ , calcoli tutte le permutazioni di  $n$  oggetti.

Scrivere un programma che calcoli  $\binom{n}{k}$ .

Scrivere un programma che calcoli tutte le disposizioni semplici di  $n$  oggetti di classe  $k$ .

Scrivere un programma che calcoli tutte le disposizioni con ripetizione di  $n$  oggetti di classe  $k$ .

Scrivere un programma che calcoli tutte le combinazioni con ripetizione di  $n$  oggetti di classe  $k$ .

Scrivere un programma che generi il triangolo di Tartaglia per vari valori di  $n$ .

*Nel circolo principio e fine fanno uno.  
Eraclito, da I FRAMMENTI, n. 30*

Abbiamo visto vari algoritmi sugli interi. L'insieme  $\mathbb{Z}$  dei numeri interi tuttavia ha il difetto di essere un insieme infinito e questo può creare qualche problema al calcolatore. Definendo una opportuna relazione di equivalenza su  $\mathbb{Z}$ , ossia identificando opportunamente degli interi, vedremo come si riuscirà a passare dall'insieme infinito  $\mathbb{Z}$  ad un insieme finito, l'insieme quoziente modulo questa relazione di equivalenza: con tale insieme sarà più facile lavorare. Tutto il presente capitolo sarà dedicato a questa relazione, alle sue proprietà e alle sue importanti applicazioni, quali la crittografia classica e a chiave pubblica.

## 1 CONGRUENZE E LORO PROPRIETÀ

Partiamo da un esempio. Quando leggiamo l'ora su un orologio, le 10 di mattina e le 10 di sera (ossia le 22) vengono visualizzate allo stesso modo, ossia dalla stessa posizione della lancetta: e non ci importa di distinguerle, perché ovviamente siamo in grado di accorgerci se si tratta delle 10 di mattina o di sera. L'informazione che leggiamo sull'orologio ci basta per individuare l'ora esatta. Che legame c'è tra le 10 di mattina e le 22? che la loro differenza è 12. Questo avviene per tutte le ore che leggiamo sull'orologio: la lancetta continua a girare, e via via che trascorrono 12 ore ripassa per la stessa posizione. Stiamo contando modulo 12, ossia a meno di multipli di 12: ore che differiscono per multipli di 12 vengono identificate sull'orologio, infatti sull'orologio compaiono solo 12 simboli, 1, 2, ..., 12. Numeri che differiscono per un multiplo di 12 vengono considerati uguali. Il ruolo svolto per la lettura delle ore sull'orologio dal numero 12 può essere svolto da un qualunque altro intero positivo  $n$ : si parlerà allora di uguaglianza a meno di multipli di un intero positivo  $n$ .

**DEFINIZIONE 5.1** Sia  $n$  un fissato intero positivo. Si dice *relazione di congruenza modulo  $n$*  la relazione su  $\mathbb{Z}$  definita al modo seguente:

$$a \rho_n b \text{ ovvero } a \equiv b \pmod{n} \iff a - b = nh \text{ per qualche } h \in \mathbb{Z}.$$

Per visualizzare meglio questo tipo di relazione, possiamo ancora pensare ad un orologio sul cui bordo siano disegnati, a uguale distanza l'uno dall'altro, gli  $n$  interi  $1, 2, \dots, n$ : la lancetta dell'orologio permetterà di leggere l'intero sul quale è punta: via via che continua a girare, in senso orario o in senso antiorario, ripasserà per la stessa posizione, cioè punterà nuovamente su uno degli interi  $1, 2, \dots, n$ . Appare chiaro che tutti i multipli interi di  $n$  verranno a coincidere con  $n$ , gli interi che divisi per  $n$  danno per resto 1 verranno a coincidere con 1, quelli che divisi per  $n$  danno come resto 2 verranno a coincidere con 2, e così via.

**PROPOSIZIONE 5.1** Si fissi un intero positivo  $n$ .

1. La relazione di congruenza modulo  $n$  è una relazione di equivalenza su  $\mathbb{Z}$ .
2. Ogni intero  $a$  è congruente modulo  $n$  ad un intero  $r$  tale che  $0 \leq r < n$ .

DIMOSTRAZIONE.

1. Che la relazione sia di equivalenza viene lasciata negli esercizi: (cfr. eserc. 1)
2. Basta osservare che ogni intero  $a$  è congruente modulo  $n$  al resto  $r$  della divisione di  $a$  per  $n$  e che questo intero  $r$  è maggiore di 0 e minore di  $n$  (cfr. proposizione 3.4).  $\diamond$

Pensando all'orologio, si vede bene come ogni intero venga *indicato* dalla lancetta con uno e un solo intero tra 1 e  $n$  (oppure un intero tra 0 e  $n - 1$ ).

La proposizione precedente ci permette di affermare che le classi di equivalenza sono:

$$\begin{aligned}\bar{0} &= \{\text{interi che divisi per } n \text{ danno per resto 0}\} = \{kn \mid k \in \mathbb{Z}\} \\ \bar{1} &= \{\text{interi che divisi per } n \text{ danno per resto 1}\} = \{kn + 1 \mid k \in \mathbb{Z}\}\end{aligned}$$

...

$$\begin{aligned}\bar{n-1} &= \{\text{interi che divisi per } n \text{ danno per resto } n-1\} \\ &= \{kn + n - 1 \mid k \in \mathbb{Z}\}.\end{aligned}$$

Indicheremo con  $\mathbb{Z}_n$  l'insieme quoziante di  $\mathbb{Z}$  rispetto alla congruenza modulo  $n$ :

$$\mathbb{Z}_n \stackrel{\text{def}}{=} \mathbb{Z}/\equiv_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}.$$

Vorremmo ora introdurre in  $\mathbb{Z}_n$  due operazioni, legate alle operazioni definite in  $\mathbb{Z}$ , in modo da chiamare  $\mathbb{Z}_n$  *anello* quoziante di  $\mathbb{Z}$  rispetto alla relazione di congruenza modulo  $n$ . Le definizioni più naturale di operazioni da introdurre in  $\mathbb{Z}_n$  sono le seguenti:

$$(1.1) \quad \bar{a} + \bar{b} \stackrel{\text{def}}{=} \overline{a+b}, \quad \bar{a} \cdot \bar{b} \stackrel{\text{def}}{=} \overline{a \cdot b},$$

dove i simboli  $+$  e  $\cdot$  nei secondi membri di queste relazioni corrispondono rispettivamente alla addizione e moltiplicazione *ordinarie* in  $\mathbb{Z}$  e dove, per semplicità, si sono usati gli stessi simboli per le operazioni tra classi, che stiamo definendo.

C'è però un problema: chi ci garantisce che queste definizioni siano *ben poste*? Esse sono definite attraverso dei rappresentanti in ogni classe; cambiando rappresentanti, il risultato porta alla stessa classe? Cosa che assolutamente dobbiamo richiedere, perché le nuove definizioni siano delle *operazioni* in  $\mathbb{Z}_n$ .

### Esempio 5.1

Si considerino in  $\mathbb{Z}_5$  le classi  $\bar{3}$  e  $\bar{4}$ . Secondo la definizione 1.1 si ha:  $\bar{3} + \bar{4} = \overline{3+4} = \bar{7}$ . Ora,  $\bar{3} = \bar{8}$  e  $\bar{4} = \bar{19}$ . Sempre in base alla definizione 1.1 si avrà:  $\bar{8} + \bar{19} = \overline{8+19} = \bar{27}$ . Quello che si richiede è che i due risultati coincidano, ossia che  $\bar{7}$  coincida con  $\bar{27}$ . Ma questo è vero, perché  $27 \equiv 7 \pmod{5}$ .

Ebbene, la dimostrazione generale (e non solo in un caso particolare) del fatto che si tratta di definizioni ben poste viene offerta dal seguente risultato.

**PROPOSIZIONE 5.2** Se  $a, b, c, d \in \mathbb{Z}$ , allora valgono le seguenti proprietà:

$$(1.2) \quad a \equiv b \pmod{n}, \quad c \equiv d \pmod{n} \implies \begin{cases} a+c \equiv b+d \pmod{n} \\ ac \equiv bd \pmod{n}. \end{cases}$$

DIMOSTRAZIONE. Si ha  $a \equiv b \pmod{n} \iff a-b = hn$ ,  $h \in \mathbb{Z}$ ,  $c \equiv d \pmod{n} \iff c-d = kn$ ,  $k \in \mathbb{Z}$ , da cui  $a+c-(b+d) = (h+k)n$  cioè  $a+c \equiv b+d \pmod{n}$ .

Analogamente,  $ac-bd = ac-ad+ad-bd = a(c-d)+(a-b)d = akn+hnd = (ak+hd)n$  e quindi  $ac \equiv bd \pmod{n}$ .  $\diamond$

La proposizione ci dice che la relazione di congruenza definita su  $\mathbb{Z}$  è *compatibile con le due operazioni definite in  $\mathbb{Z}$* . Questo ci assicura che le due definizioni date sono *ben poste*, cioè, pur essendo definite attraverso i rappresentanti, non dipendono da questi.

Diamo qui sotto le tavole additiva e moltiplicativa di  $\mathbb{Z}_n$  nei casi  $n = 5$  e  $n = 6$ .

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$n = 5$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{1}$	$\bar{3}$

$n = 6$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$						
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Osserviamo che  $\mathbb{Z}_5$  non possiede divisori dello zero (cfr. definizione 3.1), mentre il secondo sì: per esempio  $\bar{2}$  e  $\bar{3}$  sono classi non nulle, ma il loro prodotto  $\bar{2} \cdot \bar{3} = \bar{0}$  è la classe nulla  $\bar{0}$  in  $\mathbb{Z}_6$ . Quindi,  $\mathbb{Z}_5$  è un dominio di integrità, mentre  $\mathbb{Z}_6$  non lo è. Non è difficile rendersi conto in generale che  $\mathbb{Z}_n$  è un dominio di integrità se e solo se  $n$  è un numero primo. Infatti se  $n = p$  è un numero primo, dette  $\bar{a}$  e  $\bar{b}$  due classi in  $\mathbb{Z}_p$ , tali che sia  $\bar{a}\bar{b} = \bar{0}$ , si ha che  $p|ab$ . Ma, essendo  $p$  un numero primo, o  $p|a$  (ossia  $\bar{a}$  è la classe nulla) oppure  $p|b$  (ossia  $\bar{b}$  è la classe nulla); quindi  $\mathbb{Z}_p$  è un dominio d'integrità. Viceversa, se  $\mathbb{Z}_n$  è un dominio d'integrità, necessariamente  $n = p$  è un numero primo: se non lo fosse, ossia se fosse  $n = ab$  per qualche  $a, b < n$ , le due classi  $\bar{a}$  e  $\bar{b}$  sarebbero non nulle e tali che  $\bar{a}\bar{b} = \bar{0}$ .

Per esempio  $\mathbb{Z}_{45}$  non è un dominio d'integrità, perché esistono due classi, come  $\bar{9}$  e  $\bar{5}$ , non nulle tali però che il loro prodotto è la classe nulla.

In realtà dalla tabella relativa a  $\mathbb{Z}_5$  si vede che  $(\mathbb{Z}_5, +, \cdot)$  è anche più di un dominio d'integrità: ogni classe non nulla è dotata di inversa moltiplicativa. Infatti in ogni riga e in ogni colonna (esclusa la prima riga e la prima colonna formate da tutti zeri) c'è un 1. Per provare che questo è un fatto generale per  $\mathbb{Z}_p$  con  $p$  primo, dovremo però attendere qualche paragrafo (cfr. Corollario 5.8).

Come si è visto, la relazione di congruenza gode di molte delle proprietà dell'uguaglianza tra numeri interi. Un altro risultato che rispecchia le proprietà dell'uguaglianza è il seguente:

**COROLLARIO 5.1** Sia  $n$  un fissato intero positivo. Allora per ogni  $a, b, c$  e  $d \in \mathbb{Z}$  se  $a \equiv b \pmod{n}$  si ha

$$(1.3) \quad a + c \equiv b + c \pmod{n}$$

$$(1.4) \quad ac \equiv bc \pmod{n}$$

$$(1.5) \quad a^i \equiv b^i \pmod{n} \quad \forall i \in \mathbb{N}.$$

**DIMOSTRAZIONE.** Le congruenze (1.3) e (1.4) sono casi particolari di (1.2), mentre (1.5) si ottiene da (1.2) per induzione.  $\diamond$

Ci sono tuttavia proprietà dell'uguaglianza che non si estendono alle congruenze: per esempio, la legge di cancellazione  $ac = bc \implies a = b$ , che vale in  $\mathbb{Z}$  purché sia  $c \neq 0$ , non vale per le congruenze: per esempio

$$4 \cdot 5 \equiv 2 \cdot 5 \pmod{10}$$

ma non è vero che  $4 \equiv 2 \pmod{10}$ . Tuttavia vale in forma modificata, secondo il risultato che segue:

**PROPOSIZIONE 5.3** Se  $ac \equiv bc \pmod{n}$  e  $(c, n) = 1$ , allora  $a \equiv b \pmod{n}$ .

**DIMOSTRAZIONE.** La  $(c, n) = 1$  implica che esistono  $s, t \in \mathbb{Z}$  tali che  $1 = sc + tn$ ; moltiplicando per  $a - b$  ambo i membri, si ottiene

$$a - b = (a - b)sc + (a - b)tn = (a - b)c \cdot s + (a - b)tn$$

da cui risulta che  $n$  deve dividere  $(a - b)$  dato che divide il secondo membro e quindi  $a \equiv b \pmod{n}$ .  $\diamond$

Si osservi che nell'esempio che abbiamo dato prima non era verificata l'ipotesi richiesta, perché  $(5, 10) = 5 \neq 1$ .

In realtà questa proposizione è una conseguenza del seguente risultato più generale.

**PROPOSIZIONE 5.4** Se  $ac \equiv bc \pmod{n}$ , allora  $a \equiv b \pmod{n/d}$ , dove  $d = (c, n)$ .

**DIMOSTRAZIONE.** La proposizione sostanzialmente dice che si può sempre semplificare una congruenza cancellando un fattore comune, purché si cambi opportunamente il modulo.  $ac \equiv bc \pmod{n} \iff (a - b)c = kn$ , da cui, dividendo per  $d = (c, n)$ ,  $(a - b)(c/d) = k(n/d)$  (si osservi che le frazioni  $c/d$  e  $n/d$  sono numeri interi). Ma allora  $n/d$  divide il prodotto  $(a - b) \cdot (c/d)$  e  $(c/d, n/d) = 1$ , quindi (si provi!)  $n/d | (a - b)$ , cioè  $a \equiv b \pmod{n/d}$ .  $\diamond$

Riprendendo l'esempio precedente,  $4 \not\equiv 2 \pmod{10}$ , ma  $4 \equiv 2 \pmod{\frac{10}{5}}$ . La proposizione appena dimostrata collega fra loro due congruenze rispetto a moduli diversi. Raccogliamo nella seguente proposizione altre proprietà utili, che legano fra loro congruenze relative a moduli diversi.

**PROPOSIZIONE 5.5** Sussistono le seguenti proprietà:

- (a) Se  $a \equiv b \pmod{n}$  e  $d | n$ , allora  $a \equiv b \pmod{d}$ ;
- (b) se  $a \equiv b \pmod{r}$  e  $a \equiv b \pmod{s}$ , allora  $a \equiv b \pmod{[r, s]}$ .

**DIMOSTRAZIONE.** Basta ricordare la definizione di congruenza.  $\diamond$

### Esercizi

- Provare che la relazione di congruenza modulo  $n$  è una relazione di equivalenza.
- Provare che  $(\mathbb{Z}_n, +, \cdot)$  rispetto alle due operazioni di addizione e moltiplicazione definite nel testo è un anello commutativo con unità.
- Studiare la tavola additiva di  $\mathbb{Z}_6$ : cosa si può dire della struttura algebrica di  $\mathbb{Z}_6$  rispetto all'addizione? Ogni elemento di  $\mathbb{Z}_6$  ammette un opposto? Determinare l'opposto di  $\bar{4}$  e l'opposto di  $\bar{3}$ , se esistono.
- Studiare la tavola additiva di  $\mathbb{Z}_7$ : cosa si può dire della struttura algebrica di  $\mathbb{Z}_7$  rispetto all'addizione? Ogni elemento di  $\mathbb{Z}_7$  ammette un opposto? Determinare l'opposto di  $\bar{4}$  e l'opposto di  $\bar{3}$ , se esistono.
- Determinare la tavola moltiplicativa di  $(\mathbb{Z}_8, +, \cdot)$ . Esiste l'inverso moltiplicativo della classe  $\bar{5}$ ? e della classe  $\bar{2}$ ? Esistono in  $(\mathbb{Z}_8, +, \cdot)$  divisori dello zero? Se sì, determinarne almeno una coppia.
- Studiare  $(\mathbb{Z}_7, +, \cdot)$ . Esiste l'inverso moltiplicativo della classe  $\bar{5}$ ? e della classe  $\bar{2}$ ? Esistono in  $(\mathbb{Z}_7, +, \cdot)$  divisori dello zero? Se sì, determinarne almeno una coppia.

Decidere quale degli anelli  $(\mathbb{Z}_7, +, \cdot)$  e  $(\mathbb{Z}_8, +, \cdot)$  è un dominio di integrità e in quale ogni classe non nulla è dotata di inversa.

Utilizzare le proprietà delle congruenze per trovare il resto della divisione per 10 del numero

$$3546^{2007}.$$

## ■ 2 IL PICCOLO TEOREMA DI FERMAT E CONSEGUENZE

Ci sono alcune importanti congruenze che andiamo a dimostrare.

**PROPOSIZIONE 5.6** Per ogni primo  $p$  e ogni  $x, y$  in  $\mathbb{Z}$  vale la seguente congruenza:

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

**DIMOSTRAZIONE.** In vista della formula (2.2) dello sviluppo della potenza di un binomio si ha

$$(x+y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k + y^p.$$

Dobbiamo provare che la sommatoria è congrua a zero modulo  $p$ , ossia che è divisibile per  $p$ . Ma questo è vero, perché nella sommatoria risulta  $k < p$  e  $p - k < p$ , onde ogni  $\binom{p}{k}$  che compare nella sommatoria è un intero che ha  $p$  a fattore. ♦

**TEOREMA 5.2 (PICCOLO TEOREMA DI FERMAT)** Siano  $a$  un intero e  $p$  un numero primo. Allora

$$a^p \equiv a \pmod{p}.$$

**DIMOSTRAZIONE.** Dimostriamo il teorema innanzitutto nel caso  $a \geq 0$ . In tal caso possiamo procedere per induzione prendendo come variabile di induzione  $a$  stessa. La proposizione da dimostrare per induzione è quindi la  $P(a)$ :

$$P(a) : a^p \equiv a \pmod{p} \quad \forall a \in \mathbb{N}, \text{ per ogni } p \text{ primo.}$$

Se  $a = 0$  il risultato è ovvio. Supponiamo allora vero il risultato per  $a$ , cioè

$$P(a) : a^p \equiv a \pmod{p},$$

e dimostriamo  $P(a+1)$ . Per la proposizione precedente  $(a+1)^p \equiv a^p + 1^p$ . Ma  $1^p \equiv 1$  e  $a^p \equiv a$  per l'ipotesi induttiva. Quindi vale la  $P(a+1)$ , ossia

$$(a+1)^p \equiv a+1$$

che è quanto volevamo provare.

Resta da dimostrare che il teorema è vero anche per  $a < 0$ .

Allora  $0 \equiv 0^p = (a+(-a))^p \equiv a^p + (-a)^p \pmod{p}$ . Dato che è  $-a > 0$ , per quanto provato al punto precedente è  $(-a)^p \equiv -a$ , quindi  $0 \equiv a^p - a$  cioè  $a^p \equiv a$ . ♦

**COROLLARIO 5.3** Se  $(a, p) = 1$ , allora  $a^{p-1} \equiv 1 \pmod{p}$ .

**DIMOSTRAZIONE.** Nelle ipotesi attuali possiamo semplificare per  $a$  il risultato della proposizione precedente. ♦

Proprio questo corollario sarà particolarmente utile per il calcolo di potenze modulo numeri primi, soprattutto quando l'esponente è un numero grande. Vediamo un esempio.

### Esempio 5.2

Determinare il resto della divisione per 7 del numero  $4526^{236}$ .

Si noti che chiedere il resto della divisione per 7 del numero equivale a determinare  $4526^{236} \pmod{7}$ . Innanzitutto osserviamo che  $4526 \equiv 4 \pmod{7}$ . Quindi  $4526^{236} \equiv 4^{236} \pmod{7}$ . Ora, dato che  $(4, 7) = 1$ , in base al Corollario del Piccolo Teorema di Fermat,  $4^6 \equiv 1 \pmod{7}$ . Da questa osservazione si può poi proseguire al modo seguente:

$$4526^{236} \equiv 4^{236} = 4^{39 \cdot 6 + 2} = (4^6)^{39} \cdot 4^2 \equiv 1^{39} \cdot 4^2 = 4^2 \equiv 2 \pmod{7}.$$

Il resto richiesto è quindi 2.

L'aver trovato un esponente  $h$  tale che  $a^h \equiv 1 \pmod{p}$  riduce l'esponente di partenza ad un numero minore di  $p-1$ , consentendo di tenere sotto controllo i calcoli.

Il guaio è che il Piccolo Teorema di Fermat funziona solo con moduli *primi*. Vedremo fra breve (teorema 5.7) come questo teorema si possa generalizzare al caso in cui il modulo *non* sia un numero primo.



Verificare che  $(x+y)^5 \equiv x^5 + y^5 \pmod{5}$ .

Determinare il resto della divisione per 3 di  $5^{427}$ .

## ■ 3 ALTRE APPLICAZIONI

In questo paragrafo faremo alcune utili applicazioni delle proprietà delle congruenze, quali i ben noti criteri di divisibilità e la prova del nove.

### 3.1 Criteri di divisibilità

Utilizzando le proprietà delle congruenze, siamo in grado di offrire alcuni criteri di divisibilità, senza svolgere nessuna divisione.

Come è ben noto, in base alla notazione posizionale decimale con cui scriviamo i numeri, il numero 1234567 corrisponde a scrivere

$$1 \cdot 10^6 + 2 \cdot 10^5 + 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10 + 7.$$

I numeri interi saranno quindi scritti in forma decimale, ossia nella forma

$$z = a_n a_{n-1} \cdots a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0.$$

- *Criterio di divisibilità per 3 e per 9.* Un numero intero è divisibile per 3 (per 9) se e solo se la somma delle sue cifre è divisibile per 3 (per 9).

DIMOSTRAZIONE. Infatti, qualunque sia  $n > 0$ ,  $10^n - 1 = \underbrace{999\dots9}_{n \text{ volte}} = 9 \cdot \underbrace{111\dots1}_{n \text{ volte}}$ , cioè

$$10^n \equiv 1 \pmod{9}.$$

Quindi, utilizzando le proprietà delle congruenze,

$$a_n a_{n-1} \dots a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_0 \equiv a_n + a_{n-1} + \dots + a_0 \pmod{9}$$

Quindi  $z \equiv a_n + a_{n-1} + \dots + a_0$  sia modulo 3 sia modulo 9.  $\diamond$

- *Criterio di divisibilità per 2 e per 5.* Un numero intero è divisibile per 2 o per 5 se e solo se l'ultima cifra di destra,  $a_0$ , è divisibile per 2 o per 5.

DIMOSTRAZIONE. Per ogni  $n \geq 1$ ,  $10^n \equiv 0$  sia modulo 2 sia modulo 5. Quindi  $z \equiv a_0$  sia modulo 2 sia modulo 5.  $\diamond$

- *Criterio di divisibilità per 4.* Un intero  $z$  è divisibile per 4 (o per 25) se e solo se il numero  $a_1 a_0$  formato dalle sue ultime due cifre è divisibile per 4 (o per 25).

DIMOSTRAZIONE.  $100 = 2^2 5^2 \equiv 0$  sia modulo 4 sia modulo 25. Allora ogni intero è congruo modulo 4 o modulo 25 all'intero costituito dalle sue ultime due cifre di destra. In particolare, vale il criterio di divisibilità richiesto.  $\diamond$

- *Criterio di divisibilità per  $2^k$ .* Un intero  $z$  è divisibile per  $2^k$  se e solamente se  $2^k$  divide il numero costituito dalle ultime  $k$  cifre di  $z$ .

DIMOSTRAZIONE. Infatti

$$10^n = 2^n \cdot 5^n \equiv 0 \pmod{2^k} \quad \text{per ogni } n \geq k.$$

Quindi, per esempio, per vedere se un numero è divisibile per 8 basta vedere se è divisibile per 8 il numero costituito dalle ultime 3 cifre.  $\diamond$

- *Criterio di divisibilità per 11.* Un intero è divisibile per 11 se e solo se

$$a_0 - a_1 + a_2 - \dots + (-1)^n a_n$$

è divisibile per 11.

DIMOSTRAZIONE. Basta osservare che

$$10 \equiv -1 \pmod{11} \implies \begin{cases} 10^{2p} \equiv 1 \pmod{11} \\ 10^{2p+1} \equiv -1 \pmod{11} \end{cases} \quad \diamond$$

### 3.2 La prova del nove

Ricordiamo la cosiddetta *prova del nove* per controllare l'esattezza di una moltiplicazione tra interi. Supponiamo di voler moltiplicare fra loro due interi, 1234 e 567, e supponiamo di avere trovato come risultato 698678. Vogliamo controllarne l'esattezza. Allora si procede al modo seguente: si scrive la somma delle cifre dei fattori fino ad arrivare ad un numero ad una sola cifra e si fa la moltiplicazione di questi due numeri: questa deve coincidere con la somma delle cifre del risultato da controllare. Quindi nel nostro caso

$$\begin{array}{rcl} 1234 \times & 1 + 2 + 3 + 4 = 10, & 1 + 0 = 1 \\ 567 = & 5 + 6 + 7 = 18, & 1 + 8 = 9 \\ 698678 & 6 + 9 + 8 + 6 + 7 + 8 = 44, & 4 + 4 = 8. \end{array}$$

A questo punto si fa il prodotto  $1 \cdot 9 = 9$ , che è diverso dal numero 8 che abbiamo incorniciato. Quindi abbiamo sicuramente commesso un errore.

Perché questa prova viene chiamata "prova del nove"? Abbiamo appena visto i criteri di divisibilità: ogni numero modulo 9 è congruente alla somma delle sue cifre. Ecco dove interviene il nove e la spiegazione della "prova del nove". Il test che deve essere superato è che un numero e la somma delle sue cifre siano congrui modulo nove, ossia stiano nella stessa classe modulo 9. È chiaro quindi che si tratta di una condizione necessaria, ma non sufficiente per l'esattezza dei calcoli.

Quindi il fatto di aver superato il controllo della prova del nove positivamente non garantisce che la moltiplicazione sia corretta. Per esempio potrebbe succedere che il risultato ottenuto e il risultato giusto si trovino nella stessa classe modulo 9: in questo caso non riusciremmo a individuare che abbiamo commesso un errore.

#### Esercizi

- 1 Si determini il resto della divisione per 9 del numero  $35267^{1000}$  e il resto della divisione per 3 del numero  $356^{500}$ .
- 2 Si determinino le ultime due cifre del numero  $112302^{42}$  e del numero  $5^{345}$ .
- 3 Determinare l'ultima cifra del numero  $2459^{547}$ .
- 4 In quale classe modulo 7 si trova il numero  $1000^{2000}$ ?

## 4 RISOLUZIONE DI CONGRUENZE LINEARI

Ci poniamo ora il problema di *risolvere* una congruenza, allo stesso modo di quando ci siamo posti il problema di risolvere un'equazione. Il tipo più semplice di equazione che abbiamo risolto è il caso di un'equazione lineare nell'incognita  $x$ , ossia un'equazione del tipo

$$ax = b.$$

Come ben sappiamo, a seconda del valore di  $a$  e di  $b$  questa equazione potrà avere una, infinite o nessuna soluzione. Ebbene, ci poniamo un problema analogo per le congruenze.

Partiamo dalla seguente definizione.

**DEFINIZIONE 5.2** Si definisce *congruenza lineare* nell'incognita  $x$  ogni equazione della forma  $ax \equiv b \pmod{n}$  con  $a, b \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ . ■

Vogliamo vedere se e quando una congruenza di questo tipo ammette soluzioni, dove per soluzione si intende ogni intero  $x_0$  tale che  $ax_0 \equiv b \pmod{n}$ . I seguenti esempi mostrano che si possono presentare vari casi.

#### Esempio 5.3

La  $6x \equiv 15 \pmod{4}$  non ammette soluzioni, altrimenti dovrebbe essere risolubile in  $\mathbb{Z}$  l'equazione  $6x + 4y = 15$ , mentre sappiamo che questa equazione non ammette soluzioni intere perché  $(6, 4) = 2 \nmid 15$  (cfr. proposizione 3.6).

#### Esempio 5.4

La  $24x \equiv 21 \pmod{9}$  è ovviamente equivalente (riducendo i coefficienti modulo 9) alla  $6x \equiv 3 \pmod{9}$  e ammette invece per esempio la soluzione  $x = 2$ . Ma ha anche le soluzioni  $x = 5$  e  $x = 8$ , come si vede facilmente.

#### Esempio 5.5

La  $3x \equiv 1 \pmod{5}$  ammette un'unica soluzione  $x = 2$ .

Il primo problema che affronteremo è determinare nel caso generale la *compatibilità* di una congruenza lineare, cioè *l'esistenza o meno* di soluzioni. Poi ci occuperemo, per congruenze che siano compatibili, del problema di *contarne* le soluzioni. Anche qui dovremo intenderci su cosa significhi contare le soluzioni, dato che ogni volta che c'è una soluzione, automaticamente ce ne sono infinite, tutte quelle che si ottengono da quella soluzione aggiungendo un multiplo intero di  $n$ . Le soluzioni 5 e 8 del secondo caso sono diverse e non congruenti tra loro modulo 9.

**PROPOSIZIONE 5.7** La congruenza  $ax \equiv b \pmod{n}$  ammette soluzioni se e solo se  $\text{MCD}(a, n) \mid b$ .

**DIMOSTRAZIONE.** La risoluzione della congruenza equivale alla risoluzione in interi della equazione  $ax + ny = b$  che sappiamo ammettere soluzioni intere se e solo se  $\text{MCD}(a, n) \mid b$  (cfr. proposizione 3.6). ◊

Nel caso di una congruenza compatibile, la proposizione che segue ci dice *quante* sono le sue soluzioni non congrue tra loro modulo  $n$ .

**PROPOSIZIONE 5.8** Sia  $ax \equiv b \pmod{n}$  una congruenza, sia  $d = \text{MCD}(a, n) \mid b$  e sia  $x_0$  una sua soluzione. Allora tutte e sole le soluzioni sono del tipo  $x_0 + k \cdot \frac{n}{d}$ ,  $k \in \mathbb{Z}$ . Tra queste, le soluzioni

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + 2 \cdot \frac{n}{d}, \quad \dots, \quad x_0 + (d-1) \cdot \frac{n}{d}$$

sono tutte non congruenti tra di loro modulo  $n$  e ogni altra è congruente ad una di queste. Quindi la congruenza ammette esattamente  $d$  soluzioni non congruenti modulo  $n$ .

**DIMOSTRAZIONE.** Innanzitutto è ovvio che, per ogni  $k \in \mathbb{Z}$ ,  $x_0 + k \cdot n/d$  è ancora una soluzione, perché, indicato con  $[a, n]$  il mcm tra  $a$  ed  $n$ ,  $a(x_0 + k \cdot \frac{n}{d}) = ax_0 \pm k[a, n] = b \pm$  multiplo di  $n$ . Per provare che *ogni* soluzione è di questo tipo, se  $x_0$  e  $x'_0$  sono due soluzioni, ossia se  $ax_0 = b + hn$  e  $ax'_0 = b + kn$ , allora  $a(x_0 - x'_0) = (h - k)n$  e dividendo ambo i membri per  $d = (a, n)$  si ottiene  $\frac{a}{d}(x_0 - x'_0) = (h - k)\frac{n}{d}$ , e, essendo  $(a/d, n/d) = 1$ ,  $n/(a, n)$  divide  $x_0 - x'_0$ , cioè  $x_0 - x'_0 = z \cdot n/d$ . Lasciamo per esercizio (cfr. eserc. 15) la dimostrazione dell'ultima parte del teorema. ◊

La congruenza  $24x \equiv 21 \pmod{9}$  dell'esempio 5.4 ammette infatti esattamente  $3 = \text{MCD}(6, 9)$  soluzioni incongrue modulo 9,  $x = 2$ ,  $x = 5$  e  $x = 8$ .

Il seguente corollario è un'ovvia conseguenza del risultato appena provato.

**COROLLARIO 5.4** Se  $(a, n) = 1$  (in particolare se  $n = p$  è un numero primo e  $a$  non è un multiplo di  $n$ ), allora la congruenza  $ax \equiv b \pmod{n}$  ammette un'unica soluzione modulo  $n$ .

È il caso della  $3x \equiv 1 \pmod{5}$  dell'esempio 5.5.

#### Esercizi

1. Data la congruenza  $ax \equiv b \pmod{n}$ , con  $(a, n) \mid b$ , si provi che le  $d$  soluzioni

$$(4.1) \quad x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + 2 \cdot \frac{n}{d}, \quad \dots, \quad x_0 + (d-1) \cdot \frac{n}{d}$$

non sono congrue tra loro modulo  $n$  e ogni altra soluzione è congruente ad una di queste.

2. Si trovino tutte le soluzioni (se esistono) delle seguenti congruenze:

- (a)  $2x \equiv 5 \pmod{3}$ ,
- (b)  $3x \equiv 8 \pmod{18}$
- (c)  $4x \equiv 5 \pmod{9}$ ,
- (d)  $3x \equiv 10 \pmod{9}$ .

3. Decidere se la congruenza  $12568x \equiv 14356 \pmod{20}$  è compatibile, e in caso positivo determinare tutte le soluzioni non congruenti tra loro modulo 20.

4. Determinare, se possibile, un  $a \in \mathbb{Z}$  in modo tale che la congruenza  $ax \equiv 336 \pmod{1500}$  ammetta 12 soluzioni non congrue tra loro modulo 1500.

5. Si costruisca una congruenza lineare del tipo  $ax \equiv b \pmod{143}$  che ammetta esattamente 11 soluzioni non congruenti tra loro modulo 143. Scritta tale congruenza, si determinino tutte le soluzioni.

6. Si risolva la congruenza  $4x \equiv 3 \pmod{385}$ .

7. Si consideri la congruenza  $ax \equiv 6 \pmod{20}$ .

- a. Per quali valori di  $a \in \mathbb{Z}$ ,  $0 \leq a < 20$  la congruenza ammette soluzioni?
- b. Per tutti i casi in cui ammette soluzioni, determinarle tutte.

## 5 IL TEOREMA CINESE DEI RESTI

Sappiamo risolvere congruenze lineari: ci poniamo ora il problema di risolvere un sistema di congruenze lineari, ossia un sistema del tipo:

$$(5.1) \quad \begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_sx \equiv b_s \pmod{n_s} \end{cases}$$

Una soluzione di un tale sistema è un intero che soddisfa contemporaneamente tutte le congruenze del sistema. Non è assolutamente detto che un tale sistema ammetta sempre soluzioni. Per esempio, se anche una sola delle singole congruenze non è risolubile, l'intero sistema ovviamente non ammetterà soluzioni: per esempio il sistema

$$\begin{cases} 3x \equiv 2 \pmod{12} \\ 4x \equiv 1 \pmod{5} \end{cases}$$

non ammette soluzioni, perché la prima congruenza  $3x \equiv 2 \pmod{12}$  non ammette soluzioni, dato che  $(3, 12) = 3$  non divide 2.

Ma può anche succedere che le singole congruenze siano risolubili, ma l'intero sistema non lo sia: per esempio si pensi al seguente sistema:

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 0 \pmod{2} \end{cases}$$

Tutte le soluzioni della seconda equazione sono dei numeri pari, mentre tutte le soluzioni della prima equazione sono dispari. Quindi non esiste un unico intero che soddisfi entrambe le congruenze.

Il Teorema Cinese dei Resti, che andiamo a dimostrare, ci dice che, con l'aggiunta di qualche restrizione sui moduli, un sistema di congruenze lineari che siano tutte compatibili, ammette sempre soluzione. L'ipotesi aggiuntiva è quella di imporre che i moduli siano a due a due coprimi tra loro, ossia  $(n_i, n_j) = 1$  per ogni  $i \neq j$ . Prima di arrivare alla formulazione classica del Teorema Cinese dei Resti, facciamo qualche premessa.

**LEMMA 5.5** Sia

$$\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_sx \equiv b_s \pmod{n_s} \end{cases}$$

con  $(n_i, n_j) = 1$  per  $i \neq j$  un sistema di congruenze tali che ogni congruenza del sistema ammetta soluzioni. Allora la risoluzione del sistema (5.1) equivale a risolvere un sistema del tipo

$$(5.2) \quad \begin{cases} x \equiv c_1 \pmod{n'_1} \\ x \equiv c_2 \pmod{n'_2} \\ \vdots \\ x \equiv c_s \pmod{n'_s} \end{cases}$$

con  $(n'_i, n'_j) = 1$  per  $i \neq j$ .

**DIMOSTRAZIONE.** Perché il sistema (5.1) ammetta soluzioni è necessario che, per ogni  $k = 1, \dots, s$ ,  $d_k = \text{MCD}(a_k, n_k)$  divida  $b_k$ . Una volta che siano soddisfatte queste condizioni, si può dividere la  $k$ -esima congruenza per  $d_k$ , ottenendo il nuovo sistema equivalente al precedente (nel senso che ammette le stesse soluzioni):

$$(5.1') \quad \begin{cases} a'_1x \equiv b'_1 \pmod{n'_1} \\ a'_2x \equiv b'_2 \pmod{n'_2} \\ \vdots \\ a'_sx \equiv b'_s \pmod{n'_s} \end{cases}$$

dove  $a'_k = a_k/d_k$ ,  $b'_k = b_k/d_k$  e  $n'_k = n_k/d_k$ ; inoltre, vale ancora la condizione  $(n'_i, n'_j) = 1$  per  $i \neq j$ . Ora, si noti che per ogni  $k = 1, \dots, s$  si ha  $(a'_k, n'_k) = 1$  per cui, in base al Corollario 5.4, ciascuna delle congruenze del sistema ammette un'unica soluzione  $c_k$  modulo  $n'_k$ . Possiamo allora sostituire nuovamente il sistema (5.1') con il seguente sistema:

$$(5.2) \quad \begin{cases} x \equiv c_1 \pmod{n'_1} \\ x \equiv c_2 \pmod{n'_2} \\ \vdots \\ x \equiv c_s \pmod{n'_s} \end{cases}$$

Abbiamo così provato che ogni sistema di congruenze di tipo (5.1) si può ridurre ad un sistema di tipo (5.2). ◆

Passiamo quindi a studiare sistemi di congruenze di tipo (5.2), che, come vedremo hanno anche interessanti applicazioni, che sono state studiate nella letteratura cinese (di qui il nome) del primo secolo d.C.

**TEOREMA 5.6 (TEOREMA CINESE DEI RESTI).** Siano  $n_1, n_2, \dots, n_s$  interi positivi tali che  $(n_i, n_j) = 1$  per ogni  $i \neq j$ . Allora il sistema di congruenze

$$\begin{cases} x \equiv r_1 \pmod{n_1} \\ x \equiv r_2 \pmod{n_2} \\ \vdots \\ x \equiv r_s \pmod{n_s} \end{cases}$$

ammette una soluzione che è unica modulo  $n_1 n_2 \cdots n_s$ .

**DIMOSTRAZIONE.** Se  $N = n_1 n_2 \cdots n_s$ , e  $N_k = N/n_k$ , allora  $(N_k, n_k) = 1$ , come è facile provare dall'ipotesi  $(n_i, n_j) = 1$ . Quindi per ogni  $k = 1, \dots, s$ , la congruenza  $N_k x_k \equiv r_k \pmod{n_k}$  ammette un'unica soluzione,  $\bar{x}_k$ , modulo  $n_k$ . Il numero

$$\bar{x} = N_1 \bar{x}_1 + N_2 \bar{x}_2 + \cdots + N_s \bar{x}_s$$

è una soluzione simultanea del sistema dato: infatti, essendo  $N_i$  multiplo di  $n_k$  per  $i \neq k$ , sarà  $N_i \equiv 0 \pmod{n_k}$  per  $i \neq k$ . Ne segue che

$$\begin{cases} \bar{x} \equiv N_1 \bar{x}_1 \equiv r_1 \pmod{n_1} \\ \bar{x} \equiv N_2 \bar{x}_2 \equiv r_2 \pmod{n_2} \\ \vdots \\ \bar{x} \equiv N_s \bar{x}_s \equiv r_s \pmod{n_s} \end{cases}$$

ossia  $\bar{x}$  è una soluzione del sistema.

Per quanto riguarda l'unicità modulo  $n_1 n_2 \cdots n_s$ , sia  $\bar{y}$  un'altra soluzione del sistema, cioè  $\bar{x} \equiv c_k \equiv \bar{y} \pmod{n_k} \quad \forall k = 1, \dots, s$ . Allora  $\bar{x} - \bar{y} \equiv 0 \pmod{n_k} \quad \forall n_k$ , da cui  $\bar{x} - \bar{y} \equiv 0 \pmod{n_1 n_2 \cdots n_s}$ .  $\diamond$

**Esempio 5.6**

Trovare (se esistono) tutte le soluzioni intere comprese nell'intervallo [50, 100] del seguente sistema di congruenze

$$\begin{cases} x \equiv 3 \pmod{4} \\ 2x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5}. \end{cases}$$

Il sistema è equivalente al seguente

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5}. \end{cases}$$

Posto  $N = 4 \cdot 3 \cdot 5 = 60$ ,  $N_1 = \frac{N}{4} = 15$ ,  $N_2 = \frac{N}{3} = 20$  e  $N_3 = \frac{N}{5} = 12$ , dobbiamo risolvere le seguenti congruenze:

1.  $15x_1 \equiv 3 \pmod{4}$ , ossia  $3x_1 \equiv 3 \pmod{4}$ . Dato che 3 e 4 sono coprimi, possiamo dividere per 3, da cui si ha la soluzione  $\bar{x}_1 = 1$ .
2.  $20x_2 \equiv 2 \pmod{3}$ , ossia  $2x_2 \equiv 2 \pmod{3}$ . Dato che 2 e 3 sono coprimi, possiamo dividere per 2, da cui si ha la soluzione  $\bar{x}_2 = 1$ .
3.  $12x_3 \equiv 4 \pmod{5}$ , ossia  $2x_3 \equiv 4 \pmod{5}$ . Dato che 2 e 5 sono coprimi, possiamo dividere per 2, da cui si ha la soluzione  $\bar{x}_3 = 2$ .

Tutte e sole le soluzioni del sistema sono del tipo  $\bar{x} + h \cdot 60$ ,  $h \in \mathbb{Z}$  dove  $\bar{x} = 15 \cdot 1 + 20 \cdot 1 + 12 \cdot 2 = 59$ . Nell'intervallo richiesto c'è la sola soluzione 59.

**OSSERVAZIONE** Si osservi che le ipotesi del Teorema Cinese dei Resti ci assicurano che il sistema ammette soluzione. Ma un sistema di congruenze lineari può ammettere soluzioni anche se non sono verificate le ipotesi sui moduli richieste dal Teorema Cinese dei Resti, cioè quando i moduli non sono a due a due coprimi. In tali casi però si tratterà di studiare il sistema e verificare delle condizioni di compatibilità.

**Esempio 5.7**

Decidere se il seguente sistema

$$\begin{cases} x \equiv 5 \pmod{6} \\ 7x \equiv 3 \pmod{4} \end{cases}$$

è risolubile e in caso positivo trovare tutte le soluzioni.

Le singole congruenze sono risolubili, ma in questo caso i moduli non sono a due a due coprimi, quindi dobbiamo analizzare il sistema per vedere se ammette soluzioni. La prima congruenza  $x \equiv 5 \pmod{6}$  è equivalente al sistema

$$\begin{cases} x \equiv 5 \pmod{3} \\ x \equiv 5 \pmod{2} \end{cases} \quad \text{ossia al sistema} \quad \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{2} \end{cases}$$

quindi il sistema originario è equivalente al sistema

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{2} \\ 7x \equiv 3 \pmod{4} \end{cases} \quad \text{ossia} \quad \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{4} \end{cases}.$$

Ora, la  $x \equiv 1 \pmod{2}$  è implicata dalla  $x \equiv 1 \pmod{4}$ , quindi la possiamo eliminare. Si tratta allora di risolvere il sistema

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{4} \end{cases}$$

che è un sistema con moduli coprimi, quindi sappiamo (in virtù del Teorema Cinese dei Resti) che è risolubile e ammette una sola soluzione modulo 12. Una soluzione è  $\bar{x} = 17 \equiv 5 \pmod{12}$ . Tutte le soluzioni sono  $5 + h \cdot 12$ , al variare di  $h \in \mathbb{Z}$ .

**N.B.** In realtà in questo caso potevamo vedere subito che la soluzione  $x = 5$  soddisfaceva sia la prima sia la seconda congruenza del sistema originario. Però dovevamo poi stare attenti nel trovare tutte le soluzioni: queste si ottengono aggiungendo ad una fissata soluzione tutti i multipli interi del mcm tra i moduli, ossia 12 (non il prodotto, cioè 24).

**Contare un folto gruppo di persone**

Supponiamo di dover contare un immenso numero di persone radunate in una piazza, senza doverle chiamare una ad una, perché sarebbe un'impresa impossibile. Si sa che la piazza non può contenere più di 5000 persone. Allora si può procedere al modo seguente: si chiede loro di allinearsi per 5, per 7, per 11 e per 12 (si osservi che abbiamo scelto dei numeri che sono a due a due coprimi tra loro) e ogni volta che si sono allineati, si contano le persone in eccesso: questi resti  $r_i$  non saranno rispettivamente più di 4, 6, 10, 11.

Dopo di che si risolve la congruenza:

$$\begin{cases} x \equiv r_1 \pmod{5} \\ x \equiv r_2 \pmod{7} \\ x \equiv r_3 \pmod{11} \\ x \equiv r_4 \pmod{12} \end{cases}$$

che, in virtù del Teorema Cinese dei Resti, ammette un'unica soluzione modulo  $5 \cdot 7 \cdot 11 \cdot 12 = 4620$ . Tale soluzione rappresenta il numero totale delle persone che si trovavano nella piazza.

**Calcoli in parallelo**

Si considerino gli anelli  $\mathbb{Z}_r$  e  $\mathbb{Z}_s$  delle classi resto modulo  $r$  e  $s$  rispettivamente, con  $(r, s) = 1$ . Nel prodotto cartesiano  $\mathbb{Z}_r \times \mathbb{Z}_s$  (cfr. par. 1 del cap. 1) si possono introdurre le seguenti due operazioni componenti per componente:

$$\begin{aligned} (\bar{a}_r, \bar{b}_r) + (\bar{a}'_r, \bar{b}'_r) &\stackrel{\text{def}}{=} (\bar{a}_r + \bar{a}'_r, \bar{b}_r + \bar{b}'_r) \\ (\bar{a}_r, \bar{b}_r) \cdot (\bar{a}'_r, \bar{b}'_r) &\stackrel{\text{def}}{=} (\bar{a}_r \cdot \bar{a}'_r, \bar{b}_r \cdot \bar{b}'_r) \end{aligned}$$

che trasformano l'insieme  $\mathbb{Z}_r \times \mathbb{Z}_s$  in un anello.

**PROPOSIZIONE 5.9** Siano  $r$  ed  $s$  due interi maggiori o uguali a 2 e relativamente primi. Allora la corrispondenza

$$\begin{aligned} f : \mathbb{Z}_{rs} &\longrightarrow \mathbb{Z}_r \times \mathbb{Z}_s \\ \bar{x}_{rs} &\longmapsto (\bar{x}_r, \bar{x}_s) \end{aligned}$$

è una corrispondenza biunivoca e conserva le operazioni, è tale cioè che

$$f(\bar{x}_{rs} + \bar{y}_{rs}) = f(\bar{x}_{rs}) + f(\bar{y}_{rs}), \quad e \quad f(\bar{x}_{rs} \cdot \bar{y}_{rs}) = f(\bar{x}_{rs}) \cdot f(\bar{y}_{rs}).$$

**DIMOSTRAZIONE.** In virtù del Teorema Cinese dei Resti il sistema di congruenze

$$\begin{cases} x \equiv a \pmod{r} \\ x \equiv b \pmod{s} \end{cases}$$

ammette una ed una sola soluzione modulo  $rs$ . Questo ci garantisce la suriettività e l'iniettività della applicazione. Il fatto che tale applicazione conservi le operazioni viene lasciato come esercizio (cfr. eserc. 27).  $\diamond$

#### Esempio 5.8

Scriviamo esplicitamente la corrispondenza  $f$  nel caso in cui sia  $r = 3$ ,  $s = 4$ .

$$\begin{aligned} \mathbb{Z}_{12} &\longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_4 \\ \bar{0}_{12} &\longmapsto (\bar{0}_3, \bar{0}_4) \\ \bar{1}_{12} &\longmapsto (\bar{1}_3, \bar{1}_4) \\ \bar{2}_{12} &\longmapsto (\bar{2}_3, \bar{2}_4) \\ \bar{3}_{12} &\longmapsto (\bar{0}_3, \bar{3}_4) \\ \bar{4}_{12} &\longmapsto (\bar{1}_3, \bar{0}_4) \\ \bar{5}_{12} &\longmapsto (\bar{2}_3, \bar{1}_4) \\ \bar{6}_{12} &\longmapsto (\bar{0}_3, \bar{2}_4) \\ \bar{7}_{12} &\longmapsto (\bar{1}_3, \bar{3}_4) \\ \bar{8}_{12} &\longmapsto (\bar{2}_3, \bar{0}_4) \\ \bar{9}_{12} &\longmapsto (\bar{0}_3, \bar{1}_4) \\ \bar{10}_{12} &\longmapsto (\bar{1}_3, \bar{2}_4) \\ \bar{11}_{12} &\longmapsto (\bar{2}_3, \bar{3}_4). \end{aligned}$$

In generale tale corrispondenza si ottiene rapidamente con il seguente metodo. Si scrivono sulla prima colonna tutti gli elementi di  $\mathbb{Z}_{rs}$ . Sulla seconda tutti gli elementi di  $\mathbb{Z}_r$  ripetuti  $s$  volte, sulla terza colonna tutti gli elementi di  $\mathbb{Z}_s$  ripetuti  $r$  volte. La corrispondenza  $f$  è quella che associa al  $k$ -esimo elemento di  $\mathbb{Z}_{rs}$  la coppia costituita rispettivamente dal  $k$ -esimo elemento di  $\mathbb{Z}_r$  e dal  $k$ -esimo elemento di  $\mathbb{Z}_s$ .

Fin qui non si vede il vantaggio di questa identificazione di ogni elemento di  $\mathbb{Z}_{12}$  con una coppia appartenente a  $\mathbb{Z}_3 \times \mathbb{Z}_4$ . Invece questa identificazione che conserva le operazioni ha un'applicazione importante nel campo dei calcolatori, perché permette di trasportare calcoli in  $\mathbb{Z}_{12}$  a calcoli indipendenti in  $\mathbb{Z}_3$  e  $\mathbb{Z}_4$ .

Illustriamo questa affermazione: supponiamo di dovere determinare la classe inversa della classe  $\bar{7} \in \mathbb{Z}_{12}$ . Dovremo allora risolvere la congruenza  $7x \equiv 1 \pmod{12}$ . Anziché lavorare

in  $\mathbb{Z}_{12}$ , potremo utilizzare la corrispondenza  $f$  della proposizione precedente. Trovare l'inversa della classe  $\bar{7}$  in  $\mathbb{Z}_{12}$  equivale a trovare l'inversa in  $\mathbb{Z}_3 \times \mathbb{Z}_4$  della classe  $f(\bar{7}) = (\bar{1}, \bar{3})$ . Ora  $(\bar{1}, \bar{3})^{-1} = (\bar{1}, \bar{3})$ . A questo punto dalla tavola risulta che questa coppia corrisponde all'elemento  $\bar{7}$  di  $\mathbb{Z}_{12}$ , che ovviamente è la stessa classe che si sarebbe ottenuto operando dentro  $\mathbb{Z}_{12}$ . Il fatto che le operazioni in  $\mathbb{Z}_3$  e in  $\mathbb{Z}_4$  si possono fare separatamente, ossia sono indipendenti le une dalle altre, permette per esempio di poter utilizzare due diversi calcolatori e lavorare in parallelo.

Ovviamente questo è un esempio molto semplice, da cui non si può apprezzare il vantaggio di questa tecnica. Ma supponiamo di dovere calcolare l'inverso di  $\bar{15}$  in  $\mathbb{Z}_{143}$ . Si osservi che  $143 = 13 \cdot 11$  e che  $(13, 11) = 1$ . La classe  $\bar{15}$  di  $\mathbb{Z}_{143}$  corrisponde alla coppia  $(\bar{15}_{13}, \bar{15}_{11})$  cioè alla coppia  $(\bar{2}_{13}, \bar{4}_{11})$  e l'inversa della coppia è la coppia  $(\bar{2}_{13}^{-1}, \bar{4}_{11}^{-1}) = (\bar{7}, \bar{3})$ . A questo punto, per sapere quale classe di  $\mathbb{Z}_{143}$  corrisponde a questa coppia basta risolvere il seguente sistema:

$$\begin{cases} x \equiv 7 \pmod{13} \\ x \equiv 3 \pmod{11} \end{cases}$$

che ammette 124 come unica soluzione modulo 143. Quindi l'inversa di  $\bar{15}$  in  $\mathbb{Z}_{143}$  è la classe  $\bar{124}$ .

**OSSERVAZIONE** Se fosse  $n = rs$ , ma  $r$  e  $s$  non fossero coprimi (per esempio  $n = 12$ ,  $r = 2$ ,  $s = 6$ ), la  $f$  non sarebbe biunivoca. Basta provare che non è suriettiva (o iniettiva), come mostra la seguente tabella:

$$\begin{aligned} \mathbb{Z}_{12} &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_6 \\ \bar{0}_{12} &\longmapsto (\bar{0}_2, \bar{0}_6) \\ \bar{1}_{12} &\longmapsto (\bar{1}_2, \bar{1}_6) \\ \bar{2}_{12} &\longmapsto (\bar{0}_2, \bar{2}_6) \\ \bar{3}_{12} &\longmapsto (\bar{1}_2, \bar{3}_6) \\ \bar{4}_{12} &\longmapsto (\bar{0}_2, \bar{4}_6) \\ \bar{5}_{12} &\longmapsto (\bar{1}_2, \bar{5}_6) \\ \bar{6}_{12} &\longmapsto (\bar{0}_2, \bar{0}_6) \\ \bar{7}_{12} &\longmapsto (\bar{1}_2, \bar{1}_6) \\ \bar{8}_{12} &\longmapsto (\bar{0}_2, \bar{2}_6) \\ \bar{9}_{12} &\longmapsto (\bar{1}_2, \bar{3}_6) \\ \bar{10}_{12} &\longmapsto (\bar{0}_2, \bar{4}_6) \\ \bar{11}_{12} &\longmapsto (\bar{1}_2, \bar{5}_6). \end{aligned}$$

Si vede che non è suriettiva (per esempio la coppia  $(\bar{1}, \bar{2})$  non appartiene all'immagine della  $f$ ) e non è iniettiva (per esempio  $\bar{0}$  e  $\bar{6}$  hanno la stessa immagine  $(\bar{0}, \bar{0})$ ).

Se dobbiamo lavorare in  $\mathbb{Z}_n$ , e conosciamo la fattorizzazione di  $n$ ,  $n = p_1^{h_1} p_2^{h_2} \cdots p_t^{h_t}$ , con  $p_i$  primi distinti, allora sappiamo che  $(p_i^{h_i}, p_j^{h_j}) = 1$  per  $i \neq j$ , quindi anziché lavorare in  $\mathbb{Z}_n$ , potremo lavorare indipendentemente nei singoli  $\mathbb{Z}_{p_i^{h_i}}$ , per  $i = 1, 2, \dots, t$ , con grande risparmio di calcoli.

Come si è visto nell'osservazione a proposito del Teorema Fondamentale dell'Aritmetica, si sa che ogni intero  $n$  si fattorizza in primi, ma determinare effettivamente una fattorizzazione per numeri  $n$  molto grandi può essere molto difficile dal

punto di vista computazionale: ritorneremo su questo punto quando parleremo di crittografia.



■ Dire se il seguente sistema di congruenze

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 3 \pmod{5} \end{cases}$$

ammette soluzioni, e in caso positivo determinarle.

■ Determinare la formula per la soluzione del sistema

$$\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \\ \dots \\ a_sx \equiv b_s \pmod{n_s} \end{cases}$$

con  $(a_i, n_i) = 1$  e  $(n_i, n_j) = 1$  per  $i \neq j$ .

■ Si risolva il seguente sistema di congruenze:

$$\begin{cases} 2345x \equiv 54217 \pmod{8} \\ 42x \equiv 455 \pmod{5} \\ 2x \equiv 5 \pmod{3} \end{cases}$$

■ Si consideri il seguente sistema di congruenze:

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

nel quale non si chiede che sia  $(n, m) = 1$ . Si diano le condizioni affinché tale sistema sia risolubile.

■ Se da un cesto di rose si tolgono le rose a due a due, a tre a tre, a quattro a quattro, a cinque a cinque, a sei a sei, nel sacchetto resta sempre una rosa. Se si tolgono a sette a sette, non ne resta nessuna. Si determini il minimo numero di rose che potevano trovarsi nel cesto.

■ Si provi che la corrispondenza di cui alla proposizione 5.9 conserva le operazioni.

■ Determinare  $2009^{1982} \pmod{75}$ . Si suggerisce di osservare che  $75 = 3 \cdot 25$ .

■ Risolvere, se possibile, il seguente sistema di congruenze, determinandone tutte le soluzioni:

$$\begin{cases} x \equiv 32^{511} \pmod{5} \\ 3x \equiv 1 \pmod{4} \\ x \equiv 7 \pmod{11} \end{cases}$$

■ Si consideri il seguente sistema di congruenze:

$$\begin{cases} 3x \equiv 2 - 7x \pmod{9} \\ 2x \equiv 6 \pmod{7} \\ x + 12 \equiv 0 \pmod{5} \end{cases}$$

- Si dica, *prima* di trovare le eventuali soluzioni, se il sistema ammette soluzioni.
- Determinare *tutte* le soluzioni del sistema.
- Decidere se esistono valori dell'intero  $a$  tali che, aggiungendo al sistema precedente la congruenza  $x \equiv a \pmod{11}$  il nuovo sistema

$$\begin{cases} 3x \equiv 2 - 7x \pmod{9} \\ 2x \equiv 6 \pmod{7} \\ x + 12 \equiv 0 \pmod{5} \\ x \equiv a \pmod{11} \end{cases}$$

*non* ammetta soluzioni.

■ a. Risolvere il seguente sistema di congruenze.

$$\begin{cases} x \equiv 8 \pmod{15} \\ 2x \equiv 3601 - 5x \pmod{4} \\ x \equiv 1 \pmod{7} \end{cases}$$

b. Risolvere il seguente sistema di congruenze.

$$\begin{cases} x \equiv 8 \pmod{15} \\ 2x \equiv 3601 - 5x \pmod{4} \end{cases}$$

■ Si consideri il seguente sistema di congruenze:

$$\begin{cases} 100x \equiv 1 \pmod{3} \\ 3x + 4 \equiv -5 + 2x \pmod{7} \\ 3x \equiv 235^{146} \pmod{16} \end{cases}$$

- Decidere se il sistema è risolubile.
- Se è risolubile, determinare tutte le soluzioni.
- Se è risolubile, dire quante sono le soluzioni comprese nell'intervallo  $[0, 1000]$ .

■ Determinare in  $\mathbb{Z}_{21}$  l'inversa della classe  $\bar{11}$ , servendosi della corrispondenza  $f$  della proposizione 5.9.

## ■ 6 LA FUNZIONE DI EULERO

Come si è visto, il Corollario del Piccolo Teorema di Fermat afferma che se  $p$  è un numero primo e  $a$  non è un multiplo di  $p$ , allora  $a^{p-1} \equiv 1 \pmod{p}$ .

Sarebbe utile ottenere un teorema analogo anche per moduli che non siano primi. Un risultato di questo tipo è offerto dal Teorema di Euler, che è una generalizzazione

del Piccolo Teorema di Fermat, perché si riferisce a moduli arbitrari  $n$  e non solamente a moduli primi. Il risultato è del tipo

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

Ma chi è questa funzione  $\varphi(n)$ ? Deve trattarsi di una funzione che nel caso in cui  $n$  sia un numero primo  $p$  deve coincidere con  $p - 1$ .

**DEFINIZIONE 5.3** Sia  $n \geq 1$ . Si definisce  $\varphi(n)$  la funzione di  $n$  che rappresenta il numero di interi positivi  $< n$  e relativamente primi con  $n$ . Essa prende il nome di *funzione di Eulero* o anche *funzione  $\varphi$* .

Per esempio,  $\varphi(40) = 16$  perché i numeri minori di 40 e relativamente primi con 40 sono 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39.

Se però ora volessimo calcolare  $\varphi(1204)$ , ci troveremmo in difficoltà, perché non è agevole fare il conto dei numeri minori di 1204 coprimi con 1204. Ci vengono in aiuto alcune proprietà della funzione di Eulero, che ci permetteranno di calcolare la funzione di Eulero per ogni intero  $n$  del quale si conosca la fattorizzazione.

In proprietà fondamentale della funzione di Eulero è di essere *moltiplicativa*, ossia

$$\varphi(r \cdot s) = \varphi(r)\varphi(s) \quad \forall r, s \text{ tali che } (r, s) = 1.$$

**DIMOSTRAZIONE.** Per la dimostrazione rimandiamo all'esercizio 34. ♦

**PROPOSIZIONE 5.10** Sia  $n = p_1^{h_1}p_2^{h_2}\cdots p_s^{h_s}$  la fattorizzazione di  $n$ , con i  $p_i$  ( $i = 1, \dots, s$ ) primi distinti. Allora risulta

$$(6.1) \quad \varphi(n) = \varphi(p_1^{h_1})\varphi(p_2^{h_2})\cdots\varphi(p_s^{h_s}),$$

Con questo risultato a disposizione, siamo ridotti a calcolare il valore di  $\varphi$  sulle potenze di un primo, ossia  $\varphi(p^h)$ . Ma questo è facile. Infatti

**PROPOSIZIONE 5.11** Se  $p$  è un numero primo, allora  $\varphi(p^h) = p^h - p^{h-1}$ .

**DIMOSTRAZIONE.** Basta osservare che non sono primi con  $p^h$  solo i multipli di  $p$ , e questi sono del tipo:  $p \cdot i$ ,  $1 \leq i \leq p^{h-1}$  e quindi sono in numero di  $p^{h-1}$ . Per  $h = 1$  si ottiene  $\varphi(p) = p - 1$ . ♦

Siamo quindi in grado di calcolare  $\varphi(n)$  per ogni  $n \in \mathbb{N}$  del quale si conosca la fattorizzazione. Per esempio,  $\varphi(72) = \varphi(2^3 \cdot 3^2) = \varphi(2^3)\varphi(3^2) = (2^3 - 2^2)(3^2 - 3) = 24$ .

Come già osservato alla fine del paragrafo precedente parlando di  $\mathbb{Z}_n$ , anche qui insistiamo nel dire che siamo in grado di calcolare  $\varphi(n)$  per ogni intero  $n$  del quale si conosca la fattorizzazione: ritorneremo fra breve su questo problema.

In definitiva, la funzione di Eulero  $\varphi(n)$  di un intero positivo  $n$  è proprio la funzione che cercavamo all'inizio del paragrafo: sussiste infatti il seguente Teorema di Eulero di cui non forniamo la dimostrazione.

**TEOREMA 5.7 (TEOREMA DI EULERO)** Sia  $a \in \mathbb{Z}$  tale che  $(a, n) = 1$ . Allora  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

Mettiamo subito in pratica il risultato del Teorema di Eulero.

### Esempio 5.9

Calcolare le ultime due cifre di  $237^{250}$ .

Si tratta di lavorare modulo 100. Ora,  $237 \equiv 37 \pmod{100}$  e  $(37, 100) = 1$ . La funzione di Eulero di 100 vale 40. In virtù del Teorema di Eulero  $37^{40} \equiv 1 \pmod{100}$ . Allora  $37^{242} = 37^{40 \cdot 6 + 2} = (37^{40})^6 \cdot 37^2 \equiv 1 \cdot 37^2 = 1369 \equiv 69 \pmod{100}$ .

Chiudiamo questo paragrafo con un'importante applicazione della funzione di Eulero. Sappiamo che l'insieme  $\mathbb{Z}_n$  delle classi resto modulo  $n$  è stato dotato di due operazioni:  $\bar{a} + \bar{b} = \bar{a+b}$ , e  $\bar{a} \cdot \bar{b} = \bar{a \cdot b}$  rispetto alle quali ha la struttura di anello commutativo con unità. Abbiamo anche già visto come in alcuni casi  $\mathbb{Z}_n$  è un dominio di integrità, in altri no. Vogliamo ora studiare più a fondo questo anello, in particolare vogliamo determinare gli elementi invertibili di  $\mathbb{Z}_n$ , ossia le classi  $\bar{a}$  per le quali esista una classe  $\bar{x}$  tale che  $\bar{a} \cdot \bar{x} = \bar{1}$ .

**PROPOSIZIONE 5.12** Le classi invertibili di  $\mathbb{Z}_n$  sono tutte e sole quelle classi  $\bar{a}$  tali che  $(a, n) = 1$ . Esse sono in numero di  $\varphi(n)$ . In particolare, ogni classe non nulla di  $\mathbb{Z}_p$  con  $p$  primo è invertibile.

**DIMOSTRAZIONE.** La determinazione delle classi  $\bar{a}$  invertibili in  $\mathbb{Z}_n$  equivale a risolvere la congruenza  $ax \equiv 1 \pmod{n}$ . Ora, tale congruenza ammette soluzione (ed unica!) se e solo se  $(a, n) = 1$ . Le classi invertibili sono pertanto le classi  $\bar{a}$  con  $1 \leq a < n$  e  $(a, n) = 1$ ; sono quindi in numero di  $\varphi(n)$ . Se in particolare  $n = p$ , allora ogni classe  $\bar{a}$  non nulla è tale che  $(a, p) = 1$ , quindi invertibile: le classi invertibili sono in questo caso  $p - 1 = \varphi(p)$ . ♦

**DEFINIZIONE 5.4** Un anello commutativo con unità in cui ogni elemento non nullo è invertibile prende il nome di campo.

Possiamo così concludere con il seguente risultato.

**COROLLARIO 5.8** Se  $p$  è un numero primo, l'anello  $(\mathbb{Z}_p, +, \cdot)$  è un campo.

Quindi in  $(\mathbb{Z}_8, +, \cdot)$  le classi invertibili sono  $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ . Le classi inverse sono rispettivamente  $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ , come si vede risolvendo le congruenze  $ax \equiv 1 \pmod{8}$  con  $a \in \{1, 3, 5, 7\}$ .

In  $(\mathbb{Z}_5, +, \cdot)$  tutte le classi non nulle sono invertibili, perché  $(1, 5) = (2, 5) = 3, 5) = (4, 5) = 1$ , e le loro inverse sono rispettivamente  $\bar{1}, \bar{3}, \bar{2}, \bar{4}$ .

Appare spontaneo considerare il sottoinsieme di  $\mathbb{Z}_n$  costituito da tutte le classi dotate di inversa: tale sottoinsieme è comunemente denotato con il simbolo  $U(\mathbb{Z}_n)$ .

Diamo qualche esempio di  $U(\mathbb{Z}_n)$  per qualche  $n$ :

$$\begin{aligned}\mathbb{Z}_4 &= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}, & U(\mathbb{Z}_4) &= \{\bar{1}, \bar{3}\}; \\ \mathbb{Z}_6 &= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}, & U(\mathbb{Z}_6) &= \{\bar{1}, \bar{5}\}; \\ \mathbb{Z}_8 &= \{\bar{0}, \bar{1}, \dots, \bar{7}\}, & U(\mathbb{Z}_8) &= \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}.\end{aligned}$$

Si noti che  $\varphi(4) = 2$ ,  $\varphi(6) = \varphi(2)\varphi(3) = 1 \cdot 2$ ,  $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$ .

### Esercizi

- ➊ Provare che la funzione di Eulero è moltiplicativa nel senso che se  $(r, s) = 1$  allora  $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$ .
- ➋ Provare che la relazione  $\varphi(rs) = \varphi(r)\varphi(s)$  è falsa, se  $(r, s) \neq 1$ .
- ➌ Determinare gli elementi invertibili in ciascuno degli anelli  $(\mathbb{Z}_8, +, \cdot)$ ,  $(\mathbb{Z}_{10}, +, \cdot)$ ,  $(\mathbb{Z}_{20}, +, \cdot)$ . Di ogni elemento invertibile calcolare l'inverso.
- ➍ Determinare il resto delle divisioni per 5, per 7 e per 11 di  $2^{677}$ .
- ➎ Determinare il resto della divisione per 385 di  $2^{677}$ . Si suggerisce di utilizzare i risultati dell'esercizio precedente e il Teorema Cinese dei Resti.
- ➏ Determinare le ultime due cifre della rappresentazione decimale dei numeri  $9^{201}$  e  $3^{950}$ .
- ➐ Sia  $U(\mathbb{Z}_n)$  l'insieme delle classi invertibili di  $(\mathbb{Z}_n, +, \cdot)$ . Si provi che il prodotto di elementi di  $U(\mathbb{Z}_n)$  è ancora un elemento di  $U(\mathbb{Z}_n)$  e che l'inverso di elementi di  $U(\mathbb{Z}_n)$  è ancora un elemento di  $U(\mathbb{Z}_n)$ .
- ➑ Si provi che  $\mathbb{Z}_n$  è un campo se e solo se  $n$  è un numero primo.
- ➒ Si determini l'inversa della classe  $\bar{7}$  in  $\mathbb{Z}_{18}$ .
- ➓ Calcolare  $\text{MCD}(\varphi(n), e)$  in ciascuno dei seguenti casi (si dia per noto che i numeri 8191, 11953, 11971 sono numeri primi, non si chiede di verificarlo).
  - a.  $n = 97907023 = 8191 \cdot 11953$   $e = 913$ .
  - b.  $n = 97907023 = 8191 \cdot 11953$   $e = 1111$ .
  - c.  $n = 143089363 = 11971 \cdot 11953$   $e = 391$ .
  - d.  $n = 143089363 = 11971 \cdot 11953$   $e = 195$ .
  - e.  $n = 705812697 = 59049 \cdot 11953$   $e = 139$ .

## 7 CONGRUENZE E TEST DI PRIMALITÀ

Abbiamo visto che i numeri primi sono i mattoni che stanno alla base di tutti i numeri interi. È quindi importante possedere dei test per verificare se un dato numero  $n$  è o non è primo. Le congruenze ci verranno in aiuto.

1. In base al Piccolo Teorema di Fermat, se  $p$  è un numero primo, allora, qualunque sia  $a$ , deve valere la  $a^p \equiv a \pmod p$ .

Quindi vale il seguente risultato.

**PROPOSIZIONE 5.13** Se  $n$  è un numero tale che esista un  $a \in \mathbb{Z}$  tale che  $a^n \not\equiv a \pmod n$ , allora  $n$  non è primo.

Per esempio,  $n = 9$  è tale che  $2^9 = 512 \not\equiv 2 \pmod 9$ , quindi 9 non è primo.

Si noti che questo test, pur assicurandoci che il numero non è primo, non fornisce una fattorizzazione di  $n$ .

2.  $p$  è primo se e solo se  $(p-1)! + 1$  è divisibile per  $p$ . Questo è il contenuto del Teorema di Wilson.

**TEOREMA 5.9 (TEOREMA DI WILSON)**  $p$  è un numero primo se e solo se  $(p-1)! \equiv -1 \pmod p$ .

### DIMOSTRAZIONE.

1. Proviamo che se  $p$  è primo, allora vale la  $(p-1)! \equiv -1 \pmod p$ . Per  $p = 2$  e  $p = 3$  il teorema è evidente. Supponiamo quindi  $p > 3$ . Se  $a$  è uno degli interi  $1, 2, \dots, p-1$ , si consideri la congruenza  $ax \equiv 1 \pmod p$ . Dato che  $(a, p) = 1$ , questa congruenza ammette una e una sola soluzione  $a'$  modulo  $p$ ,  $1 \leq a' < p$ . Per quali valori di  $a$  risulta  $a = a'$ ? Questo corrisponde a risolvere la  $a^2 \equiv 1 \pmod p$ , che equivale a dire che  $p$  divide  $(a+1)(a-1)$  e quindi  $p$  divide  $a+1$  oppure divide  $a-1$  (si ricordi che  $p$  è primo). Ne segue che  $a-1 \equiv 0 \pmod p$  cioè  $a = 1$ , oppure  $a+1 \equiv 0$ , ossia  $a = p-1$ . Tralasciando questi due valori estremi, gli altri elementi  $2, 3, \dots, p-2$  si possono raggruppare in  $(p-3)/2$  coppie  $\{a, a'\}$  con  $a \neq a'$  tali che  $aa' \equiv 1 \pmod p$ . Moltiplicando tra loro le corrispondenti congruenze, si ottiene  $2 \cdot 3 \cdots (p-2) = (p-2)! \equiv 1 \pmod p$ . Ma allora, moltiplicando ambo i membri per  $p-1 \equiv -1 \pmod p$ , si ha che  $(p-1)! \equiv -1 \pmod p$ .
2. Proviamo il viceversa, ossia che se  $n$  è tale che  $(n-1)! \equiv -1 \pmod n$ , allora  $n$  è un numero primo. Se  $n$  non fosse primo, avrebbe un divisore  $d$ ,  $1 < d < n$ , che, in quanto divisore di  $n$ , dividerà anch'esso  $(n-1)! + 1$ . Ma, dato che  $1 < d < n$ ,  $d$  comparirà tra i fattori di  $(n-1)!$  e quindi  $d \mid (n-1)!$ . Dalle due relazioni ottenute si ottiene l'assurdo che  $d$  divide 1. ◇

Abbiamo così dato una caratterizzazione dei numeri primi.

### Esempio 5.10

Possiamo dedurre che 5 è primo verificando che  $(5-1)! = 4! = 24 \equiv -1 \pmod 5$ .

Se provassimo a utilizzare questo test per provare che 11 è un numero primo dovremmo provare che  $10! + 1 \equiv 0 \pmod{11}$ , cioè che  $3628801 \equiv 0 \pmod{11}$ , il che è vero, ma non particolarmente immediato e comodo da verificare.

Questo criterio è quindi *inutilizzabile* in pratica, dato che  $(n - 1)!$  cresce troppo rapidamente e non si conosce un algoritmo per un calcolo rapido della funzione fattoriale.

### 3. Test di primalità relativi a numeri particolari

Per numeri che hanno forma particolare, come per esempio numeri di Fermat o numeri di Mersenne, esistono test di primalità speciali.

- *Test di Pépin.* Un numero di Fermat  $F_n$  è primo se e solo se esiste un intero  $a$  tale che

$$a^{2^{(2^n-1)}} = a^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

- *Test di Lucas* (cfr. proposizione 3.10). Il numero di Mersenne  $2^k - 1$  ( $k \geq 2$ ) è un numero primo se e solo se  $M_k$  divide  $S_k$ , dove  $S_k$  è definito per ricorrenza al modo seguente:  $S_2 = 4$ ,  $S_k = S_{k-1}^2 - 2$ .

## 8 FATTORIZZAZIONE DI INTERI

Strettamente legato al precedente punto, e tuttavia distinto dal problema di decidere se un numero è o no primo, è il problema della *fattorizzazione di un intero*. È ovviamente legato a quel problema, dato che se di un numero conosciamo una fattorizzazione non banale, sicuramente possiamo concludere che non è primo. Tuttavia spesso (per esempio con i test di primalità cui abbiamo accennato) si riesce a provare che un numero *non* è primo, ma non se ne riesce a trovare una fattorizzazione. Il problema di fattorizzare un intero è un problema difficile dal punto di vista computazionale, nel senso che non esistono a tutt'oggi algoritmi efficienti (ossia di tipo polinomiale), per risolvere il problema.

### (i) Fattorizzazione attraverso il crivello di Eratostene.

Il metodo più elementare per fattorizzare un intero  $n$  è attraverso il crivello di Eratostene che abbiamo già visto nel paragrafo 6.1 del capitolo 3. Si procede al modo seguente: si prova a vedere se è divisibile per  $2, 3, 4, 5, \dots, \sqrt{n}$ , ossia per tutti i numeri  $\leq \sqrt{n}$ : se non è divisibile per nessuno di questi, allora  $n$  è un numero primo (abbiamo già visto (cfr. eserc. 18 del cap. 3) perché basta fermarsi a  $\sqrt{n}$ ), altrimenti, detto  $n_1$  un numero che divide  $n$  e posto  $n = n_1 n_2$ , si ripete con  $n_1$  e  $n_2$  lo stesso procedimento e alla fine si arriverà alla fattorizzazione completa di  $n$ . In realtà ci si rende conto che una volta che si sia accertato che non è divisibile per 2, non dobbiamo più dividerlo per 4 o per 6, così, se non è divisibile per 3, non sarà divisibile nemmeno per i multipli di 3 e così via. Quindi basta provare a dividere  $n$  per tutti i primi minori o uguali a  $\sqrt{n}$ . Se è divisibile per un primo  $p$ , allora abbiamo trovato una fattorizzazione  $n = p \cdot m$ . Dopo di che si continua fattorizzando  $m$ .

Proviamo a renderci conto del tempo che richiede questo metodo. Supponiamo di dovere fattorizzare un intero  $n$  di 200 cifre (in base 10), e pensiamo di utilizzare il metodo di dividerlo per tutti i numeri primi minori o uguali a  $\sqrt{n}$ . Vediamo i vari passi:

- Se  $n$  ha 200 cifre decimali, sarà dell'ordine di  $10^{200}$  e quindi  $\sqrt{n}$  dell'ordine di  $10^{100}$ .

- In virtù del teorema 3.4, il numero di primi  $\leq \sqrt{n}$  è

$$\pi(\sqrt{n}) = \pi(10^{100}) \sim \frac{10^{100}}{\ln 10^{100}} = \frac{10^{100}}{100 \cdot \ln 10} \sim \frac{10^{100}}{230} \sim 10^{98}.$$

- Il numero del punto precedente rappresenta il *numero di divisioni* che dovremo eseguire per ottenere un fattore di  $n$ .
- Supponiamo che il computer impieghi  $10^{-9}$  secondi per operare una singola divisione. Allora impiegherà

$$10^{-9} \cdot 10^{98} \text{ secondi} = 10^{89} \text{ secondi}$$

per eseguire tutte le divisioni.

- Dato che 1 anno =  $365 \cdot 24 \cdot 60 \cdot 60 = 31\,536\,000 \sim 3 \cdot 10^7$  secondi, ne segue che per fare tutte le divisioni si impiegherebbero  $\frac{10^{89}}{3 \cdot 10^7}$  anni ossia circa  $10^{82}$  anni. Si pensi che l'età dell'universo è stata stimata da  $10^{10}$  a  $10^{11}$  anni!!!!

Questo serve per rendersi conto che è importante trovare degli algoritmi efficienti per la fattorizzazione di un intero.

### (ii) Il metodo di fattorizzazione di Fermat.

Per fattorizzare un numero  $n$  in molti casi è più efficiente il seguente metodo dovuto a Fermat. Esso si basa sui seguenti punti:

- Si può supporre senz'altro  $n$  dispari.
- Nel caso in cui  $n$  sia dispari, fattorizzare  $n$ , cioè trovare due interi (*non necessariamente primi*)  $a$  e  $b$  tali che risulti  $n = a \cdot b$ , equivale a determinare due interi  $x$  e  $y$  tali che

$$n = x^2 - y^2.$$

Infatti, se  $n \triangleq x^2 - y^2$ , allora  $n = (x + y)(x - y)$  è una fattorizzazione di  $n$ . Viceversa, se  $n = ab$ , allora, supposto  $a \geq b \geq 1$ , si può scrivere

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

dove  $(a+b)/2$  e  $(a-b)/2$  sono interi non negativi, perché, essendo  $n$  dispari, anche  $a$  e  $b$  saranno dispari, e quindi  $a \pm b$  è pari.

- Determinare  $x$  e  $y$  tali che  $n = x^2 - y^2$  equivale a determinare  $x$  tali che  $x^2 - n$  sia un quadrato ( $= y^2$ ). Si determina innanzitutto il più piccolo intero positivo  $k$  tale che  $k^2 \geq n$ , ossia  $k = [\sqrt{k}] + 1$ , dopodiché si calcolano successivamente le seguenti differenze:  $k^2 - n$ ,  $(k+1)^2 - n$ ,  $(k+2)^2 - n$ , ... fino a che si trova un valore  $t \geq \sqrt{n}$  tale che  $t^2 - n$  sia un quadrato.

- Il processo *termina*, perché sicuramente si ha

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2$$

che si ottiene quando il numero  $n$  è primo, e quindi ha una fattorizzazione banale

$$n = \left( \frac{n+1}{2} + \frac{n-1}{2} \right) \left( \frac{n+1}{2} - \frac{n-1}{2} \right) = n \cdot 1.$$

L'algoritmo per fattorizzare un intero dispari  $n$  è quindi semplice e consiste dei seguenti passi:

1. Passo 1: si pone  $k = \lfloor \sqrt{n} \rfloor + 1$  e si calcola  $k^2 - n$ . Se  $k^2 - n$  è un quadrato abbiamo trovato una fattorizzazione di  $n$ , altrimenti si va al passo successivo.
2. Passo  $i$ -esimo: si calcola  $(k+i)^2 - n$ : se  $(k+i)^2 - n$  è un quadrato, abbiamo finito, altrimenti si pone  $k+i := k+i+1$ .

#### Esempio 5.11

Fattorizzare in primi l'intero 250 669.

Si ha  $k = \lfloor \sqrt{250\,669} \rfloor + 1 = 501$ .

$501^2 - 250\,669 = 251\,001 - 250\,669 = 332$  non è un quadrato perfetto.

$502^2 - 250\,669 = 252\,004 - 250\,669 = 1335$  non è un quadrato perfetto.

$503^2 - 250\,669 = 253\,009 - 250\,669 = 2340$  non è un quadrato perfetto.

$504^2 - 250\,669 = 254\,016 - 250\,669 = 3347$  non è un quadrato perfetto.

$505^2 - 250\,669 = 255\,025 - 250\,669 = 4356 = 66^2$ .

Quindi  $250\,669 = (505 + 66)(505 - 66) = 571 \cdot 439$ : essendo sia 571 sia 439 numeri primi (si controlli!) questa è la fattorizzazione in primi di 250 669.

Ci sono altri metodi di fattorizzazione, che però esulano dagli scopi di questo testo: spesso si tratta di variazioni del metodo di Fermat. Tuttavia tutti gli algoritmi finora conosciuti, anche quelli più sofisticati, hanno complessità computazionale esponenziale, quindi non sono efficienti. Proprio sulla difficoltà di fattorizzare un numero (grande) si basa la sicurezza di alcuni sistemi crittografici, di cui andiamo a parlare nel paragrafo 10.

#### Esercizi

• Fattorizzare in primi i numeri 81 217, 5719 e 33 792.

• Fattorizzare in primi il numero 8 999 919.

• Fattorizzare in primi il numero 4 999 955.

• a. Decidere se  $\mathbb{Z}_{5719}$  è un campo o no.

b. Determinare, nel caso in cui siano invertibili, gli inversi in  $\mathbb{Z}_{5719}$  delle classi:  $\bar{38}$ ,  $\bar{2}$  e  $\bar{14}$ .

• Si provi che il numero di Fermat  $F_5 = 2^{32} + 1$  è divisibile per 641.

• Si provi che, se un intero positivo  $n$  è prodotto di due primi, la conoscenza di  $\varphi(n)$  equivale a sapere fattorizzare  $n$ .

• Sia  $n = 2279$ . Supponiamo di sapere che  $n = pq$ , con  $p, q$  primi e che  $\varphi(2279) = 2184$ . Trovare la fattorizzazione di  $n$ . Si determini la fattorizzazione di  $n$  anche con il metodo di fattorizzazione di Fermat.

• Stesso esercizio del numero precedente con  $n = 3053$  e  $\varphi(3053) = 2940$ .

## 9 CALCOLO DI POTENZE MODULO $n$

Il Teorema di Eulero ci offre un valido aiuto quando dobbiamo calcolare una potenza  $a^m$  modulo  $n$ : infatti, se  $(a, n) = 1$ , allora sappiamo che  $a^{\varphi(n)} \equiv 1 \pmod{n}$ , il che ci permette di ridurre l'esponente ad un numero minore di  $\varphi(n)$ . Però il Teorema di Eulero potrebbe non essere applicabile perché  $a$  e  $n$  non sono coprimi, oppure se l'esponente  $m$  risulta minore di  $\varphi(n)$ . Per esempio, supponiamo di dover calcolare

$$102^{11} \pmod{247}.$$

Dato che  $247 = 13 \cdot 19$ , si ha  $\varphi(247) = 12 \cdot 18 = 216$ . Ora, 216 è maggiore dell'esponente 11, e quindi possiamo dimenticarci il Teorema di Eulero. Come possiamo fare allora? Possiamo dividere via via l'esponente per due, ossia fare le seguenti operazioni

$$(9.1) \quad 102^{11} = 102^{5 \cdot 2+1} = (102^5)^2 \cdot 102 = (102^{2 \cdot 2+1})^2 \cdot 102 = ((102^2)^2 \cdot 102)^2 \cdot 102$$

con l'avvertenza, via via che si eleva al quadrato o si moltiplica per 102, di ridurre contestualmente modulo 247. Osservando che  $102^2 \equiv 30 \pmod{247}$ , che  $30^2 \equiv 159 \pmod{247}$ , ecc. si ottiene come risultato che  $102^{11} \equiv 201 \pmod{247}$ .

Osserviamo ora che la 9.1 si può leggere come

$$102^{11} = ((102^2)^2 \cdot 102)^2 \cdot 102 = 102^8 \cdot 102^2 \cdot 102$$

dove gli esponenti sono sempre potenze di 2. Per capire quali delle potenze di 2 intervengono e quali non intervengono, ci viene in aiuto la scrittura in base due (cfr. par. 4 del cap. 3) dell'esponente. Scriviamo in base 2 l'esponente 11. Si ha  $11 = (1011)_2$ . Ebbene, gli esponenti  $2^h$  che dovremo utilizzare sono quelli corrispondenti alle posizioni in cui c'è un 1, quindi

$$102^{11} = 102^8 \cdot 102^2 \cdot 102,$$

dopo di che si riduce tutto modulo 247 e si ottiene ovviamente ancora 201.

In generale, se dobbiamo calcolare  $a^m \pmod{n}$ , procediamo al modo seguente.

• Si calcolano tutte le potenze

$$a^1 \pmod{n}$$

$$a^2 \pmod{n}$$

$$a^{2^2} \pmod{n}$$

$$\begin{aligned} a^{2^3} &\mod n \\ a^{2^4} &\mod n \\ \dots & \\ a^{2^t} &\mod n \end{aligned}$$

essendo  $t$  il massimo intero tale che  $2^t \leq m$ .

- Si scrive l'esponente  $m$  in base 2.
- Si scrive  $a^m$  come prodotto delle sole potenze  $a^{2^k}$  corrispondenti ai valori 1 della scrittura in base 2 di  $m$ .
- Si riduce via via modulo  $n$ .

Se per esempio  $m = 59$  scriveremo

$$\begin{aligned} a^1 &\mod n \\ a^2 &\mod n \\ a^{2^2} &\mod n \\ a^{2^3} &\mod n \\ a^{2^4} &\mod n \\ a^{2^5} &\mod n \end{aligned}$$

e qui terminiamo, perché  $2^6 = 64$  è maggiore di 59. La scrittura in base 2 di 59 è  $(111011)_2$  e quindi tra le potenze della lista precedente prendiamo solo  $a^{2^5}, a^{2^4}, a^{2^3}, a^{2^2}a^{2^0}$ , e in definitiva

$$a^m = a^{2^5} \cdot a^{2^4} \cdot a^{2^3} \cdot a^{2^2} \cdot a^{2^0};$$

dopo di che si fanno i calcoli riducendo via via modulo  $n$  per tenere i conti sotto controllo.

Questa tecnica ci sarà di aiuto nel prossimo paragrafo dove si parla di crittografia.

## ■ 10 CRITTOGRAFIA

Arriviamo ora ad un'importantissima applicazione degli argomenti trattati in questo capitolo: la crittografia. La crittografia è la scienza delle comunicazioni segrete sicure, dei messaggi cioè che possono essere decifrati solo dai veri destinatari. Oggigiorno siamo in grado di comunicare velocemente e con chiunque da un capo all'altro del pianeta, possiamo con facilità da casa controllare il nostro conto in banca, fare versamenti, fare acquisti con carta di credito e bancomat, ecc. Tutte queste operazioni vengono fatte inserendo opportune password, per impedire che estranei possano operare o venire a conoscenza dei nostri movimenti o prelevare denaro dal nostro conto in banca. Questa facilità di comunicazioni, impensabile fino a poche decine di anni fa, ha trasformato il nostro mondo e creato un grosso problema: quello della *sicurezza* delle operazioni. In queste poche pagine dedicate alla crittografia parleremo proprio di questo problema. Premettiamo alcune considerazioni storiche.

Il problema di *comunicare in segreto* è antico quanto il mondo, soprattutto a livello militare: quindi il problema della segretezza di certe comunicazioni non è una prerogativa del nostro mondo attuale (anche se ora questa necessità è estesa a quasi tutti, e non solo a certe categorie di persone, come militari, politici, ecc.). Già nelle *Storie* di Erodoto (V secolo a.C.) si parla di messaggi segreti nascosti su tavolette di cera o nascosti sulla testa di messaggeri. Giulio Cesare aveva ideato un sistema di cifratura dei messaggi che consisteva nel traslare di un fissato numero le lettere dell'alfabeto. Per esempio il messaggio *ciao*, traslato di tre lettere diventa *FLDR*. È chiaro che un messaggio cifrato in questo modo (cioè per traslazione) può essere molto facilmente decifrato anche da chi non conosce la *chiave*, ossia il numero che rappresenta di quante posizioni deve essere traslato il messaggio: con 25 tentativi si riesce a decifrarlo. Ci sono stati perfezionamenti di questo sistema di cifratura, sostituendo alle semplici traslazioni permutazioni arbitrarie delle lettere dell'alfabeto. In questo caso la *chiave* per la cifratura è costituita dalla permutazione delle 26 lettere dell'alfabeto. Per esempio, se decidiamo di usare come chiave di cifratura la permutazione che manda 1 in 3, 3 in 9, 9 in 10, 10 in 15, 15 in 6 e 6 in 1 e lascia fissi tutti gli altri numeri, pensando di associare alla lettera *A* il numero 1 e alla *Z* il numero 26, la parola *ciao* verrebbe cifrata come *IJCF*.

In questo caso la decifrazione da parte di un estraneo diventa molto complicata, perché dovrebbe fare  $25!$  tentativi, che è un numero molto grande. Ma a questo punto entrano in gioco altre considerazioni, quali la frequenza delle lettere in un lingua, il fatto per esempio che nella lingua italiana la maggior parte delle parole con più di tre lettere termina con una vocale, che, se ci sono delle doppie, significa che queste sono consonanti, ecc. Quindi un'impresa che sembrava impossibile diventa fattibilissima, come sa benissimo chi si diletta di risolvere questioni del genere per esempio sulla *Settimana Enigmistica*. In tutti questi esempi di cifratura c'è un fatto che li accomuna: chi deve scambiarsi messaggi deve conoscere la *parola chiave*, cioè mittente e destinatario si devono comunicare la parola chiave: Cesare doveva comunicare ai suoi comandanti il numero chiave di traslazione, ecc. Ora, è chiaro che il momento dello scambio delle chiavi è un momento molto delicato: come avviene lo scambio? Incontrandosi? Non è molto comodo, se si sta molto lontani. Per telefono, per mail, per posta? In ogni caso la comunicazione della chiave è altamente vulnerabile: la conoscenza della chiave da parte di intrusi è deleteria per la comunicazione segreta.

Una rivoluzione nel campo della crittografia si è avuta con l'avvento (1976) del sistema di crittografia a chiave pubblica, ideato da Diffie e Hellman, ma chiamato comunemente sistema *RSA*, dai nomi di Rivest, Shamir e Adleman, che per primi lo hanno realizzato. Lo illustreremo qui di seguito brevemente. Premettiamo una osservazione: in tutti i sistemi classici di crittografia, il processo di decifratura, una volta nota la chiave, non è sostanzialmente più complicato del sistema di cifratura. Si pensi alla decifratura di un messaggio cifrato per traslazione: per decifrarlo occorre semplicemente "tornare indietro" del numero di passi dato dalla cifratura. Nel caso di messaggi cifrati mediante una permutazione, per decifrarli basta calcolare la permutazione inversa che è semplice da calcolare, come vedremo nel paragrafo 3 del capitolo 8. Quindi i sistemi di cifratura utilizzati fino all'avvento della cosiddetta chiave pubblica avevano due caratteristiche: necessità di scambiarsi la chiave e *simmetria*, ossia pari difficoltà di cifratura e decifratura. Ebbene, un cifrario a chiave pubblica è un cifrario che permette di divulgare il metodo e addirittura la chiave di cifratura, senza per-

questo rivelare il modo di decifrare. In altre parole, in tali sistemi, per decifrare in tempo ragionevolmente breve un messaggio, è necessario essere in possesso di qualche informazione ulteriore che non è resa pubblica.

Un esempio di cifrario non simmetrico è il seguente. La ricerca nell'elenco telefonico del numero di telefono di un dato abbonato è una operazione molto facile, dato che gli abbonati sono elencati in ordine alfabetico. Provate invece, dato un numero di telefono e utilizzando l'elenco telefonico, a trovare il nome dell'abbonato che possiede quel numero di telefono! Le due operazioni non sono simmetriche.

Precisiamo questi concetti con una definizione.

**DEFINIZIONE 5.5** Siano  $A$  e  $B$  due insiemi e sia  $f$  una funzione da  $A$  a  $B$ . Si dice che  $f$  è a senso unico se è facile da calcolare, ma riesce invece molto più difficile, dato un qualunque elemento  $b$  appartenente all'immagine di  $f$ , determinare un  $a \in A$  tale che  $f(a) = b$ .

#### Esempio 5.12

Siano  $A = B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$  e sia  $f$  la funzione definita al modo seguente:  $f(x) = 6^x$  per ogni  $x \in A$ .

Il calcolo di  $f(x)$  non è difficile, dato che abbiamo a disposizione le tecniche del paragrafo precedente, ma trovare la funzione inversa è complicato: dato un elemento dell'immagine, ossia del tipo  $6^x$ , come trovare  $x$ ? Si tratta del cosiddetto problema del logaritmo discreto che è un problema computazionalmente complesso.

### 10.1 Il sistema RSA

Innanzitutto, stabilendo una corrispondenza biunivoca che assegna ad ogni lettera dell'alfabeto e ad ogni segno di interpunkzione un numero a un certo numero di cifre, un messaggio  $M$  può considerarsi un numero intero positivo. Ci sono molti modi di associare un numero ad ogni lettera dell'alfabeto e ad ogni carattere: per esempio nell'*American Standard Code for Information Interchange* alle lettere da  $a$  a  $z$  corrispondono nell'ordine i numeri da 065 a 090. Tuttavia ci sono altri modi di associare ad una lettera un numero: è particolarmente utile per esempio associare ad ogni lettera un numero scritto in notazione binaria, cioè una sequenza di 0 e di 1.

Vediamo ora come funziona il sistema. Ogni utente  $U$  del sistema consegna una coppia di interi positivi,  $(n_U, e_U)$ , da inserire accanto al suo nome in un elenco pubblico. Il primo intero  $n_U$  deve essere il prodotto di due numeri primi distinti,  $p_U, q_U$  che devono essere grandi e tenuti segreti (conosciuti cioè solamente dall'utente  $U$ ), il secondo numero deve essere scelto da  $U$  in modo tale che  $(e_U, p_U - 1) = 1$  e  $(e_U, q_U - 1) = 1$ . Sottolineiamo quindi che la coppia  $(n_U, e_U)$  è di dominio pubblico, ossia un qualunque utente che lo desideri può consultarla, mentre non è di dominio pubblico la fattorizzazione di  $n_U$ , nota solamente a  $U$ .

Supponiamo che Alice debba mandare un messaggio  $M$  a Bob.

Consultando l'elenco ufficiale, Alice controlla innanzitutto la coppia di numeri relativa a Bob, cioè la coppia  $(n_B, e_B)$ . Se il messaggio  $M$  da inviare è maggiore del numero  $n_B$ , allora Alice spezzerà  $M$  in vari blocchi (messaggi unitari) che risultino minori

di  $n_B$ , che verranno inviati separatamente. Esistono metodi standard e pubblici per dividere il messaggio in messaggi unitari: per esempio suddividendolo in messaggi unitari di  $k$  cifre, essendo  $k$  il numero di cifre di  $n_B$  diminuito di una unità: in questo modo si è sicuri che ogni messaggio unitario è minore di  $n_B$ . Anche Bob conosce questo sistema, quindi questa parte non è segreta. Inoltre si può senz'altro supporre che sia  $(M, n_B) = 1$ : se così non fosse, il MCD tra i due numeri sarebbe un fattore non banale di  $n_B$ , cosa molto inverosimile, a meno che Bob non abbia fatto una scelta poco accorta di  $n_B$ .

Quindi, senza perdita di generalità, si può supporre che il messaggio  $M$  soddisfi alle seguenti due condizioni:

$$M < n_B, \quad (M, n_B) = 1.$$

Per codificare il messaggio  $M$  da inviare a Bob, Alice procede al modo seguente: eleva  $M$  alla potenza  $e_B$  e poi la riduce modulo  $n_B$ . Il messaggio  $M'$  che viene ricevuto da Bob è quindi  $M'$  dove

$$M' \equiv M^{e_B} \pmod{n_B}.$$

Prima di procedere alla fase di decodifica da parte di Bob, facciamo alcune osservazioni.

Nel momento in cui ha consegnato al pubblico la sua coppia  $(n_B, e_B)$ , Bob ha tenuto per sé una chiave segreta  $d_B$ : questo numero è tale che

$$1 \leq d_B < \varphi(n_B) = (p_B - 1)(q_B - 1),$$

ed è soluzione della

$$(10.1) \quad e_B d_B \equiv 1 \pmod{\varphi(n_B)}$$

dove  $\varphi$  è la funzione di Eulero.

**OSSERVAZIONE** Si noti che questa congruenza ammette una e una sola soluzione modulo  $\varphi(n_B)$ , perché il coefficiente  $e_B$  è tale che  $(e_B, p_B - 1) = 1$  e  $(e_B, q_B - 1) = 1$  per la scelta di  $e_B$  e quindi anche  $(e_B, (p_B - 1)(q_B - 1)) = 1$ . Si noti inoltre che l'utente  $B$  è l'unico che può risolvere la congruenza (10.1), perché è l'unico a conoscere la funzione di Eulero di  $n_B$ , conoscendo i fattori primi  $p_B$  e  $q_B$ .

Ebbene, la possibilità di risolvere la congruenza (10.1) (e quindi il possesso della chiave segreta  $d_B$ ) consente a  $B$  di decifrare il messaggio  $M'$  ricevuto.

Vale infatti la seguente proposizione.

**PROPOSIZIONE 5.14** Il messaggio originario  $M$  è tale che

$$M \equiv M'^{d_B} \pmod{n_B}.$$

**DIMOSTRAZIONE.** Si ha  $M'^{d_B} \equiv (M^{e_B})^{d_B} = M^{e_B d_B} \pmod{n_B}$ ; ora,  $e_B d_B \equiv 1 \pmod{\varphi(n_B)}$   $\Rightarrow e_B d_B - 1$  è un multiplo di  $\varphi(n_B)$ . Quindi,  $M^{e_B d_B} = M^{1 + \varphi(n_B) \cdot k} = M \cdot (M^{\varphi(n_B)})^k$ . Essendo  $(M, n_B) = 1$ , in base al Teorema di Eulero risulta  $M^{\varphi(n_B)} \equiv 1 \pmod{n_B}$ , da cui  $M^{e_B d_B} \equiv M \pmod{n_B}$ . Quindi  $M \equiv M'^{d_B} \pmod{n_B}$  e pertanto  $B$  riesce a leggere il messaggio  $M$ .  $\diamond$

Ripetiamo che  $B$  ha potuto decifrare il messaggio  $M$  perché era in possesso della fattorizzazione di  $n_B$  (che è *equivalente* alla conoscenza di  $\varphi(n_B)$ , cfr. eserc. 49). La sicurezza di questo sistema risiede nel fatto che  $B$  non ha dovuto mandare la chiave ad  $A$ : ha semplicemente pubblicato una coppia di numeri. Ora, mentre per *inviare* il messaggio la conoscenza di questa coppia è sufficiente, per *decifrare* il messaggio ciò non è sufficiente: occorre conoscere la fattorizzazione di  $n_B$ , che solo  $B$  conosce. Se un estraneo tentasse di decifrare il messaggio  $M'$ , dovrebbe trovare la fattorizzazione di  $n_B$ : ora per trovare questa, nel caso per esempio in cui  $n_B$  sia prodotto di due primi ciascuno di 60 cifre, anche utilizzando i più sofisticati algoritmi e i calcolatori più veloci, occorrerebbero molti mesi, se non addirittura anni, di calcoli. Se poi si scelgono i due primi con 100 e più cifre, la fattorizzazione di  $n$  è addirittura, in generale, impossibile. Diciamo *in generale*, perché nel 1994 è stato decodificato dal matematico Lenstra in collaborazione con molti altri scienziati e con migliaia di calcolatori al lavoro, un messaggio relativo ad un modulo di 129 cifre che secondo gli inventori stessi del sistema RSA, che lo avevano lanciato come sfida, avrebbe richiesto qualcosa come  $10^{15}$  anni!. Questo episodio sta ad indicare che un sistema ritenuto sicuro oggi può non esserlo più domani.

Resta un problema: come fa ogni utente  $U$  a trovare due numeri primi grandi in modo da produrre  $n_u$ ?

- Si genera a caso un numero  $m$  dispari dell'ordine di grandezza voluto.
- Si sottopone  $m$  a un test di primalità.
- Se  $m$  supera il test abbiamo finito, altrimenti passiamo all'intero  $m + 2$ .
- In base al Teorema dei Numeri Primi (cfr. teorema 3.4) dopo  $\log m$  tentativi si dovrebbe ottenere un primo.

Potrebbe sorgere il dubbio che non ci siano sufficienti numeri primi di una certa grandezza. Possiamo stare tranquilli perché, sempre in virtù del Teorema dei Numeri Primi, il numero di primi di lunghezza 512 bit è più di  $10^{150}$ . Se non fossimo convinti dell'enormità di questo numero, pensiamo che questo numero è maggiore del numero di atomi dell'universo!!

#### Esempio 5.13

Giuseppe deve inviare a Carlo come messaggio segreto la lettera "D", usando il sistema RSA. La coppia di interi associata a Carlo è ( $n_C = 143$ ,  $e_C = 7$ ). Per trasformare una sequenza di lettere in cifre viene usata la seguente tabella.

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21

- Quale numero riceverà Carlo?
- Come farà a decifrarlo?

a.  $143 = 11 \cdot 13$  quindi 143 è prodotto di due numeri primi distinti.  $\varphi(143) = \varphi(11)\varphi(13) = 10 \cdot 12 = 120$ .  $e_C = 7$  è coprimo sia con 10 sia con 12. Quindi la coppia di numeri di Carlo soddisfa le condizioni richieste.  $D$  corrisponde al numero 04, quindi per inviare il messaggio, Giuseppe verifica innanzitutto che 4 sia minore di  $n_C = 143$  e sia coprimo con 143: entrambe le condizioni sono verificate. Dopo di che eleva 4 a  $e_C = 7$  e lo riduce modulo 143: ottiene  $4^7 = 4^4 \cdot 4^3 = 256 \cdot 64 \equiv 82 \pmod{143}$ .

Quindi Carlo riceve il numero 82.

b. Innanzitutto Carlo, che è in possesso di una informazione supplementare, ossia la fattorizzazione di  $143 = 11 \cdot 13$ , e quindi conosce la funzione di Eulero di 143, 120, risolve la congruenza  $e_C x \equiv 1 \pmod{120}$  che gli permette di determinare la propria chiave segreta  $d_C = 103$ . A questo punto eleva 82 alla chiave segreta 103 e riduce tale potenza modulo 143. Ora possiamo servirci dei metodi del paragrafo 9:  $103 = (1100111)_2$  quindi  $82^{103} = 82^{2^6} \cdot 82^{2^5} \cdot 82^{2^2} \cdot 82^2 \cdot 82$ .

Con un po' di conti si vede che  $82^{103} \equiv 4 \pmod{221}$  e Carlo (e solo lui) riesce a decifrare il messaggio di Giuseppe.

#### Esercizi

50 Supponiamo che Alice debba mandare il messaggio  $M = 4$  a Bob la cui coppia di numeri (che ha trovato nell'elenco ufficiale) è ( $n_B = 221$ ,  $e_B = 7$ ). Quale messaggio riceverà Bob? Come farà a decifrarlo?

51 Alice e Bob vogliono comunicare tra di loro con il sistema crittografico RSA. Ciascuno dei due ha depositato la propria coppia di interi: Alice la coppia ( $n_A = 247$ ,  $e_A = 7$ ), e Bob la coppia ( $n_B = 253$ ,  $e_B = 3$ ).

- Verificare che entrambe le coppie siano accettabili;
- Alice deve inviare a Bob il risultato del suo esame di Matematica Discreta in cui ha ottenuto un bel 30. Quale numero riceverà Bob?
- Come farà Bob a decifrare il messaggio ricevuto?

52 a. Usando il metodo computazionalmente più efficiente che conoscete, verificare che i seguenti interi sono primi: 503, 607, 701.  
b. Determinare una coppia di interi  $n$  ed  $e$  che siano accettabili come chiave pubblica per il sistema RSA, in modo che  $n$  sia il prodotto di due primi fra quelli indicati al punto precedente.  
c. Quale fra le possibili scelte di  $n$  nel punto precedente è la più efficace dal punto di vista della sicurezza (cioè della difficoltà di decifrare il messaggio da parte di un estraneo)? Spiegare il motivo della vostra risposta.

53 Supponiamo che un utente  $B$  abbia scelto come coppia di interi pubblici per un sistema crittografico RSA la coppia ( $n_B = 46$ ,  $e_B = 13$ ).

Un utente  $A$  vuole mandare il messaggio  $x = 8$  all'utente  $B$ .

- Qual è il messaggio in codice (cioè quello che  $B$  riceverà)?
- Come riesce  $B$  a decifrarlo?

## ■ 11 L'AUTENTICAZIONE DELLE FIRME

Supponiamo che Bob riceva un messaggio da qualcuno che si firma Alice. Come può essere certo che sia stata proprio Alice a inviarlo? Il sistema RSA permette di inviare una autenticazione della firma, che consenta al destinatario di essere certo della provenienza del messaggio. Vediamo come. Per far sì che Bob sia sicuro dell'autenticità del messaggio, Alice scrive il suo messaggio  $M_1$ , in fondo al quale comparirà la sua firma  $F$ ; immediatamente sotto il messaggio  $M_1$  aggiunge il seguente messaggio  $M_2$

$$M_2 \equiv F^{d_A} \pmod{n_A}$$

dove  $d_A$  è la propria chiave segreta, ossia quella che Alice solo conosce, conoscendo la fattorizzazione della chiave pubblica  $n_A$ . Poi manda a Bob l'intero messaggio  $M = M_1 + M_2$  al solito modo, ossia elevando l'intero messaggio alla potenza  $e_B$  e riducendolo modulo  $n_B$ . Nel ricevere il messaggio, Bob legge il messaggio (utilizzando la propria chiave segreta  $d_B$ ). Dalla decifrazione del messaggio  $M_1$ , Bob capisce che il messaggio gli è stato inviato da Alice. Dopo la lettura della firma  $F$  di Alice, seguono dei caratteri illeggibili, che però contengono la prova della autenticità della firma. Infatti ora Bob deve procedere al modo seguente: per decifrare questa parte  $M_2$  del messaggio non deve utilizzare la *propria chiave segreta*  $d_B$ , perché il messaggio originario che deve leggere, ossia  $F$ , è già stato alterato, cioè elevato alla chiave segreta della vera Alice. Utilizza allora la chiave pubblica  $e_A$  di Alice. In tal modo gli viene fuori la firma  $F$  di Alice, perché

$$M_2^{e_A} \equiv (F^{d_A})^{e_A} = F^{d_A e_A} \equiv F \pmod{n_A}.$$

Tale firma non può essere che quella autentica, perché solamente Alice è a conoscenza della propria chiave segreta. Nel caso in cui non fosse comparsa la firma  $F$  di Alice, il messaggio sarebbe stato un falso. In sostanza, per l'autenticazione di una firma è il mittente che utilizza la *propria chiave segreta*, anziché il ricevente.

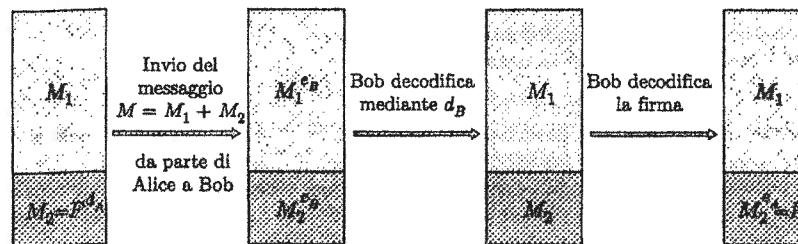


Figura 5.1. L'autenticazione della firma.

La figura 5.1 mostra i vari stadi del processo di invio di un messaggio segreto e del controllo di autenticità della firma.



Supponiamo che Alice abbia la coppia  $(n_A = 77, e_A = 13)$ . Nell'inviare un messaggio a Bob, Alice ha autenticato la sua firma (che è  $F = 70$ ). Come fa Bob a ricavare che il messaggio è autentico, cioè che proviene effettivamente da Alice?

### Esercizi di programmazione

■ Si scriva un programma che verifichi se un dato intero è divisibile per 2, 3, 4, 5, 7, 9, 11,  $2^k$ .

■ Si scriva un programma che stampi la tavola additiva di  $Z_n$  e quella moltiplicativa.

■ Fare un programma che determini se una data congruenza lineare  $ax \equiv b \pmod{n}$  ammette soluzioni, e, in caso positivo, determini tutte le  $d$  soluzioni non congruenti mod  $n$ , dove  $d = \text{MCD}(a, n)$ .

■ Fare un programma che risolva un sistema di congruenze del tipo

$$\begin{cases} x \equiv c_1 \pmod{r_1} \\ x \equiv c_2 \pmod{r_2} \\ \dots \\ x \equiv c_s \pmod{r_s} \end{cases}$$

con  $(r_i, r_j) \neq 1$  per  $i \neq j$ . Si utilizzi il Teorema Cinese dei Resti.

■ Si scriva un programma che trovi esplicitamente, per  $r$  e  $s$  tali che  $(r, s) = 1$ , la corrispondenza biunivoca tra  $Z_{rs}$  e  $Z_r \times Z_s$  garantita dal Teorema Cinese dei Resti, quella cioè che associa ad ogni  $\bar{a}_{rs}$  la coppia  $(\bar{a}_r, \bar{a}_s)$  (dove  $\bar{a}_k$  rappresenta la classe resto modulo  $k$ ). Si consiglia di utilizzare il seguente metodo efficiente che permette, noto  $(\bar{x}_r, \bar{x}_s)$ , di ricavare  $\bar{x}_{rs}$ :

(i) Si risolve prima il problema per  $(\bar{1}_r, \bar{0}_s)$  e per  $(\bar{0}_r, \bar{1}_s)$ : si tratta di risolvere i seguenti due sistemi di congruenze:

$$\begin{cases} x \equiv 1 \pmod{r}, \\ x \equiv 0 \pmod{s}, \end{cases} \quad \begin{cases} y \equiv 0 \pmod{r}, \\ y \equiv 1 \pmod{s}. \end{cases}$$

Per risolvere questi sistemi si può utilizzare l'algoritmo di Euclide, ed esprimere 1 nella forma  $1 = r\alpha + s\beta$ , per opportuni  $\alpha$  e  $\beta$  in  $\mathbb{Z}$  e poi prendere  $x = s\beta$ ,  $y = r\alpha$ , eventualmente ridotti modulo  $rs$ .

(ii) Una volta che si conosca il corrispondente di  $(\bar{1}_r, \bar{0}_s)$  e  $(\bar{0}_r, \bar{1}_s)$ , la determinazione del corrispondente di  $(\bar{x}_r, \bar{x}_s)$  in  $Z_{rs}$  è immediata. Infatti, se  $\bar{a}_{rs}$  e  $\bar{b}_{rs}$  sono gli elementi di  $Z_{rs}$  corrispondenti rispettivamente a  $(\bar{1}_r, \bar{0}_s)$  e a  $(\bar{0}_r, \bar{1}_s)$ , allora l'elemento di  $Z_{rs}$  corrispondente alla coppia  $(\bar{x}_r, \bar{x}_s)$  è  $(\bar{a}_{rs} + \bar{b}_{rs})_{rs}$  (si verifichi).

■ Si scriva un programma che calcoli la funzione di Eulero  $\varphi(n)$  per ogni intero  $n$ .

■ Si scriva un programma che calcoli gli elementi invertibili di  $Z_n$  e i loro inversi modulo  $n$ .

■ Stampare la tavola moltiplicativa  $(\pmod{n})$  di  $U(Z_n)$ .

- a. Fare un programma che trovi una fattorizzazione per un intero  $n$  dispari calcolando tutti i primi minori o uguali a  $\sqrt{n}$ .
- b. Fare un programma che trovi una fattorizzazione di un intero dispari utilizzando il metodo di fattorizzazione di Fermat.
- c. Si confrontino i due metodi.

■■■ Fare un programma che calcoli le potenze  $a^m \pmod n$ , servendosi della scrittura in base 2 dell'esponente.

■■■ Scrivere un programma che verifichi se una coppia  $(n_U, e_U)$  per il sistema RSA sia corretta.

■■■ Fare un programma che decifri un codice a chiave pubblica RSA, secondo le indicazioni date.

# 6

## Polinomi e algoritmi

*Tutto ciò che è nascosto e ciò che è palese io lo so,  
perché mi ha istruito la sapienza, artefice di tutte le cose.*

SAPIENZA, 7, 21

Questo capitolo è dedicato allo studio dei polinomi a coefficienti in un campo (che può essere  $\mathbb{R}$ ,  $\mathbb{Q}$ , o  $\mathbb{Z}_p$ ,  $p$  primo). Ogni studente è già sicuramente venuto in contatto nel corso dei suoi studi superiori con questo argomento, e conosce le operazioni di addizione e moltiplicazione di polinomi, scomposizione in fattori, ecc. Studieremo quindi l'insieme  $\mathbb{K}[x]$  di tutti i polinomi a coefficienti in un campo  $\mathbb{K}$ , e mostreremo come questo insieme, dotato delle ordinarie operazioni di addizione e moltiplicazione tra polinomi, si comporta bene, nel senso che gode di molte delle proprietà dell'anello  $(\mathbb{Z}, +, \cdot)$ , e, in più, gode di altre proprietà che studieremo. Il capitolo si chiude con alcune osservazioni sulla crescita di funzioni e sulla complessità degli algoritmi.

### ■ 1 PRIME DEFINIZIONI RELATIVE AI POLINOMI

Prima di tutto daremo la definizione di *polinomio in una indeterminata  $x$  a coefficienti in un campo  $\mathbb{K}$* . Il campo potrà essere  $\mathbb{R}$ ,  $\mathbb{Q}$ , o  $\mathbb{Z}_p$ ,  $p$  primo. Per quanto riguarda l'indeterminata  $x$ , possiamo pensarla come un simbolo attraverso il quale si possono costruire altri "simboli", per l'appunto i polinomi a coefficienti in  $\mathbb{K}$ . Come è ben noto, un polinomio nell'indeterminata  $x$  a coefficienti nel campo  $\mathbb{K}$  è una somma di termini, detti *monomi*, ciascuno dei quali è il prodotto di un coefficiente, che è un elemento di  $\mathbb{K}$ , per una potenza  $x^i$  della indeterminata  $x$ , con  $i \in \mathbb{N}$ . In definitiva,

**DEFINIZIONE 6.1** Sia  $\mathbb{K}$  un campo. Dicesi *polinomio  $f(x)$  a coefficienti in  $\mathbb{K}$  nell'indeterminata  $x$*  una espressione formale del tipo

$$(1.1) \quad f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_i \in \mathbb{K}, \quad n \in \mathbb{N}.$$

Gli elementi  $a_i \in \mathbb{K}$  prendono il nome di *coefficienti* del polinomio.

L'insieme di tutti i polinomi nell'indeterminata  $x$  a coefficienti nel campo  $\mathbb{K}$  si denota con  $\mathbb{K}[x]$ .

Per esempio, i seguenti sono polinomi su  $\mathbb{Q}$ , ossia appartengono a  $\mathbb{Q}[x]$ :

$$x^2 - 4, \quad 4x^6 - 5x^3 + \frac{3}{5}, \quad 3, \quad \frac{3}{4}x^3 + 2,$$

mentre i seguenti sono polinomi a coefficienti in  $\mathbb{Z}_5$ , cioè appartengono a  $\mathbb{Z}_5[x]$ :

$$x^3 + \bar{1}, \quad 4x^7 - \bar{3}, \quad \bar{2}.$$

I seguenti invece *non* sono polinomi:

$$x^4 + \frac{1}{x}, \quad \frac{1}{x^3} + 2x^2 + 2$$

perché la indeterminata  $x$  compare anche elevata ad *esponente negativo*.

La (1.1) si può scrivere sotto forma di sommatoria nel modo seguente:

$$\sum_{i=0}^n a_i x^i, \quad a_i \in \mathbb{K}, \quad n \in \mathbb{N}.$$

### Uguaglianza tra polinomi

Dato che un polinomio è un'espressione *formale* del tipo (1.1), due polinomi che abbiano diverso anche un solo coefficiente sono da considerarsi diversi. Quindi

**DEFINIZIONE 6.2** Due polinomi  $f(x) = \sum_{i=0}^n a_i x^i$  e  $g(x) = \sum_{j=0}^m b_j x^j$  si dicono *uguali* se e solo se  $a_i = b_i$  per ogni  $i \geq 0$ .  $\blacksquare$

Quindi  $f(x) = 3x^4 - 2x^3 + 5x - 1$  è uguale al polinomio  $g(x) = 3x^4 + 5x - 2x^3 - 1$ , perché, indicati con  $a_i$  e  $b_i$  rispettivamente i coefficienti di  $f(x)$  e  $g(x)$ ,  $a_0 = -1 = b_0$ ,  $a_1 = 5 = b_1$ ,  $a_2 = 0 = b_2$ ,  $a_3 = -2 = b_3$ ,  $a_4 = 3 = b_4$  ma è diverso dal polinomio  $h(x) = 3x^4 - 2x^3 - 1$  dato che, indicati con  $c_i$  i coefficienti di  $h(x)$ ,  $a_1 = 5 \neq c_1 = 0$ .

### Operazioni tra polinomi

Siano  $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n = \sum_{i=0}^n a_i x^i$  e  $g(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m = \sum_{j=0}^m b_j x^j$  due elementi di  $\mathbb{K}[x]$ . Supponiamo, per fissare le idee,  $m \geq n$ . Pensiamo per il momento i polinomi come espressioni letterali le cui lettere stanno in  $\mathbb{K}$ : sfruttando tutte le proprietà di tali espressioni (commutatività, distributività, ecc.) si hanno le seguenti uguaglianze:

$$f(x) + g(x) = (a_0 + b_0)x^0 + (a_1 + b_1)x^1 + \dots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \dots + b_m x^m$$

e

$$f(x) \cdot g(x) = a_0 \cdot b_0 + (a_0 b_1 + a_1 b_0)x^1 + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \dots + (a_0 b_h + a_1 b_{h-1} + a_2 b_{h-2} + \dots + a_h b_0)x^h + \dots + a_n b_m x^{n+m}$$

Ebbene, forti di queste uguaglianze, diamo le seguenti *definizioni di addizione e moltiplicazione tra polinomi nella indeterminata x*:

$$f(x) + g(x) \stackrel{\text{def}}{=} \sum_{h=0}^m (a_h + b_h)x^h \text{ se } m \geq n$$

e

$$f(x)g(x) \stackrel{\text{def}}{=} \sum_{h=0}^{n+m} \left( \sum_{i+j=h} a_i b_j \right) x^h.$$

Quindi

$$f(x) + g(x) = \sum_{h=0}^m c_h x^h \text{ con } c_h = a_h + b_h$$

e

$$f(x) \cdot g(x) = \sum_{h=0}^{n+m} c_h x^h \text{ con } c_h = \sum_{i+j=h} a_i b_j.$$

Si tratta delle ordinarie definizioni di addizione e moltiplicazione tra polinomi che ogni studente ben conosce. Quindi per esempio se  $f(x) = 4x^3 + 2x^2 + x - 5$  e  $g(x) = x^6 + 3x + 3$ , allora  $f(x) + g(x) = (4x^3 + 2x^2 + x - 5) + (x^6 + 3x + 3) = (0 + 1)x^6 + (0 + 0)x^5 + (0 + 0)x^4 + (4 + 0)x^3 + (2 + 0)x^2 + (1 + 3)x + (-5 + 3) = x^6 + 4x^3 + 2x^2 + 4x - 2$ .

Se  $f(x) = x^3 + 2x - 1$  e  $g(x) = x^2 + x + 3$ , allora  $f(x)g(x) = (x^3 + 2x - 1)(x^2 + x + 3) = x^5 + x^4 + 3x^3 + 2x^2 + 6x - x^2 - x - 3 = x^5 + x^4 + 5x^3 + x^2 + 5x - 3$  e si vede che effettivamente il coefficiente di  $x^h$  nel prodotto dei due polinomi è dato dalla somma dei prodotti del tipo  $a_i b_j$  con  $i + j = h$ :

- Il coefficiente di  $x^5$  nel prodotto dei due polinomi è semplicemente  $1 \cdot 1 = 1$  (cioè il prodotto del coefficiente di  $x^3$  per il coefficiente di  $x^2$ ) ( $5=3+2$ ).
- Il coefficiente di  $x^4$  nel prodotto dei due polinomi è 1 perché prodotto del coefficiente di  $x^3$  in  $f(x)$  (che è 1) per il coefficiente di  $x$  in  $g(x)$  (che è 1) ( $4 = 3 + 1 = 2 + 2 = 1 + 3$ , ma gli unici che danno un contributo sono i coefficienti di  $x^3$  in  $f(x)$  per il coefficiente di  $x$  in  $g(x)$ ).
- Il coefficiente di  $x^3$  nel prodotto dei due polinomi è il prodotto del coefficiente 1 di  $x^3$  in  $f(x)$  per il termine noto 3 in  $g(x)$  sommato al prodotto del coefficiente 2 di  $x$  in  $f(x)$  per il coefficiente 1 di  $x^2$  in  $g(x)$ , cioè  $1 \cdot 3 + 2 \cdot 1 = 5$ .
- Il coefficiente di  $x^2$  nel prodotto dei due polinomi è il prodotto del coefficiente 2 di  $x$  in  $f(x)$  per il coefficiente 1 di  $x$  in  $g(x)$  sommato al prodotto del coefficiente -1 di  $x^0$  in  $f(x)$  per il coefficiente 1 di  $x^2$  in  $g(x)$ , cioè  $2 \cdot 1 + (-1) \cdot 1 = 1$ .
- Il coefficiente di  $x$  nel prodotto dei due polinomi è il prodotto del coefficiente 2 di  $x$  in  $f(x)$  per il coefficiente 3 di  $x^0$  in  $g(x)$  sommato al prodotto del coefficiente -1 di  $x^0$  in  $f(x)$  per il coefficiente 1 di  $x$  in  $g(x)$ , cioè  $2 \cdot 3 + (-1) \cdot 1 = 5$ .
- Il coefficiente di  $x^0$  (ossia il termine noto) nel prodotto dei due polinomi è il prodotto del coefficiente -1 di  $x^0$  in  $f(x)$  per il coefficiente 3 di  $x^0$  in  $g(x)$ , cioè  $-1 \cdot 3 = -3$ .

### Struttura di $(\mathbb{K}[x], +, \cdot)$

È facile vedere che, rispetto alle operazioni appena definite,  $(\mathbb{K}[x], +, \cdot)$  gode delle stesse proprietà (cfr. par. 1 del cap. 3) degli interi, ossia diventa un anello commutativo con unità. Lo zero di  $\mathbb{K}[x]$ , ossia l'elemento neutro rispetto all'addizione, è il polinomio con tutti i coefficienti nulli; così, l'opposto del polinomio  $f(x) = \sum_{i=0}^n a_i x^i$  è il polinomio che ha come coefficienti gli opposti dei coefficienti  $a_i$ , l'unità (ossia l'elemento neutro rispetto alla moltiplicazione) è il polinomio 1, ecc.

Ma c'è di più. Faremo vedere che, come  $(\mathbb{Z}, +, \cdot)$ , anche  $(\mathbb{K}[x], +, \cdot)$  è un dominio di integrità, ossia non possiede divisori dello zero. Per arrivare a questo risultato occorre dare alcune definizioni.

**DEFINIZIONE 6.3** Sia  $f(x) = \sum_{i=0}^n a_i x^i$ , con  $a_n \neq 0$ . Allora l'intero  $n$  prende il nome di *grado* del polinomio e si indica con  $\deg f(x)$  o con  $\partial f(x)$ .

Quindi il grado di un polinomio è l'esponente massimo con cui compare  $x$  con coefficiente diverso da zero nell'espressione del polinomio. Tale coefficiente prende il nome di *coefficiente direttivo* di  $f(x)$ . Un polinomio con coefficiente direttivo uguale ad 1 si dice *monico*.

Si noti che il grado di un polinomio  $f(x) = a_0$ , cioè di una costante, è zero. Al polinomio nullo non si attribuisce in genere un grado (oppure, convenzionalmente, gli si attribuisce il grado  $-\infty$ ).

Vale la seguente proposizione.

**PROPOSIZIONE 6.1** L'anello  $(\mathbb{K}[x], +, \cdot)$  è un dominio di integrità.

**DIMOSTRAZIONE.** Basta provare che è privo di divisori dello zero. Siano  $f(x) = \sum_{i=0}^n a_i x^i$  e  $g(x) = \sum_{j=0}^m b_j x^j$  due polinomi non nulli (cioè che abbiano almeno un coefficiente non nullo). Supponiamo che  $\partial f(x) = n$  e  $\partial g(x) = m$ ; ciò significa che  $a_n \neq 0$  e  $b_m \neq 0$ . Dalla definizione di polinomio prodotto  $f(x)g(x)$ , risulta che il coefficiente di  $x^{m+n}$  è  $a_n b_m$ , che è diverso da zero perché  $a_n$  e  $b_m$  sono diversi da zero e sono elementi di un campo, in cui non esistono divisori dello zero (cfr. eserc. 3). Quindi  $f(x)g(x)$  non può essere il polinomio nullo.

Notiamo esplicitamente le seguenti relazioni tra i gradi di due polinomi a coefficienti in un campo e i gradi della loro somma e del loro prodotto:

$$\partial(f(x) + g(x)) \leq \max(\partial f(x), \partial g(x)), \quad \partial(f(x)g(x)) = \partial f(x) + \partial g(x).$$

### Esempio 6.1

La somma dei due polinomi  $3x^3 + 2x - 1$  e  $-3x^3 - 4x^2 + 1$  (entrambi di grado 3) è il polinomio  $-4x^2 + 2x$  che ha grado 2 ( $< 3$ ). Se due polinomi hanno gradi diversi, allora la loro somma è un polinomio di grado uguale al  $\max(\partial f(x), \partial g(x))$ .

### Gestione dei polinomi al calcolatore

Sorge ora il problema di come si possano manipolare i polinomi al calcolatore.

Conviene fare la seguente osservazione. Un polinomio  $f(x) = \sum_{i=0}^n a_i x^i$  è individuato non appena conosciamo tutti i suoi coefficienti. Quindi potremmo pensare di identificare il polinomio  $f(x)$  con la stringa dei suoi coefficienti. Tuttavia per poter rappresentare *tutti* i polinomi (di qualunque grado) identifieremo il polinomio  $f(x) = \sum_{i=0}^n a_i x^i$  con la successione *infinita*

$$(a_0, a_1, a_2, \dots, a_i, \dots)$$

di elementi di  $\mathbb{K}$  soddisfacente però la condizione che *tutti gli  $a_n$  da un certo punto in poi sono uguali a zero*.

Quindi per esempio il polinomio  $f(x) = 2 + 4x + 5x^4 - 3x^7 - x^{10}$  sarà identificato con la successione infinita (che però da un certo punto in poi è costituita da soli zeri)

$$(2, 4, 0, 0, 5, 0, 0, -3, 0, 0, -1, 0, 0, \dots, 0, 0, \dots).$$

A questo punto dobbiamo però stabilire come addizionare e moltiplicare tali successioni.

Nell'insieme di tutte queste successioni definiamo addizione e moltiplicazione di successioni al modo seguente:

$$(a_0, a_1, a_2, \dots, a_i, \dots) + (b_0, b_1, b_2, \dots, b_i, \dots) \stackrel{\text{def}}{=} (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots, a_i + b_i, \dots)$$

e

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) \stackrel{\text{def}}{=} (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots)$$

posto che  $(b_{i+1}) = 0$

L'identificazione tra una successione così definita ed un polinomio è data dalla corrispondenza (biunivoca):

$$(a_0, a_1, a_2, \dots, a_n, \underbrace{0, 0, 0, 0, 0, \dots}_{\text{d'ora in poi tutti } = 0}) \longleftrightarrow \sum_{i=0}^n a_i x^i.$$

In particolare si hanno le seguenti identificazioni:

$$(1, 0, 0, 0, \dots) \equiv 1$$

$$(0, 1, 0, 0, \dots) \equiv x$$

$$(0, 0, 1, 0, \dots) \equiv x^2$$

...

$$(0, 0, 0, \dots, \underbrace{1}_{\text{posizione } i+1-\text{ma}}, 0, 0, \dots) \equiv x^i.$$

Si capisce ora il significato dell'indeterminata  $x$  e delle sue potenze: sono delle specie di "segnaposto". È chiaro anche che la definizione di addizione e moltiplicazione tra successioni corrisponde alle definizioni delle analoghe operazioni dei relativi polinomi.

Nella pratica, a seconda dei tipi di polinomi con cui dovremo lavorare, ci serviremo di stringhe di una lunghezza fissata  $N$ , con  $N$  sufficientemente grande.

### Esercizi

● Determinare somma e prodotto dei seguenti polinomi in  $\mathbb{Q}[x]$ :

a.  $f(x) = x^4 + 3x^5 - 3x + 1$ ,  $g(x) = x^3 + x^2 + 3x - 1$ .

b.  $f(x) = 2x^3 + 3x^2 + x + 5$ ,  $g(x) = -2x^3 - x^2 - 2x + 8$ .

Determinare somma e prodotto dei seguenti polinomi in  $\mathbb{Z}_5[x]$ :

- $f(x) = x^4 + 3x^5 + x + 1$ ,  $g(x) = x^3 + x^2 + 3x + 1$ .
- $f(x) = 2x^3 + 2x^2 + x + 2$ ,  $g(x) = 3x^3 + x^2 + 2x + 4$ .

Provare che un campo  $K$  non possiede divisori dello zero, ossia è un dominio di integrità.

Scrivere sotto forma di successioni i seguenti polinomi di  $\mathbb{Q}[x]$ , e sommarli e moltiplicarli tra di loro:

- $f(x) = x^6 - 4x^3 + x - 2$ .
- $g(x) = x^4 + 5x^3 - 6x^2 + x + 1$ .

Stesso esercizio del punto precedente, pensando però i polinomi con coefficienti in  $\mathbb{Z}_3$ .

Quanti sono i polinomi di secondo grado su  $\mathbb{Z}_2$ ? e su  $\mathbb{Z}_3$ ?

Quanti sono i polinomi di terzo grado su  $\mathbb{Z}_2$ ? e su  $\mathbb{Z}_3$ ?

## 2 INTERI E POLINOMI A CONFRONTO

Come avevamo preannunciato, molte delle definizioni e proprietà degli interi si possono estendere ai polinomi a coefficienti in un campo.

**PROPOSIZIONE 6.2 (DIVISIONE TRA POLINOMI)** Sia  $K$  un campo e siano  $f(x)$ ,  $g(x) \in K[x]$  due polinomi, con  $g(x) \neq 0$ . Allora esistono, e sono univocamente individuati, due polinomi  $q(x)$  (quoziente) e  $r(x)$  (resto) in  $K[x]$  tali che

$$f(x) = g(x) \cdot q(x) + r(x) \quad \partial r(x) < \partial g(x) \quad \text{oppure} \quad r(x) = 0.$$

**DIMOSTRAZIONE.** Lasciamo la dimostrazione di questo teorema negli esercizi (cfr. eserc. 8). Notiamo solamente che, mentre l'analogo teorema per gli interi era stato dimostrato per induzione sull'intero  $a$  che volevamo dividere (se  $a \geq 0$ ) (e il caso  $a < 0$  si riconduceva al caso positivo), nel caso dei polinomi la dimostrazione si fa sempre per induzione, ma sul grado di  $f(x)$  che è un intero maggiore o uguale a zero.  $\diamond$

### Esempio 6.2

Dividere il polinomio  $f(x) = x^3 - 4x^2 + 1$  per il polinomio  $g(x) = x^2 + 1$ .

$$\begin{array}{r} x^3 & -4x^2 & +1 \\ x^3 & & \\ \hline 0 & -4x^2 & -x & +1 \\ & -4x^2 & & -4 \\ & & -x & +5 \end{array}$$

Cioè  $x^3 - 4x^2 + 1 = (x^2 + 1)(x - 4) + (-x + 5)$ . Il quoziente è  $x - 4$  e il resto è  $-x + 5$ .

**OSSERVAZIONE** Abbiamo insistito nel confrontare interi con polinomi a coefficienti in un campo. Infatti la possibilità di dividere tra loro due polinomi (di cui il secondo non nullo) vale solo per polinomi a coefficienti in un campo: infatti se lavoriamo in  $\mathbb{Z}[x]$ , per esempio, non si può dividere  $x^3 - 3x + 1$  per il polinomio  $2x^2 + 1$ : facendo la divisione otterremmo un polinomio a coefficienti in  $\mathbb{Q} \setminus \mathbb{Z}$ . Per potere asserire che dati comunque due polinomi (il secondo dei quali diverso dal polinomio nullo) questi si possano dividere tra di loro è essenziale che i coefficienti varino in un campo.

**DEFINIZIONE 6.4** Si dice che un polinomio  $g(x) \in K[x]$  divide un polinomio  $f(x) \in K[x]$ , e si scrive  $g(x) | f(x)$ , se esiste un  $q(x) \in K[x]$  tale che  $f(x) = g(x) \cdot q(x)$ .  $\blacksquare$

**DEFINIZIONE 6.5** Un elemento  $f(x)$  in  $K[x]$  si dice invertibile se esiste un polinomio  $g(x)$  in  $K[x]$  tale che  $f(x)g(x) = 1$ .  $\blacksquare$

È ovvio, date le relazioni tra i gradi di un prodotto e quelli dei singoli fattori, che gli unici elementi invertibili di  $K[x]$  sono le costanti non nulle (cioè gli elementi non nulli del campo  $K$ ).

I polinomi invertibili, a seconda della scelta del campo  $K$ , sono quindi i seguenti:

$K$	polinomi invertibili su $K$
$\mathbb{C}$	numeri complessi non nulli
$\mathbb{R}$	numeri reali non nulli
$\mathbb{Q}$	numeri razionali non nulli
$\mathbb{Z}_2$	classi modulo 2 diverse da zero, cioè $\bar{1}$
$\mathbb{Z}_3$	classi modulo 3 diverse da zero, cioè $\bar{1}, \bar{2}$
$\mathbb{Z}_5$	classi modulo 5 diverse da zero, cioè $\bar{1}, \bar{2}, \bar{3}, \bar{4}$

**DEFINIZIONE 6.6** Due elementi  $f(x)$  e  $g(x) \in K[x]$  si dicono associati se esiste un elemento invertibile  $u$  di  $K[x]$  tale che  $f(x) = g(x) \cdot u$ .  $\blacksquare$

### Esempio 6.3

Per esempio, il polinomio  $3x^3 + 5x^2 + 2x + 6$  è associato in  $\mathbb{Z}_7[x]$  sia al polinomio  $2x^3 + x^2 + 6x + 4$  sia al polinomio  $x^3 + 4x^2 + 3x + 2$ : infatti  $2x^3 + x^2 + 6x + 4 = 3(3x^3 + 5x^2 + 2x + 6)$  e  $x^3 + 4x^2 + 3x + 2 = 5(3x^3 + 5x^2 + 2x + 6)$  in  $\mathbb{Z}_7[x]$  e 3 e 5 sono entrambi invertibili in  $\mathbb{Z}_7$ .

La relazione di "essere associati" è una relazione d'equivalenza e in ogni classe di polinomi tra loro associati se ne può sempre scegliere uno monico, tale cioè che il suo coefficiente direttivo sia uguale ad 1. Per esempio,  $3x^3 + 30x^2 - 12x + 3$  in  $\mathbb{Q}[x]$  è associato al polinomio monico  $x^3 + 10x^2 - 4x + 1$ . Così, nell'esempio precedente, il polinomio monico associato a  $3x^3 + 5x^2 + 2x + 6$  in  $\mathbb{Z}_7[x]$  è  $x^3 + 4x^2 + 3x + 2$ .

**DEFINIZIONE 6.7** Siano  $f(x)$  e  $g(x)$  due polinomi appartenenti a  $K[x]$  e non entrambi nulli. Si definisce massimo comun divisore tra  $f(x)$  e  $g(x)$ , e si indica con  $MCD(f(x), g(x))$  o semplicemente con  $(f(x), g(x))$ , un polinomio  $d(x) \in K[x]$  tale che

- (a)  $d(x) \mid f(x)$ ,  $d(x) \mid g(x)$ ,  
 (b) se  $d'(x) \mid f(x)$ ,  $d'(x) \mid g(x)$ , allora  $d'(x) \mid d(x)$ .

Siano  $d(x)$  e  $\tilde{d}(x)$  due elementi che rispondano entrambi alla definizione di massimo comun divisore tra  $f(x)$  e  $g(x)$ . È facile vedere che essi sono associati. Allora si può (per convenzione) dire che il massimo comun divisore tra  $f(x)$  e  $g(x)$  è l'unico massimo comun divisore monico.

Valgono per il MCD tra polinomi gli stessi algoritmi che valevano per gli interi: in particolare l'analogo dell'algoritmo euclideo delle divisioni successive, che garantisce l'esistenza del MCD tra due polinomi non entrambi nulli.

- *L'algoritmo euclideo delle divisioni successive per la ricerca del MCD.*

Siano  $f(x)$  e  $g(x)$  polinomi di  $\mathbb{K}[x]$ , non entrambi nulli. Si svolgano le seguenti divisioni:

$$\begin{array}{ll} f(x) = g(x)q_0(x) + r_0(x) & \partial r_0(x) < \partial g(x) \\ g(x) = r_0(x)q_1(x) + r_1(x) & \partial r_1(x) < \partial r_0(x) \\ \dots & \\ r_i(x) = r_{i+1}(x)q_{i+2}(x) + r_{i+2}(x) & \partial r_{i+2}(x) < \partial r_{i+1}(x) \\ \dots & \\ r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x) & \partial r_n(x) < \partial r_{n-1}(x) \\ r_{n-1}(x) = r_n(x)q_{n+1}(x) + 0 & \end{array}$$

Ebbene, con una dimostrazione identica a quella svolta nel caso degli interi (cfr. par. 3 del cap. 3), l'ultimo resto non nullo rappresenta il MCD tra  $f(x)$  e  $g(x)$ .

- *L'identità di Bézout*

Siano  $f(x)$  e  $g(x)$  polinomi in  $\mathbb{K}[x]$ : detto  $d(x)$  il loro massimo comun divisore, esistono  $h(x)$  e  $k(x)$  in  $\mathbb{K}[x]$  tali che

$$d(x) = h(x)f(x) + k(x)g(x).$$

Si dimostra allo stesso modo dell'analogo risultato per gli interi (cfr. par. 5 del cap. 3).

**DEFINIZIONE 6.8** Due polinomi  $f(x)$  e  $g(x)$  si dicono coprimi o relativamente primi se  $\text{MCD}(f(x), g(x)) = 1$ .

**DEFINIZIONE 6.9** Un polinomio  $f(x)$  in  $\mathbb{K}[x]$  che non sia il polinomio nullo e non sia invertibile si dice irriducibile su  $\mathbb{K}$  se

$$f(x) = g(x)h(x), \quad g(x), h(x) \in \mathbb{K}[x] \implies g(x) \text{ o } h(x) \text{ è invertibile}.$$

Se non è irriducibile, il polinomio si dice riducibile.

Possiamo quindi dire che un polinomio è irriducibile su un campo  $\mathbb{K}$  se, ogni volta che si fattorizza, uno dei due fattori è una costante non nulla.

**DEFINIZIONE 6.10** Un polinomio  $f(x)$  in  $\mathbb{K}[x]$  che non sia il polinomio nullo e non sia invertibile si dice primo se ogni volta che  $f(x)$  divide un prodotto  $g(x)h(x)$  (con  $g(x)$  e  $h(x)$  in  $\mathbb{K}[x]$ ), allora divide uno dei due fattori.

La dimostrazione della proposizione seguente è pressoché identica a quella fatta negli interi.

**PROPOSIZIONE 6.3** *Un polinomio in  $\mathbb{K}[x]$  è irriducibile se e solo se è primo.*

Vale un teorema di fattorizzazione unica, analogo a quello degli interi. Anche in questo caso si invita lo studente a ripercorrere la dimostrazione fatta, adattandola alla situazione attuale.

**TEOREMA 6.1 (FATTORIZZAZIONE UNICA)** *Ogni polinomio  $f(x)$  di grado  $\geq 1$  in  $\mathbb{K}[x]$  si fattorizza in un prodotto di un numero finito di polinomi irriducibili. Tale fattorizzazione è unica nel senso che se*

$$f(x) = p_1(x)p_2(x) \cdots p_s(x) = q_1(x)q_2(x) \cdots q_t(x),$$

$p_i(x), q_j(x)$  irriducibili in  $\mathbb{K}[x]$ , allora  $s = t$  ed esiste una corrispondenza biunivoca tra  $\{p_1(x), p_2(x), \dots, p_s(x)\}$  e  $\{q_1(x), q_2(x), \dots, q_t(x)\}$  tale che se  $q_j(x)$  corrisponde a  $p_i(x)$ , allora  $p_i(x)$  è associato a  $q_j(x)$ .

Concludiamo questo paragrafo con uno schema riassuntivo del parallelismo tra molte proprietà degli interi e quelle dei polinomi.

$(\mathbb{Z}, +, \cdot)$	$(\mathbb{K}[x], +, \cdot)$
È un dominio di integrità $ab = 0 \implies a = 0 \text{ o } b = 0$	È un dominio di integrità $f(x)g(x) = 0 \implies f(x) = 0 \text{ o } g(x) = 0$
Divisione tra interi $a = bq + r, 0 \leq r <  b $	Divisione tra polinomi $f(x) = g(x)q(x) + r(x), r = 0 \text{ oppure } 0 \leq \partial r(x) < \partial g(x)$
Dimostrazione per induzione su $a$ , se $a \geq 0$ e per $a < 0$ ci si riduce al caso $a > 0$	Dimostrazione per induzione su $\partial f(x)$
Divisibilità tra interi $a \mid b$ se $\exists c$ tale che $b = ac$ . Cioè il resto della divisione di $b$ per $a$ è nullo.	Divisibilità tra polinomi $f(x) \mid g(x)$ se $\exists h(x)$ tale che $g(x) = f(x)h(x)$ . Il resto della divisione di $g(x)$ per $f(x)$ è il polinomio nullo
Interi invertibili $a$ invertibile in $\mathbb{Z}$ se $\exists b \in \mathbb{Z}$ tale che $ab = 1$ Gli elementi invertibili in $\mathbb{Z}$ sono $\pm 1$	Polinomi invertibili $f(x)$ invertibile in $\mathbb{K}[x]$ se $\exists b \in \mathbb{K}[x]$ tale che $f(x)b(x) = 1$ . Gli elementi invertibili in $\mathbb{K}[x]$ sono gli elementi non nulli di $\mathbb{K}$ (costanti $\neq 0$ )
Interi associati $a$ è associato a $b$ se $\exists u$ invertibile tale che $a = b \cdot u$ da cui $a = \pm b$	Polinomi associati $f(x)$ è associato a $g(x)$ se $\exists u(x)$ invertibile tale che $f(x) = g(x) \cdot u(x)$ , cioè $f(x) = g(x)k, k \in \mathbb{K} \setminus \{0\}$

$(\mathbb{Z}, +, \cdot)$	$(\mathbb{K}[x], +, \cdot)$
MCD( $a, b$ ) Esiste il MCD tra due qualunque interi non entrambi nulli	MCD( $f(x), g(x)$ ) Esiste il MCD tra due qualunque polinomi non entrambi nulli
Algoritmo euclideo per interi Permette di trovare MCD tra interi	Algoritmo euclideo per polinomi Permette di trovare MCD tra polinomi
Identità di Bézout Il MCD $d$ tra $a$ e $b$ è esprimibile come $d = \alpha a + \beta b$ , $\alpha, \beta \in \mathbb{Z}$	Identità di Bézout Il MCD $d(x)$ tra $f(x)$ e $g(x)$ è esprimibile come $d(x) = \alpha(x)f(x) + \beta(x)g(x)$ , $\alpha(x), \beta(x) \in \mathbb{K}[x]$
Elementi irriducibili in $\mathbb{Z}$ $p \neq 0$ e non invertibile è irriducibile se $p = ab \implies a$ o $b$ invertibili	Elementi irriducibili su $\mathbb{K}$ in $\mathbb{K}[x]$ $p(x) \neq 0$ e non invertibile è irriducibile su $\mathbb{K}$ se $p(x) = f(x)g(x) \implies f(x)$ o $g(x)$ invertibili
Elementi primi in $\mathbb{Z}$ $p$ primo in $\mathbb{Z}$ se $[p ab \implies p a$ o $p b]$	Elementi primi in $\mathbb{K}[x]$ $p(x)$ primo in $\mathbb{K}[x]$ se $[p(x) f(x)g(x) \implies p(x) f(x)$ o $p(x) g(x)]$
Equivalenza irriducibile-primo in $\mathbb{Z}$	Equivalenza irriducibile-primo in $\mathbb{K}[x]$
Teorema di fattorizzazione unica Ogni intero non nullo e non invertibile ha una fattorizzazione (unica) in irriducibili (o primi)	Teorema di fattorizzazione unica Ogni polinomio non nullo e non invertibile ha una fattorizzazione (unica) in irriducibili (o primi)

Fin qui le somiglianze tra il comportamento degli interi rispetto al comportamento dei polinomi a coefficienti in un campo. Ora però le strade si dividono, perché i polinomi hanno una proprietà che gli interi non hanno: possiedono delle *radici*. A partire da questo punto quindi quello che diremo è strettamente di competenza dei polinomi e non più degli interi.

**DEFINIZIONE 6.11** Sia  $f(x) \in \mathbb{K}[x]$ . Un elemento  $\alpha \in \mathbb{K}$  tale che  $f(\alpha) = 0$  (cioè tale che per  $x = \alpha$  l'elemento  $f(\alpha) \in \mathbb{K}$  è lo zero di  $\mathbb{K}$ ) si dice *radice* o *zero* di  $f(x)$ .  $\diamond$

Per esempio 1 è una radice del polinomio  $f(x) = x^3 - 2x + 1 \in \mathbb{Q}[x]$  perché  $f(1) = 1^3 - 2 \cdot 1 + 1 = 0$ .

**TEOREMA 6.2 (DI RUFFINI.)** Se  $f(x) \in \mathbb{K}[x]$  e  $\alpha \in \mathbb{K}$  è tale che  $f(\alpha) = 0$ , allora  $(x - \alpha) | f(x)$ .

**DIMOSTRAZIONE.** Dividendo  $f(x)$  per  $(x - \alpha)$ , si ha

$$(2.1) \quad f(x) = (x - \alpha)q(x) + r(x), \quad \partial r(x) < \partial(x - \alpha) = 1.$$

Quindi  $r(x)$  deve essere un elemento  $r$  di  $\mathbb{K}$ . Valutando la (2.1) per  $x = \alpha$ , si ottiene  $f(\alpha) = 0 = (\alpha - \alpha)q(\alpha) + r$ , da cui segue che la costante  $r$  è uguale a zero, cioè  $f(x)$  è divisibile per  $x - \alpha$ .  $\diamond$

Il Teorema di Ruffini ci dice che se  $\alpha$  è una radice per  $f(x)$ , allora  $x - \alpha$  divide  $f(x)$ . Ha senso allora la seguente definizione, che precisa un concetto che avevamo già introdotto (cfr. par. 4 del cap. 2 a proposito delle equazioni caratteristiche).

**DEFINIZIONE 6.12** Una radice  $\alpha \in \mathbb{K}$  di  $f(x) \in \mathbb{K}[x]$  si dice *semplice* se  $(x - \alpha) | f(x)$  ma  $(x - \alpha)^2 \nmid f(x)$ . Si dice di *molteplicità*  $m$  se  $(x - \alpha)^m | f(x)$ , ma  $(x - \alpha)^{m+1} \nmid f(x)$ . Una radice con molteplicità  $m > 1$  si dice *multipla*.  $\blacksquare$

**PROPOSIZIONE 6.4** Sia  $\mathbb{K}$  un campo e  $f(x)$  un polinomio non nullo in  $\mathbb{K}[x]$  di grado  $n$ . Allora  $f(x)$  ammette al più  $n$  radici in  $\mathbb{K}$ , contate con la loro molteplicità.

**DIMOSTRAZIONE.** Rimandiamo la dimostrazione all'esercizio 9.  $\diamond$

**OSSERVAZIONE** La proposizione è valida anche se il polinomio anziché essere a coefficienti in un campo è a coefficienti in un dominio di integrità, come per esempio in  $\mathbb{Z}$ . Se invece il polinomio è a coefficienti in un anello che *non* è un dominio di integrità la proposizione non è più vera. Per esempio il polinomio di secondo grado  $x^2 + 7$ , pensato come polinomio a coefficienti in  $\mathbb{Z}_8$ , ha 4 radici: 1, 3, 5, 7.

### Esercizi

• Provare per induzione sul grado di  $f(x)$  la proposizione 6.2.

• Provare la proposizione 6.4.

• Si determinino i MCD delle seguenti coppie di polinomi a coefficienti in  $\mathbb{Q}$ :

$$(x^4 + x - 1, x^3 - 2)$$

$$(x^5 - x^3 + x^2 - 2x + 1, x^4 + x^3 + 2x^2 + x + 1)$$

e della seguente a coefficienti in  $\mathbb{Z}_7$ :

$$(x^3 + x^2 - 6x + 1, x^4 - 2x^3 - 2x - 1).$$

• Si determinino  $h(x)$  e  $k(x)$  in  $\mathbb{Q}[x]$ , se esistono, tali che

$$h(x)(x^2 + 1) + k(x)(x^3 - 3) = 20.$$

• Determinare un Massimo Comun Divisore  $d(x)$  fra i polinomi  $p(x) = x^4 + x^3 + 2x^2 + x + 1$  e  $q(x) = x^5 + x^3 + x^2 + 1$ . Determinare almeno due polinomi  $r(x)$  ed  $s(x)$  tali che  $d(x) = p(x)r(x) + q(x)s(x)$ .

• Determinare un Massimo Comun Divisore  $d(x)$  fra i polinomi  $p(x) = x^4 + x^3 + 2x^2 + x + 1$  e  $q(x) = 1/2x^5 + 1/2x^3 + 1/2x^2 + 1/2$ . Determinare almeno due polinomi  $r(x)$  ed  $s(x)$  tali che  $d(x) = p(x)r(x) + q(x)s(x)$ .

### ■ 3 POLINOMI IRRIDUCIBILI SU $\mathbb{C}$ E SU $\mathbb{R}$ E LORO CARATTERIZZAZIONE

Nel caso degli interi abbiamo parlato di elementi irriducibili (o numeri primi) e abbiamo visto alcuni criteri di primalità. Ci accingiamo ad esaminare lo stesso problema per i polinomi. Innanzitutto ricordiamo che nel caso dei polinomi non si può parlare semplicemente di riducibilità o irriducibilità: occorre precisare *su quale campo*.

Infatti dalla definizione 6.9 appare chiaro che la nozione di irriducibilità di un polinomio *dipende dal campo  $K$* . Per esempio, il polinomio  $x^2 - 5$  (che è a coefficienti in  $\mathbb{Q}$ , e quindi anche in  $\mathbb{R}$ ) è riducibile su  $\mathbb{R}$ , perché  $x^2 - 5 = (x + \sqrt{5})(x - \sqrt{5})$ , essendo  $x + \sqrt{5}$  e  $x - \sqrt{5}$  polinomi a coefficienti in  $\mathbb{R}$ , mentre è irriducibile su  $\mathbb{Q}$ , dato che  $\sqrt{5} \notin \mathbb{Q}$  e quindi  $x \pm \sqrt{5} \notin \mathbb{Q}[x]$ .

Partiamo dalla riducibilità o irriducibilità di un polinomio quando  $K$  è uguale a  $\mathbb{C}$  o  $\mathbb{R}$ .

#### Polinomi irriducibili su $\mathbb{C}$

Ricordiamo che (cfr. proposizione 6.4) il numero di radici di un polinomio a coefficienti in un campo  $K$  è minore o uguale al grado del polinomio. Ci sono casi in cui un polinomio ammette in  $K$  meno radici del suo grado: per esempio, il polinomio  $x^2 - 3$  non ammette in  $\mathbb{Q}$  radici (pur avendo grado 2). Su  $\mathbb{R}$  invece lo stesso polinomio ammette due radici, cioè tante quante il suo grado. Il polinomio  $x^2 + 1$  non ammette su  $\mathbb{R}$  nessuna radice. Supponiamo ora di lavorare nel campo  $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}, i^2 = -1\}$  dei numeri complessi, rispetto alle operazioni

$$(a + ib) + (c + id) = (a + c) + i(b + d), \quad (a + ib) \cdot (c + id) = (ac - bd) + i(ad + bc).$$

In questo caso *ogni* polinomio ammette esattamente tante radici quanto è il suo grado. È questo il contenuto del cosiddetto *Teorema Fondamentale dell'Algebra*, che è di fondamentale importanza in tutta la matematica. Di tale teorema esistono diverse dimostrazioni che utilizzano di volta in volta vari settori della matematica, ma noi ce ne asteniamo, non avendo sufficienti strumenti.

#### TEOREMA 6.3 (TEOREMA FONDAMENTALE DELL'ALGEBRA.)

Ogni polinomio  $f(x) \in \mathbb{C}[x]$  di grado  $n$  ammette in  $\mathbb{C}$  esattamente  $n$  radici.

In virtù del teorema di Ruffini ciò significa che su  $\mathbb{C}$  ogni polinomio  $f(x)$  si fattorizza in fattori *lineari*: se  $n$  è il grado del polinomio, dette  $\alpha_1, \alpha_2, \dots, \alpha_n$  le sue radici (eventualmente coincidenti), si ha

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

Possiamo così concludere con la seguente *caratterizzazione dei polinomi irriducibili su  $\mathbb{C}$* :

Tutti e soli i polinomi in  $\mathbb{C}[x]$  irriducibili su  $\mathbb{C}$  sono i polinomi di grado 1.

#### Polinomi irriducibili su $\mathbb{R}$

Passiamo ora a studiare i polinomi irriducibili su  $\mathbb{R}$ .

Sia  $f(x)$  un polinomio appartenente a  $\mathbb{R}[x]$ , di grado  $> 1$ . Sia  $\alpha = a + ib \in \mathbb{C}$  una radice di  $f(x)$  pensato come polinomio a coefficienti complessi ( $\alpha$  esiste per il

*Teorema Fondamentale dell'Algebra*). Ora, essendo  $f(x)$  a coefficienti reali, anche il numero  $\bar{\alpha} = a - ib$  complesso coniugato di  $\alpha$  è radice del polinomio  $f(x)$ . Sia infatti  $f(x) = \sum_{k=0}^n a_k x^k$ ; allora  $0 = f(\alpha) = \sum_{k=0}^n a_k \alpha^k$ , da cui, coniugando entrambi i membri, e osservando che i numeri reali sono autoconiugati,

$$0 = \bar{0} = \overline{f(\alpha)} = \overline{\sum_{k=0,n} a_k \alpha^k} = \sum_{k=0}^n a_k \bar{\alpha}^k = f(\bar{\alpha})$$

cioè  $\bar{\alpha}$  è radice anch'essa di  $f(x)$ .

Ciò premesso, supponiamo  $f(x)$  (di grado  $> 1$ ) irriducibile su  $\mathbb{R}$ . Allora non avrà radici reali. La sua fattorizzazione in fattori lineari su  $\mathbb{C}$  sarà pertanto

$$f(x) = a_n(x - \alpha_1)(x - \bar{\alpha}_1)(x - \alpha_2)(x - \bar{\alpha}_2) \cdots (x - \alpha_t)(x - \bar{\alpha}_t)$$

con  $\deg f(x) = n = 2t$ . Ora,  $\forall i = 1, \dots, t$   $(x - \alpha_i)(x - \bar{\alpha}_i) = x^2 - (\alpha_i + \bar{\alpha}_i)x + \alpha_i \bar{\alpha}_i$ ,  $\alpha_i + \bar{\alpha}_i, \alpha_i \bar{\alpha}_i \in \mathbb{R}$  è un polinomio a coefficienti reali, quindi  $f(x)$  si scrive come prodotto di  $t$  polinomi di secondo grado a coefficienti reali. Essendo per ipotesi  $f(x)$  irriducibile su  $\mathbb{R}$ , tali fattori si dovranno ridurre ad uno solamente, quindi  $f(x)$  è necessariamente di secondo grado e privo di radici reali (cioè si tratta di un polinomio di secondo grado con discriminante  $\Delta < 0$ ). Dato che ovviamente un polinomio di secondo grado privo di radici reali è irriducibile, possiamo concludere dicendo:

Tutti e soli i polinomi in  $\mathbb{R}[x]$  irriducibili su  $\mathbb{R}$  sono i polinomi di primo grado e quelli di secondo grado con  $\Delta < 0$ .

**OSSERVAZIONE** Abbiamo messo in corsivo la parola *secondo grado*, perché il fatto di essere privo di radici nel campo  $K$  non comporta che il polinomio sia irriducibile.

Per esempio, il polinomio a coefficienti reali  $x^4 + 6x^2 + 5$  è privo di radici reali, perché, per ogni  $x$ , è maggiore di zero, ma è fattorizzabile al modo seguente:  $x^4 + 6x^2 + 5 = (x^2 + 1)(x^2 + 5)$ .

Quando però il polinomio  $f(x) \in \mathbb{R}[x]$  è di grado 2 o 3, allora la mancanza di radici nel campo  $\mathbb{R}$  assicura la irriducibilità di  $f(x)$ . Infatti, se  $f(x)$  si fattorizzasse, uno almeno dei suoi fattori sarebbe di grado 1, e questo comporterebbe (in base al teorema di Ruffini) l'esistenza di una radice in  $\mathbb{R}$ .

Riassumendo, qualunque sia il campo  $K$ , se un polinomio  $f(x)$  di grado  $> 1$  a coefficienti in un campo  $K$  possiede una radice in  $K$ , allora  $f(x)$  è fattorizzabile (un fattore è lineare). Tuttavia un polinomio può essere fattorizzabile anche se non possiede nessuna radice nel campo (ad eccezione dei polinomi di grado 2 o 3 per i quali l'esistenza di una radice equivale alla riducibilità).

**OSSERVAZIONE** Abbiamo caratterizzato i polinomi irriducibili su  $\mathbb{C}$  e su  $\mathbb{R}$ . Sappiamo quindi per esempio che un polinomio di terzo grado su  $\mathbb{R}$  è sicuramente riducibile, ma non per questo ne conosciamo la fattorizzazione in irriducibili (che pure sappiamo esistere ed essere unica in virtù del Teorema Fondamentale dell'Aritmetica). Questo è tutto un altro problema (equivalente al fatto che sapere che un intero non è primo non ci fornisce la sua fattorizzazione).

## ■ 4 RIDUCIBILITÀ E IRRIDUCIBILITÀ DI POLINOMI SU $\mathbb{Q}$

Abbiamo caratterizzato i polinomi irriducibili su  $\mathbb{C}$  e su  $\mathbb{R}$ . Non saremo in grado di fare altrettanto per  $\mathbb{Q}$ . Dovremo accontentarci di stabilire alcuni criteri che ci permettano di dire se un dato polinomio è irriducibile su  $\mathbb{Q}$  e dare indicazioni per affrontare il problema della irriducibilità su  $\mathbb{Q}$  di un polinomio.

Premettiamo alcuni lemmi, dai quali vedremo come la fattorizzazione di un polinomio su  $\mathbb{Q}$  sia strettamente collegata alla sua fattorizzazione su  $\mathbb{Z}$ . Questo stretto legame è dovuto al fatto che  $\mathbb{Q}$  è il campo dei quozienti di  $\mathbb{Z}$ , ossia ogni elemento di  $\mathbb{Q}$  è quoziante di due elementi di  $\mathbb{Z}$  (di cui il secondo diverso da 0) (cfr. cap. 11).

Per studiare la fattorizzazione di polinomi a coefficienti in  $\mathbb{Q}$  dovremo considerare polinomi a coefficienti in  $\mathbb{Z}$  e studiarne alcune proprietà. Si noti che finora abbiamo definito solo polinomi a coefficienti in un campo  $\mathbb{K}$  e abbiamo dimostrato molte loro proprietà. Nessuno ci vieta tuttavia di definire anche polinomi a coefficienti in un anello commutativo con unità (come  $\mathbb{Z}$ ). L'importante è non pretendere che valgano per tali polinomi i risultati che valevano per il caso in cui i coefficienti appartenevano ad un campo.

**LEMMA 6.4** Sia  $f(x) \in \mathbb{Q}[x]$ . Allora  $f(x) = \frac{d}{m} f^*(x)$  dove  $f^*(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ ,  $(a_0, a_1, \dots, a_n) = 1$  e  $d, m \in \mathbb{Z}$ ,  $(d, m) = 1$ .

**DIMOSTRAZIONE.** Sia  $f(x) = q_0 + q_1 x + q_2 x^2 + \dots + q_n x^n$ ,  $q_i = b_i/c_i \in \mathbb{Q} \forall i$ , e  $b_i, c_i \in \mathbb{Z}$ . Quindi  $f(x) = \frac{b_0}{c_0} + \frac{b_1}{c_1} x + \dots + \frac{b_n}{c_n} x^n$ . Indicato con  $m'$  il mcm( $c_0, c_1, \dots, c_n$ ), il polinomio  $m'f(x) = b'_0 + b'_1 x + \dots + b'_n x^n$  è un polinomio a coefficienti interi. Posto  $d' = \text{MCD}(b'_0, b'_1, \dots, b'_n)$ , risulterà  $m'f(x) = d'(a_0 + a_1 x + \dots + a_n x^n)$  con  $a_i \in \mathbb{Z}$  e  $\text{MCD}(a_0, a_1, \dots, a_n) = 1$ . Dividendo, se necessario, per il MCD( $d', m'$ ) entrambi i membri, si ottiene  $mf(x) = d \sum_{i=0}^n a_i x^i$  che è la relazione richiesta.  $\diamond$

Il lemma dice che ogni polinomio a coefficienti in  $\mathbb{Q}$  si può scrivere come prodotto di un opportuno numero razionale  $\frac{d}{m}$  per un polinomio a coefficienti interi e coprimi tra di loro.

**DEFINIZIONE 6.13** Sia  $f(x) \in \mathbb{Z}[x]$ . Si definisce *divisore* o *contenuto* di  $f(x)$  il massimo comun divisore dei suoi coefficienti.  $\blacksquare$

**DEFINIZIONE 6.14** Un polinomio  $f(x) = \sum_{k=0}^n a_k x^k \in \mathbb{Z}[x]$  si dice *primitivo* se il massimo comun divisore dei suoi coefficienti (cioè il suo contenuto) è 1.  $\blacksquare$

Il lemma precedente mostra che ogni polinomio  $f(x) \in \mathbb{Q}[x]$  si può scrivere come prodotto di un opportuno numero razionale per un polinomio a coefficienti in  $\mathbb{Z}$  primitivo: quindi esiste un polinomio  $f^*(x) \in \mathbb{Z}[x]$  e primitivo associato in  $\mathbb{Q}[x]$  a  $f(x)$ .

### Esempio 6.4

Sia  $f(x) = \frac{5}{3} + \frac{4}{5}x - \frac{3}{7}x^2$ . Allora  $m' = \text{mcm}(3, 5, 7) = 105$  e  $105f(x) = 175 + 84x - 45x^2$ . Si tratta di un polinomio primitivo dato che  $\text{MCD}(175, 84, 45) = 1$ . Quindi il polinomio primitivo associato a  $f(x) = \frac{5}{3} + \frac{4}{5}x - \frac{3}{7}x^2$  è  $f^*(x) = 105f(x) = 175 + 84x - 45x^2$ .

Quanto ora detto ci permette di concludere che, quando si è interessati alla fattorizzazione di un polinomio  $f(x)$  a coefficienti in  $\mathbb{Q}$ , si può sempre supporre che il polinomio sia a coefficienti interi (primitivo o no a seconda dei casi).

Vale il seguente risultato, che non è assolutamente ovvio.

**LEMMA 6.5 (DI GAUSS.)** Il prodotto di due polinomi primitivi è ancora un polinomio primitivo.

**DIMOSTRAZIONE.** Rimandiamo all'esercizio 14.  $\diamond$

**COROLLARIO 6.6** Il contenuto del prodotto di due polinomi  $f(x)$  e  $g(x)$  uguaglia il prodotto dei contenuti dei due polinomi fattori.

**DIMOSTRAZIONE.** Basta estrarre il contenuto da  $f$  e  $g$  e ricordare che il prodotto di polinomi primitivi è un polinomio primitivo.  $\diamond$

**TEOREMA 6.7 (DI GAUSS.)** Se un polinomio  $f(x) \in \mathbb{Z}[x]$  si decompone nel prodotto di due polinomi a coefficienti razionali, allora si decompone anche nel prodotto di due polinomi degli stessi gradi a coefficienti interi.

**DIMOSTRAZIONE.** Dimostreremo il teorema supponendo che  $f(x)$  sia primitivo. Il caso in cui non sia primitivo viene lasciato negli esercizi (cfr. eserc. 15). Sia quindi  $f(x)$  primitivo e sia  $f(x) = g(x)h(x)$ ,  $g(x), h(x) \in \mathbb{Q}[x]$ . Ora, in virtù del Lemma 6.4, sarà  $g(x) = \frac{d_1}{m_1} g^*(x)$  e  $h(x) = \frac{d_2}{m_2} h^*(x)$ , con  $g^*(x), h^*(x) \in \mathbb{Z}[x]$  primitivi e  $d_1$  e  $m_1$  interi. In definitiva,  $f(x) = (d/m)g^*(x)h^*(x)$ ,  $d = d_1 d_2$ ,  $m = m_1 m_2$ . In virtù del Lemma di Gauss, il polinomio  $f^*(x) = g^*(x)h^*(x)$  è primitivo, e risulta

$$(4.1) \quad mf(x) = df^*(x), \quad f(x) \text{ e } f^*(x) \text{ primitivi.}$$

I due polinomi del primo e secondo membro devono avere lo stesso contenuto: ma questo è rispettivamente  $m$  e  $d$  (essendo  $f(x)$  e  $f^*(x)$  primitivi). Quindi  $m = d$  e la (4.1) diventa  $f(x) = g^*(x)h^*(x)$  che è una fattorizzazione su  $\mathbb{Z}$  con i fattori dello stesso grado della fattorizzazione originaria su  $\mathbb{Q}$ .  $\diamond$

### Esempio 6.5

$f(x) = x^4 + 7x^2 + 10$  è un polinomio in  $\mathbb{Z}[x]$  primitivo. Risulta fattorizzabile su  $\mathbb{Q}$ , come è facile controllare, per esempio al modo seguente:  $f(x) = (\frac{1}{2}x^2 + 1)(2x^2 + 10)$ . Allora, procedendo come nel corso della dimostrazione del teorema,

$$f(x) = \frac{d_1}{m_1} g^*(x) \frac{d_2}{m_2} h^*(x) = \frac{1}{2} (x^2 + 2)(2x^2 + 5) = (x^2 + 2)(x^2 + 5),$$

che è una fattorizzazione su  $\mathbb{Z}$ .

**OSSERVAZIONE** Il teorema di Gauss ci dice che se un polinomio a coefficienti in  $\mathbb{Z}$  è fattorizzabile su  $\mathbb{Q}$ , allora esso è fattorizzabile anche su  $\mathbb{Z}$ , o, equivalentemente, se è irriducibile su  $\mathbb{Z}$ , allora è irriducibile anche su  $\mathbb{Q}$ . Sembrerebbe allora di poter

concludere che un polinomio a coefficienti in  $\mathbb{Z}$  è irriducibile su  $\mathbb{Z}$  se e solo se esso è irriducibile su  $\mathbb{Q}$ . Infatti, dato che, per esempio, un polinomio in  $\mathbb{Q}[x]$  irriducibile su  $\mathbb{R}$  è ovviamente irriducibile anche su  $\mathbb{Q}$ , si potrebbe pensare che debba valere anche la analoga proprietà che un polinomio a coefficienti in  $\mathbb{Z}$  irriducibile su  $\mathbb{Q}$  debba necessariamente essere irriducibile su  $\mathbb{Z}$ . Ma si pensi alla definizione di polinomio irriducibile: un polinomio  $f(x)$  è irriducibile se, potendosi scrivere come prodotto di due polinomi, allora uno dei due è invertibile. Allora, esaminiamo per esempio il polinomio  $f(x) = 5x^2 + 20$ : esso è irriducibile su  $\mathbb{Q}$ , perché è associato al polinomio  $x^2 + 4$ , che è chiaramente irriducibile su  $\mathbb{Q}$  (essendo di secondo grado privo di radici razionali). Tuttavia  $f(x)$  è riducibile su  $\mathbb{Z}$ , perché la fattorizzazione  $5(x^2 + 4)$  è una fattorizzazione non banale su  $\mathbb{Z}$ , perché 5 non è invertibile su  $\mathbb{Z}$ ! In altri termini, i due polinomi  $5x^2 + 20$  e  $x^2 + 4$  non sono associati in  $\mathbb{Z}[x]$ . Gli elementi invertibili di  $\mathbb{Z}[x]$  non sono le costanti non nulle, ma sono gli elementi invertibili di  $\mathbb{Z}$ , ossia  $\pm 1$ . Quindi, non sono le costanti non nulle, ma sono gli elementi invertibili di  $\mathbb{Z}$ , ossia  $\pm 1$ . Quindi, la riducibilità su  $\mathbb{Z}$  non implica la riducibilità su  $\mathbb{Q}$ ! Dato che  $\mathbb{Z}$  non è un campo, non si possono estendere a  $\mathbb{Z}[x]$  risultati del tipo: se un polinomio è riducibile su  $\mathbb{Q}$ , che è contenuto in  $\mathbb{R}$ , allora è riducibile su  $\mathbb{R}$ ; infatti  $\mathbb{Q}$  ed  $\mathbb{R}$  sono entrambi campi, l'uno contenuto nell'altro e un elemento di  $\mathbb{Q}$  è invertibile in  $\mathbb{Q}$  se e solo se è invertibile in  $\mathbb{R}$ . Si noti infine che volutamente, quando abbiamo dato (cfr. definizione 6.9) la definizione di irriducibilità di un polinomio a coefficienti in un campo, non abbiamo detto che un polinomio è irriducibile se, ogni volta che si fattorizza, uno dei due fattori è una costante non nulla (cosa che peraltro avremmo potuto fare, dato che nel caso di polinomi a coefficienti in un campo le due nozioni di polinomio invertibile e di costante non nulla coincidono). Il motivo per cui abbiamo fatto ciò è che in questo modo la definizione data si può applicare ad anelli più generali.

A questo punto però possiamo affermare:

$f(x) \in \mathbb{Z}[x]$  è primitivo e irriducibile su  $\mathbb{Z}$  se e solo se è irriducibile su  $\mathbb{Q}$ .

Infatti, nel caso in cui il polinomio sia *primitivo*, non potrà avere una fattorizzazione in cui uno dei fattori è un elemento di  $\mathbb{Z}$  diverso da  $\pm 1$ .

Per decidere la riducibilità o irriducibilità di un polinomio  $f(x) \in \mathbb{Z}[x]$  di grado  $> 1$  su  $\mathbb{Q}$  è utile innanzitutto avere un metodo che permetta di stabilire se il polinomio ha o no radici *razionali*; se le avesse, sarebbe senz'altro riducibile. La seguente proposizione ci offre una utile informazione in questo senso.

**PROPOSIZIONE 6.5** Sia  $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in \mathbb{Z}[x]$ . Sia  $\alpha = r/s$  una radice di  $f(x)$ , con  $r, s \in \mathbb{Z}$ ,  $(r, s) = 1$ . Allora  $r \mid a_0$  e  $s \mid a_n$ .

**DIMOSTRAZIONE.** Se  $\alpha = r/s$  è una radice di  $f(x)$ , risulterà  $0 = f(r/s) = a_0 + a_1(r/s) + \dots + a_n(r/s)^n$ . Moltiplicando ambo i membri per  $s^n$  si ottiene  $0 = s^n a_0 + s^{n-1} a_1 r + \dots + a_n r^n = s(s^{n-1} a_0 + s^{n-2} a_1 r + \dots + a_{n-1} r^{n-1}) + a_n r^n = s^n a_0 + r(s^{n-1} a_1 + \dots + a_n r^{n-1})$ . Dalla  $0 = s(s^{n-1} a_0 + \dots + a_{n-1} r^{n-1}) + a_n r^n$  segue che  $s \mid a_n r^n$ , e dalla  $0 = s^n a_0 + r(s^{n-1} a_1 + \dots + a_n r^{n-1})$  segue  $r \mid a_0 s^n$ . Essendo  $(r, s) = 1$ , possiamo concludere che  $s \mid a_n$  e  $r \mid a_0$ .  $\diamond$

**COROLLARIO 6.8** Se un polinomio monico a coefficienti interi ha una radice razionale, questa è un numero intero.

La proposizione ci dice che le possibili radici razionali di un polinomio  $f(x) \in \mathbb{Z}[x]$  sono da ricercarsi tra i numeri razionali della forma  $r/s$ , dove  $r$  varia tra i divisori del termine noto  $a_0$  e  $s$  tra i divisori del coefficiente direttivo  $a_n$ . Quindi la ricerca si limita ad un insieme finito.

### Esempio 6.6

Se il polinomio  $2x^3 - 5x^2 - 3$  ha radici razionali, queste devono trovarsi nel seguente insieme:  $\{\pm 1, \pm 3, \pm 1/2, \pm 3/2\}$ . Basta allora controllare se queste sono radici di  $f(x)$ . Come è facile verificare, nessuno dei numeri razionali elencati è radice di  $f(x)$ , quindi si può essere certi che  $f(x)$  non possiede radici razionali.

Esiste poi un criterio molto utile che permette direttamente dall'esame dei coefficienti di stabilire se un polinomio a coefficienti interi è irriducibile su  $\mathbb{Q}$ .

**PROPOSIZIONE 6.6 (CRITERIO DI IRRIDUCIBILITÀ DI EISENSTEIN)** Sia  $f(x) = a_0 + a_1x + \dots + a_nx^n$  un polinomio in  $\mathbb{Z}[x]$ . Sia  $p$  un numero primo tale che

- (a)  $p \nmid a_n$ ;
- (b)  $p \mid a_i \forall i = 0, \dots, n-1$ ;
- (c)  $p^2 \nmid a_0$ .

Allora  $f(x)$  è irriducibile su  $\mathbb{Q}$ .

**DIMOSTRAZIONE.** Per il Teorema di Gauss basta provare che è irriducibile su  $\mathbb{Z}$ . Supponiamo per assurdo che sia  $f(x) = g(x)h(x)$ , con  $g(x) = b_0 + b_1x + \dots + b_rx^r$ ,  $h(x) = c_0 + c_1x + \dots + c_sx^s$ , ( $b_i, c_i \in \mathbb{Z}$ ) polinomi di gradi  $r < n$  e  $s < n$ , se  $n = \deg(f)$ . Allora  $r+s = n$  e  $b_0c_0 = a_0$ ;  $p \mid a_0$ , per cui  $p \mid b_0$  o  $p \mid c_0$ . Non può dividere entrambi (altrimenti sarebbe  $p^2 \mid a_0$ ). Supponiamo quindi, per esempio, che  $p$  divida  $b_0$  ma non divida  $c_0$ . Sia  $b_i$  il coefficiente con indice più basso non diviso da  $p$  ( $p$  non può dividere tutti i  $b_i$ , altrimenti  $p$  dividerebbe tutti gli  $a_i$ , contro l'ipotesi). Allora per  $i \leq r < n$   $a_i = b_i c_0 + b_{i-1} c_1 + \dots + b_0 c_i$  da cui  $p \mid c_0$ : infatti  $p$  divide  $a_i$  ( $i < n$ ),  $p$  divide tutti i  $b_k$  con  $k = 0, \dots, i-1$ , da cui  $p$  deve dividere  $b_i c_0$ ; non potendo  $p$  dividere  $b_i$ , deve necessariamente dividere  $c_0$ . L'assurdo nasce dall'avere supposto  $f(x)$  riducibile.  $\diamond$

**OSSERVAZIONE** Si noti che il criterio di Eisenstein offre una condizione sufficiente di irriducibilità, ma non una condizione necessaria! Questo significa che un polinomio può benissimo essere irriducibile, ma che non esiste nessun primo  $p$  che soddisfi le condizioni del criterio di Eisenstein.

**OSSERVAZIONE** Attenti anche a non utilizzare il criterio di Eisenstein per vedere se un polinomio è irriducibile su  $\mathbb{Z}_p$  per qualche  $p$  primo! Il criterio vale solo per testare la irriducibilità di un polinomio a coefficienti in  $\mathbb{Z}$  su  $\mathbb{Q}$ .

Vorremo però trovare altri metodi che permettano, dato un polinomio a coefficienti interi, di decidere se si tratta di un polinomio riducibile o no su  $\mathbb{Q}$ . Un metodo possibile (che però si può utilizzare solo nei casi in cui il grado del polinomio non

è troppo elevato) è quello di cercare direttamente una fattorizzazione del polinomio dato. Se per esempio  $f(x)$  è un polinomio (che si può sempre supporre a coefficienti interi e primitivo) di grado 5 e se abbiamo preventivamente controllato che il polinomio è privo di radici razionali, allora, se  $f(x)$  si fattorizza, esso potrà fattorizzarsi solo nel prodotto di un polinomio di secondo grado per uno di terzo. Uguagliando allora i coefficienti, si ottiene un sistema, per il quale cerchiamo soluzioni *interne*, dato che, come sappiamo, ci si può sempre ridurre a una fattorizzazione in  $\mathbb{Z}[x]$ . Se il sistema è incompatibile, allora il polinomio originario è irriducibile.

### Esempio 6.7

Si provi che  $x^4 + x + 1$  è irriducibile su  $\mathbb{Q}$ .

Il polinomio non ha radici razionali, quindi si può fattorizzare solo nel prodotto di due polinomi di secondo grado. Ricordando che il coefficiente direttivo del prodotto è il prodotto dei coefficienti direttivi, e il termine noto del prodotto è il prodotto dei termini noti dei fattori, si può scrivere  $x^4 + x + 1 = (x^2 + ax \pm 1)(x^2 + bx \pm 1)$  dove, per i termini noti, verranno scelti o entrambi i segni + o entrambi i segni -. I sistemi che si ottengono uguagliando i coefficienti sono

$$\begin{cases} a+b=0 \\ ab=-2 \\ a+b=1 \end{cases} \quad \text{e} \quad \begin{cases} a+b=0 \\ ab=2 \\ a+b=-1 \end{cases}$$

nessuno dei quali ammette soluzioni intere.

Questo metodo però può diventare impraticabile non appena il grado del polinomio cresce.

Il metodo che presenteremo qui di seguito è assai utile per il controllo della irriducibilità di un dato polinomio a coefficienti interi.

#### Test di irriducibilità mod $p$

Sia  $f(x) = \sum_{i=0}^n a_i x^i$  un polinomio a coefficienti in  $\mathbb{Z}$  e primitivo. Riduciamo i coefficienti modulo un numero primo  $p$  (cioè pensiamo il polinomio  $f(x)$  in  $\mathbb{Z}_p[x]$ ). Indichiamo con  $\bar{f}(x)$  il nuovo polinomio. Ebbene, se  $p$  è scelto in modo da non dividere  $a_n$ , allora  $f(x)$  e  $\bar{f}(x)$  hanno lo stesso grado. Se  $f(x) = g(x)h(x)$ ,  $g(x)$  e  $h(x)$  in  $\mathbb{Z}[x]$ , allora risulta anche  $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ , quindi se  $f(x)$  è riducibile su  $\mathbb{Q}$ , allora è riducibile anche  $\bar{f}(x)$  in  $\mathbb{Z}_p[x]$ . Possiamo quindi concludere al modo seguente:

$f(x)$  irriducibile su  $\mathbb{Z}_p$  per qualche  $p \nmid a_n \implies f(x)$  irriducibile su  $\mathbb{Q}$

**OSSERVAZIONE** Si noti che non è vero il viceversa, cioè non è vero che se, per qualche  $p$ ,  $\bar{f}(x)$  è riducibile su  $\mathbb{Z}_p$ , allora  $f(x)$  è riducibile su  $\mathbb{Q}$ . Per esempio,  $x^4 + 1$  è irriducibile su  $\mathbb{Q}$  (si provi con il metodo con cui abbiamo provato che  $x^4 + x + 1$  è irriducibile su  $\mathbb{Q}$ ), tuttavia,  $x^4 + 1$  è riducibile su  $\mathbb{Z}_2$ , perché  $x^4 + 1 = (x^2 + 1)(x^2 + 1)$  in  $\mathbb{Z}_2[x]$ .

Il vantaggio di questo test è che si tratta di un test finito.

### Esempio 6.8

Diamo un esempio per mostrare come funziona questo metodo. Si provi che il polinomio  $5x^4 - 8x^3 + 11x - 3$  è irriducibile su  $\mathbb{Q}$ .

Pensato come polinomio a coefficienti in  $\mathbb{Z}_2$ , il polinomio è  $x^4 + x + 1$  (i coefficienti pari diventano 0 in  $\mathbb{Z}_2$ ). Ora, questo polinomio non ha radici in  $\mathbb{Z}_2$ , quindi, se si fattorizza, si fattorizza nel prodotto di due fattori di secondo grado, precisamente  $x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$ , tenendo conto del modo in cui si trovano coefficiente direttivo e termine noto del prodotto (e del fatto che siamo in  $\mathbb{Z}_2$ ). È facile vedere che questa fattorizzazione non è possibile. Quindi  $x^4 + x + 1$  è irriducibile su  $\mathbb{Z}_2$ , per cui il polinomio originario è irriducibile su  $\mathbb{Q}$ .

Avendo provato che  $x^4 + x + 1$  è irriducibile su  $\mathbb{Z}_2$  possiamo anche concludere per esempio che  $3x^4 + 20x^3 + 18x^2 + 11x + 27$  è irriducibile su  $\mathbb{Q}$ , dato che pensato come polinomio su  $\mathbb{Z}_2$  diventa proprio  $x^4 + x + 1$ .

Per comodità, riassumiamo qui di seguito i metodi visti per decidere se un polinomio è irriducibile su  $\mathbb{Q}$ , senza che questo significhi che questi sono tutti i modi possibili per affrontare questo problema, né che vadano eseguiti nell'ordine dato.

## ■ 5 METODI PER STUDIARE LA IRRIDUCIBILITÀ DI UN POLINOMIO SU $\mathbb{Q}$

- (a) Ridursi ad un polinomio  $f(x) \in \mathbb{Z}[x]$  e primitivo.
- (b) Se  $f(x)$  è di grado 2 o 3,  $f(x)$  è irriducibile su  $\mathbb{Q}$  se e solo se è privo di radici in  $\mathbb{Q}$ .
- (c) Test di esistenza di radici razionali (esistenza di radici implica la riducibilità del polinomio).
- (d) Criterio di irriducibilità di Eisenstein.
- (e) Per gradi non eccessivamente alti, fattorizzazione diretta in polinomi a coefficienti interi, combinando questo metodo col test di esistenza di radici razionali, per eliminare fattorizzazioni con un fattore lineare.
- (f) Test di irriducibilità mod  $p$ .

### Esercizi

- 1 Dimostrare il Lemma di Gauss 6.5.
- 2 Dimostrare il teorema 6.7 nel caso in cui il polinomio  $f(x)$  non sia primitivo.
- 3 Decidere se il polinomio  $3x^7 + 30x^5 + 150x^3 + 60$  è irriducibile:
  - (a) su  $\mathbb{C}$
  - (b) su  $\mathbb{R}$
  - (c) su  $\mathbb{Q}$
  - (d) su  $\mathbb{Z}_2$ .

■ Dire se il polinomio  $5x^7 + 30x^5 + 90x^3 + 60$  è irriducibile

- (a) su  $\mathbb{C}$     (b) su  $\mathbb{R}$     (c) su  $\mathbb{Q}$     (d) su  $\mathbb{Z}_2$ .

■ Scomporre il polinomio  $x^6 - 1$  in fattori irriducibili su  $\mathbb{R}$ , su  $\mathbb{Q}$ , su  $\mathbb{Z}_3$ .

■ Fattorizzare in irriducibili il polinomio di  $\mathbb{Q}[x]$ :  $x^6 - 2x^5 - 15x^3 + 36x^2 - 9x - 6$ .

■ Si consideri il polinomio  $2x^6 + 2x^5 + 15x^4 + 15x^3 + 75x + 75$ .

- Dire se è irriducibile o riducibile su  $\mathbb{C}$  e su  $\mathbb{R}$ ;
- determinare una fattorizzazione in irriducibili su  $\mathbb{Q}$ ;
- determinare una fattorizzazione in irriducibili su  $\mathbb{Z}_5$ .

■ Si considerino i polinomi di  $\mathbb{Q}[x]$   $f(x) = x^4 + x^2 + 1$  e  $g(x) = x^4 + 2x^3 + x^2 - 1$ .

- Determinare un MCD fra  $f(x)$  e  $g(x)$ ;
- dire se  $f(x)$  è irriducibile su  $\mathbb{Q}[x]$ ;
- scomporre  $g(x)$  in fattori irriducibili su  $\mathbb{Q}[x]$ .

■ Scomporre il polinomio  $x^5 - x^4 - 4x + 4$  in fattori irriducibili su  $\mathbb{Q}$ , su  $\mathbb{R}$ , su  $\mathbb{Z}_3$ .

■ Dire se il polinomio  $3x^3 + x^2 + 5x + 2$  è irriducibile rispettivamente su  $\mathbb{Q}$ , su  $\mathbb{R}$ , su  $\mathbb{Z}_5$ .

■ Fattorizzare il polinomio  $x^4 - x^3 - 7x^2 + 5x + 10$  in fattori irriducibili (a) su  $\mathbb{Q}$ ; (b) su  $\mathbb{R}$ ; (c) su  $\mathbb{Z}_5$ .

■ Fattorizzare in irriducibili il seguente polinomio di  $\mathbb{Q}[x]$ :

$$x^6 - 2x^5 - 15x^3 + 36x^2 - 9x - 6.$$

■ Scomporre in fattori irriducibili il polinomio  $x^3 - x^2 - 5x + 2$  su  $\mathbb{R}$ , su  $\mathbb{Q}$  e su  $\mathbb{Z}_5$ .

■ Dire se il polinomio  $\frac{1}{5}x^4 + 6x^3 + 15x^2 + 18x + 30$  è irriducibile rispettivamente su  $\mathbb{C}$ , su  $\mathbb{R}$  e su  $\mathbb{Q}$ .

■ Spesso ad un polinomio non è applicabile direttamente il criterio di Eisenstein. Può succedere però che modificando opportunamente il polinomio si ottenga un polinomio al quale invece si possa applicare il criterio. Tuttavia occorre essere certi che la irriducibilità del polinomio modificato sia equivalente alla irriducibilità del polinomio originario. A questo scopo ci vengono in aiuto le seguenti osservazioni.

(a) Sia  $p(x)$  un fissato polinomio in  $\mathbb{K}[x]$ . L'applicazione

$$\begin{aligned} T_p : \mathbb{K}[x] &\longrightarrow \mathbb{K}[x] \\ f(x) &\longmapsto f(p(x)) \end{aligned}$$

che sostituisce ad  $x$  il polinomio  $p(x)$  conserva le operazioni tra polinomi, cioè  $T_p(f(x) + g(x)) = T_p(f(x)) + T_p(g(x))$  e  $T_p(f(x) \cdot g(x)) = T_p(f(x)) \cdot T_p(g(x))$ .

(b) Nel caso in cui come  $p(x)$  si prenda un polinomio lineare del tipo  $x - \alpha$ , allora la  $T_p$  è biunivoca, e  $f(x)$  e il polinomio trasformato  $f(x - \alpha)$  hanno lo stesso grado. Quindi, come è facile vedere,  $f(x)$  è irriducibile su  $\mathbb{K}$  se e solo se  $f(x - \alpha)$  è irriducibile su  $\mathbb{K}$ . Analogamente risulta, per  $\alpha \neq 0$ ,  $f(x)$  è irriducibile su  $\mathbb{K}$  se e solo se  $f(x/\alpha)$  è irriducibile su  $\mathbb{K}$ . Si noti che la (a) vale anche nel caso in cui il polinomio appartenga a  $\mathbb{Z}[x]$ . Utilizzando queste proprietà, si riesce a volte a trasformare un polinomio in un nuovo polinomio al quale si può applicare il criterio di Eisenstein.

■ Servendosi dell'esercizio precedente, dimostrare che, se  $p$  è un numero primo, il polinomio  $x^{p-1} + x^{p-2} + \dots + x^2 + x + 1$  è irriducibile su  $\mathbb{Q}$ .

■ Fattorizzare il polinomio  $2x^6 + 4x^5 + 10x^4 + 16x^3 + 36x^2 + 56x + 28$  in fattori irriducibili su  $\mathbb{Q}$ ,  $\mathbb{Z}_5$ ,  $\mathbb{Z}_7$ ,  $\mathbb{R}$ .

## 6 ALGORITMI A CONFRONTO

Abbiamo già visto vari esempi di algoritmi: l'algoritmo euclideo delle divisioni successive, l'algoritmo del crivello di Eratostene, il test per vedere se un polinomio a coefficienti interi possiede radici razionali, ecc. In ogni caso un algoritmo è una successione finita di *istruzioni* che permettono di risolvere un dato problema. Per esempio, ogni ricetta di cucina è un algoritmo: prevede infatti un certo numero di istruzioni: ingredienti, dosi, procedimento, temperatura del forno, ecc. La ricetta per cucinare un dolce è quindi un algoritmo che permette in un numero finito di passi di fare per esempio una buonissima torta al cioccolato.

Tuttavia, non ogni problema è risolubile mediante un algoritmo. Un problema si dice *decidibile* se esiste un algoritmo che risolve il problema, ossia che per ogni istanza dell'input di ingresso produce la soluzione corrispondente. Un problema si dice *indecidibile* in caso contrario.

Un esempio di problema non decidibile è il cosiddetto *problema della fermata*, formulato dal matematico A. Turing nel 1937: dato un qualunque programma e dei generici dati d'ingresso, decidere se l'esecuzione del programma con quell'input termina oppure no. Noi siamo interessati allo studio dei problemi decidibili e al confronto di più algoritmi che li risolvono.

Supponiamo di dovere costruire una casa. Cominceremo a chiedere a vari ingegneri o architetti di fare un progetto. Non tutti i progetti andranno bene, ossia saranno soddisfacenti. Innanzitutto infatti devono essere *corretti*: devono rispettare le esigenze del committente, le norme di sicurezza, utilizzare certi materiali e non altri, avere la distanza di legge dalle abitazioni circostanti, ecc. Ma, anche se fossero corretti, non tutti saranno soddisfacenti per altri motivi, per esempio perché troppo costosi, oppure perché richiedono troppo tempo per essere realizzati. Confrontando tra loro i vari progetti corretti sceglieremo allora quello che ci soddisfa di più.

Così accade per gli algoritmi. Un algoritmo deve innanzitutto essere *corretto*, ossia in corrispondenza di ogni input deve produrre l'output giusto. Ma noi daremo per scontato questo punto. In secondo luogo deve essere *efficiente*. Per fare questo dovremo valutarne la complessità: *spaziale* (quantità di memoria utilizzata) o *temporale* (misurata dal numero di operazioni elementari che il processore deve eseguire). Ora, è chiaro che l'efficienza di un algoritmo è funzione della lunghezza dell'input.

Saremo interessati alla sola complessità *temporale*.

Per risolvere uno stesso problema ci possono essere vari algoritmi e qui sorge un problema di fondamentale importanza: quale tra una serie di algoritmi è migliore di un altro? Cosa significa migliore? Qui entriamo nel campo dell'*analisi degli algoritmi e della teoria della complessità*. Non intendiamo sviluppare questi argomenti, che verranno trattati in modo approfondito in appositi corsi. Ci limiteremo tuttavia ad alcune semplici considerazioni.

È importante, una volta che si sia ideato un algoritmo, esaminarne la praticabilità, ossia capire *a priori*, prima cioè di implementarlo, il tempo che impiegherà a condurre a termine il suo compito. Se per esempio si scopre che impiegherà cento anni, dovremo pensare ad un altro algoritmo più efficiente. Non ci addentreremo in questo tipo di problemi, tuttavia faremo vedere come in ogni caso occorra esprimere la complessità di un algoritmo come *funzione della dimensione dei dati di ingresso*, contando il numero di operazioni richieste dall'algoritmo per terminare il suo compito. Una volta fatta questa operazione, occorre *valutare la crescita della funzione*. È proprio questo il punto su cui ci soffermeremo maggiormente.

Vogliamo determinare dei criteri per valutare l'efficienza di un algoritmo: questa efficienza è indipendente dal linguaggio con cui viene implementato l'algoritmo e dalla potenza del calcolatore su cui verranno eseguiti i calcoli. Il criterio dell'efficienza di un algoritmo si calcola generalmente contando *quante sono le operazioni che devono essere eseguite* per condurre a termine il suo compito, in funzione del numero  $n$  dei dati di ingresso. Una volta stabilita l'efficienza dell'algoritmo mediante questa funzione  $f(n)$ , dovremo studiare questa funzione e vedere *quanto velocemente cresce al crescere della variabile n*. Nel prossimo paragrafo studieremo proprio l'andamento di alcune semplici funzioni, essendo interessati non tanto al valore esatto della funzione quanto al suo *ordine di grandezza*. Introdurremo quindi delle *funzioni di riferimento* e parleremo di vari tipi di complessità: complessità costante, logaritmica, lineare, polinomiale, esponenziale, fattoriale, ecc.

## 7 CRESCITA DI FUNZIONI E LORO CONFRONTO

Partiamo da tre semplici funzioni da  $N$  in  $N$ :

$$f(n) = n, \quad g(n) = n^2, \quad h(n) = n^3.$$

Come è ben noto, l'andamento è il seguente.

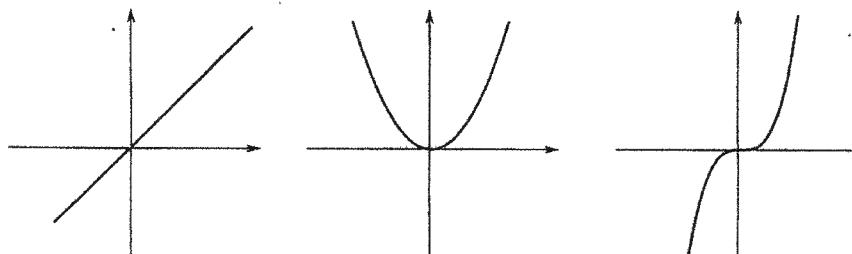


Figura 6.1.

Qui di seguito riportiamo alcuni valori di  $f$ ,  $g$  e  $h$ .

$n$	$f(n) = n$	$g(n) = n^2$	$h(n) = n^3$
2	2	4	8
4	4	16	64
8	8	64	512
16	16	256	4096
32	32	1024	32768
64	64	4096	262144

Passiamo ora ad altre funzioni note: la funzione logaritmo, la funzione esponenziale e la funzione fattoriale. Qui di seguito riportiamo alcuni valori delle tre funzioni:

$n$	$\log_2 n$	$2^n$	$n!$
2	1	4	2
4	2	16	24
8	3	256	40320
16	4	$6,5 \cdot 10^4$	$2,1 \cdot 10^{13}$
32	5	$4,2 \cdot 10^9$	$2 \cdot 10^{35}$
64	6	$1,84 \cdot 10^{19}$	$> 10^{89}$

Si noti che  $10^5$  secondi corrisponde circa ad un giorno,  $10^8$  secondi a circa tre anni,  $10^{20}$  secondi a  $3 \cdot 10^{12}$  anni, cioè più di mille miliardi di anni. L'età dell'universo è di circa  $1,5 \cdot 10^{10}$  anni!

Come si vede, mentre per  $n$ ,  $n^2$ ,  $n^3$ , ecc., al crescere di  $n$  la funzione cresce, ma non tantissimo, per le funzioni esponenziali e fattoriali la crescita è incredibilmente più veloce. L'andamento delle varie funzioni è dato dalla figura 6.2.

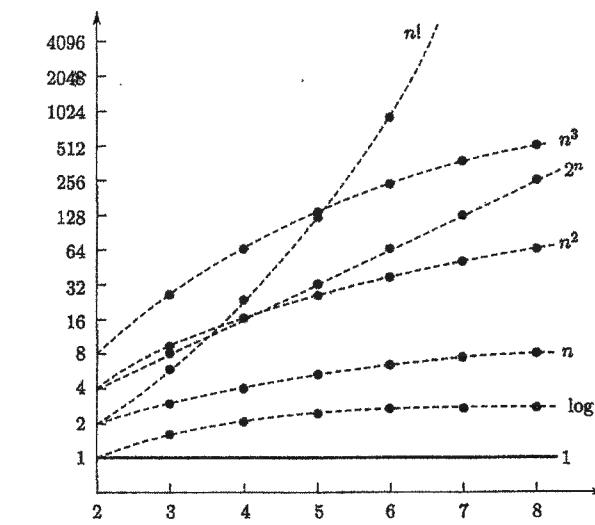


Figura 6.2.

**OSSERVAZIONE** È utile esprimere una potenza in base 2 come potenza in base 10 e viceversa. Cioè che legame c'è tra gli esponenti  $n$  e  $m$  se  $2^n = 10^m$ ? Passando ai logaritmi in base 10, la precedente uguaglianza diventa  $\log_{10} 2^n = m$ , ossia  $n \cdot \log_{10} 2 = m$ . Dato che  $\log_{10} 2$  vale circa 0,3, si ha che  $m \sim 0,3 \cdot n$  e  $n \sim 3m$ . Per esempio  $2^{100} \sim 10^{33}$ .

**OSSERVAZIONE** È utile anche sapere quanto vale  $n!$  al crescere di  $n$ . Ci viene in aiuto la cosiddetta *formula di Stirling*. Si tratta di una approssimazione per fattoriali grandi, ideata da J. Stirling intorno al 1750. Egli provò che

$$\lim_{n \rightarrow \infty} \frac{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n}{n!} = 1$$

il che corrisponde a dire che, per valori molto grandi di  $n$ ,  $n!$  si può approssimare al modo seguente:

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n.$$

## ■ 8 L'ORDINE DI GRANDEZZA DI UNA FUNZIONE: LA NOTAZIONE $\mathcal{O}$

È arrivato il momento di introdurre un importante simbolo, il cosiddetto  $\mathcal{O}$  o *big-o*. Esso è stato introdotto da Bachmann alla fine dell'800. La sua importanza risiede nel fatto che esso ci fornisce l'*ordine di grandezza* di una funzione, ossia evidenzia il comportamento saliente di una funzione, trascurandone gli aspetti marginali e inessenziali.

**DEFINIZIONE 6.15** Siano  $f$  e  $g$  due funzioni definite sui naturali e a valori positivi. Si dice che  $g$  *domina*  $f$  se esistono due costanti  $c$  ed  $n_0$  tali che

$$(8.1) \quad f(n) \leq c \cdot g(n) \quad \forall n \geq n_0.$$

Si scrive  $f \in \mathcal{O}(g)$  o che  $f$  è di classe  $\mathcal{O}(g)$ .

### Esempio 6.9

$5n^3 - n^2 \in \mathcal{O}(n^3)$ . Infatti si ha  $5n^3 > 5n^3 - n^2 \quad \forall n \geq 1$ , cioè, posto  $f(n) = 5n^3 - n^2$  e  $g(n) = n^3$ ,

$$f(n) \leq 5g(n) \quad \forall n \geq 1.$$

La 8.1 è quindi verificata per  $c = 5$  e  $n_0 = 1$ .

### Esempio 6.10

$6n^4 + 4n^2 + n + 1 \in \mathcal{O}(n^4)$ . Infatti

$$f(n) = 6n^4 + 4n^2 + n + 1 < 6n^4 + 4n^4 + n^4 + n^4 \quad \forall n > 0,$$

da cui

$$f(n) = 6n^4 + 4n^2 + n + 1 < 6n^4 + 4n^4 + n^4 + n^4 = 12n^4 \quad \forall n > 0.$$

Quindi  $f(n) \in \mathcal{O}(n^4)$  ( $c = 12, n_0 = 1$ ).

Per verificare la complessità di un algoritmo, una volta accertato che il numero di operazioni è rappresentato per esempio dalla funzione  $f(n) = 5n^3 - n^2$ , basta dire che la complessità è del tipo  $n^3$ , tralasciando tutti i termini di grado più basso. Abbiamo scelto una *funzione di riferimento* particolarmente semplice, come  $n^3$ . Nel secondo esempio la funzione di riferimento è  $n^4$ . La tavola che segue mostra l'andamento delle due funzioni dell'esempio 6.10 per valori grandi di  $n$ .

$n$	$g(n)$	$f(n)$
10	$10^4$	$6 \cdot 10^4 + 4 \cdot 10^2 + 10 + 1 = 6 \cdot 10^4 + 101$
$10^2$	$10^8$	$6 \cdot 10^8 + 4 \cdot 10^4 + 10^2 + 1 = 6 \cdot 10^8 + 40101$
$10^3$	$10^{12}$	$6 \cdot 10^{12} + 4 \cdot 10^8 + 10^3 + 1 = 6 \cdot 10^{12} + 4001001$

Si osserva che per valori grandi di  $n$  il termine di grado più alto è dominante: 101 è trascurabile rispetto a  $10^4$ , 40101 è trascurabile rispetto a  $10^8$ , ecc.

La notazione  $\mathcal{O}$  gode delle seguenti proprietà.

1.  $f(n) \in \mathcal{O}(f(n))$ ;
2.  $c\mathcal{O}(f(n)) = \mathcal{O}(f(n))$ ;
3.  $\mathcal{O}(f(n)) + \mathcal{O}(f(n)) = \mathcal{O}(f(n))$ ;
4.  $\mathcal{O}(f(n)) \cdot \mathcal{O}(g(n)) = \mathcal{O}(f(n)g(n))$ ;
5.  $\mathcal{O}(f(n)g(n)) = f(n)\mathcal{O}(g(n))$ .

### Esempio 6.11

$f(n) = 3n^3 + 4n + 1 \in \mathcal{O}(n^3)$ . Anche  $f(n) + f(n) = 6n^3 + 8n + 2 \in \mathcal{O}(n^3)$ .



Stimare in termini di  $\mathcal{O}$  le seguenti funzioni:

- a.  $f(n) = n^5 + \log n + 8$ ;
- b.  $f(n) = \log n + \log^2 n + 10$ ;
- c.  $f(n) = n^{10} + n^5 + n^3 + 7 + n!$

Stimare in termini di  $\mathcal{O}$  l'algoritmo del calcolo della somma dei primi  $n$  interi positivi.

## ■ 9 TIPI DI COMPLESSITÀ

Come si è visto nel paragrafo precedente, la notazione *big-o* ci offre l'ordine di grandezza di una data funzione. Non ci importa se l'algoritmo impiega  $n$ ,  $30n$ ,  $200n$ ,  $\frac{n}{4}$  secondi per portare a termine il suo compito. In tutti questi casi diremo che il tempo

di esecuzione è dell'ordine di  $n$ , ossia  $\mathcal{O}(n)$ . In tutti i casi il tempo cresce linearmente al crescere dell'input.

Quelle che seguono sono le principali classi di complessità per gli algoritmi, in funzione della dimensione degli input di ingresso:

$k$	costante
$\log n$	logaritmica
$n$	lineare
$n^2$	quadratica
$n^3$	cubica
$n^t$	polinomiale
$k^n$	esponenziale
$n!$	fattoriale

Quali sono le complessità *trattabili*? Dalla tabella che segue (cfr. [14] par. 2.2) ce ne renderemo subito conto. Gli input sono rappresentati da  $10$ ,  $10^2$ , ecc., mentre la prima colonna  $N$ ,  $N^2$ , ecc. rappresenta le funzioni in gioco. Il computo è stato fatto per un computer in grado di gestire  $10^9$  operazioni al secondo.

	10	$10^2$	$10^3$	$10^4$
$N$	$\frac{10}{10^9} = 10^{-8}$ s.	$\frac{10^2}{10^9} = 10^{-7}$ s	$\frac{10^3}{10^9} = 10^{-6}$ s	$10^{-5}$ s
$N^2$	$\frac{10^2}{10^9} = 10^{-7}$ s	$\frac{10^4}{10^9} = 10^{-5}$ s	$\frac{(10^3)^2}{10^9} = 10^{-3}$ s	$\frac{(10^4)^2}{10^9} = 10^{-1}$ s
$2^N$	$\frac{2^{10}}{10^9} \sim \frac{10^3}{10^9} = 10^{-6}$ s	$\frac{2^{100}}{10^9} = 4 \cdot 10^{13}$ anni	*	*
$N!$	$\frac{3 \cdot 10^6}{10^9} = 3 \cdot 10^{-3}$ s	*	*	*

Gli asterischi stanno ad indicare tempi superiori a  $10^{100}$  anni.

Si noti che il numero di protoni dell'universo conosciuto ha circa 126 cifre, e che il numero di microsecondi che sono trascorsi dal BigBang ha 24 cifre.

Gli algoritmi trattabili o ragionevoli sono quelli polinomiali. La classe di tutti i problemi *trattabili* si indica comunemente con la lettera  $P$ . Quindi la classe  $P$  consiste dei problemi *trattabili*, ovvero quelli la cui soluzione è offerta da un algoritmo di complessità al più polinomiale.

La classe  $NP$  riunisce tutti i problemi di decidibilità per i quali la risposta *sì* può essere decisa da un algoritmo *non deterministico* in tempo polinomiale. Equivalentemente è la classe dei problemi che, una volta *data* una soluzione del problema  $NP$  (ossia un *certificato*), è capace di *verificarla* con un algoritmo a complessità polinomiale. La classe  $NP$  si dice anche classe non deterministica polinomiale. Un altro modo intuitivo di indicare la classe  $NP$  è dicendo che i problemi di  $NP$  sono tutti i problemi che possono essere risolti elencando tutte le possibili soluzioni e verificandole con un algoritmo polinomiale.

Per esempio, la determinazione di un ciclo hamiltoniano, ossia un ciclo di un grafo (cfr. cap. 10) che passa per tutti i vertici del grafo esattamente una volta, appartiene alla classe  $NP$  perché può ottersi con i seguenti passi:

- generazione di tutti i possibili cicli del grafo;
- verifica se i cicli sono hamiltoniani.

Ora, il primo algoritmo è esponenziale, mentre la verifica se un ciclo è hamiltoniano è polinomiale.

Chiaramente  $P \subseteq NP$ . Non è noto se  $P \subset NP$  o se  $P = NP$ . Il problema  $P = NP?$  è stato posto nel 1971 ed è tuttora irrisolto. È uno dei più grossi problemi dell'informatica teorica e fa parte dei cosiddetti *problemi del millennio*. Dire che  $P = NP$  equivale a dimostrare che tutti i problemi  $NP$  possono essere resi di tipo  $P$ . La maggior parte degli studiosi di questo settore ritiene che sia  $P \neq NP$ .

#### F-6-14. Algoritmi polinomiali

- Scrivere un programma che esegua l'addizione di due polinomi.
- Scrivere un programma che esegua la moltiplicazione di due polinomi.
- Scrivere un programma che esegua la divisione tra due polinomi.
- Scrivere un programma che calcoli il MCD  $d(x)$  tra due polinomi  $f$  e  $g$  mediante l'algoritmo euclideo delle divisioni successive, ed esprima tale MCD nella forma  $d(x) = h(x)f(x) + k(x)g(x)$  (identità di Bézout).
- Scrivere un programma che determini tutte le radici di un polinomio  $f(x) \in \mathbb{Z}_p[x]$ .
- Scrivere un programma che, partendo da un polinomio a coefficienti razionali, determini il polinomio monico primitivo ad esso associato.
- Scrivere un programma che ricerchi le radici razionali di un polinomio a coefficienti interi.
- Scrivere un programma che testi la irriducibilità di un polinomio a coefficienti interi con il criterio di irriducibilità di Eisenstein.
- Scrivere un programma che controlli la irriducibilità su  $\mathbb{Q}$  di un polinomio a coefficienti in  $\mathbb{Z}$  pensandolo come polinomio a coefficienti in  $\mathbb{Z}_p$  per vari primi  $p$ .
- Scrivere un programma che determini tutti i polinomi di dato grado su  $\mathbb{Z}_p$  ( $p$  primo).
- Scrivere un programma che determini tutti i polinomi *irriducibili* di dato grado su  $\mathbb{Z}_p$  ( $p$  primo).

## 7

# Campi finiti

*O amici, so bene che verità alberga negli argomenti  
che ora voglio esporre; ma assai travagliato e sospettoso  
è il passaggio della convinzione dentro l'animo umano.*

Empedocle POEMA LUSTRALE N. 101  
a cura di C. Gallavotti

Abbiamo già visto esempi di campi *infiniti* (il campo  $\mathbb{Q}$  dei numeri razionali, il campo  $\mathbb{R}$  dei numeri reali, il campo  $\mathbb{C}$  dei numeri complessi, ecc.) ed esempi di campi *finiti* (i campi  $\mathbb{Z}_p$  delle classi resto modulo un primo  $p$ ). Vogliamo ora approfondire lo studio dei campi finiti, dato che con questi la matematica discreta ha maggiormente a che fare e dato che molteplici sono le loro applicazioni in vari campi: se ne renderà conto ad esempio chi intende studiare gli attuali sviluppi della crittografia. L'interessante dei campi finiti è che si possono materialmente costruire.

In questo capitolo metteremo a frutto le conoscenze acquisite sui polinomi a coefficienti in un campo per spingere oltre il parallelismo tra l'anello degli interi e l'anello dei polinomi a coefficienti in un campo, e questo ci consentirà di costruire nuovi campi finiti.

## ■ 1 DALLA CONGRUENZA TRA INTERI ALLA CONGRUENZA TRA POLINOMI: I CORRISPONDENTI ANELLI QUOZIENTE

Continuiamo il parallelismo tra l'anello  $\mathbb{Z}$  degli interi e l'anello  $\mathbb{K}[x]$  dei polinomi a coefficienti in un campo  $\mathbb{K}$  (cfr. cap. 3). Ricordiamo la relazione (di equivalenza), definita su  $\mathbb{Z}$ , di congruenza modulo un intero positivo  $n$ . Fissato un intero positivo  $n$ , si dice che  $a$  è congruente a  $b$  modulo  $n$  se la differenza  $a - b$  è un multiplo intero di  $n$ , ossia  $a \equiv b \pmod{n} \Leftrightarrow a - b = hn$  per qualche  $h \in \mathbb{Z}$ .

Abbiamo indicato con  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$  il corrispondente insieme quoziante dove, ricordiamo, in ogni classe  $\bar{a}$  si può prendere come rappresentante il resto della divisione di  $a$  per  $n$ , che è un intero maggiore o uguale a zero e minore di  $n$ . Introdotte in  $\mathbb{Z}_n$  le seguenti due operazioni

$$\bar{a} + \bar{b} := \overline{a+b}, \quad \bar{a} \cdot \bar{b} := \overline{a \cdot b}$$

•  $(\mathbb{Z}_n, +, \cdot)$  acquista la struttura di anello commutativo con unità.

Introduciamo ora per convenienza il seguente simbolo,

$$(n) := \{hn \mid h \in \mathbb{Z}\}$$

per indicare tutti i multipli interi di  $n$ . Il sottoinsieme  $(n)$  gode di una particolare proprietà: non solo è un sottoanello di  $\mathbb{Z}$  (ossia è un sottoinsieme di  $\mathbb{Z}$  che è esso stesso un anello rispetto alle medesime operazioni di  $\mathbb{Z}$ ), ma c'è di più: moltiplicando un qualunque elemento di  $(n)$  per un *qualsiasi* elemento di  $\mathbb{Z}$  si ottiene ancora un elemento di  $(n)$ . Un sottoanello che gode di questa ulteriore proprietà prende il nome di *ideale*. Il sottoinsieme  $(n)$  di  $\mathbb{Z}$  prende il nome di *ideale generato da n*.

La relazione di congruenza si può allora esprimere anche al modo seguente:

$$a \equiv b \pmod{n} \Leftrightarrow a - b \in (n)$$

cioè dichiariamo equivalenti due elementi  $a$  e  $b$  la cui differenza appartiene all'ideale  $(n)$ . Allora anziché utilizzare il simbolo  $\mathbb{Z}_n$  si può scrivere

$$\mathbb{Z}/(n).$$

Nel quoziente vengono così *identificati* due interi  $a$  e  $b$  la cui differenza  $a - b$  appartiene all'ideale  $(n)$ . La classe che contiene  $n$  e tutti i suoi multipli è lo zero nel quoziente.

Ripetiamo ora quanto detto per  $\mathbb{Z}$  nell'anello  $\mathbb{K}[x]$  dei polinomi a coefficienti in un campo  $\mathbb{K}$ . Fissato un polinomio  $f(x)$  appartenente a  $\mathbb{K}[x]$ , con il simbolo  $(f(x))$  si intende

$$(f(x)) := \{f(x) \cdot h(x) \mid h(x) \in \mathbb{K}[x]\},$$

ossia l'insieme di tutti i polinomi divisibili per  $f(x)$ .

### Esempio 7.1

Se  $\mathbb{K} = \mathbb{Q}$ ,  $(x^2 + 1) = \{(x^2 + 1) \cdot h(x) \mid h(x) \in \mathbb{Q}[x]\}$ . Quindi ad esempio il polinomio  $x^3 - 3x^2 + x - 3 \in (x^2 + 1)$  perché  $x^3 - 3x^2 + x - 3 = (x^2 + 1)(x - 3)$ , mentre  $x^3 + 5x^2 + x + 6 \notin (x^2 + 1)$  perché  $x^3 + 5x^2 + x + 6$  diviso per  $x^2 + 1$  dà un resto non nullo.

Analogamente a quanto detto nel caso degli interi, il sottoinsieme  $(f(x))$  prende il nome di *ideale generato dal polinomio f(x)*.

Definiamo ora su  $\mathbb{K}[x]$  la seguente relazione:

$$g(x) \equiv h(x) \pmod{f(x)} \Leftrightarrow g(x) - h(x) \in (f(x)),$$

ossia se  $g(x) - h(x)$  è un multiplo di  $f(x)$ . Questa è una *relazione di equivalenza*, detta *congruenza modulo f(x)*, analoga alla relazione, definita su  $\mathbb{Z}$ , di congruenza modulo  $n$ .

Indicheremo con  $\mathbb{K}[x]/(f(x))$  l'insieme quoziante dell'anello  $\mathbb{K}[x]$  rispetto a questa relazione. Gli elementi di  $\mathbb{K}[x]/(f(x))$  sono le *classi di equivalenza modulo la relazione data*. Indichiamo con  $\bar{g}(x)$  una classe di equivalenza: essa è costituita da tutti i polinomi che differiscono da  $g(x)$  per un multiplo di  $f(x)$ , ossia

$$\bar{g}(x) = \{g(x) + f(x) \cdot h(x) \mid h(x) \in \mathbb{K}[x]\} = g(x) + (f(x)).$$



Analogamente a quanto visto in  $\mathbb{Z}$  riguardo alla relazione di congruenza modulo  $n$ , dato un polinomio  $g(x) \in \mathbb{K}[x]$ , esso è congruo modulo  $f(x)$  al resto della divisione di  $g(x)$  per  $f(x)$ . Quindi le classi di equivalenza modulo  $f(x)$  sono tante quanti i possibili resti delle divisioni per  $f(x)$ : se il polinomio  $f(x)$  ha grado  $n$ , i resti saranno polinomi di grado  $< n$ . Quindi le classi di equivalenza possono essere rappresentate da polinomi di grado minore del grado di  $f(x)$ , cioè

$$\mathbb{K}[x]/(f(x)) = \overline{\{r_0 + r_1x + r_{n-1}x^{n-1}, r_i \in \mathbb{K}\}}.$$

Se non vogliamo fare intervenire le classi, se  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ , allora possiamo pensare a  $\mathbb{K}[x]/(f(x))$  come all'insieme dei polinomi di grado minore di  $n$  con la condizione però che  $x^n = -a_{n-1}x^{n-1} - \dots - a_1x - a_0$ : cioè consideriamo uguali due polinomi che differiscono per un multiplo di  $f(x)$ . È semplicemente un altro modo di scrivere le classi. In definitiva

$$\mathbb{K}[x]/(f(x)) = \{r_0 + r_1x + r_{n-1}x^{n-1}, r_i \in \mathbb{K}, x^n = -a_{n-1}x^{n-1} - \dots - a_1x - a_0\}$$

Ora, per ogni campo  $\mathbb{K}$ , nell'insieme  $\mathbb{K}[x]/(f(x))$  si possono introdurre due operazioni (a partire dalle operazioni definite in  $\mathbb{K}[x]$ ) al modo seguente:

$$(1.1) \quad \overline{g(x)} + \overline{h(x)} := \overline{g(x) + h(x)},$$

$$(1.2) \quad \overline{g(x) \cdot h(x)} := \overline{g(x) \cdot h(x)},$$

e queste operazioni sono ben poste, nel senso che, pur essendo definite attraverso i rappresentanti, sono indipendenti dai rappresentanti. Rispetto a queste due operazioni  $(\mathbb{K}[x]/(f(x)), +, \cdot)$  diventa un anello, commutativo con unità.

Ha senso chiedersi: quand'è che questo anello è un campo?

Ricordiamo che  $\mathbb{Z}_n$  è un campo se e solo se  $n = p$  è un numero primo. Ebbene, una condizione analoga vale per il caso dei polinomi.

$(\mathbb{K}[x]/(f(x)), +, \cdot)$  è un campo se e solo se il polinomio  $f(x)$  è irriducibile su  $\mathbb{K}$ .

L'essere o no un campo dipende quindi dal polinomio  $f(x)$ .

Infatti una classe  $\overline{g(x)} = g(x) + (f(x))$  non nulla è invertibile se e solo se il MCD tra  $g(x)$  e  $f(x)$  è 1. Se vogliamo che ogni elemento non nullo sia invertibile occorre che il polinomio  $f(x)$  sia irriducibile. Come trovare la classe inversa della classe  $\overline{g(x)} = \overline{a_0 + a_1x + \dots + a_{n-1}x^{n-1}}$ ? Consideriamo il polinomio  $g(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ . Dato che la classe  $\overline{g(x)} \neq \overline{0}$ ,  $g(x)$  non è multiplo di  $f(x)$ . Allora  $(g(x), f(x)) = 1$  e quindi esistono  $s(x), t(x)$  in  $\mathbb{Q}[x]$  tali che  $1 = s(x)g(x) + t(x)p(x)$ .

Passando al quoziente si ottiene

$$\overline{1} = \overline{s(x)g(x) + t(x)p(x)} = \overline{s(x)g(x)} = \overline{s(x)} \cdot \overline{g(x)}$$

La classe  $\overline{s(x)}$  è l'inversa cercata di  $\overline{g(x)}$ .

### Esempio 7.2

In  $\mathbb{Q}[x]$ , fissiamo il polinomio  $x^2 - 3$  appartenente a  $\mathbb{Q}[x]$  e irriducibile su  $\mathbb{Q}$ . Si ha

$$\mathbb{Q}[x]/(x^2 - 3) := \{\overline{a_0 + a_1x} \mid a_i \in \mathbb{Q}\}.$$

ricordiamo infatti che come rappresentanti delle classi possiamo prendere polinomi di grado minore del grado di  $f(x)$  (2 in questo caso). Dato che  $x^2 - 3$  è irriducibile su  $\mathbb{Q}$ , questo anello quoziante è un campo. Come riusciamo a determinare ad esempio l'inversa della classe  $\overline{x+1}$ ? L'inverso di un polinomio non è un polinomio, ad eccezione dei polinomi di grado zero. Ma, ricordiamoci, gli elementi del quoziante  $\mathbb{Q}[x]/(x^2 - 3)$  non sono polinomi, ma classi di equivalenza di polinomi. Allora si procede come si è detto nella teoria: si lavora innanzitutto nell'anello  $\mathbb{Q}[x]$  (e non ancora nel quoziante): qui si determina il  $\text{MCD}(x^2 - 3, x + 1)$  con l'algoritmo euclideo delle divisioni successive. Risulta  $x^2 - 3 = (x + 1)(x - 1) - 2$ . Quindi  $\text{MCD}(x^2 - 3, x + 1) = 2$  (cioè i due polinomi sono coprimi). Ora esprimiamo il MCD come combinazione di  $x^2 - 3$  e  $x + 1$  (identità di Bézout). Si ottiene immediatamente

$$2 = -(x^2 - 3) + (x + 1)(x - 1).$$

A noi ora interessa esprimere 1 (e non 2) come combinazione dei due polinomi: basta allora dividere primo e secondo membro per 2, ottenendo

$$1 = -\frac{1}{2}(x^2 - 3) + \frac{1}{2}(x + 1)(x - 1).$$

Passando alle classi modulo  $x^2 - 3$  (ossia lavorando ora nel quoziante  $\mathbb{Q}[x]/(x^2 - 3)$ ), ricordando che la classe  $\overline{x^2 - 3}$  è la classe nulla in  $\mathbb{Q}[x]/(x^2 - 3)$ , si ottiene

$$\overline{1} = \overline{\frac{1}{2}(x+1) \cdot (x-1)}$$

per cui l'inversa della classe  $\overline{x+1}$  è la classe  $\overline{\frac{1}{2}(x-1)}$ .

Verifichiamolo:  $\overline{(x+1)\frac{1}{2}(x-1)} = (\text{ricordando che } x^2 \equiv 3) = \overline{\frac{3}{2} - \frac{1}{2}} = \overline{1}$ .

**OSSERVAZIONE** Si osservi che il campo  $\mathbb{Q}[x]/(x^2 - 3)$  contiene al suo interno il campo  $\mathbb{Q}$  perché contiene le classi di tutti i polinomi di grado zero (cioè i polinomi  $a_0 + a_1x$  con  $a_1 = 0$ , ossia gli  $a_0$ ) che sono ovviamente in corrispondenza biunivoca con  $\mathbb{Q}$  ed è contenuto in  $\mathbb{R}$ . Indicheremo tale campo con  $\mathbb{Q}(\sqrt{3})$  e diremo che è stato ottenuto da  $\mathbb{Q}$  aggiungendo il numero (reale)  $\sqrt{3}$ . Gli elementi di  $\mathbb{Q}(\sqrt{3})$  sono tutti e soli gli elementi del tipo  $\alpha\sqrt{3} + \beta$ , con  $\alpha$  e  $\beta$  in  $\mathbb{Q}$ .

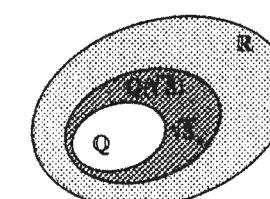


Figura 7.1. Il campo  $\mathbb{Q}(\sqrt{3})$ .

Partendo da un altro polinomio irriducibile su  $\mathbb{Q}$  si possono costruire altri campi che contengono  $\mathbb{Q}$ . Ad esempio, se partiamo dal polinomio, anch'esso irriducibile su  $\mathbb{Q}$ ,  $x^2 - 7$ , il quoziente  $\mathbb{Q}[x]/(x^2 - 7)$  è un campo che indicheremo con  $\mathbb{Q}(\sqrt{7})$ .



- Determinare gli elementi invertibili dell'anello

$$\mathbb{R}[x]/(x^2 - 2x + 2).$$

- Studiare l'anello quoziante  $\mathbb{Q}[x]/(x^4 - 3x - 1)$ . Determinare, se esiste, l'inversa della classe  $\overline{x^3 + 2}$ .

- Dire se l'anello  $\mathbb{Q}[x]/(x^4 + 3x + 1)$  è un campo e determinare, se esiste, l'inversa della classe  $\overline{x^2 + x}$ .

- Decidere se il polinomio  $x^5 - 5x^3 + 1 \in \mathbb{Q}[x]$  appartiene all'ideale generato da  $f(x) = x^3 - 2x - 3$ .

- Trovare, se esiste, l'inversa della classe  $\overline{x^2 + 2x - 1}$  nel quoziante  $\mathbb{Z}_3[x]/(x^2 + 1)$ .

## 2 CAMPI FINITI

Abbiamo visto nel paragrafo precedente che, qualunque sia il campo  $\mathbb{K}$ , il quoziante  $\mathbb{K}[x]/(f(x))$  è un campo se e solo se il polinomio  $f(x)$  è irriducibile su  $\mathbb{K}$ . Nell'esempio 7.2 si è visto che partendo dal campo  $\mathbb{Q}$  dei numeri razionali, prendendo il polinomio  $x^2 - 3$ , che è irriducibile su  $\mathbb{Q}$ , il quoziante  $\mathbb{Q}[x]/(x^2 - 3)$  è un campo. Questa possibilità di costruire nuovi campi si rivela particolarmente utile nel caso in cui vogliamo costruire campi finiti. Partendo da  $\mathbb{K}[x]$  con  $\mathbb{K}$  infinito, chiaramente anche il quoziante  $\mathbb{K}[x]/(f(x))$ , che coincide con  $\{r_0 + r_1x + r_{n-1}x^{n-1} \mid r_i \in \mathbb{K}\}$  è infinito, dato che gli  $r_i$  variano in un insieme infinito. Se siamo interessati a costruire anelli quoziensi finiti dobbiamo quindi partire da un campo  $\mathbb{K}$  finito che sia noto. Finora di campi finiti conosciamo solo quelli con  $p$  elementi,  $\mathbb{Z}_p$ ,  $p$  primo. Partiamo quindi da  $\mathbb{Z}_p[x]$  e fissiamo un polinomio  $f(x) \in \mathbb{Z}_p[x]$  di grado  $n$ : in tal caso il quoziante  $\mathbb{Z}_p[x]/(f(x))$  è un insieme finito con  $p^n$  elementi: infatti è costituito dalle classi  $r_0 + r_1x + r_{n-1}x^{n-1}$  con  $r_i \in \mathbb{Z}_p$  e questa volta le classi, essendo individuate dai polinomi di grado  $< n$  con coefficienti variabili in un insieme finito con  $p$  elementi saranno in numero di  $p^n$ . Quindi

$$|\mathbb{Z}_p[x]/(f(x))| = p^n$$

In particolare, questa osservazione ci permette di costruire campi finiti.

Per ogni primo  $p$  e ogni intero  $n$  esiste un campo di ordine  $p^n$ : basta partire dall'anello  $\mathbb{Z}_p[x]$ , fissare un polinomio *irriducibile* su  $\mathbb{Z}_p$  di grado  $n$ : il quoziante  $\mathbb{Z}_p[x]/(f(x))$  è un campo con  $p^n$  elementi.

Ma, senza dimostrarlo, possiamo dire molto di più.

- Ogni campo finito ha sempre un numero di elementi pari a  $p^n$  per un opportuno  $p$  primo. Quindi non esistono campi finiti con 20 elementi, 10 elementi, 50 elementi, ecc.

- Per ogni primo  $p$  ed ogni intero positivo  $n$  esiste uno (lo abbiamo già detto) ed un solo (a meno di isomorfismi) campo finito con  $p^n$  elementi.

Facciamo qualche esempio.

### Esempio 7.3

Si costruisca, se esiste, un campo con 8 elementi.

Un campo con 8 elementi esiste, perché  $8 = 2^3$  è la potenza di un numero primo. Per costruire un tale campo si parte dall'anello  $\mathbb{Z}_2[x]$  dei polinomi a coefficienti in  $\mathbb{Z}_2$ , poi si prende un polinomio di terzo grado a coefficienti in  $\mathbb{Z}_2$  e irriducibile in  $\mathbb{Z}_2[x]$ , ad esempio  $x^3 + x + 1$  (uno qualunque di terzo grado va bene, purché sia irriducibile), e si considera l'insieme

$$\mathbb{K} = \{a + bx + cx^2 \mid a, b, c \in \mathbb{Z}_2, |x^3 = x + 1\rangle\}$$

cioè dei polinomi di grado 2, con la condizione che ogni volta che nella moltiplicazione troviamo  $x^3$  lo sostituiamo con  $x + 1$  (si osservi che avremmo dovuto scrivere  $x^3 = -x - 1$ , ma, trovandoci in  $\mathbb{Z}_2$   $a = -a$ , quindi possiamo trascurare il segno). Naturalmente, se troviamo  $x^4$  scriveremo  $x^4 = x^3 \cdot x = (x + 1)x = x^2 + x$ , ecc. Si tratta dell'insieme delle classi rispetto alla relazione di equivalenza che dichiara equivalenti due polinomi di  $\mathbb{Z}_2[x]$  quando la loro differenza è un multiplo di  $x^3 + x + 1$ .  $\mathbb{K}$  è quindi

$$\{\bar{0}, \bar{1}, \bar{x}, \bar{x}^2, \bar{1+x}, \bar{1+x^2}, \bar{x+x^2}, \bar{1+x+x^2}\}.$$

con l'operazione di addizione (1.1) e moltiplicazione (1.2). Si invita lo studente a scrivere le tavole additiva e moltiplicativa di tale anello e verificare che si tratta effettivamente di un campo. Nel fare le moltiplicazioni tra classi si deve tener presente che si deve porre  $\bar{x}^3 = \bar{x+1}$  e quindi (verificare!)  $\bar{x}^4 \equiv \bar{x^2+x}$ ,  $\bar{x}^5 \equiv \bar{x^2+x+1}$ ,  $\bar{x}^6 \equiv \bar{x^2+1}$ ,  $\bar{x}^7 \equiv \bar{1}$ , ecc.

Si invita lo studente a verificare anche che, scegliendo l'altro polinomio irriducibile di terzo grado su  $\mathbb{Z}_2$ , ossia  $x^3 + x^2 + 1$ , si ottiene la stessa tavola additiva (ovviamente), e una tavola moltiplicativa diversa, ma i due campi ottenuti sono isomorfi.

### Esempio 7.4

Per ogni polinomio di secondo grado  $f(x) \in \mathbb{Z}_2[x]$  si consideri l'anello quoziante  $\mathbb{Z}_2[x]/(f(x))$ . Intendiamo studiare tali quozienti, stabilendo quali sono domini di integrità, quali possiedono divisori dello zero, quali sono campi, quali sono gli elementi invertibili. E scriveremo per ogni  $f(x)$  la corrispondente tavola moltiplicativa del quoziante.

In  $\mathbb{Z}_2[x]$  i polinomi di secondo grado sono  $x^2$ ,  $x^2+x$ ,  $x^2+1$ ,  $x^2+x+1$ . Esaminiamoli separatamente:

- $x^2$  è riducibile perché  $x^2 = x \cdot x$ . Il quoziante quindi possiede divisori dello zero, ossia non è un dominio d'integrità.

$$\mathbb{Z}_2[x]/(x^2) = \{a + bx \mid a, b \in \mathbb{Z}_2, x^2 = 0\} = \{\bar{a+bx} \mid a, b \in \mathbb{Z}_2\}$$

La tavola moltiplicativa è la seguente:

	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{1+x}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{1+x}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\bar{0}$	$\bar{x}$
$\bar{1+x}$	$\bar{0}$	$\bar{1+x}$	$\bar{x}$	$\bar{1}$

- Si vede che la classe  $\bar{x}$  è un divisore dello zero. Esistono due elementi invertibili,  $\bar{1}$  e  $\bar{1+x}$ .
- b.  $x^2 + x$  è riducibile perché  $x^2 = x \cdot (x+1)$ . Il quoziente quindi possiede divisori dello zero, ossia non è un dominio d'integrità.

$$\mathbb{Z}_2[x]/(x^2 + x) = \{a + bx \mid a, b \in \mathbb{Z}_2, x^2 = x\} = \{\bar{a} + \bar{b}\bar{x} \mid a, b \in \mathbb{Z}_2\}$$

Si noti che utilizziamo lo stesso simbolo  $\bar{a} + \bar{b}\bar{x}$  per indicare una classe sia in questo caso, sia nel caso precedente, ma si tratta di classi di equivalenze rispetto a congruenze diverse, una modulo  $x^2$ , l'altra modulo  $x^2 + x$ . Anche nelle successive tavole continueremo ad indicarle allo stesso modo.

La tavola moltiplicativa è la seguente:

.	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{1+x}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{1+x}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\bar{x}$	$\bar{0}$
$\bar{1+x}$	$\bar{0}$	$\bar{1+x}$	$\bar{0}$	$\bar{1+x}$

- Si vede che  $\bar{x}$  e  $\bar{1+x}$  sono divisori dello zero. L'unica classe invertibile è la classe  $\bar{1}$ .
- c.  $x^2 + 1 = (x+1)(x+1)$ , quindi il quoziente non è un campo né un dominio di integrità.

La tavola moltiplicativa del quoziente  $\mathbb{Z}_2[x]/(x^2 + 1) = \{a + bx \mid a, b \in \mathbb{Z}_2, x^2 = 1\}$  è

.	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{1+x}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{1+x}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\bar{1}$	$\bar{1+x}$
$\bar{1+x}$	$\bar{0}$	$\bar{1+x}$	$\bar{1+x}$	$\bar{0}$

- Esiste un solo divisore dello zero,  $\bar{1+x}$ , ed esistono due elementi invertibili,  $\bar{1}$  e  $\bar{x}$ .
- d.  $x^2 + x + 1$  è irriducibile su  $\mathbb{Z}_2$  perché di secondo grado e privo di radici in  $\mathbb{Z}_2$ . Quindi l'anello quoziente è un campo.

La tavola moltiplicativa del quoziente  $\mathbb{Z}_2[x]/(x^2 + x + 1) = \{a + bx \mid a, b \in \mathbb{Z}_2, x^2 = x + 1\}$  è

.	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{1+x}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{1+x}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\bar{1+x}$	$\bar{1}$
$\bar{1+x}$	$\bar{0}$	$\bar{1+x}$	$\bar{1}$	$\bar{x}$

Dalla tavola si vede che ogni classe non nulla è invertibile, come deve essere in un campo. I due anelli  $\mathbb{Z}_2[x]/(x^2)$  e  $\mathbb{Z}_2[x]/(x^2 + 1)$  sono isomorfi. Basta considerare l'applicazione così

definita:

$$\mathbb{Z}_2[x]/(x^2) \longrightarrow \mathbb{Z}_2[x]/(x^2 + 1)$$

$$\bar{0} \longrightarrow \bar{0}$$

$$\bar{1} \longrightarrow \bar{1}$$

$$\bar{x} \longrightarrow \bar{1+x}$$

$$\bar{1+x} \longrightarrow \bar{x}$$

Si tratta di un'applicazione ovviamente biunivoca che conserva entrambe le operazioni. Quindi è un isomorfismo di anelli.

Invece  $\mathbb{Z}_2[x]/(x^2 + x)$  non è isomorfo a nessuno degli altri.

### Esercizi

1. Si considerino i due anelli  $\mathbb{Z}_5[x]/(x^3 + 1)$  e  $\mathbb{Z}_5[x]/(x^2 + x + 1)$ .

- a. Quanti elementi ha ciascuno dei due anelli?  
 b. Per ciascuno dei due, decidere se si tratta di un dominio di integrità e/o di un campo.  
 c. In entrambi i casi, calcolare il prodotto delle classi  $\bar{x+1}$  e  $\bar{2x+3}$ .

2. Si considerino i due anelli  $\mathbb{Z}_7[x]/(x^3 + 2)$  e  $\mathbb{Z}_7[x]/(x^2 + x + 1)$ .

- a. Quanti elementi ha ciascuno dei due anelli?  
 b. Per ciascuno dei due, decidere se si tratta di un dominio di integrità e/o di un campo.  
 c. In entrambi i casi, calcolare il prodotto delle classi  $\bar{x+1}$  e  $\bar{2x+3}$ .

3. Si consideri l'anello  $\mathbb{Z}_{1683}$  delle classi resto modulo 1683.

- a. Decidere se è un campo.  
 b. Se non è un campo, dire se esistono delle classi non nulle  $\bar{a}$  e  $\bar{b}$  tali che il loro prodotto sia la classe nulla.  
 c. Decidere se la classe  $\bar{4}$  è invertibile: in caso positivo determinare l'inversa.

4. Si consideri l'anello  $\mathbb{Z}_{2079}$  delle classi resto modulo 2079.

- a. Decidere se è un campo.  
 b. Se non è un campo, dire se esistono delle classi non nulle  $\bar{a}$  e  $\bar{b}$  tali che il loro prodotto sia la classe nulla.  
 c. Decidere se la classe  $\bar{4}$  è invertibile: in caso positivo determinare l'inversa.

5. a. Per quali valori di  $k \in \mathbb{Q}$  il polinomio  $f(x) = x^3 + 2kx^2 + x + 2 \in \mathbb{Q}[x]$  è divisibile per  $x^2 + 1$  (cioè appartiene all'ideale  $(x^2 + 1)$ )?  
 b. Determinare il MCD( $f(x), x^2 + 1$ ).

6. Sia  $A = \mathbb{Z}_5[x]/I$ , dove  $I = (x^3 + 4x^2 + 2x + 3)$ .

$A$  è un campo?  $\bar{3x^3 + x}$  è un divisore dello zero in  $A$ ?

7. Si studi l'anello  $\mathbb{Z}_5[x]/(x^3 + 3x + 2)$ . Dire se la classe  $\bar{x^5 + 4x + 1}$  è invertibile e, in caso positivo, si determini l'inversa.

- Per quali valori  $a \in \mathbb{Z}$  il polinomio  $3x^3 + 20ax^2 + 50a^2x + 60$  è irriducibile rispettivamente su  $\mathbb{Q}$ ,  $\mathbb{R}$  e  $\mathbb{C}$ ?
- a. Dire per quali valori di  $c \in \mathbb{Z}_5$  il quoziente  $\mathbb{Z}_5[x]/(x^2 - c)$  è un campo.  
 b. Determinare tutti gli elementi invertibili (se esistono) in  $\mathbb{Z}_5[x]/(x^2 - 2)$ .  
 c. Si determinino i divisori dello zero (se esistono) di  $\mathbb{Z}_5[x]/(x^2 - 4)$ .
- Costruire un campo con 9 elementi.

**Esercizi di programmazione**

- Scrivere un programma che decida, dato un intero positivo  $n$ , se esiste un campo finito con  $n$  elementi.
- Scrivere un programma che, dati un primo  $p$  e un intero positivo  $n$ , costruisca un campo con  $p^n$  elementi.
- Scrivere un programma che, partendo da un campo con  $p^n$  elementi, costruito come al punto precedente, determini l'inverso moltiplicativo di ogni classe non nulla.
- Scrivere un programma che, dati un primo  $p$  e un intero positivo  $n$ , costruisca un anello che non sia un campo, con  $p^n$  elementi e individui le classi che sono invertibili.
- Scrivere un programma che stampi le tabelle additive e moltiplicative dei campi fino all'ordine 16.

**8****Strutture algebriche**

*Questa montagna è tale  
che sempre al cominciar di sotto è grave;  
e quant'uom più va su, e men fa male.*

*però, quand'ella ti parrà soave  
tanto, che su andar ti fia leggero  
com'a seconda giù andar per nave;  
allor sarai al fin d'esto sentiero;  
quivi di riposar l'affanno aspetta.*

Dante, PURGATORIO IV 88-95

Nei capitoli precedenti abbiamo a lungo parlato di interi e di polinomi e abbiamo osservato che, rispetto alle ordinarie operazioni di addizione e moltiplicazione, l'insieme degli interi e l'insieme dei polinomi hanno la struttura di anello. È arrivato ora il momento di presentare in modo sistematico le principali strutture algebriche per far capire che esistono molti altri esempi di gruppi, anelli, ecc. oltre a quelli studiati finora. In questo capitolo raccoglieremo quindi le principali definizioni e proprietà delle più importanti strutture algebriche, anche se in realtà molte delle definizioni e proprietà sono già state viste. Tuttavia riteniamo utile raccoglierle in questo capitolo, in modo che lo studente abbia una visione complessiva dei vari risultati.

A differenza di quanto fatto finora, dove per motivi didattici si è preferito studiare prima gli anelli e i campi, ossia strutture algebriche con due operazioni, perché di queste strutture avevamo subito a disposizione esempi significativi e noti allo studente, ora esamineremo innanzitutto le strutture con una sola operazione, per poi passare alle strutture algebriche dotate di due operazioni.

**■ 1 PRIMI ESEMPI DI INSIEMI CON UNA SOLA OPERAZIONE:  
GRUPPOIDI, SEMIGRUPPI, MONOIDI**

Ricordiamo innanzitutto che una *operazione* (binaria) definita su un insieme  $S$  è un'applicazione di  $S \times S$  in  $S$ . Se l'insieme  $S$  è finito e non tanto grande, possiamo rappresentare un'operazione con una *tavola*.

### Esempio 8.1

#### Esempi di operazioni attraverso la tavola

1. Sia  $S = \{a, b, c\}$  e sia  $*$  l'operazione che assegna l'elemento  $c$  ad ogni coppia di elementi di  $S$ : questa operazione è rappresentata dalla tabella.

*	a	b	c
a	c	c	c
b	c	c	c
c	c	c	c

2. Sia  $S = \{a, b, c\}$ . La seguente tavola rappresenta una operazione in  $S$  perché ad ogni coppia di elementi di  $S$  resta associato un ben determinato elemento ancora in  $S$ :

*	a	b	c
a	c	a	a
b	b	c	a
c	c	b	a

La seguente tavola invece non rappresenta una operazione in  $S = \{a, b, c\}$  perché l'elemento  $d$  associato alla coppia  $(a, c)$  non appartiene a  $S$ :

*	a	b	c
a	c	a	d
b	b	c	a
c	c	b	a

Così, la sottrazione non è un'operazione in  $\mathbb{N}$  perché la differenza di due numeri naturali non è sempre un numero naturale: per esempio  $4 - 7 = -3 \notin \mathbb{N}$ . Oppure la divisione in  $\mathbb{Q}$  non è un'operazione, perché  $\frac{a}{b}$  non è definito.

Come abbiamo già visto, una *struttura algebrica* è un insieme  $S$  dotato di una o più operazioni definite su  $S$ . Cominciamo con le più generali strutture algebriche dotate di *una operazione*, per poi arrivare, nel prossimo paragrafo, alla struttura algebrica di *gruppo*.

**DEFINIZIONE 8.1** Si definisce *gruppoide* un insieme  $S$  dotato di una operazione ■

### Esercizio 8.3

### Esempi di gruppidi

1. L'insieme  $\mathbb{Z}$  degli interi rispetto all'addizione.
  2. L'insieme  $\mathbb{Z}$  degli interi rispetto alla sottrazione.
  3. L'insieme  $\mathbb{Z}$  rispetto alla moltiplicazione.
  4. L'insieme  $\mathbb{Q}$  rispetto alla moltiplicazione.
  5. L'insieme  $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$  rispetto alla moltiplicazione (si ricordi che il prodotto di due razionali non nulli è ancora un razionale non nullo).

6. L'insieme  $\Omega^* = \Omega \setminus \{0\}$  rispetto alla divisione

In tutti gli esempi precedenti dobbiamo controllare di volta in volta che l'addizione o la sottrazione o la moltiplicazione o la divisione siano delle operazioni negli insiemi che via via vengono esaminati.

- Sia  $X$  un insieme e sia  $S = \{f : X \rightarrow X\}$ . L'insieme  $S$  rispetto al prodotto operatorio è un gruppoido: infatti la composizione di due funzioni da  $X$  in  $X$  è ancora una funzione da  $X$  in  $X$ , cioè appartiene a  $S$ .
  - Sia  $X$  un insieme non vuoto e sia  $S = \mathcal{P}(X)$  l'insieme delle parti di  $X$ . L'insieme  $S$  rispetto all'intersezione è un gruppoido, perché l'intersezione di due sottoinsiemi di  $X$  è ancora un sottoinsieme di  $X$ , cioè  $\in \mathcal{P}(X)$ .

Invece, come si è visto sopra, l'insieme  $\mathbb{N}$  dei numeri naturali rispetto alla sottrazione  $-n\in\mathbb{Z}$  è un gruppoide. Così non è un gruppoide l'insieme  $\mathbb{Q}$  rispetto alla divisione.

Per indicare che un insieme  $S$  è dotato di una operazione  $*$  scriveremo in genere



**DEFINIZIONE 8.2** Dicesi *semigruppo* un insieme dotato di una operazione associativa.

Esempio R.3

### Esempi di semigruppi

1.  $(\mathbb{Z}, +)$ .
  2.  $(\mathbb{Z}, \cdot)$ .
  3.  $(2\mathbb{Z}, \cdot)$ .
  4.  $(\mathbb{Q}, +)$ .
  5.  $(\mathbb{Q}, \cdot)$ .
  6.  $(\mathbb{Q}^*, \cdot)$ .
  7. L'insieme  $S$  dotato dell'operazione della tabella (1) dell'esempio 8.1.
  8. L'insieme  $S$  delle funzioni da un insieme  $X$  in sé rispetto al prodotto operatorio  $\circ$  : infatti la composizione di funzioni è associativa.
  9.  $S = \mathcal{P}(X)$  rispetto all'intersezione perché l'intersezione è associativa.

L'insieme  $(\mathbb{Z}, -)$  o l'insieme  $(\mathbb{Q}, -)$  non sono semigruppi, pur essendo gruppoidi, dato che la sottrazione non è associativa, perché per esempio

$$(1 - 1) = 1 \equiv -1 \neq 1 = (1 - 1) \equiv 1$$

**DEFINIZIONE 8.3** Dicesi *monoide* un semigruppo dotato di elemento neutro.

**Esempio 8.4**

Esempi di monoidi

1.  $(\mathbb{Z}, +)$ .
  2.  $(\mathbb{Z}, \cdot)$ .
  3.  $(\mathbb{Q}, +)$ .
  4.  $(\mathbb{Q}, \cdot)$ .
  5.  $(\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \cdot)$ .
  6. L'insieme  $S$  delle funzioni da un insieme  $X$  in sé rispetto al prodotto operatorio  $\circ$ : infatti l'applicazione identica  $i_X(x) = x \forall x \in X$  funge da elemento neutro.
- .....

Non sono invece monoidi per esempio:

1.  $(2\mathbb{Z}, \cdot)$ .
2. L'insieme  $S$  dotato dell'operazione della tabella (1) dell'esempio 8.1.
3.  $S = \mathcal{P}(X)$  rispetto all'intersezione.

**Esercizi**1 Studiare cosa si può dire di  $(\mathbb{N}, -)$ .2 Sia  $X$  un insieme non vuoto e sia  $S = \mathcal{P}(X)$  l'insieme delle parti di  $X$ . Dire che tipo di struttura algebrica è  $(S, \cup)$ .**2 I GRUPPI**

In questo paragrafo parleremo della struttura algebrica per eccellenza dotata di una sola operazione, il gruppo.

DEFINIZIONE 8.4 Un *gruppo*  $(G, *)$  è un insieme  $G$  dotato di una operazione binaria  $*$ 

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a * b \end{aligned}$$

che verifica le seguenti proprietà:

- (a)  $*$  è *associativa*, cioè  $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$ ;
  - (b) esiste un elemento  $e \in G$  *neutro* rispetto all'operazione, tale cioè che  $e * a = a * e = a \quad \forall a \in G$ ;
  - (c) per ogni  $a \in G$  esiste un elemento  $a' \in G$ , detto *inverso* di  $a$ , tale che  $a * a' = a' * a = e \quad \forall a \in G$ .
- .....

Si noti che non si richiede la *commutatività* dell'operazione. Un gruppo  $(G, *)$  in cui l'operazione è commutativa prende il nome di *gruppo abeliano*.

Dagli assiomi appena elencati di gruppo si dimostra che l'elemento neutro è unico e così l'inverso di ogni elemento (cfr. Esercizi 3 e 4).

In genere, se utilizziamo la notazione moltiplicativa, scriviamo  $ab$  in luogo di  $a \cdot b$ , e denoteremo con  $a^{-1}$  l'inverso di  $a$ . Se invece utilizziamo la notazione additiva  $+$ , l'elemento neutro è lo zero e l'inverso di  $a$  prende il nome di opposto e si indica con  $-a$ .Diamo ora alcuni esempi di gruppi. Nei prossimi esempi l'operazione  $*$  sarà, a seconda dei casi, l'ordinaria addizione  $+$  o la moltiplicazione  $\cdot$ .

- (a)  $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Z}_n, +), (\mathbb{Q}[x], +)$ .
- (b)  $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot), (\mathbb{Z}_p \setminus \{0\}, \cdot)$ ,  $p$  primo.
- (c)  $(U(\mathbb{Z}_n), \cdot) = \{\text{elementi invertibili di } \mathbb{Z}_n\}$ .

Tutti questi gruppi sono abeliani. Per dare esempi di gruppi non abeliani, conviene cercarli tra insiemi di matrici rispetto alla moltiplicazione. I prossimi esempi riguardano quindi le matrici. Ricordiamo le principali definizioni sulle matrici. Le operazioni fondamentali che si possono fare sulle matrici sono la addizione e la moltiplicazione.

DEFINIZIONE 8.5 Siano  $A = (a_{ij})$  e  $B = (b_{ij})$  due matrici  $n \times m$ , ossia aventi  $n$  righe e  $m$  colonne. La *somma* delle due matrici si indica con  $A + B$  ed è la matrice che alla posizione  $ij$  (cioè all'incrocio tra la  $i$ -esima riga e la  $j$ -esima colonna) contiene l'elemento  $a_{ij} + b_{ij}$ .**Esempio 8.5**

Date le due matrici

$$A = \begin{pmatrix} 1 & 3 & -1 \\ 2 & -1 & 0 \\ 2 & 3 & 5 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 0 & -1 & 2 \\ 1 & -3 & 2 \\ 1 & 4 & -2 \end{pmatrix}$$

si ha

$$A + B = \begin{pmatrix} 1 & 2 & 1 \\ 3 & -4 & 2 \\ 3 & 7 & 3 \end{pmatrix}.$$

.....

Ebbene, i seguenti sono esempi di gruppi (ancora abeliani):

- $$(M_{mn}(R), +) \stackrel{\text{def}}{=} \{\text{matrici } m \times n \text{ su } R, \text{ dove } R = \mathbb{Z} \text{ o un qualunque campo}\};$$
- $$(M_n(R), +) \stackrel{\text{def}}{=} \{\text{matrici quadrate } n \times n \text{ su } R = \mathbb{Z} \text{ o un qualunque campo}\}.$$

DEFINIZIONE 8.6 Siano  $A = (a_{ij})$  e  $B = (b_{ij})$  due matrici quadrate  $n \times n$ . Il loro *prodotto* (cosiddetto righe per colonne) è la matrice, che si indica con  $AB$ , il cui elemento di posizione  $ij$  è

$$(2.1) \quad c_{ij} = \sum_{k=1}^n a_{ik} b_{kj} = a_{i1} b_{1j} + a_{i2} b_{2j} + \dots + a_{in} b_{nj}.$$

.....

**Esempio 8.6**

Se  $A$  e  $B$  sono le matrici dell'esempio precedente,

$$\begin{aligned} AB &= \begin{pmatrix} 1 \cdot 0 + 3 \cdot 1 + (-1) \cdot 1 & 1 \cdot (-1) + 3 \cdot (-3) + (-1) \cdot 4 & 1 \cdot 2 + 3 \cdot 2 + (-1) \cdot (-2) \\ 2 \cdot 0 + (-1) \cdot 1 + 0 \cdot 1 & 2 \cdot (-1) + (-1) \cdot (-3) + 0 \cdot 4 & 2 \cdot 2 + (-1) \cdot 2 + 0 \cdot (-2) \\ 2 \cdot 0 + 3 \cdot 1 + 5 \cdot 1 & 2 \cdot (-1) + 3 \cdot (-3) + 5 \cdot 4 & 2 \cdot 2 + 3 \cdot 2 + 5 \cdot (-2) \end{pmatrix} = \\ &= \begin{pmatrix} 2 & -14 & 10 \\ -1 & 1 & 2 \\ 8 & 9 & 0 \end{pmatrix}. \end{aligned}$$

Se facciamo il prodotto nell'altro ordine, ossia il prodotto  $BA$ , otteniamo un risultato diverso (si verifichi). Infatti il prodotto tra matrici non è abeliano, ossia non è vero che per ogni  $A$  e  $B$   $AB = BA$ .

Sarà questa quindi l'operazione che renderà il gruppo non abeliano. Ma andiamo per gradi. La matrice che funge da elemento neutro per la moltiplicazione è la matrice

$$I = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

ossia la matrice  $n \times n$  che ha tutti zeri salvo che sulla diagonale principale (ossia nelle posizioni  $ii$ , dove ha tutti 1). L'inversa  $A^{-1}$  di una matrice  $A$  è la matrice tale che

$$A \cdot A^{-1} = A^{-1} \cdot A = I.$$

Ricordando che il determinante di una matrice  $2 \times 2$  è definito come

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc,$$

è noto che l'essere il determinante diverso da 0 assicura che la matrice è invertibile e che  $\det(AB) = \det A \cdot \det B$ . Si hanno allora i seguenti ulteriori due esempi di gruppi (questa volta non abeliani):

$$(GL_2(\mathbb{R}), \cdot) \stackrel{\text{def}}{=} \{A \in M_2(\mathbb{R}) \text{ dotate di inversa, cioè con } \det A \neq 0\};$$

$$(SL_2(\mathbb{R}), \cdot) \stackrel{\text{def}}{=} \{A \in M_2(\mathbb{R}) \mid \det A = 1\}.$$

Nei prossimi paragrafi avremo modo di studiare altre due classi di gruppi non abeliani: i *gruppi simmetrici* e i *gruppi diedrali*.

Se un gruppo  $(G, *)$  è finito, con  $n$  (non troppo grande) elementi  $g_1, g_2, \dots, g_n$ , si può rappresentarlo attraverso la sua *tavola moltiplicativa* al modo seguente:

*	$g_1$	$g_2$	$g_3$	$\dots$	$g_j$	$\dots$	$g_n$
$g_1$							
$g_2$							
$g_3$							
$\vdots$							
$g_i$	$\dots$	$\dots$	$\dots$	$\dots$	$g_i * g_j$	$\dots$	$\dots$
$\vdots$							
$g_n$							

**DEFINIZIONE 8.7** Un *sottogruppo*  $S$  di un gruppo  $(G, \cdot)$  è un sottoinsieme non vuoto di  $G$  che è esso stesso un gruppo rispetto alla medesima operazione di  $G$ .  $\blacksquare$

Quindi un sottoinsieme  $S$  di un gruppo  $(G, \cdot)$  è un sottogruppo se e solo se

- (a) l'elemento neutro  $e$  di  $G$  appartiene a  $S$ ;
- (b)  $S$  è chiuso rispetto all'operazione di  $G$ , ossia  $\forall s, t \in S$  si ha  $st \in S$ ; in altre parole, l'operazione  $\cdot$  di  $G$  è anche operazione in  $S$ , ossia

$$\cdot : S \times S \longrightarrow S;$$

- (c) per ogni  $s$  in  $S$ ,  $s^{-1} \in S$ .

Si noti che l'associatività di  $S$  viene "ereditata" dall'associatività di  $G$ .

**OSSERVAZIONE**  $S = \{1, -1\}$  è un sottoinsieme non vuoto di  $\mathbb{Q}$ , ed è un gruppo rispetto alla moltiplicazione, ma non è un sottogruppo di  $(\mathbb{Q}, +)$ , perché le operazioni di  $S$  e di  $\mathbb{Q}$  sono diverse.

Per indicare che un sottoinsieme  $H$  di un gruppo  $G$  è un sottogruppo di  $G$  si scrive  $H \leq G$ , oppure  $H < G$  se  $H \neq G$ .

Sussiste il seguente comodo criterio, per verificare se un sottoinsieme di un gruppo  $G$  è un sottogruppo.

**PROPOSIZIONE 8.1** Un sottoinsieme non vuoto  $S$  di un gruppo  $(G, \cdot)$  è un sottogruppo di  $G$  se e solo se, dati comunque  $a$  e  $b$  in  $S$ , si ha  $ab^{-1} \in S$ .

**DIMOSTRAZIONE.** Lasciamo la dimostrazione di questo fatto agli esercizi (cfr. Eserc. 7).  $\diamond$

Diamo ora la definizione seguente.

**DEFINIZIONE 8.8** Siano  $(G, *)$  un gruppo,  $g$  un suo elemento e  $i$  un intero. Si definisce *potenza*  $g^i$  di  $g$  con esponente  $i$  il seguente elemento di  $G$ :

$$g^i = \begin{cases} \underbrace{g * g * \dots * g}_{i \text{ volte}} & \text{se } i > 0 \\ e & \text{se } i = 0 \\ \underbrace{g^{-1} * g^{-1} * \dots * g^{-1}}_{-i \text{ volte}} & \text{se } i < 0. \end{cases}$$

Come è facile verificare, valgono, per ogni  $i, j \in \mathbb{Z}$ , le seguenti relazioni:

$$g^i * g^j = g^{i+j}, \quad (g^i)^j = g^{ij}.$$

La definizione appena data si applica qualunque sia la operazione  $*$  del gruppo. Fare la potenza di un elemento  $x$  di un gruppo  $G$  equivale infatti ad iterare a partire da  $x$  o da  $x^{-1}$  (o  $-x$  nel caso additivo) l'operazione del gruppo.

Per esempio, data una matrice quadrata  $A$ , se ne possono fare le potenze: la potenza  $A^k$ ,  $k \geq 0$  è definita per ricorrenza al modo seguente:

$$A^0 = I, \quad A^k = A^{k-1}A.$$

Se  $k < 0$ ,  $A^k = (A^{-1})^{-k}$ . Vale la pena di confrontare le varie definizioni viste finora secondo che l'operazione  $*$  sia la moltiplicazione  $\cdot$  o l'addizione  $+$ :

$*$	.	$+$
elemento neutro $e$	1	0
inverso (o opposto)	$a^{-1}$ (inverso)	$-a$ (opposto)
elevamento a potenza	$a^i = \underbrace{a \cdot a \cdots a}_{i \text{ volte}}$ $a^i = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{-i \text{ volte}}$	$ia = \underbrace{a + a + \cdots + a}_{i \text{ volte}}$ se $i > 0$ $ia = \underbrace{(-a) + (-a) + \cdots + (-a)}_{-i \text{ volte}}$ se $i < 0$ .

**DEFINIZIONE 8.9** Sia  $G$  un gruppo e  $X$  un sottoinsieme di  $G$ . Si definisce *sottogruppo generato da  $X$* , e si indica con  $\langle X \rangle$ , il più piccolo sottogruppo di  $G$  contenente  $X$ .  $\blacksquare$

Il sottogruppo generato da un sottoinsieme  $X$  di  $G$  deve quindi per prima cosa essere un sottogruppo, deve contenere  $X$  e tra tutti i sottogruppi contenenti  $X$  deve essere il più piccolo. Ciò significa che  $\langle X \rangle$  coincide con l'intersezione di tutti i sottogruppi di  $G$  contenenti  $X$ , ossia

$$\langle X \rangle \triangleq \bigcap_{X \subseteq H \leq G} H$$

**OSSERVAZIONE** Se il sottoinsieme  $X$  è già un sottogruppo di  $G$ , allora ovviamente  $\langle X \rangle$  è  $X$  stesso.

Se  $X = \{g\} \subseteq G$  è costituito da un solo elemento, allora (cfr. eserc. 11)

$$\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}.$$

Esso prende il nome di *sottogruppo ciclico* generato dall'elemento  $g$ .

La seguente proposizione ci dice chi sono nel caso generale gli elementi del sottogruppo generato da un sottoinsieme  $X$ .

**PROPOSIZIONE 8.2** Sia  $X = \{x_1, x_2, \dots, x_n, \dots\}$  un sottoinsieme (finito o infinito) di un gruppo  $G$ . Allora

$$\langle X \rangle = \{t_1 \cdot t_2 \cdot t_3 \cdots t_r, \mid t_i \in X \text{ oppure } t_i^{-1} \in X, r \in \mathbb{N}\}.$$

**DIMOSTRAZIONE.** Basta provare che si tratta effettivamente di un sottogruppo di  $G$ , che contiene  $X$  e che è contenuto in ogni sottogruppo di  $G$  che contiene  $X$ .  $\diamond$

Per capire perché si devono includere in  $\langle X \rangle$  quegli elementi, facciamo un esempio, che mostri soprattutto come cambiano le cose tra il caso commutativo e quello non commutativo. Nel caso abeliano di  $(\mathbb{Z}, +)$  il sottogruppo generato dai due elementi 2 e 3 è  $\langle 2, 3 \rangle = \{2s + 3t \mid s, t \in \mathbb{Z}\}$  (che poi coincide con  $\mathbb{Z}$ ), perché si possono *raccogliere* tutti i 2 assieme e tutti i 3 assieme. Nel caso non abeliano invece non possiamo fare questo. Per esempio, se  $X = \{a, b\}$ ,  $\langle X \rangle$  sarà costituito da elementi del tipo

$$(2.2) \quad aba^{-1}baab^{-1}aaab^{-1},$$

cioè da parole di lunghezza variabile formate con un alfabeto costituito dalle lettere  $a$ ,  $b$ ,  $a^{-1}$  e  $b^{-1}$ . Si noti che una parola in cui le due lettere  $a$  e  $a^{-1}$  (o  $b$  e  $b^{-1}$ ) sono adiacenti si può semplificare cancellando il prodotto  $aa^{-1}$  (o  $bb^{-1}$ ); inoltre una parola che abbia varie lettere  $a$  adiacenti (come la (2.2)) si può semplificare ponendo  $\underbrace{aaa \cdots a}_k = a^k$ . Quindi la (2.2) coincide con l'elemento  $aba^{-1}ba^2b^{-1}a^3b^{-1}$ . A seconda del tipo di elementi che generano  $G$  ci possono essere ulteriori semplificazioni: per esempio, se il gruppo è abeliano, o se uno dei generatori, elevato ad una certa potenza, dà come risultato  $e$ , ecc.

Esempi di sottogruppi generati da un sottoinsieme

a) Sia  $G = (\mathbb{Z}, +)$ .

- (i)  $X = \{1\}$ :  $\langle 1 \rangle = \mathbb{Z}$ ;
- (ii)  $X = \{7\}$ :  $\langle 7 \rangle = 7\mathbb{Z} = \{\text{multipli di } 7\}$ ;
- (iii)  $X = \{3, 5\}$ :  $\langle 3, 5 \rangle = \mathbb{Z}$  (spiegare perché);
- (iv)  $X = \{3, 6\}$ :  $\langle 3, 6 \rangle = 3\mathbb{Z}$  (spiegare perché);
- (v)  $X = \{a, b\}$ :  $\langle a, b \rangle = d\mathbb{Z}$ , dove  $d = \text{MCD}(a, b)$ .

b) Sia  $G = (\mathbb{Z}_n, +)$ . Allora  $\langle \bar{1} \rangle = \mathbb{Z}_n$ .

c) Sia  $G = (\mathbb{Q} \setminus \{0\}, \cdot)$ . Se  $X = \{3\}$ , allora

$$\langle 3 \rangle = \{3^i \mid i \in \mathbb{Z}\} = \{\dots, \frac{1}{27}, \frac{1}{9}, \frac{1}{3}, 1, 3, 9, 27, \dots\}.$$

Sia  $g$  un elemento di un gruppo  $(G, \cdot)$ . Può succedere che per qualche  $h \in \mathbb{N}$  sia  $g^h = e$  (elemento neutro di  $G$ ): questo accade certamente nel caso in cui  $G$  è finito. Infatti dovendo il sottogruppo  $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$  essere finito, esisteranno due esponenti interi distinti  $s$  e  $t$  ( $s > t$ ) tali che  $g^s = g^t$ , da cui, posto  $h = s - t \in \mathbb{N}$ , si ha  $g^h = e$ . Ha senso allora la seguente definizione.

**DEFINIZIONE 8.10** Se  $(G, \cdot)$  è un gruppo e  $g \in G$ , si definisce *ordine* o *periodo* di  $g$  il più piccolo intero positivo  $r$ , se esiste, tale che  $g^r = e$ . Se un tale intero non esiste, si dice che  $g$  ha periodo infinito.  $\blacksquare$

Per esempio, in  $(\mathbb{Z}_8, +)$  la classe  $\bar{1}$  ha periodo 8, la classe  $\bar{2}$  ha periodo 4. In  $(\mathbb{Z}, +)$  1 ha periodo infinito (e così ogni elemento non nullo), in  $(\mathbb{C} \setminus \{0\}, \cdot)$  l'elemento  $i$  ha periodo 4. L'elemento neutro di ogni gruppo ha periodo 1.

**DEFINIZIONE 8.11** Sia  $G$  un gruppo finito. Dicesi *ordine* di  $G$ , e si indica con  $|G|$ , la sua cardinalità.

L'ordine di un elemento è strettamente legato alla cardinalità del sottogruppo da esso generato. Infatti un elemento  $g$  di un gruppo ha ordine  $n$  se e solo se il sottogruppo  $\langle g \rangle$  generato da  $g$  ha ordine  $n$ .

Abbiamo visto che ogni elemento  $g$  di un gruppo  $G$  genera un sottogruppo che si dice sottogruppo ciclico generato da  $G$ , che è contenuto (in genere propriamente) in  $G$ . Ora ci poniamo il seguente problema: dato un qualunque gruppo  $G$ , esiste un elemento  $g \in G$  tale che il sottogruppo  $\langle g \rangle$  generato da  $g$  coincide con tutto  $G$ ? In questo caso, diremo che il gruppo  $G$  è ciclico. Si dà pertanto la seguente definizione.

**DEFINIZIONE 8.12** Un gruppo  $G$  si dice *ciclico* se esiste un elemento  $g \in G$  tale che  $G = \langle g \rangle$ .

I gruppi ciclici godono di particolari proprietà.

1. Ogni gruppo ciclico è abeliano.
2. Ogni sottogruppo di un gruppo ciclico è anch'esso ciclico (cfr. eserc. 12).
3. Sia  $G = \langle g \mid g^n = 1 \rangle$  un gruppo ciclico di ordine  $n$ . Allora
  - a) l'ordine di ogni suo sottogruppo è un divisore di  $n$ ;
  - b) per ogni divisore  $k$  di  $n$  esiste uno e un solo sottogruppo di  $G$  di ordine  $k$  (cfr. eserc. 13).

#### Esempio 8.7

In  $G = \langle g \mid g^{15} = e \rangle$ , gruppo ciclico di ordine 15, il sottogruppo di ordine 5 è quello generato da  $g^{15/5} = g^3$  ed è

$$\{g^3, (g^3)^2 = g^6, (g^3)^3 = g^9, (g^3)^4 = g^{12}, (g^3)^5 = g^{15} = e\}.$$

**PROPOSIZIONE 8.3** Sia  $G$  un gruppo. Se  $g \in G$  ha periodo infinito e se  $h \neq k$ , allora  $g^h \neq g^k$ , e quindi  $\langle g \rangle$  è un sottogruppo ciclico infinito. Se invece  $g$  ha periodo  $n$ , allora  $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$  e quindi la cardinalità di  $\langle g \rangle$  è  $n$ . Inoltre  $g^h = g^k$  se e solo se  $h \equiv k \pmod{n}$ .

**DIMOSTRAZIONE.** Per la dimostrazione si rimanda all'esercizio 14.

#### Esercizi

- Sia  $(G, \cdot)$  un gruppo. Allora l'elemento neutro  $e$  è unico.
- Sia  $(G, \cdot)$  un gruppo. Provare che l'inverso di ogni elemento  $a$  di  $G$  è unico.
- Provare che l'inverso del prodotto di due elementi di  $G$  è il prodotto dei loro inversi, in ordine inverso, ossia  $(ab)^{-1} = b^{-1}a^{-1}$ . Inoltre  $(a^{-1})^{-1} = a$ .
- Si provi che in un gruppo  $(G, \cdot)$  valgono le due leggi di cancellazione:  $[ax = ay \Rightarrow x = y]$  e  $[xa = ya \Rightarrow x = y]$ .
- Provare che un sottoinsieme non vuoto  $S$  di un gruppo  $(G, \cdot)$  è un sottogruppo di  $G$  se e solo se, dati comunque  $a$  e  $b$  in  $S$ , si ha  $ab^{-1} \in S$ .
- Si provi che tutti i sottogruppi di  $(\mathbb{Z}, +)$  sono i sottoinsiemi del tipo  $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ . Se ne deduca che tutti i sottogruppi di  $\mathbb{Z}$  sono ciclici.
- Si provi che l'intersezione arbitraria di sottogruppi di un gruppo  $G$  è un sottogruppo di  $G$ .
- Si provi che l'unione insiemistica di due sottogruppi di un gruppo  $G$  è un sottogruppo di  $G$  se e solo se uno dei due sottogruppi è contenuto nell'altro. Si verifichi questo fatto nel caso di due sottogruppi di  $(\mathbb{Z}, +)$ .
- Si verifichi che, se  $G$  è un gruppo e  $g$  è un suo elemento, il sottoinsieme  $\{g^i \mid i \in \mathbb{Z}\}$  è un sottogruppo contenente  $g$  e che è il più piccolo tra tutti i sottogruppi contenenti  $g$  e che quindi  $\{g^i \mid i \in \mathbb{Z}\} = \langle g \rangle$ .
- Provare che ogni sottogruppo di un gruppo ciclico  $G$  è un gruppo ciclico.
- Sia  $G = \langle g \mid g^n = 1 \rangle$  un gruppo ciclico di ordine  $n$ . Allora
  - a. L'ordine di ogni suo sottogruppo è un divisore di  $n$ .
  - b. Per ogni divisore  $k$  di  $n$  esiste uno e un solo sottogruppo di  $G$  di ordine  $k$ .
- Sia  $G$  un gruppo e sia  $g$  un suo elemento. Provare che
  - a. Se  $g \in G$  ha periodo infinito e se  $h \neq k$ , allora  $g^h \neq g^k$ , e quindi  $\langle g \rangle$  è un sottogruppo ciclico infinito.
  - b. Se invece  $g$  ha periodo  $n$ , allora  $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$  e quindi la cardinalità di  $\langle g \rangle$  è  $n$ . Inoltre  $g^h = g^k$  se e solo se  $h \equiv k \pmod{n}$ .
- Siano  $S$  e  $T$  due sottogruppi di un gruppo  $G$ . Indicato con  $ST = \{st \mid s \in S, t \in T\}$ , si provi che  $ST$  è un sottogruppo se e solo se  $ST = TS$  (uguaglianza di sottoinsiemi).
- Si provi che l'insieme  $S$  delle matrici  $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$  dove  $a, b \in \mathbb{R}$  e non sono contemporaneamente nulli è un sottogruppo di  $(GL_2(\mathbb{R}), \cdot)$ .

- Si dimostri che, se  $a$  e  $b$  sono elementi di un gruppo  $G$  tali che  $ab = ba$ , allora il sottogruppo generato da  $X = \{a, b\}$  è abeliano.
- Sia  $G$  un gruppo abeliano e  $n$  un intero positivo. Sia  $S$  il sottoinsieme di  $G$  formato da tutte le potenze  $n$ -esime degli elementi di  $G$ , ossia  $S \stackrel{\text{def}}{=} \{g^n \mid g \in G\}$ . Si provi che  $S$  è un sottogruppo di  $G$ .
- Si provi che per ogni  $n \in \mathbb{N}$  l'insieme  $U(\mathbb{Z}_n)$  degli elementi invertibili di  $\mathbb{Z}_n$  è un gruppo rispetto alla moltiplicazione.
- Si provi che in un gruppo  $(G, \cdot)$ , dati comunque due elementi  $a$  e  $b$  di  $G$ , ciascuna delle equazioni  $ax = b$ ,  $ya = b$  ammette un'unica soluzione.
- Sia  $(G, \cdot)$  un gruppo. Sia  $s$  un fissato elemento di  $G$ . Si definisca in  $G$  una nuova operazione  $*$  al modo seguente:  $a * b \stackrel{\text{def}}{=} a \cdot s \cdot b \quad \forall a, b \in G$ . Si dica se  $(G, *)$  è un gruppo.
- Si consideri il gruppo  $(\mathbb{Q} \setminus \{0\}, \cdot)$ . Decidere se il sottoinsieme  $S := \{\frac{1}{n} \mid n \in \mathbb{Z} \setminus \{0\}\}$  è un sottogruppo.
- Si consideri il gruppo  $(\mathbb{Q} \setminus \{0\}, \cdot)$ . Decidere se il sottoinsieme  $S := \{n \mid n \in \mathbb{Z} \setminus \{0\}\}$  è un sottogruppo.
- Si considerino i sottoinsiemi  $X = \{\bar{0}, \bar{2}, \bar{4}\}$  e  $Y = \{\bar{1}, \bar{3}, \bar{5}\}$  di  $\mathbb{Z}_6$ . Dire se  $X$  e  $Y$  sono sottogruppi di  $(\mathbb{Z}_6, +)$ .
- Si consideri l'insieme  $S = \mathbb{R} \setminus \{-1\}$  costituito da tutti i numeri reali diversi da  $-1$ .
  - Si dica, motivando la risposta, se  $S$  è un gruppo rispetto all'ordinaria moltiplicazione tra numeri reali.
  - Si dica se è un gruppo rispetto alla moltiplicazione:  $x * y \stackrel{\text{def}}{=} x + y + xy, \quad \forall x, y \in S$ .
- Determinare tutti i sottogruppi di  $\mathbb{Z}$  che contengono il numero 6.
- Sia  $*$  l'operazione su  $\mathbb{N}$  così definita:  $a * b$  si ottiene a partire da  $a$  e  $b$  rappresentando  $a$  e  $b$  in base 10 e sommando modulo 10 le cifre corrispondenti. In pratica,  $a * b$  si ottiene facendo l'addizione di  $a$  e  $b$  secondo le regole usuali, ma dimenticandosi del riporto. Per esempio,
- $$1097 * 9023 = 10, \quad 342 * 1773 = 1015.$$
- Dire se  $(\mathbb{N}, *)$  è un gruppo. Si ripeta lo stesso esercizio, sostituendo la base 10 con una base arbitraria  $n$ .
- Si provi che un gruppo non abeliano non è mai ciclico.
- Si provi che se  $g$  è un elemento di un gruppo  $G$  tale che  $g^n = e$  per qualche  $n \in \mathbb{N}$ , allora il periodo  $m$  di  $g$  è un divisore di  $n$ .
- Provare che un elemento  $\bar{a} \in \mathbb{Z}_n$  ha ordine  $n/d$ , dove  $d = \text{MCD}(a, n)$ .
- Si determinino in  $\mathbb{Z}_{10000}$  tutti gli elementi di ordine 4 e 8.

### 3 IL GRUPPO SIMMETRICO $S_n$

Sia  $X$  un insieme e sia  $S(X)$  l'insieme di tutte le corrispondenze biunivoche di  $X$  in sé. Se introduciamo in  $S(X)$  la composizione  $\circ$  di funzioni, questa è una *operazione* in  $S(X)$  perché la composizione di corrispondenze biunivoche è ancora una corrispondenza biunivoca. Non è difficile provare che  $(S(X), \circ)$  è un gruppo. Se  $X = \{x_1, x_2, \dots, x_n\}$  ha cardinalità  $n$ , allora  $S(X)$  si indica con  $S_n$  e  $(S_n, \circ)$  prende il nome di *gruppo simmetrico di grado  $n$* . Dato che è uno dei primi esempi di gruppo non abeliano che incontriamo, vale la pena di studiarlo un po' più in dettaglio.

Sia  $X = \{1, 2, \dots, n\}$ . Ogni elemento  $\sigma$  di  $S_n$ , in quanto corrispondenza biunivoca di  $X$  in sé, rappresenta una *permutazione* di  $\{1, 2, \dots, n\}$ . Quindi la cardinalità  $|S_n|$  di  $S_n$  è  $n!$

Sia  $n = 5$ ,  $X = \{1, 2, 3, 4, 5\}$  e sia  $\sigma$  la corrispondenza (biunivoca) che agisce al modo seguente:

$$\begin{aligned} \sigma : X &\longrightarrow X \\ 1 &\longmapsto 5 \\ 2 &\longmapsto 1 \\ 3 &\longmapsto 4 \\ 4 &\longmapsto 3 \\ 5 &\longmapsto 2. \end{aligned}$$

Per ridurre lo spazio, scrivremo  $\sigma$  come matrice  $2 \times 5$  (cioè a 2 righe e 5 colonne) al modo seguente:

$$(3.1) \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}.$$

Si noti che, in virtù della biunivocità della  $\sigma$ , nella seconda riga, che contiene le immagini degli elementi di  $X$ , figurano tutti e soli gli elementi della prima riga, in ordine diverso. In generale, un elemento di  $S_n$  si indicherà con una matrice  $2 \times n$  del tipo seguente:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ i_1 & i_2 & i_3 & i_4 & \dots & i_n \end{pmatrix}.$$

Il *composto* delle due permutazioni  $\sigma$  e  $\tau$ , dove per esempio,  $\sigma$  è la permutazione di prima e  $\tau$  è la permutazione

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$

è la permutazione che si ottiene operando dapprima su  $X$  con la  $\tau$  e poi con la  $\sigma$ , cioè il prodotto

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$

si deve fare da *destra a sinistra* (trattandosi di un ordinario prodotto operatorio); il risultato è la permutazione

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}.$$

Se facciamo il prodotto nell'ordine inverso, cioè  $\tau \circ \sigma$ , il risultato è:

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$$

che è diversa dalla precedente. Il gruppo  $(S_n, \circ)$  è pertanto, per  $n > 2$ , un gruppo non abeliano: per  $n = 2$ ,  $S_2$  contiene solo due elementi, di cui uno l'identità, quindi è ovviamente abeliano. D'ora in poi scriveremo  $\sigma \circ \tau = \sigma\tau$ .

Indicheremo con  $id$  l'elemento neutro di  $S_n$ , ossia la permutazione identica

$$id = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}.$$

È facile calcolare l'inversa di una permutazione: è la permutazione ottenuta semplicemente scambiando le due righe e poi riordinando le colonne in modo che gli elementi della prima riga siano nell'ordinamento naturale. Per esempio, l'inversa della permutazione

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}$$

è la permutazione

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 4 & 2 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}.$$

A partire da una permutazione  $\sigma$  si possono costruire tutte le sue potenze  $\sigma^k$  ad esponenti interi. Sia  $r$  il minimo intero positivo tale che  $\sigma^r = id$ . Tale intero esiste sicuramente, come si è visto nel paragrafo precedente, ed è l'ordine o periodo della permutazione  $\sigma$  (cfr. definizione 8.10).

#### Esempio 8.8

Calcoliamo il periodo della permutazione

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}.$$

Le varie potenze di  $\sigma$  sono

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \neq id, \quad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} \neq id,$$

$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} \neq id, \quad \sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = id.$$

Quindi il periodo di  $\sigma$  è 5.

Se il periodo è elevato, si dovranno fare tante moltiplicazioni per arrivare ad individuarlo e d'altra parte l'esame della permutazione non ci dà nessuna informazione di quale possa essere il suo periodo. Vedremo ora che, utilizzando una diversa notazione per una permutazione  $\sigma$ , la scrittura stessa di  $\sigma$  ci fornirà direttamente il suo periodo. Dobbiamo premettere alcune definizioni.

Si fissi una permutazione  $\sigma$  in  $S_n$  e si definisca in  $X$  la seguente relazione:

$$(3.2) \quad x =_{\sigma} y \iff y = \sigma^i(x) \text{ per qualche } i \in \mathbb{Z}.$$

Si verifica facilmente che si tratta di una relazione di equivalenza definita su  $X$ . Ne segue che  $X$  viene ripartito in classi di equivalenza. Queste classi hanno un nome speciale, come risulta dalla seguente definizione.

**DEFINIZIONE 8.13** Fissata una permutazione  $\sigma \in S_n$ , si definisce orbita  $\mathcal{O}_\sigma(x)$  dell'elemento  $x \in X$  sotto l'azione di  $\sigma$  la classe di equivalenza di  $x$  rispetto alla relazione 3.2, ossia

$$\mathcal{O}_\sigma(x) \stackrel{\text{def}}{=} \{y \in X \mid y = \sigma^i(x) \text{ per qualche } i \in \mathbb{Z}\}. \quad \blacksquare$$

Essendo  $X$  finito, dato comunque un  $x \in X$ , esisterà un intero positivo minimo  $m = m(x)$  tale che  $\sigma^m(x) = x$ : infatti, dovranno esistere due interi distinti  $h$  e  $k$  ( $h > k$ ) tali che  $\sigma^h(x) = \sigma^k(x)$ , da cui, applicando  $\sigma^{-k}$  ad ambo i membri, si ottiene  $\sigma^{h-k}(x) = x$

La seguente proposizione chiarisce come sono fatte le orbite.

**PROPOSIZIONE 8.4** Sia  $\sigma \in S_n$ . Detto  $m = m(x)$  l'intero positivo minimo tale che  $\sigma^m(x) = x$ , l'orbita dell'elemento  $x$  sotto l'azione di  $\sigma$  è il sottoinsieme di  $X$   $\mathcal{O}_\sigma(x) = \{x = \sigma^0(x), \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x)\}$ .

**DIMOSTRAZIONE.** Si tratta di mostrare che ogni  $\sigma^i(x)$ , con  $i \in \mathbb{Z}$ , coincide con uno degli  $m$  elementi  $x = \sigma^0(x), \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x)$  di  $X$ . Infatti, dalla  $i = mq + r$ ,  $0 \leq r < m$  si ottiene

$$\sigma^i(x) = \sigma^{\frac{mq+r}{m}}(x) = \sigma^r(\sigma^m)^q(x) = \sigma^r(\sigma^{\pm m}(\sigma^{\pm m} \cdots (\sigma^{\pm m}(x)))) = \sigma^r(x). \quad \diamond$$

**DEFINIZIONE 8.14** Un ciclo di  $\sigma$  è l'insieme ordinato

$$(x, \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x)).$$

L'intero  $m$  dicesi lunghezza del ciclo. \blacksquare

---

#### Esempio 8.9

Sia  $\sigma \in S_6$  la permutazione

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{pmatrix}.$$

Partendo da  $1 \in X$ , l'orbita di 1 mediante  $\sigma$  è il sottoinsieme di  $X$

$$\mathcal{O}_\sigma(1) = \{1, 3, 2\}.$$


---

Si noti che l'orbita di 1 mediante  $\sigma$ , essendo un sottoinsieme di  $X$ , può essere rappresentata anche come il sottoinsieme  $\{1, 2, 3\}$ , ossia è semplicemente il sottoinsieme di  $X$  costituito dagli elementi 1, 2, 3, e quindi l'ordine con cui si scrivono i suoi elementi all'interno della parentesi graffa non ha importanza. Se ora ordiniamo gli elementi di  $\mathcal{O}_\sigma(x)$  in modo che ogni elemento sia il trasformato mediante la  $\sigma$  del precedente e il primo sia il trasformato dell'ultimo, allora otteniamo un *ciclo* della permutazione  $\sigma$ . In questo caso il ciclo che si ottiene partendo dall'elemento 1 è  $(1, 3, 2)$ . Per distinguere le due nozioni, gli elementi di un ciclo si dispongono tra parentesi tonde. È chiaro che anche  $(3, 2, 1)$  coincide con il ciclo  $(1, 3, 2)$ , e così anche  $(2, 1, 3)$ , ma non così il ciclo  $(1, 2, 3)$ , perché l'elemento 2 non è il trasformato mediante la  $\sigma$  di 1.

Partiamo ora da un elemento che non stia nell'orbita  $\mathcal{O}_\sigma(1)$ , per esempio 5, e calcoliamo la sua orbita mediante la  $\sigma$ . Sarà  $\mathcal{O}_\sigma(5) = \{4, 5, 6\}$ . Il ciclo corrispondente è  $(5, 6, 4) = (6, 4, 5) = (4, 5, 6)$ .

Non ci sono altri elementi in  $X$  che non siano già contenuti nei cicli considerati, quindi i cicli della permutazione  $\sigma$  sono  $(1, 3, 2)$  e  $(5, 6, 4)$ .

**OSSERVAZIONE** Si noti che ciascuno dei cicli  $(1, 3, 2)$  e  $(5, 6, 4)$  rappresenta una permutazione, precisamente quella che manda ogni elemento del ciclo nel successivo e l'ultimo nel primo, e lascia fissi tutti gli altri elementi. Quindi  $\gamma_1 = (1, 3, 2)$  è un altro modo di scrivere la permutazione  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 5 & 6 \end{pmatrix}$  e  $\gamma_2 = (5, 6, 4)$  è la permutazione  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 & 4 \end{pmatrix}$ .

Il fatto notevole è che la permutazione originaria  $\sigma$  risulta uguale al prodotto dei suoi due cicli  $\gamma_1$  e  $\gamma_2$  (ed è indipendente dall'ordine con cui li prendiamo, dato che i due cicli  $\gamma_1$  e  $\gamma_2$  sono disgiunti):

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 & 4 \end{pmatrix}.$$

Potremo quindi scrivere direttamente

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{pmatrix} = \gamma_1 \gamma_2 = (1, 3, 2)(5, 6, 4) = \gamma_2 \gamma_1 = (5, 6, 4)(1, 3, 2).$$

Il risultato vale in generale. La dimostrazione è lasciata negli esercizi (cfr. eserc. 32).

**PROPOSIZIONE 8.5** Ogni permutazione  $\sigma \in S_n$  è prodotto dei suoi cicli (che sono ovviamente disgiunti).

Siamo finalmente arrivati al punto cui tendevamo: una volta che si scriva una permutazione come prodotto dei suoi cicli, è immediato determinarne il periodo. Si osservi innanzitutto che un ciclo di lunghezza  $m$  ha periodo  $m$ . Ciò premesso, vale il seguente risultato, la cui dimostrazione lasciamo negli esercizi (cfr. eserc. 33).

**PROPOSIZIONE 8.6** Il periodo di una permutazione  $\sigma \in S_n$  è il minimo comune multiplo delle lunghezze dei suoi cicli.

**COROLLARIO 8.1** Ogni permutazione è prodotto di 2-cicli (o trasposizioni).

**DIMOSTRAZIONE.** Ogni ciclo si può scrivere come prodotto di trasposizioni; per esempio

$$(1, 2, 3, \dots, m) = (1, m)(1, m-1)(1, m-2) \cdots (1, 3)(1, 2).$$

Dato che ogni permutazione è prodotto dei suoi cicli, il corollario è provato.  $\diamond$

Si noti che la scrittura di una permutazione come prodotto di trasposizioni non è unica. Per esempio

$$\begin{aligned} (3.3) \quad \sigma &= (1, 2, 3)(4, 5, 6, 7) = (1, 3)(1, 2)(4, 7)(4, 6)(4, 5) \\ &= (2, 3, 1)(6, 7, 4, 5) = (1, 2)(2, 3)(6, 5)(6, 4)(6, 7). \end{aligned}$$

**DEFINIZIONE 8.15** Una permutazione si dice *pari* se è prodotto di un numero pari di trasposizioni, si dice *dispari* se è prodotto di un numero dispari di trasposizioni.  $\blacksquare$

Questa definizione potrebbe essere priva di significato se una permutazione si potesse scrivere al tempo stesso come prodotto di un numero pari e di un numero dispari di trasposizioni. Tuttavia questa eventualità non si può presentare, come si prova nel seguente teorema (che non dimostreremo).

**PROPOSIZIONE 8.7** Se una permutazione si scrive come prodotto di un numero pari (dispari) di trasposizioni, ogni altra sua scrittura come prodotto di trasposizioni è ancora costituita da un numero pari (dispari) di trasposizioni.

#### Esempio 8.10

Nella (3.3)  $\sigma$  si scrive in due modi diversi come prodotto di trasposizioni, ma la parità è la stessa.

**DEFINIZIONE 8.16** Nel gruppo simmetrico  $S_n$  il sottoinsieme costituito dalle permutazioni pari si indica con la seguente notazione:

$$A_n \stackrel{\text{def}}{=} \{\text{permutazioni pari di } S_n\}.$$

Si tratta di un sottogruppo di  $S_n$  (cfr. eserc. 36), che prende il nome di *sottogruppo alterno*.

**PROPOSIZIONE 8.8** Il sottogruppo alterno  $A_n$  ha  $\frac{n!}{2}$  elementi.

**DIMOSTRAZIONE.** Siano  $\pi_1, \pi_2, \dots, \pi_k$  le  $k$  permutazioni pari (tutte diverse) che dobbiamo contare. Sia  $\tau$  una qualunque trasposizione. Allora le permutazioni  $\pi_1\tau, \pi_2\tau, \dots, \pi_k\tau$  sono permutazioni dispari e tutte distinte. Che siano dispari è ovvio. Quanto al fatto che siano tutte distinte, supponiamo che sia  $\pi_i\tau = \pi_j\tau$  per qualche indice  $i \neq j$ . Allora, per le leggi di cancellazione dei gruppi (cfr. eserc. 6 del par. 2)

$$\pi_i\tau\tau^{-1} = \pi_j\tau\tau^{-1} \implies \pi_i = \pi_j.$$

Abbiamo quindi trovato *almeno*  $k$  permutazioni dispari, cioè il numero  $h$  delle permutazioni dispari è maggiore o uguale del numero  $k$  delle permutazioni pari. Ma ora ripetiamo lo stesso discorso partendo dalle permutazioni dispari. Siano  $\delta_1, \delta_2, \dots, \delta_h$  le  $h$  permutazioni dispari. Allora  $\delta_1\tau, \delta_2\tau, \dots, \delta_h\tau$  sono  $h$  permutazioni pari, da cui segue che  $k \geq h$ . Confrontando con la relazione precedente, possiamo concludere che  $k = h$ .  $\diamond$

Esaminiamo in dettaglio il caso  $n = 3$ . Il gruppo  $S_3$  ha 6 elementi,

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

che nella notazione ciclica sono

$$id, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2).$$

La tavola di moltiplicazione di questo gruppo è la seguente:

$\circ$	$id$	$(1, 2, 3)$	$(1, 3, 2)$	$(1, 2)$	$(1, 3)$	$(2, 3)$
$id$	$id$	$(1, 2, 3)$	$(1, 3, 2)$	$(1, 2)$	$(1, 3)$	$(2, 3)$
$(1, 2, 3)$	$(1, 2, 3)$	$(1, 3, 2)$	$id$	$(1, 3)$	$(2, 3)$	$(1, 2)$
$(1, 3, 2)$	$(1, 3, 2)$	$id$	$(1, 2, 3)$	$(2, 3)$	$(1, 2)$	$(1, 3)$
$(1, 2)$	$(1, 2)$	$(2, 3)$	$(1, 3)$	$id$	$(1, 3, 2)$	$(1, 2, 3)$
$(1, 3)$	$(1, 3)$	$(1, 2)$	$(2, 3)$	$(1, 2, 3)$	$id$	$(1, 3, 2)$
$(2, 3)$	$(2, 3)$	$(1, 3)$	$(1, 2)$	$(1, 3, 2)$	$(1, 2, 3)$	$id$

Il sottogruppo alterno  $A_3$  è

$$A_3 = \{id, (1, 2, 3), (1, 3, 2)\}.$$

Esistono in  $S_3$  altri sottogruppi. Diamo qui di seguito l'elenco completo dei sottogruppi di  $S_3$ , invitando lo studente inanzitutto a verificare che si tratta effettivamente di sottogruppi, e che non ce ne sono altri.

$$\begin{aligned} H_1 &= \{id\}, & H_2 &= \{id, (1, 2)\} = \langle (1, 2) \rangle, \\ H_3 &= \{id, (1, 3)\} = \langle (1, 3) \rangle, & H_4 &= \{id, (2, 3)\} = \langle (2, 3) \rangle, \\ A_3 &= \{id, (1, 2, 3), (1, 3, 2)\} = \langle (1, 2, 3) \rangle, & S_3 & \end{aligned}$$

Il primo e l'ultimo nella lista (cioè il sottogruppo ridotto al solo elemento neutro, e l'intero gruppo) prendono il nome di sottogruppi *banali*. Si noti anche che ogni sottogruppo di  $S_3$  diverso dall'intero gruppo è abeliano.

**OSSERVAZIONE** Chiudiamo ponendoci una domanda. Di che tipo sono le possibili scritture di una permutazione come prodotto di cicli disgiunti? In  $S_3$  abbiamo visto che le permutazioni si possono scrivere:

1. Come prodotto di 3 cicli di lunghezza 1.
2. Come prodotto di un ciclo di lunghezza 2 per un ciclo di lunghezza 1.

### 3. Come ciclo di lunghezza 3:

In definitiva le possibili *strutture cicliche* di  $S_3$  sono in tutto tre e dei seguenti tipi:

$$(-)(-)(-), \quad (-,-)(-), \quad (-,-,-) :$$

la permutazione identica corrisponde al primo tipo, le trasposizioni, ossia le permutazioni  $(1, 2), (1, 3), (2, 3)$  corrispondono al secondo tipo, mentre le due permutazioni  $(1, 2, 3)$  e  $(1, 3, 2)$  al terzo tipo. Ciascuna delle sei permutazioni di  $S_3$  è di uno dei tre tipi di cui sopra.

Passiamo a  $S_4$ . I possibili tipi di strutture cicliche sono cinque e dei seguenti tipi:

$$(-)(-)(-)(-), \quad (-,-)(-)(-), \quad (-,-,-)(-), \quad (-,-,-,-), \quad (-,-)(-,-) .$$

Ancora, la permutazione identica è l'unica del primo tipo, le permutazioni come  $(1, 2)$ , o  $(3, 4)$ , ecc. (ossia le trasposizioni) del secondo tipo, le permutazioni che sono dei 3-cicli, come  $(1, 3, 4)$  o  $(1, 4, 2)$  del terzo tipo, i 4-cicli, ossia le permutazioni come  $(1, 2, 3, 4)$  del quarto e infine i prodotti di due trasposizioni, come  $(1, 2)(3, 4)$ , dell'ultimo tipo.

Diamo la seguente definizione.

**DEFINIZIONE 8.17** Fissato l'intero  $n$ , si dice che la successione di interi positivi  $n_1, n_2, \dots, n_t$  con  $n_1 \geq n_2 \geq n_3 \dots \geq n_t$  costituisce una *partizione* dell'intero  $n$  se  $n = n_1 + n_2 + \dots + n_t$ .  $\blacksquare$

Per esempio, le partizioni dell'intero 3 sono:

$$\begin{aligned} 3 &= 3 \\ 3 &= 2 + 1 \\ 3 &= 1 + 1 + 1 . \end{aligned}$$

Le partizioni dell'intero 4 sono

$$\begin{aligned} 4 &= 4 \\ 4 &= 3 + 1 \\ 4 &= 2 + 2 \\ 4 &= 2 + 1 + 1 \\ 4 &= 1 + 1 + 1 + 1 . \end{aligned}$$

Le partizioni di 5 sono

$$\begin{aligned} 5 &= 5 \\ 5 &= 4 + 1 \\ 5 &= 3 + 2 \\ 5 &= 3 + 1 + 1 \\ 5 &= 2 + 2 + 1 \\ 5 &= 2 + 1 + 1 + 1 \\ 5 &= 1 + 1 + 1 + 1 + 1 . \end{aligned}$$

Le partizioni di 6 sono

$$\begin{aligned} 6 &= 6 \\ 6 &= 5 + 1 \\ 6 &= 4 + 2 \\ 6 &= 4 + 1 + 1 \\ 6 &= 3 + 3 \\ 6 &= 3 + 2 + 1 \\ 6 &= 3 + 1 + 1 + 1 \\ 6 &= 2 + 2 + 2 \\ 6 &= 2 + 2 + 1 + 1 \\ 6 &= 2 + 1 + 1 + 1 + 1 \\ 6 &= 1 + 1 + 1 + 1 + 1 + 1. \end{aligned}$$

Si possono rappresentare come nelle Figure 8.1, 8.2, 8.3, 8.4.

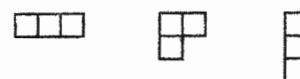


Figura 8.1. Le partizioni di 3.

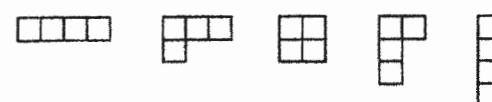


Figura 8.2. Le partizioni di 4.

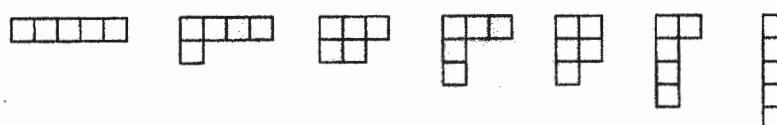


Figura 8.3. Le partizioni di 5.

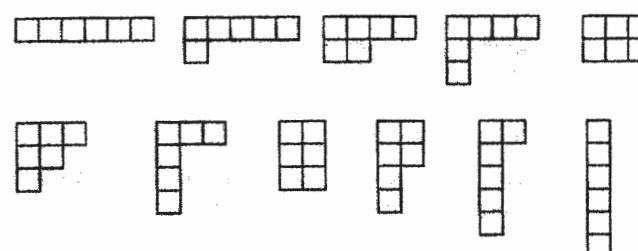


Figura 8.4. Le partizioni di 6.

Ora, si riconoscerà che ogni partizione dell'intero 3 corrisponde ad una delle tre strutture cicliche di una permutazione di  $S_3$  (l'ultima corrisponde all'identità, la prima ad un 3-ciclo). Ogni partizione dell'intero 4 corrisponde ad una delle cinque strutture cicliche di una permutazione di  $S_4$  (l'ultima corrisponde all'identità, la prima ad un 4-ciclo), ecc.

Il numero di partizioni distinte dell'intero  $n$  si indica con  $p(n)$ :  $p(3) = 3$ ,  $p(4) = 5$ ,  $p(5) = 7$ ,  $p(6) = 11$ . Non esiste una formula chiusa per determinare  $p(n)$  per ogni  $n$ . I numeri  $p(n)$  compaiono come coefficienti in una serie (detta *funzione generatrice* di  $p(n)$ ). Precisamente si ha

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty} \frac{1}{1-x^k}.$$

Indichiamo con  $p_k(n)$  il numero di partizioni di  $n$  con esattamente  $k$  parti: per esempio  $p_1(5) = 1$ ,  $p_2(5) = 2$ ,  $p_3(5) = 2$ ,  $p_4(5) = 1$ ,  $p_5(5) = 1$ . Convenzionalmente si pone  $p_0(0) = p(0) = 1$ . Si ha sempre  $p_n(n) = 1$  per ogni  $n$ ,  $p_1(n) = 1$  e  $p_{n-1}(n) = 1$  se  $n > 1$ . Non è difficile verificare la seguente relazione ricorsiva che permette di determinare  $p_k(n)$  per  $k$  e  $n$  sufficientemente piccoli:

$$p_k(n) = p_{k-1}(n-1) + p_k(n-k).$$

La teoria delle partizioni di un intero è un settore affascinante della matematica.

### Esercizi

(1) Provare la proposizione 8.5.

(2) Dimostrare la proposizione 8.6.

(3) Nel gruppo simmetrico  $S_4$  si considerino le seguenti permutazioni:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

a. Determinare il periodo di  $\sigma$  e di  $\tau$ .

b. Determinare  $\sigma^{-1}$  e  $\tau^{-1}$ .

c. Decidere se il sottoinsieme di  $S_4$   $S = \{id, \sigma, \tau\}$  è un sottogruppo di  $S_4$ .

(4) Nel gruppo simmetrico  $S_4$  si considerino le seguenti permutazioni:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

a. Determinare il periodo di  $\sigma$  e di  $\tau$ .

b. Determinare  $\sigma^{-1}$  e  $\tau^{-1}$ .

c. Decidere se il sottoinsieme di  $S_4$   $S = \{id, \sigma, \tau\}$  è un sottogruppo di  $S_4$ .

Si provi che il sottoinsieme di  $S_n$  costituito dalle permutazioni pari è un sottogruppo. E il sottoinsieme costituito dalle permutazioni dispari?

In  $S_4$  calcolare la cardinalità dell'insieme delle permutazioni che hanno una fissata struttura ciclica. Verificare che la somma delle cardinalità di tali sottoinsiemi al variare della struttura ciclica è 24 (ossia la cardinalità di  $S_4$ ).

Stesso esercizio per  $S_5$ . Verificare che la somma delle cardinalità di tali sottoinsiemi al variare della struttura ciclica è 120 (ossia la cardinalità di  $S_5$ ).

#### 4 ALTRI ESEMPI DI GRUPPI: I GRUPPI DIEDRALI

Sia data una figura nel piano. I movimenti rigidi (cioè le corrispondenze biunivoche del piano che conservano le distanze tra punti, o *isometrie del piano*) che la mutano in sé corrispondono alle *simmetrie* della figura stessa. Più simmetrica è la figura, maggiori saranno i movimenti che potremo fare sulla figura mutandola in sé.

Si pensi per esempio alla figura seguente:

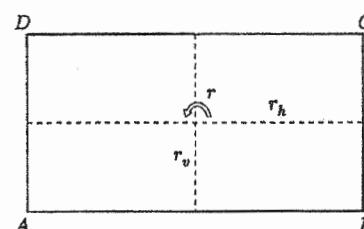


Figura 8.5. Simmetrie di un rettangolo.

Ribaltando il rettangolo rispetto a ciascuna delle rette tratteggiate, il rettangolo viene mutato in sé. È facile vedere che l'insieme dei movimenti che mutano in sé il rettangolo è costituito da quattro elementi: l'identità  $e$  (ossia il "movimento" che non muove nulla), il ribaltamento  $r_h$  rispetto all'asse tratteggiato orizzontale, il ribaltamento  $r_v$  rispetto all'asse tratteggiato verticale, e infine la rotazione  $r$  in senso antiorario di  $\pi$  attorno al centro del rettangolo. L'insieme di questi movimenti forma un gruppo, come si verifica immediatamente. Tale gruppo prende il nome di *gruppo di Klein* e si indica anche con la lettera  $V$  (da *vier* = quattro). La sua tavola di moltiplicazione è la seguente:

$\circ$	$e$	$r$	$r_h$	$r_v$
$e$	$e$	$r$	$r_h$	$r_v$
$r$	$r$	$e$	$r_v$	$r_h$
$r_h$	$r_h$	$r_v$	$e$	$r$
$r_v$	$r_v$	$r_h$	$r$	$e$

Se, anziché partire da un rettangolo, si parte da un quadrato, saranno di più i movimenti rigidi che si possono fare senza mutare la figura, cioè sono maggiori le simmetrie della figura. In questo caso il gruppo dei movimenti rigidi che mutano in sé il quadrato è costituito dall'identità, dalle tre rotazioni in senso antiorario (di  $\pi/2$ , di  $\pi$ , di

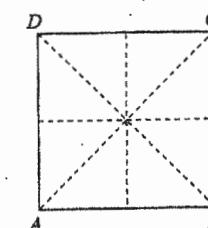


Figura 8.6. Simmetrie di un quadrato.

$3\pi/2$  rispettivamente), e dai quattro ribaltamenti (rispetto alle due rette orizzontali e verticali e alle due diagonali).

Si consideri ora il gruppo, che indicheremo con  $D_3$ , dei movimenti rigidi che mutano in sé un triangolo equilatero (fig. 8.7).

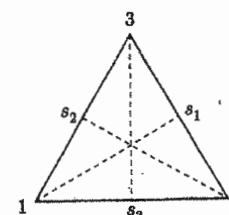


Figura 8.7. Simmetrie di un triangolo equilatero.

I possibili movimenti sono  $r_1$  = rotazione di  $\frac{2\pi}{3}$ ,  $r_2$  = rotazione di  $\frac{4\pi}{3}$ ,  $r_0$  = rotazione identica; inoltre i tre ribaltamenti  $s_1$ ,  $s_2$ ,  $s_3$  rispetto ai tre assi di simmetria del triangolo.

La tavola di moltiplicazione di questo gruppo è la seguente:

$\circ$	$id$	$r_1$	$r_2$	$s_1$	$s_2$	$s_3$
$id$	$id$	$r_1$	$r_2$	$s_1$	$s_2$	$s_3$
$r_1$	$r_1$	$r_2$	$id$	$s_3$	$s_1$	$s_2$
$r_2$	$r_2$	$id$	$r_1$	$s_2$	$s_3$	$s_1$
$s_1$	$s_1$	$s_2$	$s_3$	$id$	$r_1$	$r_2$
$s_2$	$s_2$	$s_3$	$s_1$	$r_2$	$id$	$r_1$
$s_3$	$s_3$	$s_1$	$s_2$	$r_1$	$r_2$	$id$

Si vede immediatamente che questa tavola coincide con la tavola di moltiplicazione di  $S_3$ , non appena si ponga

$$r_1 = (1, 2, 3), \quad r_2 = (1, 3, 2), \quad s_1 = (2, 3), \quad s_2 = (1, 3), \quad s_3 = (1, 2)$$

cioè non appena si faccia corrispondere ad ogni movimento rigido la corrispondente permutazione dei vertici del triangolo. Quindi il gruppo dei movimenti che mutano in sé un triangolo equilatero si può identificare con il gruppo  $(S_3, \circ)$ , la corrispondenza essendo data associando ad ogni movimento rigido che muta in sé il triangolo la

corrispondente permutazione dei vertici. Tale gruppo rientra in una classe importante di gruppi, la classe dei *gruppi diedrali*.

**DEFINIZIONE 8.18** Dicesi *gruppo diedrale*  $D_n$  il gruppo dei movimenti rigidi che mutano in sé un poligono regolare di  $n$  lati. ■■■

Vediamo in generale di studiare  $D_n$ . Esso possiede  $n$  rotazioni  $r_k(2\pi/n)$ ,  $k = 1, \dots, n$ , attorno al centro del poligono, corrispondenti agli angoli

$$\frac{2\pi}{n}, \quad 2 \cdot \frac{2\pi}{n}, \quad 3 \cdot \frac{2\pi}{n}, \dots, \quad k \cdot \frac{2\pi}{n}, \dots, \quad n \cdot \frac{2\pi}{n} = id.$$

Inoltre  $D_n$  possiede  $n$  ribaltamenti  $s_i$  ( $i = 1, \dots, n$ ) rispetto agli  $n$  assi di simmetria del poligono: se  $n$  è dispari, questi assi di simmetria sono le bisettrici degli angoli del poligono, se  $n = 2k$  è pari, sono le  $k$  bisettrici e i  $k$  assi, come si vede dalla figura 8.8:

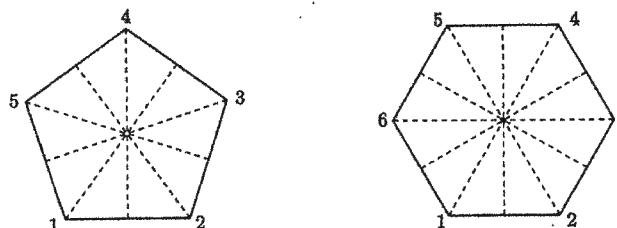


Figura 8.8. Assi di simmetria di poligoni regolari.

In definitiva  $|D_n| = 2n$ . Dato che i movimenti rigidi di un poligono regolare si possono pensare come permutazioni dei vertici, risulta  $D_n \subseteq S_n$ .

Per  $n = 3$  abbiamo visto che  $D_3 = S_3$ ; per  $n > 3$  risulta  $D_n \subsetneq S_n$ , dato che  $|D_n| = 2n$ ,  $|S_n| = n!$ , e  $2n \leq n!$ , e sono uguali solo per  $n = 3$ .

Indichiamo con  $r$  la rotazione di  $2\pi/n$ ; essa ha ordine  $n$ , e genera il sottogruppo di tutte le rotazioni, nel senso che ogni rotazione è una opportuna potenza di  $r$  (cfr. definizione 8.8). Infatti  $r^k = r_k(2\pi/n)$ ,  $k = 1, \dots, n$ : Inoltre, l'ordine della rotazione  $r^k$  è  $n/d$ , con  $d = \text{MCD}(n, k)$ . L'ordine di ogni ribaltamento  $s_i$  è ovviamente 2.

#### Esercizi

(a) Si provi che  $D_n$ , per  $n > 2$  è un gruppo non abeliano.

(b) Si studi in dettaglio il gruppo  $D_4$  delle simmetrie di un quadrato, determinando il periodo di ciascuno dei suoi elementi.

## ■ 5 ANELLI

Passiamo ora allo studio delle altre strutture algebriche, gli *anelli*, che abbiamo già incontrato. Esempi di tali strutture sono gli interi rispetto alle ordinarie operazioni di addizione e moltiplicazione, i polinomi rispetto alle ordinarie operazioni di addizione e moltiplicazione tra polinomi, ecc. Riprendiamo la definizione formale di anello.

**DEFINIZIONE 8.19** Un *anello*  $(R, +, \cdot)$  è un insieme  $R$  dotato di due operazioni binarie,  $+$  (addizione) e  $\cdot$  (moltiplicazione), tali che valgano le seguenti proprietà:

- (i)  $a + b = b + a$ ,  $\forall a, b \in R$   
(proprietà commutativa dell'addizione);
- (ii)  $(a + b) + c = a + (b + c)$ ,  $\forall a, b, c \in R$   
(proprietà associativa dell'addizione);
- (iii) esiste un unico elemento  $0 \in R$  tale che  $a + 0 = 0 + a = a$ ,  $\forall a \in R$  (esistenza dell'elemento neutro rispetto all'addizione);
- (iv) per ogni  $a \in R$  esiste un unico elemento,  $-a$ , tale che  $a + (-a) = (-a) + a = 0$  (esistenza dell'opposto);
- (v)  $a \cdot b = b \cdot a$ ,  $\forall a, b \in R$   
(proprietà commutativa della moltiplicazione);
- (vi)  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ ,  $\forall a, b, c \in R$   
(proprietà associativa della moltiplicazione);
- (vii) esiste in  $R$  un unico elemento,  $1$ , tale che  $a \cdot 1 = 1 \cdot a = a$ ,  $\forall a \in R$   
(esistenza dell'elemento neutro rispetto alla moltiplicazione);
- (viii)  $a \cdot (b + c) = a \cdot b + a \cdot c$ ,  $(a + b) \cdot c = a \cdot c + b \cdot c$ ,  $\forall a, b, c \in R$  (distributività della moltiplicazione rispetto all'addizione). ■■■

#### Esempi di anelli

- (a)  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  rispetto alle ordinarie operazioni di addizione e moltiplicazione.
- (b)  $\mathbb{Z}$  rispetto all'ordinaria addizione e con moltiplicazione definita ponendo  $ab = 0$  per ogni  $a, b \in \mathbb{Z}$ .
- (c)  $\mathbb{K}[x]$  e  $\mathbb{K}[x_1, x_2, \dots, x_n]$  rispetto alle ordinarie operazioni di addizione e moltiplicazione tra polinomi.
- (d) L'anello  $(\mathbb{Z}_n, +, \cdot)$  delle classi resto modulo  $n$ .
- (e) L'insieme  $M_n(\mathbb{K})$  delle matrici quadrate  $n \times n$  sopra un campo  $\mathbb{K}$ , o sopra un anello (per esempio gli interi), rispetto alle ordinarie operazioni di addizione elemento per elemento e moltiplicazione righe per colonne.
- (f) Sia  $X$  un insieme e  $\mathcal{P}(X)$  sia l'insieme delle parti di  $X$ . Definiamo in  $\mathcal{P}(X)$  le seguenti due operazioni:

$$A + B \stackrel{\text{def}}{=} (A \cup B) \cap \complement(A \cap B), \quad A \cdot B \stackrel{\text{def}}{=} A \cap B.$$

È facile vedere che si tratta di un gruppo abeliano rispetto alla prima operazione (elemento neutro è  $\emptyset$  e l'opposto di  $A \in \mathcal{P}(X)$  è l'elemento  $A$  stesso). Anche la seconda operazione è associativa, e valgono inoltre le proprietà distributive, per cui si tratta di un anello (commutativo). In questo anello ogni elemento è *idempotente*, cioè  $A^2 = A \cdot A = A$  per ogni  $A \in \mathcal{P}(X)$ .

- (g) Sia  $R$  un anello e  $X$  un arbitrario insieme non vuoto. Nell'insieme  $R^X \stackrel{\text{def}}{=} \{f : X \rightarrow R\}$  si definiscano le seguenti operazioni:

$$(f+g)(x) \stackrel{\text{def}}{=} f(x) + g(x), \quad (fg)(x) \stackrel{\text{def}}{=} f(x)g(x)$$

$\forall f, g \in R^X, \forall x \in X$ .  $(R^X, +, \cdot)$  diventa un anello: è un anello commutativo se e solo se  $R$  è commutativo, è unitario se e solo se  $R$  è unitario (la funzione unità è la funzione costante che manda ogni elemento di  $X$  nell'unità di  $R$ ). Attenzione a non confondere questa definizione di prodotto fra funzioni con la definizione di prodotto operatorio o tra funzioni!

- (h) Siano  $(R_1, +, \cdot)$  e  $(R_2, +, \cdot)$  due anelli. Nel prodotto cartesiano  $R_1 \times R_2$  si definiscano le seguenti operazioni:

$$\begin{aligned} (a_1, a_2) + (b_1, b_2) &\stackrel{\text{def}}{=} (a_1 + b_1, a_2 + b_2) \\ (a_1, a_2) \cdot (b_1, b_2) &\stackrel{\text{def}}{=} (a_1 b_1, a_2 b_2), \end{aligned}$$

dove le operazioni nel primo elemento della coppia sono le operazioni in  $R_1$ , mentre quelle nel secondo elemento della coppia sono le operazioni in  $R_2$ . L'insieme  $R_1 \times R_2$  con queste due operazioni diventa un anello che prende il nome di *prodotto cartesiano* di  $R_1$  e  $R_2$ . Spesso si indica come  $R_1 \oplus R_2$  e si chiama *somma diretta* di  $R_1$  e  $R_2$ .

La definizione ora data può estendersi al prodotto cartesiano di  $n$  anelli.

**OSSERVAZIONE** Si osservi che l'ordine con cui compaiono le operazioni in un anello è essenziale: infatti, nella definizione di anello si richiede che rispetto alla *prima* operazione sia un gruppo abeliano, mentre nel caso della seconda si richiede di meno: ossia le due operazioni *non* sono intercambiabili. Facciamo un esempio banalissimo:  $(\mathbb{Z}, +, \cdot)$  è un anello. Cosa possiamo dire di  $(\mathbb{Z}, \cdot, +)$ ? Non si tratta di un anello, perché  $(\mathbb{Z}, \cdot)$  non è un gruppo abeliano.

Un anello *finito* può essere visualizzato attraverso le sue tavole additiva e moltiplicativa, come si è visto nel caso dell'anello delle classi resto modulo 5 e modulo 6.

Dagli assiomi di anello si deducono le seguenti proprietà, che abbiamo già incontrato a proposito degli interi:

$$\begin{aligned} a \cdot 0 = 0 \cdot a = 0 & \quad \forall a \in R \\ (-a)b = a(-b) = -(ab) & \quad \forall a, b \in R. \end{aligned}$$

L'essere un dominio di integrità *non* è invece conseguenza degli assiomi di anello, dato che abbiamo esempi di anelli che sono domini di integrità (per esempio  $(\mathbb{Z}, +, \cdot)$  e  $(\mathbb{K}[x], +, \cdot)$ ) ed esempi di anelli che non lo sono, come l'anello  $(\mathbb{Z}_n, +, \cdot)$  delle classi resto modulo un numero non primo, l'anello delle matrici  $2 \times 2$  a coefficienti in  $\mathbb{Z}$  o in un campo, rispetto all'ordinaria addizione tra matrici e al prodotto righe per colonne: per esempio  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ .

Un'altra proprietà che *non* è conseguenza degli assiomi di anello è la divisione con resto (algoritmo euclideo della divisione). Basta dare un esempio di anello in cui tale

proprietà non vale. Si pensi all'anello  $(\mathbb{Z}[x], +, \cdot)$  dei polinomi a coefficienti nell'anello degli interi. Se pensiamo di dividere il polinomio  $x^2 - 2x + 2$  per  $2x^2 + 1$ , vediamo che non possiamo farlo, perché

$$x^2 - 2x + 2 = (2x^2 + 1) \cdot \frac{1}{2} - 2x + \frac{3}{2}$$

e il quoziente  $\frac{1}{2}$  e il resto  $-2x + \frac{3}{2}$  non sono elementi di  $\mathbb{Z}[x]$

**DEFINIZIONE 8.20** Un *sottoanello*  $S$  di un anello  $(R, +, \cdot)$  è un sottoinsieme di  $R$  che è esso stesso un anello rispetto alle stesse operazioni di  $R$ . ■

Per esempio, il sottoinsieme  $2\mathbb{Z}$  dei numeri pari è un sottoanello di  $(\mathbb{Z}, +, \cdot)$ , e così il sottoinsieme dei multipli di  $n$ ,  $n\mathbb{Z}$ , ecc. In  $(\mathbb{Z}_8, +, \cdot)$  il sottoinsieme  $\{0, 2, 4, 6\}$  è un sottoanello.

Tra i sottoanelli una classe importante è costituita dagli *ideali*, che abbiamo già incontrato in un contesto particolare (cfr. es. 7.1). Diamonole qui la definizione generale.

**DEFINIZIONE 8.21** Un *ideale*  $I$  di un anello  $(R, +, \cdot)$  è un sottoanello di  $R$  che verifica l'ulteriore proprietà che  $\forall r \in R$  e  $\forall i \in I$   $r \cdot i \in I$ ,  $i \cdot r \in I$ . ■

Per indicare che  $I$  è un ideale di un anello  $R$  si scrive  $I \trianglelefteq R$ .

**DEFINIZIONE 8.22** Dati due anelli  $R$  e  $R'$ , un *omomorfismo* di  $R$  in  $R'$  è una funzione  $\varphi$  da  $R$  a  $R'$  che "conserva le operazioni", cioè tale che per ogni  $a, b \in R$

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b).$$

Se la  $\varphi$  è biunivoca, allora si parla di *isomorfismo*. ■

C'è uno stretto legame tra la nozione di ideale e quella di omomorfismo tra anelli, e il legame è offerto dalla nozione di *nucleo* di un omomorfismo.

**DEFINIZIONE 8.23** Siano  $R$  e  $R'$  due anelli e sia  $\varphi$  un omomorfismo da  $R$  a  $R'$ . Si definisce *nucleo* di  $\varphi$  l'insieme degli  $r \in R$  tali che  $\varphi(r) = 0_{R'}$ . Esso si indica con  $\text{Ker } (\varphi)$ . ■

In altre parole, il nucleo di un omomorfismo è la controimmagine di  $0_{R'}$ . Non è difficile verificare che  $\text{Ker } (\varphi)$  è un ideale di  $R$  (cfr. eserc. 42). Quindi ad ogni omomorfismo resta associato un ideale di  $R$ , che è il suo nucleo. Ma vale anche il viceversa, ossia, dato comunque un ideale  $I \trianglelefteq R$ , resta definita in  $R$  una relazione  $\rho_I$  (che è di equivalenza) così definita:

$$(5.1) \quad \forall a, b \in R \quad a\rho_I b \iff a - b \in I.$$

Si può allora parlare di quoziente modulo la relazione di equivalenza  $\rho_I$ , cioè l'insieme  $R/\rho_I$  delle classi di equivalenza rispetto a  $\rho_I$ .  $R/\rho_I$  diventa un anello, che si dice *anello quoziente*, rispetto alle operazioni (ben poste).

$$(5.2) \quad \bar{a} + \bar{b} := \overline{a+b}, \quad \bar{a} \cdot \bar{b} := \overline{ab}.$$

La corrispondenza da  $R$  a  $R/\rho_I$  che associa ad ogni elemento  $r \in R$  la sua classe di equivalenza è un omomorfismo di anelli e il suo nucleo è proprio  $I$ .

Dunque, dato comunque un ideale  $I \trianglelefteq R$ , ad esso resta associato un omomorfismo di dominio  $R$  che lo ammette come nucleo e viceversa, dato comunque un omomorfismo di dominio  $R$ , il suo nucleo è un ideale.

Ci sarebbe molto di più da dire ma ce ne asteniamo. Facciamo invece un esempio.

### Esempio 8.11

Si consideri in  $(\mathbb{Z}, +, \cdot)$  l'ideale  $I = 3\mathbb{Z}$ . La  $\rho_I$  è la relazione che dichiara in relazione due interi quando la loro differenza appartiene a  $I$ : si tratta della relazione di congruenza modulo 3.  $I$  è il nucleo dell'omomorfismo

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$$

che manda  $a$  in  $\bar{a}$ . È facile vedere che la controimmagine della classe  $\bar{0}$  è esattamente  $3\mathbb{Z}$ .

Chiudiamo con un argomento che avevamo in un certo senso lasciato in sospeso. In  $\mathbb{Z}$  e in  $\mathbb{K}[x]$  abbiamo definito due concetti, la nozione di elemento irriducibile e la nozione di elemento primo (cfr. definizioni 3.6 e 3.7) e avevamo dimostrato che le due nozioni coincidono in questi anelli. Per giustificare l'introduzione di queste due definizioni che in realtà in  $\mathbb{Z}$  e in  $\mathbb{K}[x]$  coincidono, vogliamo ora dare un esempio di anello in cui le due nozioni *non coincidono*. Ricordiamo che quando abbiamo provato in  $\mathbb{Z}$  o in  $\mathbb{K}[x]$  che ogni elemento primo è irriducibile, si sono sfruttati i soli assiomi di anello. Per provare il viceversa, cioè che ogni irriducibile è primo, nella dimostrazione ci siamo invece serviti della nozione di MCD e dell'identità di Bézout. Ebbene, daremo un esempio di anello in cui esistono elementi irriducibili ma non primi.

### Esempio 8.12

Si consideri il sottoinsieme  $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$  dell'anello  $\mathbb{C}$  dei numeri complessi. Si tratta, come è facile vedere, di un sottoanello di  $\mathbb{C}$ . Proveremo che l'elemento 3 è irriducibile in  $R$  ma non primo.

**È irriducibile:** supponiamo che 3 si possa scrivere come prodotto di due numeri di  $R$ ,

$$3 = (a + b\sqrt{-5})(c + d\sqrt{-5}).$$

Prendiamo la norma dei due numeri complessi  $z = a + b\sqrt{-5}$  e  $z' = c + d\sqrt{-5}$ , ossia  $N(z) = a^2 + 5b^2$  e  $N(z') = c^2 + 5d^2$ . Ovviamente si ha  $9 = N(3) = N(z) \cdot N(z')$  ossia  $9 = (a^2 + 5b^2)(c^2 + 5d^2)$ . Questa è una relazione in  $\mathbb{N}$ , quindi deve essere  $N(z) = 1$  e  $N(z') = 9$  oppure  $N(z) = 9$  e  $N(z') = 1$  (non può essere  $N(z) = N(z') = 3$  perché la  $a^2 + 5b^2 = 3$  non ammette soluzioni intere). Ora, se  $N(z) = 1$  significa che  $a^2 + 5b^2 = 1$  ossia  $a = \pm 1$  e  $b = 0$  da cui  $z = \pm 3$  e 3 è irriducibile. Analogamente se  $N(z') = 1$ . Quindi 3 è irriducibile.

Proviamo ora che 3 non è primo. Dalla relazione

$$21 = 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5})$$

si deduce che 3 divide il prodotto  $(4 + \sqrt{-5})(4 - \sqrt{-5})$ , tuttavia non divide nessuno dei due fattori: se 3 dividesse  $4 + \sqrt{-5}$  vorrebbe dire che  $4 + \sqrt{-5} = 3 \cdot (a + b\sqrt{-5})$ , che comporterebbe la relazione assurda  $3a = 4$ . Quindi 3 non è primo.

### Esercizi

41 Provare che il sottoinsieme di  $(\mathbb{C}, +, \cdot)$   $\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}$  rispetto alle ordinarie operazioni di addizione e moltiplicazione dei numeri complessi è un sottoanello. Provare che si tratta di un dominio di integrità. Tale anello prende il nome di *anello degli interi di Gauss*.

42 Provare che il nucleo di un omomorfismo da un anello  $R$  a un anello  $R'$  è un ideale di  $R$ .

43 Si consideri l'applicazione  $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$  che associa ad ogni  $a \in \mathbb{Z}$  il suo quadruplo  $4a$ . Decidere se si tratta di un omomorfismo di anelli.

44 Provare che le operazioni 5.1 sono ben poste e che  $R/\rho_I$  diventa rispetto a queste operazioni un anello.

### Esercizi di programmazione

1 Sia  $X$  un insieme finito dotato di un'operazione  $*$  data attraverso una tavola moltiplicativa.

- Scrivere un programma che sia capace di riconoscere se l'operazione è associativa.
- Scrivere un programma che sia capace di riconoscere se l'operazione possiede un elemento neutro.
- Scrivere un programma che sia in grado di vedere se l'insieme  $X$  rispetto all'operazione  $*$  è un gruppo.

2 Sia  $(G, *)$  un gruppo finito, dato attraverso la sua tavola moltiplicativa.

- Scrivere un programma capace di riconoscere se un sottoinsieme  $S$  di  $G$  è un sottogruppo.
- Scrivere un programma che calcoli il periodo di ogni elemento.
- Scrivere un programma capace di decidere se il gruppo è ciclico.
- Scrivere un programma che, dato comunque un elemento di  $G$ , determini il sottogruppo generato.

3 Si scriva un programma che elenchi, per ogni  $n$ , le permutazioni di  $n$  elementi.

4 Si scriva un programma che scriva ogni permutazione come prodotto di cicli disgiunti.

5 Si scriva un programma che calcoli la parità di ogni permutazione.

6 Si scriva un programma che studi tutte le proprietà del gruppo  $D_4$  delle simmetrie di un quadrato (periodo degli elementi, sottogruppi, ecc.).

# 9

## L'algebra booleana

*Poi che null'altro che vacuo vento ci resta d'ogni cosa ch'esiste,  
 Poi che difetto e sconfitta colgono al fine ogni cosa,  
 considera bene: ogni cosa che è, è in realtà nulla;  
 medita bene: ogni cosa ch'è nulla, è in realtà tutto.*  
 Omar Khayyām, QUARTINA 29  
 Trad. A. Bausani

Un circuito elettrico può essere acceso (*on*) o spento (*off*) e non può essere contemporaneamente acceso e spento. Una proposizione è un'affermazione che può essere vera o falsa, ma non contemporaneamente vera e falsa. Abbiamo a che fare con due esempi di *sistemi a due stati*: nel caso dei circuiti i due stati sono *on* e *off*, nel caso delle proposizioni sono *vero* e *falso*. Ora, come spesso accade in matematica (è uno dei suoi grandi pregi), partendo da questi esempi concreti, si tenterà di generalizzare e creare un modello generale che comprenda come casi particolari gli esempi appena visti. È quanto ci proponiamo di fare in questo capitolo, con l'introduzione dell'algebra booleana della quale saremo interessati soprattutto alle sue ricadute applicative. Questo tipo di algebra è chiamato così in onore del matematico G. Boole (1815-1864) che per primo investigò le leggi algebriche che si applicano alle proposizioni e agli insiemi.

### ■ 1 VARIABILI BOOLEANE E FUNZIONI BOOLEANE

Vorremo innanzitutto trovare dei modelli matematici che permettano di capire il funzionamento dei circuiti elettrici che compongono un computer. Ora, le regole con le quali agisce un computer sono esattamente le leggi della logica di cui abbiamo parlato nel primo capitolo. Scrivendo i numeri in forma binaria (ossia in base 2) (cfr. par. 4 del cap. 3) ogni cifra (ossia 1 o 0) contiene un *bit* di informazione: il simbolo 1 viene interpretato dal computer come il comando *on*, mentre il simbolo 0 viene interpretato come il comando *off*. Gli elementi di un circuito elettrico che permettono questa interpretazione sono le *porte logiche*.

Considereremo tre tipi di porte logiche: l'*invertitore* (o porta *NOT*), la porta *AND* e la porta *OR* che corrispondono rispettivamente alle operazioni logiche di *negazione*, *congiunzione* e *disgiunzione*. L'invertitore prende come input un bit e produce come output il suo complemento: quindi all'input 1 corrisponderà l'output 0 e viceversa all'input 0 corrisponderà l'output 1.

Si rappresenta al modo seguente:

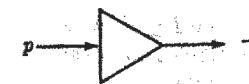


Figura 9.1. La porta NOT.

Questa porta corrisponde alla operazione logica di *complemento* o *negazione*.

La porta *AND* si comporta al modo seguente: gli input sono due bit: se sono entrambi 1 l'output è 1, negli altri casi invece l'output è 0.

Questa porta corrisponde all'operatore logico della *congiunzione*  $p \wedge q$  di due proposizioni (cfr. definizione 1.9): i valori degli output si ricavano dalla corrispondente tabella  $p \wedge q$ .

Si rappresenta al modo seguente:



Figura 9.2. La porta AND.

Il terzo tipo di porta logica, la porta *OR*, prende come input due bit: se almeno uno dei due è 1 l'output sarà 1, mentre se sono entrambi 0 l'output è 0.

Questa porta corrisponde all'operatore logico della *disgiunzione*  $p \vee q$  di due proposizioni (cfr. definizione 1.10): i valori degli output si ricavano dalla tabella  $p \vee q$ .

La rappresentazione di tale porta è



Figura 9.3. La porta OR.

Si possono costruire circuiti più complicati concatenando varie porte logiche. Per esempio vorremmo costruire un circuito corrispondente alla proposizione  $p \Rightarrow q$ . Ricordando (cfr. la (3.1) del cap. 1) che la  $p \Rightarrow q$  è logicamente equivalente alla  $(\neg p) \vee q$ , si tratta di concatenare la porta *NOT* con una porta *OR*, ottenendo il circuito della figura 9.4.

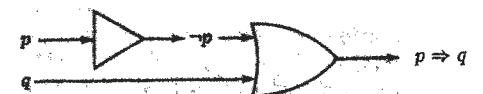


Figura 9.4.

I concetti che serviranno per modellare queste situazioni sono le *variabili booleane*, le *operazioni booleane* e le *funzioni booleane*. Tali concetti sono stati introdotti dal matematico G. Boole nella memoria *An investigation of the laws of thought* (1854) nella quale creò un sistema di logica matematica che ora è comunemente chiamata *algebra di Boole*. Quasi un secolo dopo, nel 1938, C.E.Shannon mostrò come le idee di Boole potessero essere applicate ai circuiti.

Consideriamo un insieme  $B$  costituito dai soli elementi 0 e 1:

$$B := \{0, 1\}.$$

Definiamo su  $B$  due operazioni binarie di addizione, moltiplicazione e una operazione 1-aria di complemento ponendo:

- a. Addizione:  $0 + 0 = 0, 1 + 0 = 0 + 1 = 1 + 1 = 1$ .
- b. Moltiplicazione:  $0 \cdot 0 = 1, 0 \cdot 1 = 0 \cdot 1 = 0, 1 \cdot 1 = 1$ .
- c. Complemento:  $\bar{0} = 1, \bar{1} = 0$ .

ossia con le seguenti tabelle:

$x$	$y$	$x + y$	$x$	$y$	$xy$
0	0	0	0	0	0
0	1	1	0	1	0
1	0	1	1	0	0
1	1	1	1	1	1

**DEFINIZIONE 9.1** Una variabile  $x$  prende il nome di *variabile booleana* se assume valori esclusivamente in  $B = \{0, 1\}$ , cioè se assume solo i valori 0 e 1.  $\blacksquare$

**PROPOSIZIONE 9.1** Siano  $x, y$  e  $z$  tre variabili booleane. Allora valgono le seguenti proprietà:

$\bar{\bar{x}} = x$	Legge del doppio complemento
$x + y = y + x$	Commutatività di $+$ e $\cdot$
$xy = yx$	
$(x + y) + z = x + (y + z)$	Associatività di $+$ e $\cdot$
$(xy)z = x(yz)$	
$x + yz = (x + y)(x + z)$	Distributività
$x(y + z) = xy + xz$	
$x + 0 = x$	Esistenza elemento neutro
$x \cdot 1 = x$	
$\bar{x + y} = \bar{x}\bar{y}$	Leggi di de Morgan
$\bar{xy} = \bar{x} + \bar{y}$	
$x + x = x$	Idempotenza
$x \cdot x = x$	
$x + \bar{x} = 1$	Inversi
$x\bar{x} = 0$	
$x + 1 = 1$	Dominanza
$x \cdot 0 = 0$	
$x + x \cdot y = x$	Assorbimento
$x(x + y) = x$	

**DIMOZIONE.** Basta servirsi delle tavole (1.1).  $\diamond$

### Esempio 9.1

Si provi la legge di de Morgan  $\bar{x + y} = \bar{x}\bar{y}$ .

Si legge dalla tavola seguente:

$x$	$y$	$x + y$	$\bar{x + y}$	$\bar{x}$	$\bar{y}$	$\bar{x}\bar{y}$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

Confrontando la quarta colonna con la settima si verifica la validità della legge di de Morgan.

**DEFINIZIONE 9.2** Sia  $B = \{0, 1\}$ . Dicesi *funzione booleana* di  $n$  variabili una funzione da  $B^n = \underbrace{B \times B \times \cdots \times B}_n$  in  $B$ , ossia una funzione di  $n$  variabili booleane che assume valori esclusivamente in  $B$ .  $\blacksquare$

Esempi di funzioni booleane:

1.  $f(x, y) = xy, x, y \in B$ .
2.  $f(x, y) = x\bar{y}, x, y \in B$ .
3.  $f(x, y, z) = x + \bar{y} + xz, x, y, z \in B$ .
4.  $f(x, y, z) = xyz + x\bar{y}, x, y, z \in B$ .

I valori di una funzione booleana si ottengono sostituendo 0 e 1 al posto delle variabili nell'espressione. Una funzione booleana  $f$  in  $n$  variabili  $x_1, x_2, \dots, x_n$  è determinata non appena si valuta  $f$  per ciascuno dei  $2^n$  possibili valori delle variabili  $x_1, x_2, \dots, x_n$ .

Facciamo un semplice esempio.

### Esempio 9.2

$$f(x, y, z) = xy + xz.$$

Costruiamo la seguente tabella, le cui otto righe al di sotto della intestazione corrispondono ai  $2^3$  possibili valori delle variabili:

$x$	$y$	$z$	$xz$	$xy$	$f(x, y, z) = xy + xz$
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	0	0	0
1	0	0	0	0	0
0	1	1	0	0	0
1	0	1	0	0	1
1	1	0	0	1	1
1	1	1	1	1	1

Trattandosi di funzioni, si possono definire per le funzioni booleane le ordinarie nozioni relative alle funzioni. Dunque:

**DEFINIZIONE 9.3** Due funzioni booleane si dicono *uguali* se le due rispettive tabelle sono identiche. Due funzioni booleane  $f$  e  $g$  da  $B^n$  in  $B$  si possono *addizionare* e *moltiplicare* al modo seguente:

$$(f+g)(x_1, x_2, \dots, x_n) := f(x_1, x_2, \dots, x_n) + g(x_1, x_2, \dots, x_n),$$

$$(f \cdot g)(x_1, x_2, \dots, x_n) := f(x_1, x_2, \dots, x_n) \cdot g(x_1, x_2, \dots, x_n).$$

Inoltre il complemento di una funzione booleana  $f$  si indica con  $\bar{f}$  ed è definito da

$$\bar{f}(x_1, x_2, \dots, x_n) := \overline{f(x_1, x_2, \dots, x_n)}.$$

Possiamo riassumere nella seguente tabella le principali leggi che valgono per tutte le *funzioni booleane* e non solo per le *variabili booleane*:

$\bar{\bar{f}} = f$	Legge del doppio complemento
$f + g = g + f$	Commutatività di + e ·
$fg = gf$	
$(f + g) + h = f + (g + h)$	Associatività di + e ·
$(fg)h = f(gh)$	
$f + gh = (f + g)(f + h)$	Distributività
$f(g + h) = fg + fh$	
$f + 0 = f$	Esistenza dell'elemento neutro
$f \cdot 1 = f$	
$f + g = \bar{f}\bar{g}$	Leggi di de Morgan
$\bar{fg} = \bar{f} + \bar{g}$	
$f + f = f$	Idempotenza
$f \cdot f = f$	
$f + \bar{f} = 1$	Leggi dell'inverso
$f\bar{f} = 0$	
$f + 1 = 1$	Leggi di dominanza
$f \cdot 0 = 0$	
$f + f \cdot g = f$	Leggi di assorbimento
$f(f + g) = f$	

Con il simbolo 0 (1) abbiamo indicato la funzione booleana costante che assume sempre il valore 0 (1). Si osservi che le leggi che si trovano all'interno di uno stesso riquadro sono ottenute l'una dall'altra scambiando + con · e 0 con 1 (e viceversa): sono leggi *duali*.

Per esempio la duale della  $x + 0 = x$  è la  $x \cdot 1 = x$ .

### Esempio 9.3

Dualizzare l'uguaglianza tra funzioni booleane  $xyz + \bar{x}yz = yz$ .

Innanzitutto si osservi che la precedente formula è vera, perché  $xyz + \bar{x}yz = (x + \bar{x})yz = (1)yz = yz$ .

La duale è (si verifichi che l'uguaglianza è vera):  $(x + y + z)(\bar{x} + y + z) = y + z$ .

Le proprietà elencate nella tabella corrispondono (verificare!) alle analoghe proprietà che valgono tra gli insiemi e nella logica delle proposizioni, una volta che si facciano le seguenti posizioni:

funzioni booleane	insiemi	logica
·	$\cap$	congiunzione
+	$\cup$	disgiunzione
-	complemento	$\neg$

Una volta ottenuto un risultato per le funzioni booleane, lo stesso risultato varrà per le proposizioni e per gli insiemi. Ancora una volta insistiamo sui vantaggi dell'algebrizzazione e della astrazione.

#### ESERCIZI

• Dare la forma duale di ciascuna delle seguenti espressioni booleane:

- $xyz + 1$ ;
- $\bar{x}_1\bar{x}_2 \dots \bar{x}_n$ .

• Semplificare la seguente espressione booleana:

$$x + y + (\bar{x} + y + z).$$

• Dualizzare la seguente espressione:  $x + \bar{x}y = x + y$ .

• Provare che  $x\bar{y} + y\bar{z} + \bar{x}z = \bar{x}y + \bar{y}z + x\bar{z}$ .

• Determinare il numero di funzioni booleane in  $n$  variabili.

## 2 LA FORMA NORMALE DISGIUNTIVA DI UNA FUNZIONE BOOLEANA

Tra le funzioni booleane in  $n$  variabili  $x_1, x_2, \dots, x_n$  ci sono ovviamente le *espressioni* ottenute a partire dalle variabili booleane  $x_1, x_2, \dots, x_n$  e le operazioni di +, · e complemento. Le espressioni booleane si possono definire *induttivamente* al modo seguente:

- 0, 1,  $x_1, x_2, \dots, x_n$  (ossia le variabili booleane) sono espressioni booleane;
- Se  $\mathcal{E}_1, \mathcal{E}_2$  sono espressioni booleane, allora  $\mathcal{E}_1 + \mathcal{E}_2, \mathcal{E}_1 \cdot \mathcal{E}_2$  sono espressioni booleane.

Tutti gli esempi di funzioni booleane viste nel paragrafo precedente sono espressioni booleane.

È chiaro che ad ogni espressione booleana in  $n$  variabili corrisponde una sola funzione in  $n$  variabili. Viceversa, ogni funzione booleana in  $n$  variabili  $x_1, x_2, \dots, x_n$  si può rappresentare mediante una *espressione booleana* (chiaramente non unica!). E quanto ci accingiamo a provare.

Supponiamo di conoscere tutti i valori di una funzione booleana (ossia di conoscere una funzione booleana): come facciamo a trovare un'*espressione booleana* che rappresenti questa funzione?

#### Esempio 9.4

Si consideri la seguente funzione in due variabili:

$x$	$y$	$f(x, y)$
0	0	0
0	1	1
1	0	0
1	1	1

Vorremmo trovare un'*espressione* in due variabili corrispondente alla funzione  $f$ . La  $f$  è chiaramente somma (OR) delle seguenti due funzioni,  $f_1$  e  $f_2$ :

$$\begin{array}{|c|c|c|} \hline x & y & f(x, y) \\ \hline 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ \hline \end{array} = \begin{array}{|c|c|c|} \hline x & y & f_1(x, y) \\ \hline 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ \hline \end{array} + \begin{array}{|c|c|c|} \hline x & y & f_2(x, y) \\ \hline 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ \hline \end{array}$$

Ora, la  $f_1$  si può rappresentare come  $\bar{x}y$ : infatti quando  $x = 0$  e  $y = 1$  il prodotto  $\bar{x}y$  assume il valore 1, mentre assume il valore 0 in tutti gli altri casi. Così  $f_2$  si può rappresentare come  $xy$ . In definitiva, la  $f(x, y)$  si può rappresentare come  $\bar{x}y + xy$ .

#### Esempio 9.5

Una espressione per la funzione booleana  $f$  di tre variabili booleane  $x, y$  e  $z$  che assume il valore 1 se e solo se  $x = 0$  e  $y = z = 1$  è rappresentata con la seguente tabella:

$x$	$y$	$z$	$f(x, y, z)$
0	0	0	0
0	0	1	0
0	1	0	0
1	0	0	0
0	1	1	1
1	0	1	0
1	1	0	0
1	1	1	0

Se scegliamo l'espressione  $\bar{x} \cdot y \cdot z$  le cose funzionano. Infatti la tabella corrispondente a  $\bar{x} \cdot y \cdot z$  è

$x$	$y$	$z$	$\bar{x}$	$\bar{x} \cdot y \cdot z$
0	0	0	1	0
0	0	1	1	0
0	1	0	1	0
1	0	0	0	0
0	1	1	1	1
1	0	1	0	0
1	1	0	0	0
1	1	1	0	0

che uguaglia la tabella precedente: quindi le due funzioni sono uguali.

Questi erano casi semplici. Esiste però un metodo che ci viene in aiuto per risolvere in generale il problema di cui sopra. Premettiamo due definizioni.

**DEFINIZIONE 9.4** Una *lettera* è una variabile booleana  $x$  oppure il suo complemento  $\bar{x}$ . ■

**DEFINIZIONE 9.5** Una *congiunzione fondamentale* delle variabili booleane  $x_1, x_2, \dots, x_n$  è un prodotto  $y_1 y_2 \cdots y_n$  dove  $y_i = x_i$  oppure  $y_i = \bar{x}_i$ . In altri termini, una congiunzione fondamentale è il prodotto di  $n$  lettere distinte. ■

Un'*espressione booleana*  $\mathcal{E}$  di  $n$  variabili che sia scritta come somma di congiunzioni fondamentali nelle  $n$  variabili prende il nome di *forma normale disgiuntiva* (*f.n.d.*) di  $\mathcal{E}$ .

Gli esempi precedenti mostrano che le funzioni da cui siamo partiti sono state scritte in forma normale disgiuntiva. Ma è vero in generale? Chi ci dice cioè che per ogni funzione booleana esista la sua forma normale disgiuntiva?

La risposta è affermativa: data una funzione booleana  $f$  in  $n$  variabili, daremo un metodo che permette al tempo stesso di trovare una espressione booleana che corrisponda alla  $f$  in modo tale che questa espressione sia somma di congiunzioni fondamentali nelle  $n$  variabili.

È cruciale a questo scopo la seguente osservazione :

una congiunzione fondamentale  $y_1 y_2 \cdots y_n$  assume il valore 1 per una e una sola combinazione dei valori delle sue variabili.

Precisamente, questo avviene quando e solo quando ogni  $y_i$  uguaglia 1, il che significa se e solo se  $x_i = 1$  per  $y_i = x_i$  e  $x_i = 0$  per  $y_i = \bar{x}_i$ .

L'osservazione precedente ci permette di trovare una espressione booleana in forma normale disgiuntiva di una qualunque funzione booleana della quale si conoscano i valori. Il procedimento è molto semplice:

- a) Per ogni valore 1 assunto dalla funzione si determina l'unica congiunzione fondamentale che ha valore 1 quando la funzione ha valore 1 e ha valore 0 quando la funzione ha valore zero.
- b) L'espressione per la funzione booleana è la somma di tutte queste congiunzioni fondamentali (che sono pertanto tante quanti sono i valori 1 assunti dalla funzione).
- c) L'espressione ottenuta è in forma normale disgiuntiva.

Gli esempi fatti precedentemente illustrano il metodo in generale.

Resta un problema: la forma normale disgiuntiva di un'espressione booleana è unica?

Ebbene, sussiste la seguente proposizione che risponde positivamente anche a questo problema.

**PROPOSIZIONE 9.2** La forma normale disgiuntiva di ogni funzione booleana di  $n$  variabili è unica (a meno ovviamente dell'ordine degli addendi).

**DIMOZIAZIONE.** Supponiamo che ci siano due forme normali disgiuntive diverse corrispondenti ad una stessa espressione booleana  $\mathcal{E}$ . In altre parole, supponiamo che sia

$$\mathcal{E} = P_1 + P_2 + \dots + P_r = P'_1 + P'_2 + \dots + P'_s$$

con  $P_i$  ( $i = 1, 2, \dots, r$ ) e  $P'_j$  ( $j = 1, 2, \dots, s$ ) prodotti di esattamente  $n$  lettere (ogni prodotto contiene quindi tutte le variabili o i loro complementi). Supponiamo che almeno uno dei  $P_i$  sia diverso da tutti i  $P'_j$ . Sia  $P_1 \neq P'_j$  per tutti i  $j$ . Allora  $x_i \in P_1$  e  $\bar{x}_i \in P'_j$  o viceversa. Quindi  $P_1 P'_j = 0$  per ogni  $i = 1, 2, \dots, s$ , da cui

$$P_1 \mathcal{E} = P_1 (P'_1 + P'_2 + \dots + P'_s) = 0 + 0 + \dots + 0 = 0.$$

Ma  $P_1$  è anche diverso da tutti gli altri  $P_i$ , per  $i = 1, 2, \dots, r$ . Quindi  $P_1 P_i = 0$  per ogni  $i = 1, \dots, r$ . Quindi  $P_1 \mathcal{E} = P_1 (P_1 + P_2 + \dots + P_r) = P_1 P_1 + 0 + \dots + 0 =$  (per le leggi di idempotenza)  $= P_1$ .

Dal confronto si ha  $P_1 = 0$  che è un assurdo, perché sappiamo che  $P_1$  è prodotto di  $n$  lettere. Ne segue che la scrittura di una espressione booleana in forma normale disgiuntiva è unica. ♦

### Esempio

Determinare la congiunzione fondamentale che vale 1 in corrispondenza ai valori  $x_2 = x_5 = x_6 = 1$  e  $x_1 = x_3 = x_4 = 0$  delle variabili booleane  $x_1, x_2, x_3, x_4, x_5, x_6$  e 0 in tutti gli altri casi.

- Determinare un'espressione booleana per la seguente funzione booleana:

$x$	$y$	$z$	$f(x, y, z)$
0	0	0	0
0	0	1	0
0	1	0	0
1	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1
1	1	1	1

- Scrivere la forma normale disgiuntiva della seguente funzione:

$$f(x, y, z) = x(y + \bar{z}).$$

### ■ 3 FORME MINIMALI DI UN'ESPRESSIONE BOOLEANA: IL METODO DI KARNAUGH

Abbiamo appena visto che ogni funzione booleana è esprimibile mediante una espressione booleana, e abbiamo anche dato un metodo che fornisce la sua (unica) espressione booleana in forma normale disgiuntiva. Tuttavia ad una stessa funzione booleana restano associate tante espressioni booleane (anche se una sola sarà quella in forma normale disgiuntiva). Un problema di fondamentale importanza è quindi il seguente: data un'espressione booleana, ridurre il più possibile il numero degli addendi, cioè trovare una *forma minimale* (f.m.) di  $f$ .

Ci sono due regole fondamentali da tenere presenti per la semplificazione di una espressione booleana (nel senso di trovare un'espressione di una funzione booleana che abbia il minor numero possibile di addendi (f.m.)).

- Se in una somma di prodotti di lettere, ossia di variabili e loro complementi, un prodotto è contenuto in un altro, allora il più lungo può essere eliminato. Ogni operazione di questo tipo *riduce di una unità* il numero totale  $n$  di addendi dell'espressione. Iterando il processo, si passa da  $n$  a  $n - 1$ , a  $n - 2$ , etc. addendi.

$$xyztuv + xyz = xyztuv + xyz\cancel{1} = xyz\underbrace{(tuv + 1)}_{=1} = xyz$$

poiché  $x + 1 = 1$ ,  $\forall x$ .

- Quando due prodotti diversi differiscono per una sola lettera, allora la loro somma è uguale al prodotto delle variabili comuni.

$$xyzt + xy\bar{z}t = xyz(\underbrace{z + \bar{z}}_{=1}) = xyz.$$

Come si vede, in entrambi i casi siamo riusciti a semplificare l'espressione.

Presenteremo ora un algoritmo che fornisce un metodo geometrico per ottenere un numero minima di addendi a partire dall'espressione f.n.d. di  $f$ . Il metodo consiste nel formare delle tabelle, dette *applicazioni di Karnaugh*, che descrivano in modo grafico le riduzioni possibili per tutte le possibili congiunzioni fondamentali presenti nell'espressione booleana.

Partiamo da una funzione booleana in  $n$  variabili, *in forma normale disgiuntiva*: sappiamo che questo è sempre possibile. Tutti i prodotti che compaiono in  $f$  sono pertanto costituiti da  $n$  fattori. Pensiamo tali prodotti come il risultato del prodotto dei primi  $k$  ( $1 \leq k \leq n$ ) fattori con gli ultimi  $n - k$ : sta a noi scegliere il  $k$  che più ci conviene, ma che deve essere lo stesso per tutte le congiunzioni. A questo punto disponiamo in una tabella sulla colonna di sinistra i prodotti di lettere che coinvolgono solamente le prime  $k$  variabili e sulla riga superiore i prodotti di lettere che coinvolgono solo le restanti  $n - k$  variabili. Si osservi che a seconda della scelta di  $k$  la forma di questa tabella varierà. Qualunque sia la forma della tabella essa risulta suddivisa in  $2^n$  quadrati, ciascuno dei quali rappresenta una delle possibili congiunzioni fondamentali di  $n$  variabili (si ricordi che il prodotto è commutativo). In ogni caso dare una tabella significa dare delle etichette sulle righe e sulle colonne che saranno dei prodotti di lettere in modo che il loro prodotto dia la congiunzione incassellata in quel quadrato.

Questo metodo funziona in modo efficiente fino a 6 variabili. Qui di seguito facciamo alcuni esempi nel caso di quattro variabili. Nel primo caso le etichette di sinistra sono costituite da una sola lettera ( $k = 1$ ), e quindi quelle in alto sono prodotti di tre lettere.

Il prodotto indicato è precisamente il prodotto delle etichette corrispondenti, ossia la congiunzione associata a quel quadrato. Nel secondo caso abbiamo scelto sia per righe sia per colonne prodotti di due lettere ( $k = 2$ ); ancora una volta il prodotto indicato è il prodotto delle etichette corrispondenti. Nel terzo caso ( $k = 3$ ) le etichette di sinistra sono costituite ciascuna da tre lettere, e quelle in alto sono costituite da una sola lettera.

Notiamo che in tutti i casi abbiamo scelto un ordine delle etichette in modo che *etichette vicine differiscano per una sola lettera*.

Come si vede, la stessa congiunzione fondamentale può trovarsi in tabelle di varie forme.

	$yzt$	$yz\bar{t}$	$y\bar{z}t$	$y\bar{z}\bar{t}$	$\bar{y}zt$	$\bar{y}\bar{z}t$	$\bar{y}\bar{z}\bar{t}$
$x$					$x\bar{y}\bar{z}\bar{t}$		
$\bar{x}$							

(3.1)

	$zt$	$z\bar{t}$	$\bar{z}t$	$\bar{z}\bar{t}$
$xy$				
$x\bar{y}$				
$\bar{x}y$		$\bar{x}\bar{y}zt$		
$\bar{x}\bar{y}$				

(3.2)

(3.3)

	$t$	$\bar{t}$
$xyz$		
$xy\bar{z}$		
$x\bar{y}z$		
$x\bar{y}\bar{z}$		
$\bar{x}yz$	$\bar{x}y\bar{z}$	
$\bar{x}\bar{y}z$		
$\bar{x}\bar{y}\bar{z}$		
$\bar{xyz}$		

In tutti i casi i quadrati della tabella sono  $2^4 = 16$ .

Diremo che due quadrati sono *adiacenti* se hanno un lato in comune: i quadrati corrispondenti della prima e ultima colonna (rispettivamente della prima e ultima riga) si considerano adiacenti anch'essi.

La semplicità di esecuzione del metodo che stiamo per descrivere si basa sulla scelta dell'ordine delle variabili che abbiamo visto nell'esempio precedente.

Data una funzione booleana  $f$  in forma normale disgiuntiva in  $n$  variabili e costruita la tabella di cui sopra, con l'ordine delle etichette appena descritto, mettiamo 1 nei quadrati corrispondenti alle congiunzioni presenti nell'espressione di  $f$  e zero altrove (in realtà lo zero si omette).

Abbiamo visto che per minimizzare il numero di addendi nell'espressione di una funzione booleana in forma normale disgiuntiva occorre individuare le coppie di congiunzioni fondamentali che differiscono per una sola lettera. Attraverso la mappa di Karnaugh tali congiunzioni sono facilmente individuabili, come quelle *coppie di quadrati adiacenti che contengono un 1*. Se poi gli 1 si trovano in quattro quadrati adiacenti a due a due, la somma delle quattro corrispondenti congiunzioni si riduce ulteriormente, e così se gli 1 coprono 8 quadrati a due a due adiacenti. Il metodo quindi consiste nell'individuare i rettangoli *massimali* costituiti da 1, 2, 4, 8 quadrati adiacenti, tutti contenenti degli 1, dove con massimali si intendono quei rettangoli che non sono contenuti in altri rettangoli che godano della stessa proprietà. Una volta individuati tali rettangoli, per trovare una somma minima di congiunzioni basta scegliere il *numero minimo di rettangoli massimali che coprano tutti gli 1 presenti*. Dai seguenti esempi capiremo più facilmente il metodo.

#### Esempio 9.6

Minimizzare la seguente espressione booleana:

$$xyz + xy\bar{z} + x\bar{y}\bar{z} + \bar{x}\bar{y}\bar{z}.$$

Osserviamo che la precedente espressione è in forma disgiuntiva normale. Partiamo dalla seguente tabella:

	$yz$	$y\bar{z}$	$\bar{y}z$	$\bar{y}\bar{z}$
$x$				
$\bar{x}$				

Mettiamo ora un 1 in corrispondenza a quegli addendi che sono presenti nell'espressione data, e lasciamo vuoti i quadrati corrispondenti ai prodotti che non sono presenti. La tabella precedente diventa:

	$yz$	$y\bar{z}$	$\bar{y}z$	$\bar{y}\bar{z}$
$x$	1	1		
$\bar{x}$		1	1	

I rettangoli massimali sono i seguenti tre:

	$yz$	$y\bar{z}$	$\bar{y}z$	$\bar{y}\bar{z}$
$x$	1	1	1	
$\bar{x}$		1	1	1

L'espressione minimale è pertanto:

$$xy + y\bar{z} + \bar{x}\bar{z}.$$

**OSSERVAZIONE** Supponiamo che i quadratini della tabella siano di area unitaria. Ai rettangoli massimali di area 1 (cioè costituiti da un solo quadrato) (corrispondente ad un prodotto per esempio di 4 lettere) corrispondono congiunzioni costituite ancora da 4 lettere (cioè la congiunzione non si semplifica), a quelli di area 2 (corrispondenti quindi alla somma di due congiunzioni fondamentali di 4 lettere) corrisponderà una congiunzione (non più la somma di due) di tre lettere. Ai rettangoli massimali di area 4 (cioè corrispondenti alla somma di 4 congiunzioni fondamentali) corrisponderà un unico prodotto di 2 sole lettere, ecc. È facile generalizzare questa osservazione al caso di funzioni booleane in forma disgiuntiva normale in  $n = 5$  o  $n = 6$  variabili.

### Esercizi

9) Trovare una espressione con un numero minimo di addendi, per la espressione booleana in forma normale disgiuntiva:

$$f = xy + \bar{x}\bar{y}.$$

10) Minimizzare il numero di addendi della espressione booleana

$$(3.4) \quad \bar{x}yzt + xyzt + x\bar{y}z\bar{t} + \bar{x}\bar{y}z\bar{t} + xyz\bar{t}.$$

## 4 PORTE LOGICHE E CIRCUITI

L'importanza delle funzioni booleane e delle loro proprietà risiede nel fatto che possono modellare i circuiti elettrici. L'implementazione di tali funzioni avviene attraverso gli elementi base del circuito, le cosiddette *porte logiche* che abbiamo già incontrato. Ogni tipo di porta implementa una operazione booleana. Servendoci di queste porte, attraverso le regole delle funzioni booleane, potremo disegnare dei circuiti che effettuano svariati compiti.

Come si è visto, tre tipi di porte (cfr. par. 1) sono: l'*invertitore*, la porta *AND* e la porta *OR*: esse corrispondono rispettivamente alle operazioni logiche di *negazione*, *congiunzione* e *disgiunzione* e quindi rispettivamente alle operazioni booleane di *complemento*, *moltiplicazione* e *addizione*.

L'invertitore prende come input il *valore di una variabile booleana* e produce il *complemento* di questo valore come output. Nella porta *AND* gli input sono i valori di due variabili booleane e l'output è il prodotto dei due valori. La porta *OR*, prende come input i valori di due variabili booleane e dà come output la loro somma.

Dato che le operazioni booleane  $+$  e  $\cdot$  sono associative, le porte *AND* e *OR* possono avere più di due input: si veda figura 9.5.



Figura 9.5.

Attraverso l'utilizzo di queste porte si possono rappresentare diverse espressioni booleane con un circuito o rete logica. Facciamo qualche esempio.

### Esempio 9.7

Un circuito logico (o rete logica) per la funzione booleana  $f(x, y) = (x + y) + \bar{x}$  è dato dalla figura 9.6.

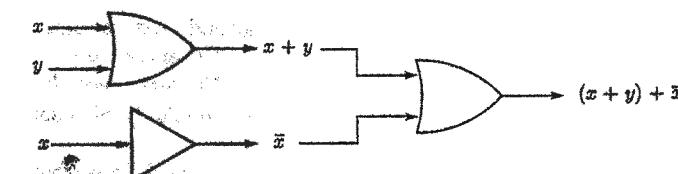


Figura 9.6.

### Esempio 9.8

Un circuito che produca l'output  $xy + xz + yz$  è rappresentato dalla figura 9.7.

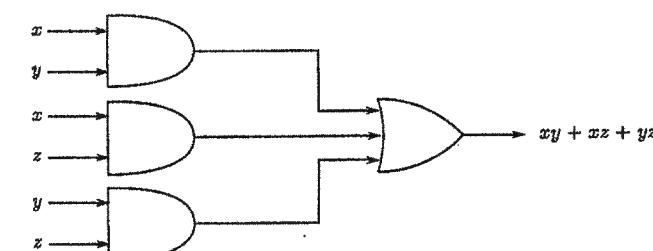


Figura 9.7.

Se vogliamo costruire un circuito che produca come output per esempio la funzione booleana

$$(4.1) \quad \bar{xyzt} + xyzt + x\bar{y}z\bar{t} + \bar{x}\bar{y}z\bar{t} + xyz\bar{t}$$

ci rendiamo conto che il numero di porte è molto elevato. Dato che l'efficienza di un circuito dipende naturalmente dal numero di porte logiche che lo compongono, è importante costruire circuiti che eseguano gli stessi compiti con maggiore efficienza, riducendo il numero di porte. Come fare? Il problema è equivalente al problema di ridurre il numero di termini in una espressione booleana che rappresenta il circuito. Ma dal paragrafo precedente sappiamo come risolvere questo problema. Abbiamo visto nell'esercizio 10 del paragrafo precedente che la funzione booleana (4.1) ha la seguente espressione minimale:

$$xyz + yzt + \bar{y}z\bar{t}$$

Allora il circuito precedente è equivalente (nel senso che esegue le stesse operazioni logiche) al circuito della figura 9.8, che chiaramente è molto più semplice:

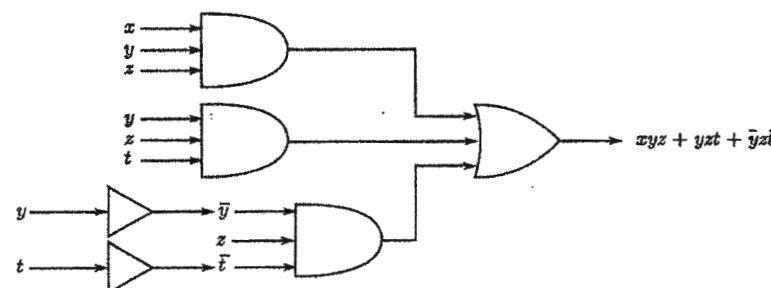


Figura 9.8.

### Esercizi

11 Disegnare dei circuiti logici corrispondenti alle seguenti espressioni booleane:

1.  $(x_1 + x_2)x_3 + x_4$ .
2.  $x_1 + x_2x_3 + x_4$ .

12 Trovare un circuito logico (o rete logica) per la seguente funzione booleana:

$$f(x, y) = xy + \bar{x}y$$

13 Trovare un circuito logico per la funzione booleana  $\overline{x+y}$ .

## 5 RETICOLI

Come si è visto, c'è un parallelismo tra la logica delle proposizioni, le funzioni booleane e gli insiemi rispetto alle operazioni di complemento, unione e intersezione. Sappiamo che l'insieme  $\mathcal{P}(X)$  delle parti di un insieme  $X$  rispetto alla relazione di inclusione

è un insieme parzialmente ordinato. Non dobbiamo quindi meravigliarci se a questo punto introduciamo un paragrafo che riprende le relazioni d'ordine (cfr. par. 6 del cap. 1).

**DEFINIZIONE 9.6** Sia  $(A, \leq)$  un insieme parzialmente ordinato. Un elemento  $t \in A$  si dice *elemento minimo* di  $A$  se per ogni  $a \in A$  si ha  $t \leq a$ . Un elemento  $t \in A$  si dice *massimo* in  $A$  se  $a \leq t$  per ogni  $a \in A$ . Un elemento  $t \in A$  si dice *minimale* in  $A$  se per ogni  $a \in A$  la  $a \leq t$  implica  $a = t$  (cioè non esiste nessun elemento di  $A$  che lo precede); un elemento  $t \in A$  si dice *massimale* in  $A$  se per ogni  $a \in A$  la  $t \leq a$  implica  $a = t$  (cioè se non precede nessun elemento di  $A$ ). ■

**OSSERVAZIONE** Non ogni insieme parzialmente ordinato possiede elementi massimali o minimali. Per esempio  $(\mathbb{Z}, \leq)$  è privo di elementi massimali e minimali. Tuttavia, se  $A$  è un insieme parzialmente ordinato *finito*, allora possiede almeno un elemento minimale e almeno un elemento massimale. Attenzione, non necessariamente un minimo o un massimo (perché?).

### Esempio 9.9

Sia  $\mathcal{P}(X)$  l'insieme delle parti dell'insieme  $X$ , ordinati per inclusione. Allora l'insieme vuoto  $\emptyset$  è un minimo, mentre  $X$  è un massimo.

### Esempio 9.10

Sia  $A = \{1, 2, 3, 4, 6, 9\}$  e sia  $\leq$  la relazione di essere divisore. Allora  $A$  si può rappresentare come in figura 9.9.

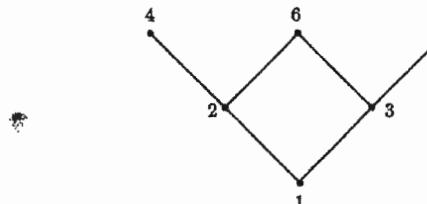


Figura 9.9.

C'è un elemento minima, 1, che è anche minimo, e ci sono 3 elementi massimali (ma non massimi): 4, 6, 9.

**DEFINIZIONE 9.7** Sia  $(A, \leq)$  un insieme parzialmente ordinato e sia  $B$  un sottoinsieme di  $A$ . Un elemento  $t \in A$  si dice *minorante* di  $B$  se risulta  $t \leq b$  per ogni  $b \in B$ . Un elemento  $t \in A$  si dice *maggiorante* di  $B$  se risulta  $b \leq t$  per ogni  $b \in B$ . ■

### Esempio 9.11

Nell'insieme  $(\mathbb{Q}, \leq)$  sia  $B = \{x \in \mathbb{Q} \mid \sqrt{3} < x < \sqrt{5}\}$ . I minoranti di  $B$  sono i numeri razionali minori di  $\sqrt{3}$  e i maggioranti sono i numeri razionali maggiori di  $\sqrt{5}$ .

**DEFINIZIONE 9.8** Sia  $(A, \preceq)$  un insieme parzialmente ordinato e sia  $B$  un sottoinsieme di  $A$ . Un elemento  $t \in A$  si dice (se esiste) l'estremo inferiore di  $B$ , e si indica con  $\inf(B)$ , se  $t$  è il massimo dei minoranti di  $B$ . Un elemento  $t \in A$  si dice estremo superiore di  $B$  (se esiste), e si indica con  $\sup(B)$ , se è il minimo dei maggioranti di  $B$ .

Non è detto che esistano, tuttavia, se esistono, sono unici.

Nell'esempio 9.11 non esiste né estremo inferiore (perché  $\sqrt{3} \notin \mathbb{Q}$ ) né estremo superiore perché  $\sqrt{5} \notin \mathbb{Q}$ .

#### Esempio 9.12

In  $\mathbb{N}$  ordinato per divisibilità (ossia ponendo  $x \preceq y$  se e solo se  $x|y$ ), sia  $B$  il sottoinsieme di  $\mathbb{N}$  costituito dai due soli elementi  $a$  e  $b$ , ossia  $B = \{a, b\}$ . Ebbene, in questo caso, l'estremo inferiore  $\inf(B)$  è il MCD( $a, b$ ) mentre l'estremo superiore  $\sup(B)$  è il mcm( $a, b$ ): si ricordino le proprietà del MCD e del mcm.

#### Esempio 9.13

In  $\mathcal{P}(X)$  ordinato per inclusione, dati comunque due sottoinsiemi  $A$  e  $B$  di  $X$ , si ha, come è immediato verificare,

$$\inf(A, B) = A \cap B, \quad \sup(A, B) = A \cup B.$$

Si noti che non è sempre vero che dati comunque due elementi  $x$  e  $y$  esistano il loro estremo superiore e il loro estremo inferiore, come mostra l'esempio della figura 9.10.

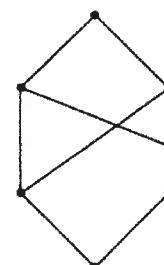


Figura 9.10.

In generale, se il sottoinsieme  $B$  di  $A$  è costituito da due elementi  $x$  e  $y$ , indicheremo l'estremo inferiore tra  $x$  e  $y$  (se questo esiste) con il simbolo  $x \wedge y$  e l'estremo superiore (se esiste) con il simbolo  $x \vee y$  e li chiameremo rispettivamente *intersezione* e *unione* di  $x$  e  $y$ . In definitiva,

$$x \wedge y = \inf(x, y) = \text{intersezione di } x \text{ e } y$$

$$x \vee y = \sup(x, y) = \text{unione di } x \text{ e } y$$

Ebbene, saremo interessati allo studio di quegli insiemi parzialmente ordinati che godono della proprietà che ogni coppia di loro elementi possiede estremo superiore e inferiore.

**DEFINIZIONE 9.9** Un reticolo  $(L, \preceq)$  è un insieme parzialmente ordinato in cui due qualunque elementi  $a$  e  $b$  possiedono estremo inferiore  $a \wedge b$  ed estremo superiore  $a \vee b$ .

#### Esempio 9.14

Ogni catena è un reticolo.

Le due operazioni  $\wedge$  e  $\vee$  godono delle seguenti proprietà:

##### 1. Commutativa:

- (a)  $a \wedge b = b \wedge a$ ,
- (b)  $a \vee b = b \vee a \quad \forall a, b \in L$ .

##### 2. Associativa:

- (a)  $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ ,
- (b)  $(a \vee b) \vee c = a \vee (b \vee c), \quad \forall a, b, c \in L$ .

(5.1)

##### 3. Assorbimento:

- (a)  $a \vee (a \wedge b) = a$ ,
- (b)  $a \wedge (a \vee b) = a, \quad \forall a, b \in L$ .

##### 4. Idempotenza:

- (a)  $a \wedge a = a$ ,
- (b)  $a \vee a = a$ .

La seguente proposizione è di facile verifica.

**PROPOSIZIONE 9.3** In un reticolo  $(L, \preceq)$  le seguenti affermazioni sono equivalenti per ogni  $a, b \in L$ :

$$a \preceq b \iff a \vee b = b \iff a \wedge b = a.$$

Questa proposizione permette una formulazione equivalente di reticolo, di natura esclusivamente algebrica, che non richiede di partire da un insieme parzialmente ordinato.

**DEFINIZIONE 9.10** Un reticolo algebrico è un insieme  $(L, \wedge, \vee)$  con due operazioni binarie  $\wedge$  e  $\vee$  che vengono anche chiamate *intersezione* o *moltiplicazione* e *unione* o *addizione* che verificano per ogni  $a, b, c \in L$  le proprietà (5.1).

Non è difficile provare che ogni reticolo è un reticolo algebrico e viceversa. Potremo quindi parlare semplicemente di reticolo. Per la dimostrazione dell'equivalenza delle due definizioni si rimanda all'esercizio 17.

**DEFINIZIONE 9.11** Sia  $(L, \preceq)$  un reticolo. Un sottoinsieme  $L'$  di  $L$  si dice *sottoreticolo* di  $L$  se per ogni  $x, y \in L'$   $x \vee y$  e  $x \wedge y$  stanno in  $L'$ .  $\blacksquare$

**DEFINIZIONE 9.12** Siano  $(L, \preceq)$  e  $(L', \preceq)$  due reticoli. Un *omomorfismo* di reticoli da  $L$  a  $L'$  è un'applicazione  $\varphi : L \rightarrow L'$  tale che

$$\varphi(x \vee y) = \varphi(x) \vee \varphi(y), \quad \varphi(x \wedge y) = \varphi(x) \wedge \varphi(y)$$

per ogni  $x, y \in L$ . Un omomorfismo di reticoli che sia biiettivo si dice *isomorfismo*.  $\blacksquare$

Si osservi che in genere in un reticolo *non* valgono le proprietà *distributive*.

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

Valgono tuttavia le seguenti relazioni (*disuguaglianze distributive*):

$$a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$$

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c).$$

La figura 9.11 fornisce due esempi di reticoli non distributivi.

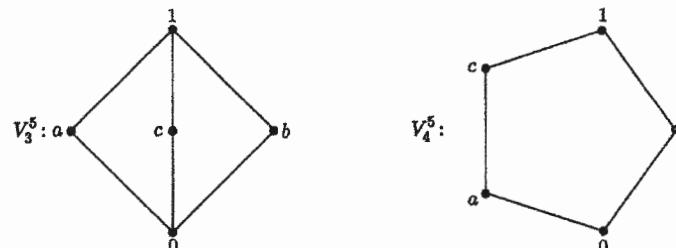


Figura 9.11. Reticoli non distributivi.

Si tratta dei più piccoli reticoli non distributivi. Prendono il nome rispettivamente di *diamante* e *pentagono*. È ovvio che un reticolo che contenga un diamante o un pentagono non può essere distributivo, perché

$$\text{in } V_3^5 \quad a \vee (b \wedge c) = a \neq 1 = (a \vee b) \wedge (a \vee c);$$

$$\text{in } V_4^5 \quad a \vee (b \wedge c) = a \neq c = (a \vee b) \wedge (a \vee c).$$

E il viceversa? Vale anche il viceversa, anche se la dimostrazione non è immediata. Enunciamo il risultato per completezza.

**TEOREMA 9.1** Un reticolo  $L$  è distributivo se e solo se non contiene un sottoreticolo isomorfo al diamante  $V_3^5$  o al pentagono  $V_4^5$  rispettivamente.

Un'altra caratterizzazione dei reticoli distributivi è la seguente.

**PROPOSIZIONE 9.4** Un reticolo  $L$  è distributivo se e solo se vale la seguente legge di cancellazione:

$$a \wedge b = a \wedge c, \quad a \vee b = a \vee c \implies b = c \quad \forall a, b, c \in L.$$

Come sappiamo, in un reticolo non sempre esiste minimo o massimo. Tuttavia, se questi esistono, il minimo viene solitamente indicato con il simbolo 0 e il massimo con il simbolo 1. Un reticolo con massimo e minimo si dice *limitato*.

**DEFINIZIONE 9.13** Un reticolo limitato  $L$  con 0 e 1 si dice *con complemento* se per ogni  $a \in L$  esiste almeno un elemento  $b \in L$  tale che

$$a \wedge b = 0, \quad a \vee b = 1.$$

Un elemento  $b$  siffatto prende il nome di *complemento* di  $a$ .  $\blacksquare$

Un esempio di reticolo di questo tipo è dato per esempio dal reticolo dei sottoinsiemi dell'insieme  $\{1, 2, 3\}$ , ordinato per inclusione. Questo reticolo è anche distributivo.

Hanno particolare importanza i reticoli con complemento che sono anche distributivi, perché sono uno dei modi con cui si possono definire le algebre di Boole, che andiamo a studiare.

### Esercizi

1. Dare un esempio di reticolo che abbia un estremo inferiore ma non superiore.

2. Dare un esempio di reticolo che abbia un estremo superiore ma non inferiore.

3. Sia  $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$  e sia  $\preceq$  la relazione d'ordine  $\leq$ .

- Provare che si tratta di un reticolo.
- Determinare  $a \wedge b$  e  $a \vee b$  per ogni  $a, b \in A$ .
- Determinare 0 e 1.
- Provare che non è un reticolo con complemento.

4. Sia  $(L, \preceq)$  un reticolo. Si ponga:  $x \wedge y := \inf(x, y)$  e  $x \vee y := \sup(x, y)$ . Si provi che  $(L, \wedge, \vee)$  è un reticolo algebrico.

5. Sia  $(L, \wedge, \vee)$  un reticolo algebrico. Si definisca  $x \preceq y \iff x \wedge y = x$ . Si provi che  $(L, \preceq)$  è un reticolo.

## 6. LE ALGEBRE DI BOOLE

In questo paragrafo arriviamo al cuore del capitolo, dando la definizione formale di algebra di Boole: essa cattura le proprietà essenziali degli insiemi e del calcolo proposizionale.

**DEFINIZIONE 9.14** Sia  $\mathcal{B}$  un insieme non vuoto che contenga due elementi privilegiati, 0 e 1, e sul quale siano assegnate due operazioni binarie,  $+$  (addizione) e  $\cdot$  (moltiplicazione) e una operazione 1-aria,  $\neg$  (complemento) che verifichino le seguenti proprietà per ogni  $a, b, c \in \mathcal{B}$ :

## 1. Comportamento di 0 e 1:

- (a)  $a + 0 = a$ ,
- (b)  $a \cdot 0 = 0$ ,
- (c)  $a + 1 = 1$ ,
- (d)  $a \cdot 1 = a$ ;

## 2. Proprietà commutative:

- (a)  $a + b = b + a$ ,
- (b)  $a \cdot b = b \cdot a$ ;

## 3. Proprietà associative:

- (a)  $(a + b) + c = a + (b + c)$ ,
- (b)  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ ;

## 4. Proprietà di assorbimento:

- (a)  $a \cdot (a + b) = a$ ,
- (b)  $a + (a \cdot b) = a$ ;

## 5. Proprietà distributiva:

- (a)  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ ,
- (b)  $a + (b \cdot c) = (a + b) \cdot (a + c)$ ;

## 6. Proprietà del complemento:

- (a)  $\bar{\bar{a}} = a$ ,
- (b)  $\overline{a+b} = \bar{a} \cdot \bar{b}$ ,
- (c)  $a \cdot \bar{a} = 0$ .

Allora  $(\mathcal{B}, +, \cdot, \bar{\phantom{x}}, 0, 1)$  prende il nome di *algebra di Boole*. ■

Alcuni autori preferiscono definire algebra di Boole ogni *reticolo limitato distributivo con complemento, che abbia almeno due elementi distinti*. Ovviamente l'operazione  $+$  diventa la  $\vee$ , mentre la moltiplicazione  $\cdot$  diventa  $\wedge$ . Useremo indifferentemente le due notazioni.

## Esempio 9.15

La più semplice algebra di Boole è l'algebra con 2 elementi 0 e 1 e operazioni date da  $+$  e  $\cdot$  e complemento (cfr. tab. (1.1)).

Questo esempio è tuttavia troppo semplice per essere significativo. Un altro esempio ancora elementare ma questa volta anche molto significativo (vedremo poi perché) è il seguente:

## Esempio 9.16

Sia  $X$  un insieme finito. Si ponga  $\mathcal{B} := \mathcal{P}(X)$ , e, per ogni  $A, B \subseteq X$  (cioè per ogni  $A, B \in \mathcal{P}(X)$ ),

$$A + B := A \cup B, \quad AB := A \cap B, \quad \bar{A} := CA \quad \text{e} \quad 0 := \emptyset, \quad 1 := X.$$

Ebbene,  $(\mathcal{B}, \cup, \cap, \bar{\phantom{x}}, \emptyset, X)$  è un'algebra di Boole.

Vale la pena di verificare su questo esempio gli assiomi dell'algebra di Boole (cfr. eserc. 9.21).

## Esempio 9.17

L'insieme di tutte le funzioni booleane di  $n$  variabili, definite nel paragrafo precedente, con le operazioni di addizione, moltiplicazione e complemento che sono state allora definite, formano un'algebra di Boole, se si pone  $0 := O$  (funzione costante nulla) e  $1 := 1$  (funzione costante unitaria).

Fin qui nulla di nuovo: abbiamo ritrovato alcuni degli esempi già studiati. Ma si possono dare altri esempi di algebre di Boole.

## Esempio 9.18

Sia  $\mathcal{B}$  l'insieme di tutti i divisori positivi di 60:  $\mathcal{B} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$ . Per ogni  $x, y \in \mathcal{B}$  si definisca

$$x + y := \text{mcm}(x, y), \quad xy := \text{MCD}(x, y) \quad \text{e} \quad \bar{x} := \frac{60}{x}.$$

Posto 1 come l'elemento 0 e 30 come l'elemento 1,  $\mathcal{B}$  diventa un'algebra di Boole.

**PROPOSIZIONE 9.5** Sia  $\mathcal{B}$  un'algebra di Boole. La relazione

$$x \leq y \iff xy = x$$

è una relazione di ordine parziale.

**DIMOSTRAZIONE.** Dato che un'algebra di Boole non è altro che un particolare reticolo, basta ripetere la dimostrazione fatta nel caso di reticolli algebrici (cfr. eserc. 17 del par. 5). ◊

**COROLLARIO 9.2** Ogni algebra di Boole si può parzialmente ordinare.

Una volta che ci siamo resi conto che ogni algebra di Boole è un insieme parzialmente ordinato, possiamo dare la seguente importante definizione.

**DEFINIZIONE 9.15** Sia  $\mathcal{B}$  un'algebra di Boole e sia 0 lo zero di  $\mathcal{B}$ . Allora un elemento  $x \neq 0, x \in \mathcal{B}$  si dice *atomo* se per ogni  $y \in \mathcal{B}$

$$y \leq x \Rightarrow y = 0 \text{ oppure } y = x.$$
■

In altre parole, un atomo di un'algebra di Boole  $\mathcal{B}$  è un elemento non nullo  $x$  tale che non esiste nessun elemento  $y \in \mathcal{B}$  con  $0 < y < x$ .

Un'altra definizione di atomo è la seguente:

**DEFINIZIONE 9.16.** Un *atomo* è un elemento non nullo  $x$  che non si può scrivere nella forma  $y \vee z$  con  $y \neq x$  e  $z \neq x$ .

Calcoliamo gli atomi di alcune algebre di Boole.

#### Esempio 9.19

Nell'algebra di Boole  $\mathcal{B} = \{0, 1\}$  c'è un solo atomo, 1.

#### Esempio 9.20

Si consideri l'algebra di Boole  $\mathcal{B}^n = \mathcal{B} \times \mathcal{B} \times \mathcal{B}$  con  $n$  fattori, ossia l'insieme delle  $n$ -uple ordinate di 0 e 1 dove

$$(a_1, a_2, \dots, a_n) \vee (b_1, b_2, \dots, b_n) = (a_1 \vee b_1, \dots, a_n \vee b_n)$$

$$(a_1, a_2, \dots, a_n) \wedge (b_1, b_2, \dots, b_n) = (a_1 \wedge b_1, \dots, a_n \wedge b_n)$$

Gli atomi sono le  $n$ -uple con esattamente un 1.

#### Esempio 9.21

Nell'algebra di Boole  $\mathcal{P}(X)$  gli atomi sono i singleton.

#### Esempio 9.22

Nell'algebra delle proposizioni gli atomi sono le congiunzioni fondamentali.

Studiamo ora alcune proprietà degli atomi di un'algebra di Boole.

**LEMMA 9.3** Sia  $\mathcal{B}$  un'algebra di Boole finita. Gli atomi di  $\mathcal{B}$  verificano le seguenti proprietà :

a. Se  $x$  è un atomo di  $\mathcal{B}$ , allora

$$\forall y \in \mathcal{B} \quad xy = 0 \quad \text{oppure} \quad xy = x.$$

b. Se  $x_1, x_2$  sono atomi distinti di  $\mathcal{B}$ , allora

$$x_1 x_2 = 0.$$

c. Se  $x_1, x_2, \dots, x_n$  sono gli atomi di  $\mathcal{B}$  e  $x$  è un elemento di  $\mathcal{B}$  tale che  $xx_i = 0$  per ogni  $i = 1, 2, \dots, n$ , allora  $x = 0$ .

DIMOSTRAZIONE.

1. Per ogni  $x, y \in \mathcal{B}$ , si ha  $xy \leq x$ : infatti  $(xy)x = x(yx) = x(xy) = (xx)y = xy$ , ossia  $xy \leq x$ . Se ora  $x$  è un atomo, la  $xy \leq x$  implica  $xy = 0$  oppure  $xy = x$ .
2. In virtù del punto precedente, e tenendo conto che ora sia  $x_1$  sia  $x_2$  sono atomi, si ha  $x_1 x_2 = 0$  oppure  $[(x_1 x_2 = x_1) \wedge (x_2 x_1 = x_2)]$ . Dato che  $x_1 x_2 = x_1$  e  $x_2 x_1 = x_2$  comportano ovviamente  $x_1 = x_2$  (che escludiamo), deve necessariamente essere  $x_1 x_2 = 0$ .

3. Supponiamo  $x \neq 0$  e sia  $T = \{t \in \mathcal{B} \mid 0 < t \leq x\}$ . Risulta  $T \neq \emptyset$ , dato che  $x \in T$ . Essendo  $T$  finito, ci sarà un elemento  $y \in T$ , tale cioè che  $0 < y \leq x$ , ma tale che nessun elemento di  $\mathcal{B}$  stia tra 0 e  $y$ . Questo significa che  $y$  è un atomo e quindi, per le ipotesi,  $xy = 0$ . Ma allora si giunge ad una contraddizione perché si avrebbe  $0 = xy = y > 0$ . Ne segue che deve essere  $x = 0$ .

**PROPOSIZIONE 9.6** Sia  $\mathcal{B}$  un'algebra di Boole con atomi  $x_1, x_2, \dots, x_n$ . Allora ogni elemento non nullo  $x \in \mathcal{B}$  si scrive come somma di atomi, ossia

$$x = \sum_{i=1}^n \delta_i x_i, \quad \delta_i \in \{0, 1\}.$$

Tale scrittura è unica, a meno dell'ordine degli addendi.

**DIMOSTRAZIONE.** Essendo  $x \neq 0$ , in base al Lemma 9.3 l'insieme  $T = \{x_i \mid xx_i \neq 0\}$  è non vuoto. Poniamo

$$T = \{x_{i_1}, x_{i_2}, \dots, x_{i_h}\} \quad \text{e} \quad y = x_{i_1} + x_{i_2} + \dots + x_{i_h}$$

In virtù della (a) del Lemma 9.3 è facile verificare che  $xy = y$ . Si consideri ora  $(xy)x_i$  per ogni  $i = 1, 2, \dots, n$ . Distinguendo il caso  $x_i \notin T$  dal caso  $x_i \in T$  si ha che per ogni  $i = 1, 2, \dots, n$   $(xy)x_i = 0$ , il che comporta, in base alla (c) del Lemma 9.3,  $xy = 0$ . Ora, dalle  $xy = y$  e  $xy = 0$  segue  $x = x \cdot 1 = x(y + \bar{y}) = y = x_{i_1} + x_{i_2} + \dots + x_{i_h}$ .

Per quanto riguarda la unicità, supponiamo  $x = x_{i_1} + x_{i_2} + \dots + x_{i_h} = x_{j_1} + x_{j_2} + \dots + x_{j_k}$  e supponiamo che  $x_{j_1}$  non compaia nella sommatoria di sinistra. Allora (in base al punto (b) del Lemma 9.3)

$$x_{j_1} = x_{j_1} x_{j_1} = x_{j_1} (x_{j_1} + x_{j_2} + \dots + x_{j_k}) = x_{j_1} x = x_{j_1} (x_{i_1} + x_{i_2} + \dots + x_{i_h}) = 0.$$

Quindi  $x_{j_1}$  (e quindi anche tutti gli altri  $x_{j_i}$ ) devono comparire nella  $x_{i_1} + x_{i_2} + \dots + x_{i_h}$ , da cui  $k \leq h$ . Con un ragionamento analogo si trova  $h \leq k$  da cui l'uguaglianza delle scritture.

**COROLLARIO 9.4** Sia  $\mathcal{B}$  un'algebra di Boole con atomi  $x_1, x_2, \dots, x_n$ . Allora  $|\mathcal{B}| = 2^n$ .

**DIMOSTRAZIONE.** In virtù della scrittura (unica!) di ogni  $x \in \mathcal{B}$  come  $x = \sum_{i=1}^n \delta_i x_i$ ,  $\delta_i \in \{0, 1\}$ , esiste una corrispondenza biunivoca tra  $\mathcal{B}$  e l'insieme delle  $n$ -uple ordinate  $(\delta_1, \delta_2, \dots, \delta_n)$ ,  $\delta \in \{0, 1\}^n$ , che sono precisamente  $2^n$ .

Ciò significa per esempio che non esistono algebre di Boole con 15 elementi o con 40 elementi, perché 15 e 40 non sono della forma  $2^h$  per qualche  $h \in \mathbb{N}$ .

Ma c'è di più. Il risultato che abbiamo appena dimostrato, ossia che ogni algebre di Boole finita ha cardinalità  $2^n$  è simile al risultato visto per i campi finiti (cfr. cap. 7): ogni campo finito ha  $p^n$  elementi, con  $p$  numero primo. Per i campi abbiamo anche dimostrato che due campi finiti con lo stesso numero  $p^n$  di elementi sono isomorfi. Possiamo dire la stessa cosa per algebre di Boole della stessa cardinalità? La risposta è positiva, come vedremo fra breve.

Occorre però a questo punto dare la nozione di isomorfismo tra algebre di Boole.

**DEFINIZIONE 9.17** Un *isomorfismo* tra due algebre di Boole  $(B, +, \cdot)$  e  $(B', +', \cdot')$  è una corrispondenza biunivoca  $\varphi$  tra  $B$  e  $B'$  tale che per ogni  $x, y \in B$

$$\varphi(x+y) = \varphi(x) +' \varphi(y), \quad \varphi(x \cdot y) = \varphi(x) \cdot' \varphi(y), \quad \varphi(\bar{x}) = \overline{\varphi(x)}'. \quad \blacksquare$$

Come sempre accade in algebra, non saremo interessati a distinguere tra loro algebre di Boole che siano isomorfe.

Ebbene, sussiste il seguente importante teorema che sostanzialmente dice che per ogni  $n$  esiste una e una sola (a meno di isomorfismi) algebra di Boole di cardinalità  $2^n$ , l'algebra di Boole costituita dai sottoinsiemi di un insieme con  $n$  elementi.

**TEOREMA 9.5 (TEOREMA DI RAPPRESENTAZIONE)** *Ogni algebra di Boole finita  $B$  è isomorfa ad un'algebra di Boole di insiemi.*

**DIMOSTRAZIONE.** Essendo  $B$  finita, avrà un numero finito di atomi, siano essi  $x_1, x_2, \dots, x_n$ . Posto  $X := \{1, 2, \dots, n\}$ , faremo vedere che  $B$  è isomorfa a  $\mathcal{P}(X)$ . Si tratta di definire opportunamente una applicazione da  $B$  in  $\mathcal{P}(X)$  che risulti un isomorfismo.

Definiamo  $\varphi : B \rightarrow \mathcal{P}(X)$  al modo seguente: se  $x = \sum_{i=1}^n \delta_i x_i$ ,  $\delta_i \in \{0, 1\}$ , poniamo

$$\varphi(x) := \{i \mid 1 \leq i \leq n, \text{ e } \delta_i = 1\}.$$

Per esempio, se  $x = x_3 + x_6 + x_8$ , allora  $\varphi(x)$  è il sottoinsieme di  $X$   $\{3, 6, 8\}$ . In particolare  $\varphi(x_i) = \{i\}$  per ogni  $i = 1, 2, \dots, n$  ossia gli atomi di  $B$  vanno negli atomi di  $\mathcal{P}(X)$ . Resta da provare che  $\varphi$  è biunivoca e che

$$\varphi(x+y) = \varphi(x) \cup \varphi(y),$$

$$\varphi(xy) = \varphi(x) \cap \varphi(y),$$

e

$$\varphi(\bar{x}) = \overline{\varphi(x)}.$$

Si lascia per esercizio (cfr. eserc. 24).  $\diamond$

Il corollario che segue mostra che gli atomi di un'algebra di Boole finita determinano l'algebra stessa.

**COROLLARIO 9.6** *Sia  $B$  un'algebra di Boole finita con atomi  $a_1, a_2, \dots, a_n$  e  $B'$  un'altra algebra di Boole finita con lo stesso numero di atomi,  $b_1, b_2, \dots, b_n$ . Allora esiste un isomorfismo  $\varphi$  di algebre di Boole da  $B$  a  $B'$  tale che  $\varphi(a_i) = b_i$  per ogni  $i = 1, 2, \dots, n$ .*

In altre parole, se due algebre di Boole finite hanno lo stesso numero di atomi, allora sono isomorfe.

### Esercizi

10 Provare che l'insieme di tutti i sottoinsiemi finiti o cofiniti (tali cioè che il loro complementare sia finito) di un insieme non vuoto  $X$  rispetto alle operazioni di intersezione e unione e passaggio al complementare forma un'algebra di Boole.

11 Se  $(R, +, \cdot)$  è un anello arbitrario, sia

$$S := \{e \in R \mid e^2 = e, er = re \forall r \in R\}$$

l'insieme degli idempotenti centrali dell'anello  $R$ . Provare che  $S$  diventa un'algebra di Boole rispetto alle seguenti operazioni:

$$e \vee f := e + f - ef, \text{ dove } + \text{ e } \cdot \text{ sono le operazioni di } R$$

$$e \wedge f := ef \quad (= \text{moltiplicazione di } R.)$$

12 Verificare gli assiomi di algebra di Boole nell'esempio 9.16.

13 (Per chi sa cos'è uno spazio topologico) Sia  $X$  uno spazio topologico. Provare che l'insieme  $A$  di tutti i sottoinsiemi di  $X$  che sono sia aperti sia chiusi in  $X$  forma un'algebra di Boole rispetto alle operazioni di unione e intersezione tra insiemi.

14 Sia  $B$  un'algebra di Boole con  $n$  atomi  $x_1, x_2, \dots, x_n$ . Si provi che  $1 = x_1 + x_2 + \dots + x_n$ .

15 Provare che la corrispondenza  $\varphi$  del teorema 9.5 è biunivoca.

# 10 Grafi

*"Ciò che abbellisce il deserto" disse il piccolo principe,  
"è che nasconde un pozzo in qualche luogo..."*

*"Sì", dissi al piccolo principe, "che si tratti di una casa, delle stelle  
o del deserto, quello che fa la loro bellezza è invisibile."*  
Antoine de Saint-Exupéry, IL PICCOLO PRINCIPE

In questo capitolo introdurremo una nozione di fondamentale importanza per modellare in maniera schematica una vasta quantità di problemi. Si tratta della nozione di *grafo*. Tale nozione si applica, oltre che all'informatica e alla matematica, anche ai campi più svariati, come la chimica, la biologia, la fisica, l'ingegneria civile, la cartografia, le reti telefoniche, i circuiti elettrici, la ricerca operativa, la sociologia, l'organizzazione industriale, la teoria dei trasporti, l'intelligenza artificiale, ecc. Ma l'elenco potrebbe continuare. Questo argomento, proprio per la sua vasta applicabilità, merita un capitolo a sé. Presenteremo solo alcuni concetti di teoria dei grafi, quelli che ci sembrano più rilevanti per i nostri scopi, tralasciandone tantissimi altri. Una trattazione completa di teoria dei grafi, d'altra parte, richiederebbe ben più di un capitolo in un libro e infatti nel corso di studi di Informatica esistono corsi specifici di Teoria dei Grafi. Queste pagine vogliono solo essere un invito a questa affascinante teoria.

## ■ 1 MOTIVAZIONI E PRIME DEFINIZIONI

Storicamente la teoria dei grafi si fa risalire al 1736, anno di pubblicazione del lavoro *Solutio problematis ad geometriam situs pertinensis* (Comm. Acad. Sc. Imperialis Petropolitanae 8 (1736)) del grande matematico svizzero L. Eulero (1707-1783). In questo lavoro egli risolve il cosiddetto *problema dei ponti di Königsberg* (Kalinigrad, ai giorni nostri). La città prussiana di Königsberg era percorsa dal fiume Pregel e questo era attraversato da sette ponti disposti come in figura 10.1.

Il problema era il seguente: è possibile fare una passeggiata per la città, attraversando tutti e sette i ponti una e una sola volta e ritornare al punto di partenza? Nessuno c'era mai riuscito.

Nel lavoro citato Eulero risolse il problema in negativo, provando che una tale passeggiata non è possibile. L'importanza di questo risultato risiede soprattutto nell'idea che Eulero introdusse per risolvere questo problema, e che per l'appunto ha dato

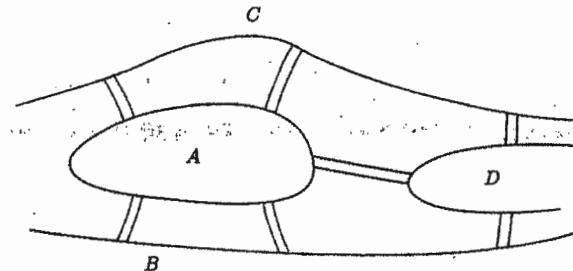


Figura 10.1. I ponti di Königsberg.

origine alla teoria dei grafi. Eulero capì che per la risoluzione del problema occorreva individuare gli *elementi essenziali* del problema, trascurando gli elementi accessori, o irrilevanti. A questo scopo considerò il *modello* della figura 10.2:

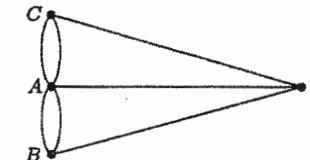


Figura 10.2. Il grafo dei ponti di Königsberg.

Questo schema è un esempio di grafo. Vedremo tra breve come il risultato generale ottenuto da Eulero (teorema 10.1) permetta di risolvere il problema dei sette ponti.

**OSSERVAZIONE** La terminologia usata in letteratura quando si parla di grafi varia moltissimo da testo a testo: l'importante è ovviamente essere consistenti, per cui è essenziale fornire le definizioni che adotteremo.

**DEFINIZIONE 10.1** Un *grafo orientato*  $G$  è una coppia  $G = (V, E)$  che consiste in un insieme finito  $V \neq \emptyset$  di elementi che si chiamano *vertici* o *nodi* o *punti* del grafo e un insieme  $E \subseteq V \times V$  di coppie ordinate di elementi di  $V$  che si chiamano *archi* o *assi*.

Un grafo orientato si chiama anche *digraph* dall'inglese *directed graph*.

Un elemento  $e = (v, w) \in E$  si rappresenta come l'arco di estremi i vertici  $v$  e  $w$ , orientato da  $v$ , che si dice *punto di partenza*, a  $w$ , che si dice *punto di arrivo*.

In altre parole, un grafo orientato altro non è che una *relazione* definita in  $V$ . Gli archi dicono come i vertici sono collegati. In un grafo orientato, dati due vertici  $v, w$ , si dice che  $w$  è *adiacente* a  $v$  se  $(v, w) \in E$ . La relazione definita da  $E$  si dice relazione di *adiacenza*. Un esempio di grafo orientato è per esempio il grafo  $G = (V, E)$ , dove  $V = \{a, b, c, d, e, f\}$ ,  $E = \{(a, a), (a, b), (b, c), (e, f)\}$  della figura 10.3.

Spesso, per schematizzare un problema, non è necessario che gli archi di un grafo siano orientati: per esempio, per fare una pianta stradale di una città dove tutte le strade sono percorribili in entrambi i sensi basta indicare l'arco (ossia la strada)

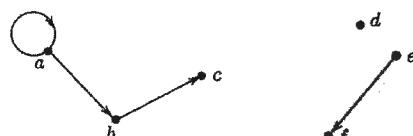


Figura 10.3. Esempio di grafo orientato.

tra due punti della città e non il verso di percorrenza. Diamo pertanto la seguente definizione:

**DEFINIZIONE 10.2** Un *grafo non orientato*, o semplicemente *grafo G* è una coppia  $G = (V, E)$  che consiste in un insieme finito  $V \neq \emptyset$  e un insieme  $E$  di coppie non ordinate di elementi (non necessariamente distinti) di  $V$ .  $\blacksquare$

Un grafo non orientato è per esempio dato da  $G = (V, E)$  dove  $V = \{a, b, c, d, e, f\}$  e  $E = \{\{a, b\}, \{a, c\}, \{f, a\}\}$  (fig. 10.4).

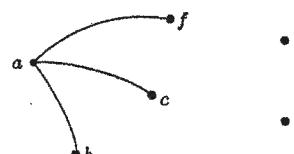


Figura 10.4. Esempio di grafo non orientato.

In generale, dato un grafo  $G = (V, E)$ , se non si specifica se è orientato o non orientato, si suppone *non orientato*. Noi per lo più considereremo grafi non orientati. Dunque quando parleremo di grafo senza ulteriore specificazione, intenderemo un grafo di questo tipo.

**DEFINIZIONE 10.3** L'*ordine* di un grafo  $G$  è il numero dei suoi vertici, mentre la *grandezza* di  $G$  è il numero dei suoi archi. Spesso un grafo di ordine  $n$  e grandezza  $m$  si denota con  $G(n, m)$ .  $\blacksquare$

Ovviamente la grandezza  $m$  di un grafo avrà le seguenti limitazioni:  $0 \leq m \leq \binom{n}{2}$ .

- Il caso  $m = 0$  (sicuramente poco interessante) corrisponde al *grafo nullo* (che spesso si indica anche con  $N_n$ ) che consiste di  $n$  vertici  $v_1, v_2, \dots, v_n$  senza alcun collegamento (fig. 10.5).



Figura 10.5. Il grafo nullo.

- Il caso  $m = \binom{n}{2}$  corrisponde al caso in cui ogni vertice è collegato con tutti gli altri.

**DEFINIZIONE 10.4** Si definisce *grafo completo* su  $n$  vertici, e si denota con  $K_n$ , un grafo  $G(n, \binom{n}{2})$ , ossia un grafo che ha  $n$  vertici e un arco per ogni coppia di vertici distinti.  $\blacksquare$

Illustriamo qui di seguito i grafi  $K_1, \dots, K_6$  (fig. 10.6).

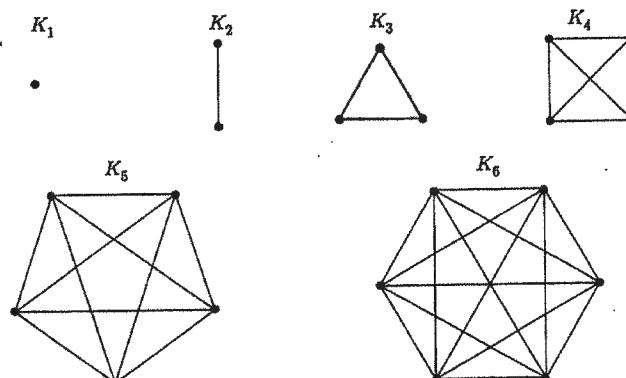


Figura 10.6. Esempi di grafi completi.

Un arco di tipo  $(a, a)$  prende il nome di *cappio*.

**DEFINIZIONE 10.5** Un *cammino* in un grafo è una successione di vertici  $v_1 v_2 \dots v_n$  dove  $(v_1, v_2), (v_2, v_3), \dots, (v_i, v_{i+1}), \dots, (v_{n-1}, v_n)$  sono archi del grafo. Un vertice può apparire più di una volta, mentre un arco no.  $\blacksquare$

Nel grafo della figura 10.7 la successione  $v_6 v_1 v_4 v_5$  rappresenta un cammino da  $v_6$  a  $v_5$ :

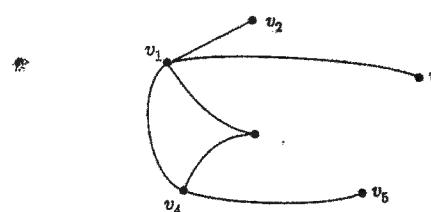


Figura 10.7.

Il cammino disegnato nella figura 10.8 ha come archi  $(v_6, v_1), (v_1, v_4), (v_4, v_5)$ :

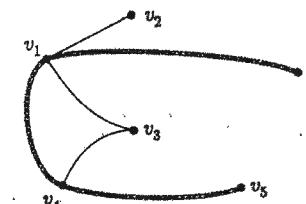


Figura 10.8.

**DEFINIZIONE 10.6** La *lunghezza* di un cammino è il numero di archi nel cammino. ■■■

Nell'esempio appena fatto il cammino disegnato ha lunghezza 3.

Se togliamo alla nozione di cammino la richiesta di avere archi distinti, si ottiene la nozione di percorso: ribadiamo che in letteratura non sempre si usano queste notazioni. Quindi

**DEFINIZIONE 10.7** Un *percorso* in un grafo è una successione di vertici  $v_1 v_2 \dots v_n$  dove  $(v_1, v_2), (v_2, v_3), \dots, (v_i, v_{i+1}), \dots, (v_{n-1}, v_n)$  sono archi del grafo. Sia i vertici sia gli archi possono apparire più di una volta. ■■■

Per esempio la successione  $v_6 v_1 v_2 v_1$  nel grafo della figura 10.7 è un percorso (che non è un cammino).

Si noti che potrebbero esserci grafi in cui c'è più di un arco che connette due vertici. In questo caso, non essendo individuato l'arco tra due vertici, occorre etichettarlo opportunamente. Un grafo tale che esistano due vertici collegati da più di un arco si dice *multigrafo*. Altrimenti (ossia nel caso in cui dati comunque due vertici, esiste al più un arco che li connette) si dice *semplice*.

Il grafo della figura 10.2 corrispondente ai ponti di Königsberg è un multigrafo.

**DEFINIZIONE 10.8** La *distanza*  $d(v_i, v_j)$  tra due vertici  $v_i$  e  $v_j$  di un grafo  $G$  è la lunghezza minima tra tutti i cammini (se questi esistono) che li congiungono. In caso contrario si pone  $d(v_i, v_j) = \infty$ . Un cammino di lunghezza minima tra due vertici di un grafo dicesi *geodetica*. ■■■

#### Esempio 10.1

Nel grafo della figura 10.8 il cammino segnato è una geodetica: un altro cammino è per esempio  $v_6 v_1 v_3 v_4 v_5$ , che però ha lunghezza 4.

**DEFINIZIONE 10.9** Un *circuito* o *ciclo* in un grafo è un cammino  $v_1 v_2 \dots v_n = v_1$  in cui il vertice iniziale  $v_1$  coincide con il vertice finale  $v_n$ . Si richiede inoltre che il cammino contenga almeno un arco. ■■■

Per esempio nel grafo della figura 10.7 il cammino  $v_1 v_3 v_4 v_1$  è un circuito.

Si osservi che la lunghezza di  $v_1 v_2 \dots v_n = v_1$  è  $n - 1$ .

**DEFINIZIONE 10.10** Un circuito si dice *pari* (*dispari*) se la sua lunghezza è pari (dispari). ■■■

Il circuito appena visto  $v_1 v_3 v_4 v_1$  è dispari perché ha lunghezza 3.

**DEFINIZIONE 10.11** Un *circuito euleriano* è un circuito che passa per tutti gli archi del grafo. ■■■

Il circuito  $v_1 v_3 v_4 v_1$  del grafo della figura 10.7 non è euleriano.

Terminiamo con un'altra definizione.

**DEFINIZIONE 10.12** Un grafo si dice *connesso* se, dati comunque due suoi vertici  $v$  e  $w$ , esiste un cammino da  $v$  a  $w$ . ■■■

Il grafo della figura 10.7 è connesso (si verifichi!). Invece i grafi delle figure 10.3 e 10.4 non lo sono.

Ogni grafo si può dividere in *componenti connesse*: per esempio il grafo della figura 10.3 ha tre componenti connesse, e così il grafo della figura 10.4.

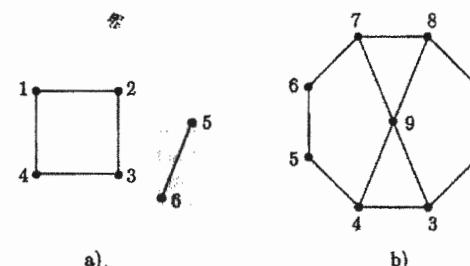
#### Esercizi

- Determinare la distanza di due qualunque vertici nei grafi delle Figure 10.4, 10.6, 10.7.
- Decidere se il grafo con vertici  $a, b, c, d, e, f$  e archi  $(b, c), (a, d), (c, a), (e, d), (f, d)$  è connesso. In caso contrario determinare le componenti connesse.
- Decidere quanti e quali sono i grafi orientati associati al grafo non orientato su quattro vertici della figura 10.9

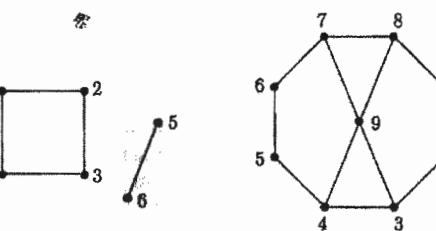


Figura 10.9.

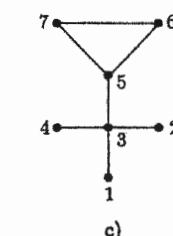
- Sia  $G$  un grafo con  $n$  archi. In quanti modi si possono orientare i suoi archi?
- Determinare tutti i cammini che congiungono il vertice 1 col vertice 5 nei grafi della figura 10.10.



a).



b).



c).

Figura 10.10.

## ■■■ 2 GRAFI EULERIANI

I grafi che contengono un circuito euleriano meritano un paragrafo a parte.

**DEFINIZIONE 10.13** Un grafo che contenga un circuito euleriano si dice *grafo euleriano*. ■■■

Abbiamo visto che il circuito  $v_1v_3v_4v_1$  del grafo della figura 10.7 non è euleriano. Ciò non basta per dire che il grafo non è euleriano. Per convincerci del fatto che non è euleriano occorre verificare che non possiede *nessun circuito euleriano*. Infatti se un circuito euleriano *parte* dal vertice  $v_2$ , non si potrà ritornare a  $v_2$  se non ripercorrendo il lato  $v_1v_2$  (operazione non lecita); se un circuito *parte* da un qualunque vertice *diverso* da  $v_2$ , quando percorrerà l'arco  $v_1v_2$  (si ricordi che un circuito euleriano deve passare per tutti gli archi), raggiungerà  $v_2$  e da  $v_2$  resterà bloccato. Quindi non esiste nessun circuito euleriano e il grafo della figura 10.7 non è euleriano.

**DEFINIZIONE 10.14** Il *grado di un vertice v* è il numero di lati incidenti a  $v$  (che cioè passano per  $v$ ).  $\diamond$

Nel grafo della figura 10.7,  $v_1$  ha grado 4,  $v_2$ ,  $v_5$  e  $v_6$  hanno grado 1,  $v_3$  ha grado 2 e  $v_4$  ha grado 3.

Nel grafo della figura 10.2 associato ai ponti di Königsberg tutti i vertici hanno grado 3, ad eccezione di  $A$  che ha grado 5.

Ebbene, vale il seguente importante teorema che caratterizza i grafi euleriani.

**TEOREMA 10.1 (EULERO)** Un grafo  $G$  privo di vertici isolati è euleriano se e solo se

a) è connesso;

b) il grado di ogni vertice di  $G$  è un numero pari.

**DIMOSTRAZIONE.** Proviamo innanzitutto che la condizione è necessaria, ossia che se un grafo privo di vertici isolati è euleriano, allora è connesso e il grado di ogni vertice è un numero pari. Siano  $v$  e  $w$  due vertici distinti arbitrari di  $G$ ; dato che il grafo è privo di vertici isolati,  $v$  e  $w$  si troveranno su degli archi (eventualmente distinti). Il grafo, essendo euleriano, conterrà un circuito euleriano, che quindi passa per *tutti* gli archi del grafo e contiene dunque i due vertici. Ne segue che  $G$  è connesso.

Proviamo ora che il grado di ogni vertice è un numero pari. Sia  $v$  un vertice: esso apparterrà ad un circuito euleriano (sicuramente esistente). Se pensiamo di partire dal vertice  $v$  lungo questo circuito euleriano, alla fine ritorneremo in  $v$  e le volte che saremo usciti da  $v$  (cioè le volte in cui  $v$  compare come punto di partenza di un arco) uguaglia il numero di volte in cui saremo tornati in  $v$  (ossia le volte in cui  $v$  appare come punto di arrivo di un arco). Quindi gli archi che entrano o che escono da  $v$  saranno in numero pari.

Proviamo ora la sufficienza. Supponiamo che il grafo sia connesso e che il grado di ogni vertice sia pari, e proviamo che il grafo è euleriano.

La dimostrazione di questa parte sarà costruttiva, nel senso che si dirà esattamente come si costruisce un circuito euleriano. Sceglieremo un vertice iniziale arbitrario, diciamo  $v$ , e percorriamo a caso gli archi senza alcun criterio, con l'unica avvertenza di non ritornare mai su un arco che sia già stato percorso: continuiamo finché non *rimaniamo bloccati* ad un vertice  $w$ , bloccati nel senso che tutti gli archi uscenti da  $w$  sono già stati percorsi. I casi sono due:

- $w \neq v$ . Questo caso non può presentarsi, perché il grado di  $w$  sarebbe un numero dispari (saremmo entrati in  $w$  una volta di più di quante ne siamo usciti), e questo contraddice le ipotesi;

- $w = v$ : significa che se restiamo bloccati, lo saremo nel punto di partenza, e pertanto gli archi percorsi fino a quel momento formano un circuito  $C = v_1v_2\dots v_n$  dove si è posto  $v_1 = w = v = v_n$ .

Può benissimo succedere però che esista un altro arco uscente da qualche vertice  $v_i$  del circuito  $C$  che non è stato percorso. Chiameremo questa situazione una *fuoriuscita* dal vertice  $v_i$ . Che facciamo allora? Basta sostituire il circuito  $C$  con il seguente *cammino*:  $v_iv_{i+1}\dots v_1v_2\dots v_iv$  essendo  $v$  l'estremo dell'arco che fuoriesce da  $v_i$ : tale cammino contiene al suo interno il circuito di partenza. Ci troviamo ora nella situazione di un cammino con ultimo vertice  $v$ : continuiamo, come abbiamo fatto inizialmente, a percorrere gli archi non ancora percorsi, mediante costruzione di circuiti e fuoriuscite, finché non saremo arrivati ad un circuito  $C'$ , dal quale non è possibile nessuna fuoriuscita: questo significa che ogni arco uscente da *ogni vertice* di  $C'$  è stato percorso. Ma questo significa che abbiamo trovato un circuito euleriano. Perché? Per costruzione, gli archi del circuito ottenuto sono stati percorsi una sola volta; resta da provare che *tutti* gli archi del grafo sono stati percorsi. Sia  $\alpha$  un qualunque arco del grafo  $G$ , di estremi  $x$  e  $y$ . Sappiamo che  $G$  è connesso: esisterà quindi certamente un cammino che congiunge il vertice  $v$  da noi scelto inizialmente con  $x$ : sia  $v w_1 w_2 \dots x$  un tale cammino. Ora, l'arco  $vw_1$  deve trovarsi sul ciclo  $C'$  (altrimenti da  $v$  ci sarebbe una fuoriuscita, cosa che abbiamo escluso). Quindi  $w_1 \in C'$  e allora anche l'arco  $w_1w_2$  deve stare sul ciclo  $C'$  sempre per lo stesso motivo. Andando avanti,  $w_3, \dots, x$  devono stare sul ciclo. Ma allora l'arco  $\alpha$  che collega  $x$  con  $y$  deve stare anch'esso sul ciclo. In definitiva il ciclo  $C'$  è euleriano.  $\diamond$

Il Teorema di Eulero per i grafi euleriani permette quindi di scoprire se un grafo è euleriano semplicemente osservando il grado dei suoi vertici: se anche uno solo dei vertici ha grado dispari, il grafo non è euleriano. Se scopriamo in questo modo che un grafo è euleriano, per trovare effettivamente un circuito euleriano, dovremo procedere come nella dimostrazione del teorema.

A questo punto abbiamo tutti gli elementi a disposizione per dare una risposta al problema dei ponti di Königsberg. Il problema è chiaramente equivalente a decidere se il grafo associato della figura 10.2 è un grafo euleriano. Per provare che *non* è euleriano basta controllare se possiede un vertice che ha grado dispari: abbiamo visto che addirittura *tutti* i vertici del grafo hanno grado dispari, quindi sicuramente non è euleriano. Pertanto la risposta al problema è negativa.

Ritroviamo anche che il grafo della figura 10.7 non è euleriano dall'esame del grado dei suoi vertici (invece che esaminando i possibili circuiti come abbiamo fatto).

Mettiamo ora in pratica la dimostrazione costruttiva del Teorema di Eulero per trovare un ciclo euleriano di un grafo euleriano.

#### Esempio 10.2

Costruire un ciclo euleriano del grafo della figura 10.11.

Innanzitutto osserviamo che tale grafo è euleriano dato che è connesso e il grado di ogni vertice è 2 o 4. Prendiamo come vertice iniziale  $v_1$ , e percorriamo a caso gli archi con l'unica avvertenza di non ritornare mai su un arco che sia già stato percorso, continuando finché non rimaniamo bloccati. Percorriamo il cammino  $v_1v_2v_3v_4v_2v_5v_6v_1$ . A questo punto siamo bloccati. In  $v_6$  c'è una fuoriuscita: quindi consideriamo il cammino  $v_6v_1v_2v_3v_4v_2v_5v_6v_3v_7v_6$ .

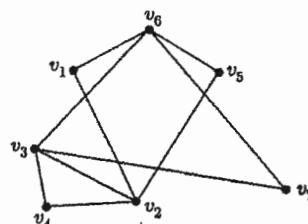


Figura 10.11. Grafo euleriano.

Si veda la figura 10.12 nella quale gli archi sono numerati, a partire dal vertice  $v_6$ , in base all'ordine con cui vengono percorsi. Si tratta di un ciclo, dal quale non ci sono fuoriuscite. Quindi si tratta di un ciclo euleriano.

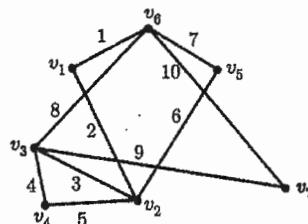


Figura 10.12. Costruzione ciclo euleriano.

Per potere enunciare l'analogo del Teorema di Eulero per i grafi *orientati* occorre sostituire la nozione di grado di un vertice con la nozione di *vertice bilanciato*.

**DEFINIZIONE 10.15** Un vertice di un grafo orientato si dice *bilanciato* se il numero di archi entranti uguaglia il numero di archi uscenti. ■

Ebbene, le condizioni che assicurano che un grafo *orientato* privo di vertici isolati sia euleriano sono che il grafo sia connesso e che ogni vertice sia bilanciato. La dimostrazione non è difficile.

Possiamo essere interessati a scoprire se un grafo contiene anziché un circuito euleriano, semplicemente un *cammino euleriano* (ossia un cammino che passa per tutti gli archi ma che non è un circuito, ossia tale che il vertice iniziale e il vertice finale non coincidano). Ebbene, non è difficile rendersi conto che vale il seguente risultato:

**TEOREMA 10.2** Sia  $G$  un grafo privo di vertici isolati. Allora  $G$  possiede un cammino euleriano se e solo se

- a) è connesso;
- b) ogni vertice di  $G$  ha grado pari eccetto esattamente due vertici.

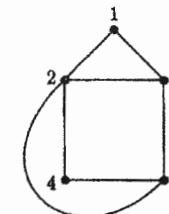


Figura 10.13.

Si pensi al grafo della figura 10.13: il punto di partenza e il punto di arrivo del cammino saranno i due vertici di grado dispari, ossia i vertici 4 e 5.



- Determinare il grado dei singoli vertici nel grafo della figura 10.14:

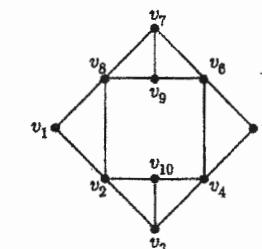


Figura 10.14.

- Decidere se il grafo dell'esercizio precedente è euleriano.

- Si consideri il grafo della figura 10.15:

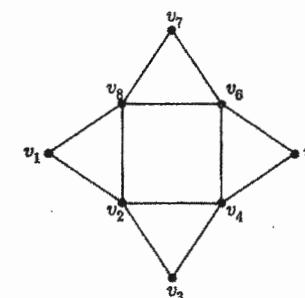


Figura 10.15.

Decidere se esiste un ciclo euleriano. In caso positivo determinarne uno.

### ■ 3 MATRICI DI ADIACENZA

Un modo utile per rappresentare un grafo è attraverso la cosiddetta *matrice di adiacenza* del grafo.

Dato un grafo semplice  $G$  con  $n$  vertici, la sua matrice di adiacenza è la matrice  $n \times n$  che ha 1 nella posizione  $(i, j)$  se il vertice  $v_i$  e il vertice  $v_j$  sono connessi da un arco, 0 altrimenti. Per esempio, la matrice di adiacenza del grafo della figura 10.7 è

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Si noti che la matrice di adiacenza di un grafo non orientato è simmetrica. Se invece il grafo (semplice) è orientato e per esempio esiste un arco dal vertice  $v_i$  al vertice  $v_j$ , porremo 1 nella posizione  $(i, j)$ , ma nella posizione  $(j, i)$  ci sarà 0. La matrice di adiacenza sarà quindi in genere non simmetrica. Per esempio, la matrice di adiacenza del grafo della figura 10.3 è :

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Nel caso di multigrafi non orientati, se esistono  $s$  archi che collegano il vertice  $v_i$  con il vertice  $v_j$ , porremo l'intero  $s$  nella posizione  $(i, j)$  e nella posizione  $(j, i)$ . Nel caso di multigrafi orientati, se esistono  $s$  archi che vanno da  $v_i$  a  $v_j$ , porremo  $s$  nella posizione  $(i, j)$  e se esistono  $t$  archi che partono da  $v_j$  e vanno in  $v_i$  porremo  $t$  al posto  $(j, i)$ , e 0 se non esiste nessun arco da  $v_j$  a  $v_i$ . La matrice di adiacenza del grafo della figura 10.2 dei ponti di Königsberg è :

$$\begin{pmatrix} 0 & 2 & 2 & 1 \\ 2 & 0 & 0 & 1 \\ 2 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

**DEFINIZIONE 10.16** Un grafo è *etichettato* se i suoi vertici sono distinguibili l'uno dall'altro perché è stato loro attribuito un nome. ■

Assegnare un grafo attraverso la sua matrice di adiacenza è il metodo più adatto per comunicare la struttura di un grafo ad un calcolatore.

#### Proprietà della matrice di adiacenza $A$ di un grafo non orientato

1.  $A$  è simmetrica.
2. La somma degli elementi di ogni riga  $i$  uguaglia il grado di  $v_i$ .
3. Se  $A_1$  e  $A_2$  sono matrici di adiacenza che corrispondono a differenti etichette di uno stesso grafo,  $A_1$  è *conjugata* ad  $A_2$ , esiste una matrice invertibile  $B$  tale che  $A_2 = B^{-1} A_1 B$ .

#### Proprietà della matrice di adiacenza $A$ di un grafo orientato

1.  $A$  non è necessariamente simmetrica.
2. La somma degli elementi di ogni riga  $i$  uguaglia il numero di archi che partono dal vertice  $v_i$ .
3. La somma degli elementi di ogni colonna  $i$  uguaglia il numero di archi che hanno come secondo estremo il vertice  $v_i$ .

#### Esempio 10.3

La matrice di adiacenza del grafo completo su 5 vertici,  $K_5$

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Si noti che si tratta di una matrice simmetrica, trattandosi di un grafo non orientato, che ha tutti zeri sulla diagonale principale, dato che non ci sono cicli.

#### Esempio 10.4

La seguente matrice

$$A = \begin{pmatrix} 0 & 0 & 2 & 2 \\ 1 & 0 & 2 & 0 \\ 3 & 0 & 0 & 1 \\ 2 & 1 & 0 & 0 \end{pmatrix}$$

è la matrice di adiacenza del grafo della figura 10.16.

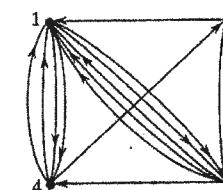


Figura 10.16.

La matrice di adiacenza di un grafo non è solamente uno strumento importante col quale si riescono a leggere molte informazioni relative al grafo. Ci dà anche molte altre informazioni. Per la definizione di addizione e moltiplicazione tra matrici quadrate si vedano le definizioni 8.5 e 8.6.

Sappiamo che, se  $A$  è la matrice di adiacenza di un (multi)grafo  $G$ , il numero che si trova nella posizione  $ij$  rappresenta il numero di archi che collegano il vertice  $v_i$  col vertice  $v_j$ . Ebbene, lo studio delle *potenze* della matrice  $A$  ci dà ulteriori informazioni sul grafo. Precisamente, come precisato dalla seguente proposizione, le potenze della matrice  $A$  danno informazioni sul numero di *percorsi* (cfr. definizione 10.7) del grafo.

**PROPOSIZIONE 10.1** Se  $A$  è la matrice di adiacenza di un grafo  $G$ , allora il numero di percorsi in  $G$  dal vertice  $v_i$  al vertice  $v_j$  di lunghezza  $k$  ( $k \geq 1$ ) è dato dall'elemento di posizione  $ij$  della matrice  $A^k$ .

**DIMOSTRAZIONE.** La dimostrazione procede per induzione su  $k$ .  $\diamond$

#### Esempio 10.5

Per calcolare quanti sono i percorsi di lunghezza 2 del grafo della figura 10.7 dobbiamo calcolare la potenza  $A^2$  dove  $A$  è la matrice di adiacenza del grafo, ossia, come si è visto, la

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Si ha

$$A^2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 3 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

In effetti, i percorsi da  $v_1$  a  $v_1$  di lunghezza 2 sono 4 ( $v_1v_2v_1, v_1v_6v_1, v_1v_3v_1, v_1v_4v_1$ ) (ricordiamo che si tratta di percorsi, non di cammini, quindi gli archi si possono ripercorrere). Non c'è nessun percorso da  $v_1$  a  $v_2$  di lunghezza 2 ( $a_{12} = 0$ ). Ci sono 3 percorsi da  $v_4$  a  $v_4$  di lunghezza 2 ( $a_{44} = 3$ ) ecc.

Le potenze della matrice di adiacenza di un grafo ci danno informazioni anche sulla *connessione* del grafo. Precisamente, si ha il seguente risultato.

**PROPOSIZIONE 10.2** Sia  $A$  la matrice di adiacenza di un grafo  $G$  con  $n$  vertici. Allora

1.  $G$  è connesso se e solo se  $I + A + A^2 + \dots + A^{n-1}$  contiene solo interi strettamente positivi.
2.  $G$  è connesso se e solo se  $(I + A)^{n-1}$  contiene solo interi strettamente positivi.

**DIMOSTRAZIONE.** Si veda l'esercizio 13.  $\diamond$

#### Esercizi

- 1) Determinare la matrice di adiacenza del grafo della figura 10.17:

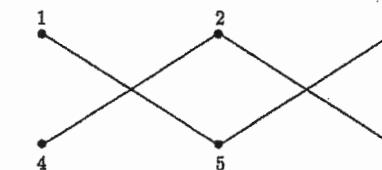


Figura 10.17.

- 2) Determinare il grafo la cui matrice di adiacenza è la seguente:

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- 3) Determinare la matrice di adiacenza del grafo della figura 10.18.

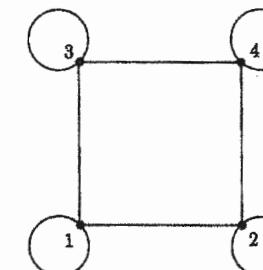


Figura 10.18.

- 4) Determinare la matrice di adiacenza del grafo orientato della figura 10.19.

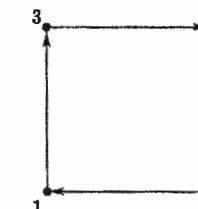


Figura 10.19.

Dimostrare la proposizione 10.2.

Si determinino la somma e il prodotto delle seguenti due matrici:

$$A = \begin{pmatrix} 1 & 2 & 3 & -1 \\ 0 & 2 & -1 & 3 \\ 1 & 1 & 0 & -2 \\ -1 & 0 & 1 & 1 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 0 & 1 & 4 & 0 \\ -1 & 1 & 1 & 1 \\ -1 & 3 & 0 & 1 \\ 3 & 0 & 0 & 1 \end{pmatrix}$$

Siano  $A$  e  $B$  le matrici dell'esercizio precedente. Si determinino  $A^2$  e  $B^2$ ,  $A^3$  e  $B^3$ .

Si determinino la somma e il prodotto delle seguenti due matrici:

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Siano  $A$  e  $B$  le matrici dell'esercizio precedente. Disegnare i grafi che hanno rispettivamente  $A$  e  $B$  come matrici di adiacenza. Dire se si tratta di grafi orientati o non orientati, e se si tratta di grafi connessi.

Sia  $A$  la matrice

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

- Disegnare il grafo che ha  $A$  come matrice di adiacenza.
- Calcolare  $A^2$  e  $A^3$ .
- Verificare la validità del teorema 10.1.

## 4 ISOMORFISMI E AUTOMORFISMI DI GRAFI

**DEFINIZIONE 10.17** Due grafi  $G = (V, E)$  e  $G' = (V', E')$  si dicono *isomorfi*, e si scrive

$$G \simeq G'$$

se esiste una corrispondenza biunivoca  $f : V \rightarrow V'$  tale che se  $(v, w) \in E$ , allora  $(f(v), f(w)) \in E'$ . In altre parole, due vertici sono adiacenti in  $G$  se e solo se le loro immagini mediante  $f$  sono adiacenti in  $G'$ .  $\blacksquare$

Si noti che grafi isomorfi hanno necessariamente lo stesso numero di vertici, lo stesso numero di archi e un ugual numero di vertici per ogni grado.

Tuttavia queste condizioni sono solamente necessarie, ma *non sono sufficienti* per garantire l'isomorfismo dei due grafi, come si vede dai grafi delle Figure 10.20 e 10.21 rispettivamente che, pur verificando tutte le condizioni, non sono isomorfi:

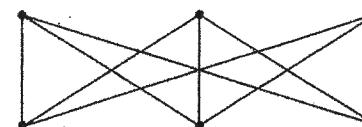


Figura 10.20.

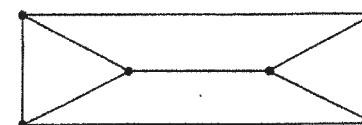


Figura 10.21.

**DEFINIZIONE 10.18** Un *automorfismo* di un grafo  $G$  è un isomorfismo di  $G$  in sé.  $\blacksquare$

L'insieme di tutti gli automorfismi di un grafo  $G$  si indica con  $\mathcal{A}(G)$  ed è un gruppo rispetto al prodotto operatorio.

Il gruppo degli automorfismi del grafo completo con  $n$  vertici è isomorfo al gruppo simmetrico di grado  $n$ ,  $S_n$ .

È stato dimostrato che ogni gruppo finito è isomorfo al gruppo degli automorfismi di un opportuno grafo. Da qui si capisce l'importanza dei grafi.

A proposito di isomorfismi tra grafi c'è una famosa *congettura di Ulam*. Prima di enunciarla premettiamo alcune definizioni.

**DEFINIZIONE 10.19** Un *sottografo* di un grafo  $G$  è un grafo che ha tutti i vertici e tutti gli archi in  $G$ .  $\blacksquare$

Cosa succede se togliamo un vertice  $v_i$  ad un grafo  $G$ ? A meno che  $v_i$  non sia un vertice isolato, otterremo qualcosa che non è un grafo, perché ci saranno archi che hanno un solo estremo. Siamo allora costretti a togliere, assieme a  $v_i$ , tutti gli archi che passano per  $v_i$ . Ebbene, si conviene di indicare con la notazione  $G - v_i$  il *sottografo* ottenuto da  $G$  togliendo  $v_i$  assieme a tutti gli archi che passano per  $v_i$ . Quindi  $G - v_i$  è il più grande sottografo di  $G$  che non contiene il vertice  $v_i$ . Si veda la figura 10.22.

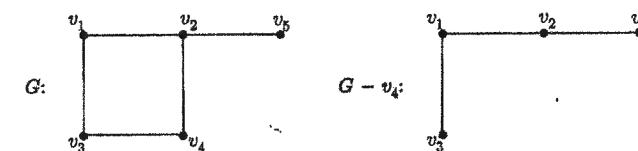


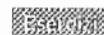
Figura 10.22.

Passiamo ora ad enunciare la congettura di Ulam.

**Congettura di Ulam**

Sia  $G$  un grafo con  $n$  vertici  $v_1, v_2, \dots, v_n$  e sia  $G'$  un grafo con  $n$  vertici  $v'_1, v'_2, \dots, v'_n$ . Se, per ogni  $i = 1, 2, \dots, n$ , i sottografi  $G_i = G - v_i$  e  $G'_i = G' - v'_i$  sono isomorfi, allora i grafi  $G$  e  $G'$  sono isomorfi anch'essi.

Su questa congettura si invita a leggere l'articolo [13].



Determinare il gruppo degli automorfismi del grafo della figura 10.23.

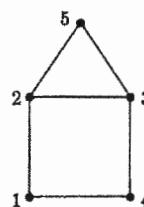


Figura 10.23.

Determinare il gruppo degli automorfismi del grafo della figura 10.24.

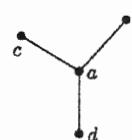


Figura 10.24.

## ■ 5 ALCUNE CLASSI DI GRAFI

In questo paragrafo illustriamo alcune importanti classi di grafi: i grafi bipartiti, gli alberi e i grafi planari.

### 5.1 Grafi bipartiti

**DEFINIZIONE 10.20** Un grafo si dice *bipartito* se l'insieme  $V$  dei suoi vertici si può scrivere come l'unione di due insiemi disgiunti  $V = V_1 \cup V_2$  in modo che ogni vertice di  $V_1$  sia unito con un lato ad ogni vertice di  $V_2$  mentre due vertici di  $V_1$  [rispettivamente  $V_2$ ] non sono collegati da un lato. ■

Se  $V_1$  è costituito da  $n$  elementi e  $V_2$  da  $m$  elementi, il grafo bipartito si indica col simbolo  $K_{n,m}$ . Nella figura 10.25 sono illustrati i grafi  $K_{2,2}$ ,  $K_{2,3}$  e  $K_{3,3}$ .

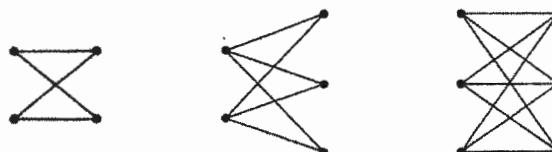


Figura 10.25.

**TEOREMA 10.3** Un grafo è bipartito se e solo se non contiene alcun ciclo dispari.

**DIMOSTRAZIONE.** La condizione è necessaria. Supponiamo il grafo  $G$  bipartito e siano  $V_1$  e  $V_2$  le due classi di vertici. Sia  $v_1v_2\dots v_n = v_1$  un ciclo in  $G$ . Possiamo supporre, senza perdita di generalità, che  $v_1$  appartenga a  $V_1$ . Allora  $v_2$  appartiene a  $V_2$ ,  $v_3 \in V_1$ , ecc. In altre parole  $v_i \in V_1$  se e solo se  $i$  è dispari. Dato che  $v_n = v_1$  sta in  $V_1$  si ha che  $n$  è dispari e quindi il ciclo  $v_1v_2\dots v_n$  è pari.

La condizione è sufficiente. Possiamo supporre, senza perdita di generalità, che il grafo sia连通的: in caso contrario si possono considerare separatamente le componenti connesse (che sono bipartite anch'esse). Sia  $v_1$  un qualunque vertice di  $G$  e sia  $V_1$  l'insieme costituito da  $v_1$  e dai vertici che hanno distanza pari da  $v_1$ . Sia  $V_2$  il complementare di  $V_1$ . Per mostrare che  $G$  è bipartito basta provare che ogni arco di  $G$  congiunge ogni vertice di  $V_1$  con un vertice di  $V_2$ : infatti, supponiamo per assurdo che esista un arco che congiunge due vertici  $x, y$  di  $V_1$ . Ma allora l'unione di tutte le geodetiche da  $v_1$  a  $x$ , di tutte le geodetiche da  $v_1$  a  $y$  e dell'arco  $xy$  contiene un ciclo dispari, il che contraddice l'ipotesi. ♦

### 5.2 Alberi e foreste

Nei capitoli precedenti abbiamo a volte utilizzato dei "diagrammi ad albero" per contare certi oggetti. Ebbene, tali strutture sono dei grafi che per l'appunto prendono il nome di *alberi* e che costituiscono una classe importante di grafi.

**DEFINIZIONE 10.21** Un albero è un grafo连通的 e privo di cicli. ■

Se si toglie la richiesta di essere连通的, un grafo privo di cicli prende il nome di *foresta*. Quindi una foresta è unione disgiunta di alberi. In altre parole ogni componenete连通的 di una foresta è un albero.

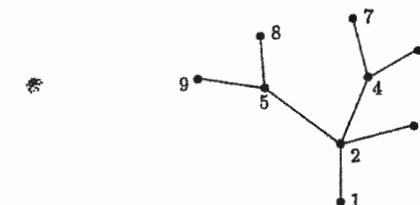


Figura 10.26. Esempio di albero.

Esistono varie caratterizzazioni di un albero.

**TEOREMA 10.4** Sia  $G$  un grafo con  $n$  vertici e  $m$  archi. Le seguenti affermazioni sono equivalenti:

1.  $G$  è un albero.
2. Due qualunque punti di  $G$  sono congiunti da un unico cammino.
3.  $G$  è连通的 e  $m = n - 1$ .
4.  $G$  è privo di cicli e  $m = n - 1$ .

Lasciamo la dimostrazione negli esercizi.



Figura 10.27. Lista degli alberi con 5 vertici.

Si noti che gli alberi sono particolari grafi bipartiti. Infatti è facile provare il seguente risultato:

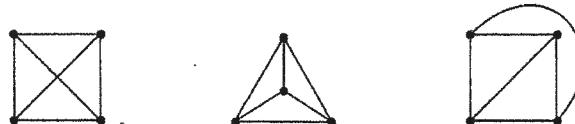
**PROPOSIZIONE 10.3** *Ogni albero è un grafo bipartito.*

**DIMOSTRAZIONE.** Dati due vertici  $v$  e  $v'$ , esiste un solo cammino che li congiunge: coloriamo allora  $v$  e  $v'$  dello stesso colore se e solo se il cammino che li congiunge ha lunghezza pari. Queste due colorazioni determinano una bipartizione dell'albero.  $\diamond$

Per provare che il grafo della figura 10.26 è bipartito, basta colorare di rosso i vertici 1, 3, 4, 5 e di nero tutti gli altri.

### 5.3 Grafi planari

Nella teoria dei grafi un arco è individuato esclusivamente dalla coppia di vertici che lo individua: non è importante la sua lunghezza, la sua forma, ecc. Per esempio le tre figure rappresentate in figura 10.28 rappresentano lo stesso grafo, il grafo completo su 4 vertici:

Figura 10.28. Diverse rappresentazioni del grafo completo  $K_4$ .

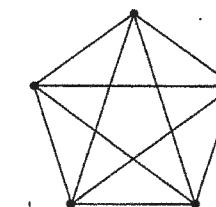
Si noti come nella prima versione ci sono due archi che si intersecano ma la loro intersezione non è un vertice: una tale situazione prende il nome di *incrocio*. Nelle altre due versioni abbiamo eliminato gli incroci.

**DEFINIZIONE 10.22** Un grafo  $G$  si dice *planare* se può essere disegnato su un piano senza incroci.  $\blacksquare$

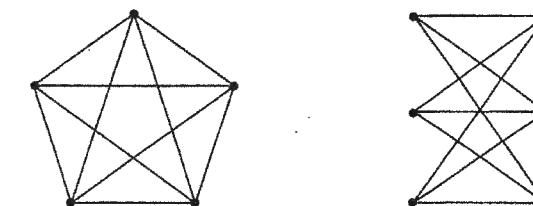
In altre parole in un grafo planare gli archi si incrociano solo nei vertici che hanno in comune. Come si è appena visto, il grafo completo  $K_4$  è planare.

Proviamo a vedere se la stessa cosa possiamo dire per  $K_5$ . Due sue rappresentazioni sono date in figura 10.29.

Possiamo variare il numero di incroci, ma non potremo mai eliminarli. Esistono vari algoritmi per decidere se un grafo è planare, oppure per capire quale è il minimo numero di incroci presenti nel grafo, ma si tratta di algoritmi complessi.

Figura 10.29. Due rappresentazioni del grafo completo  $K_5$ .

Esempi di grafi non planari sono il grafo completo su 5 vertici  $K_5$  e il grafo completo bipartito su 6 vertici  $K_{3,3}$  (cfr. figura 10.30).

Figura 10.30. Esempi di grafi non planari:  $K_5$  e  $K_{3,3}$ .

Come vedremo, questi sono i grafi che in un certo senso *generano tutti i grafi non planari*, come verrà precisato dalla seguente caratterizzazione dei grafi non planari, fornita dal matematico polacco Kuratowski.

Premettiamo una osservazione riguardo ad una operazione fondamentale sui grafi. Dato un grafo finito  $G$ , siano  $u$  e  $v$  due vertici di  $G$  collegati tra loro con un arco. Si dice che l'arco che congiunge  $u$  e  $v$  è stato *contratto* se è stato eliminato e i vertici  $u$  e  $v$  sono stati uniti (si veda figura 10.31).

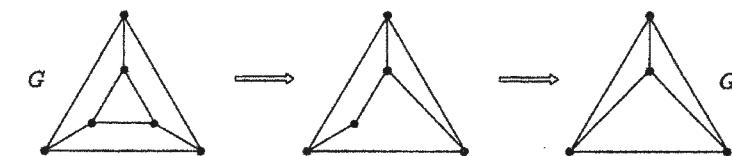


Figura 10.31. Contrazione di un grafo.

Diremo che il grafo  $G$  è *contraibile per archi* al grafo  $G'$ . Questa operazione può essere ripetuta varie volte. Ebbene, su questo tipo di operazione è basata la seguente caratterizzazione.

**TEOREMA 10.5 (TEOREMA DI KURATOWSKI)** Un grafo finito  $G$  è planare se e solo se non contiene nessun sottografo che sia contraibile per archi a  $K_5$  o a  $K_{3,3}$ .

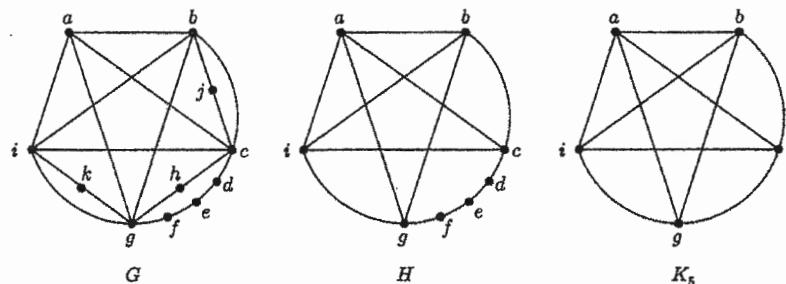


Figura 10.32. Grafo non planare.

Si veda al riguardo la figura 10.32 (da [14] pag. 506) dove si mostra che  $G$  contiene un sottografo  $H$  con traibile per archi a  $K_5$ . In pratica, il criterio di Kuratowski non è molto comodo da verificare, soprattutto se si ha fretta di decidere la planarità o non planarità di un grafo. Esistono tuttavia algoritmi efficienti in tempo  $\mathcal{O}(n)$  (cfr. par. 9 del cap. 6) (ossia lineari nel numero dei vertici) per decidere se un grafo è planare o no. Non ci soffermeremo su questi argomenti.

Vale la pena però di enunciare i seguenti risultati che costituiscono condizioni necessarie (non sufficienti!) per la planarità di un grafo. Se queste condizioni necessarie non sono verificate, possiamo concludere che il grafo *non* è planare.

**PROPOSIZIONE 10.4** *Sia  $G$  un grafo semplice, connesso e planare con  $n$  vertici e  $m$  archi. Valgono le seguenti implicazioni:*

1. *Se  $n \geq 3$  allora  $m \leq 3n - 6$ .*
2. *Se  $n > 3$  e non ci sono cicli di lunghezza 3, allora  $m \leq 2n - 4$ .*

I grafi planari hanno quindi una limitazione nel numero degli archi.

Il grafo  $K_{3,3}$  è semplice, connesso, ha  $n = 6$  vertici e  $m = 9$  archi. Ora, la prima condizione  $m \leq 3n - 6 = 18 - 6 = 12$  è soddisfatta, ma la seconda no: il grafo  $K_{3,3}$  non possiede cicli di lunghezza tre: se fosse planare dovrebbe essere  $m \leq 12 - 4 = 8$ . Quindi  $K_{3,3}$  non è planare.

Se non si possono utilizzare i due criteri della proposizione precedente esistono altri metodi. L'importante è capire che se un grafo *riconosce* i due criteri detti non possiamo concludere che è planare.

Diamo qui di seguito una applicazione sui grafi non planari.

Siano  $A$ ,  $B$  e  $C$  tre abitazioni e  $E$ ,  $F$  e  $G$  le centrali elettrica, dell'acqua e del gas (cfr. fig. 10.33).

Ci si chiede se è possibile connettere con delle tubazioni ciascuna delle tre abitazioni con ciascuna delle centrali in modo che le tubazioni non si intersechino.

Il grafo che modella questa situazione è chiaramente il grafo bipartito completo su 6 vertici  $K_{3,3}$ , che non è planare. Quindi non c'è modo di costruire tubazioni che connettano le tre abitazioni alle tre centrali senza intersecarsi.

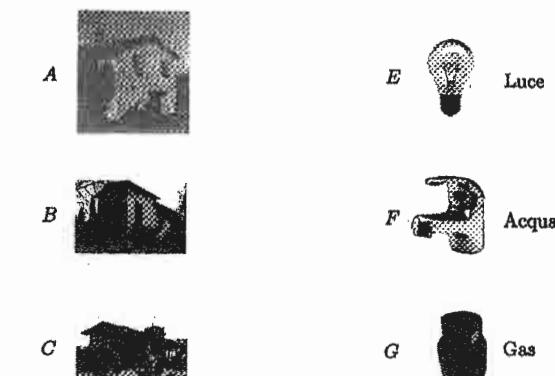


Figura 10.33. Il problema delle tre forniture.



- Decidere se il grafo della figura 10.34 è planare o no.

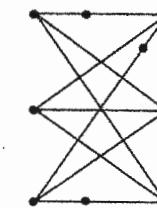


Figura 10.34.

- Decidere se il grafo della figura 10.35 è planare o no.

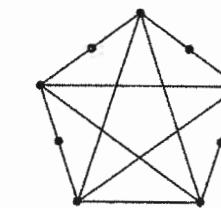


Figura 10.35.

## 6 APPLICAZIONI DEI GRAFI

In quest'ultimo paragrafo accenneremo ad alcune applicazioni della teoria dei grafi, enunciando e discutendo di alcuni problemi, della natura più svariata, che possono essere impostati, ed eventualmente risolti, usando la teoria dei grafi. Alcune applicazioni saranno semplici esercizi, altre invece sono più complesse o addirittura irrisolte. Si può fare riferimento a [4].

Provare che ad ogni riunione di sei persone ci sono tre persone che si conoscono o tre persone che non si conoscono.

La situazione si può rappresentare con un grafo  $G$  con 6 vertici rappresentanti le sei persone in questione: l'adiacenza o meno dei vertici significa che le persone si conoscono o non si conoscono. È utile a questo punto introdurre la nozione di grafo *complementare* di un grafo  $G$ : si tratta del grafo  $\bar{G}$  che ha gli stessi vertici del grafo  $G$ , e nel quale due vertici sono adiacenti (non adiacenti) in  $G$  se e solo se non sono adiacenti (adiacenti) in  $\bar{G}$ . Per esempio i due grafi con 6 vertici della figura 10.36 sono l'uno il complementare dell'altro.

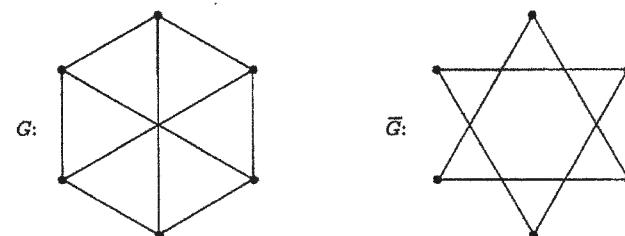


Figura 10.36. Grafi complementari.

L'esistenza di tre persone che si conoscono si traduce, nel grafo  $G$ , nella presenza di un triangolo passante per tre vertici. L'esistenza di tre persone che *non* si conoscono si traduce nell'esistenza di un triangolo che congiunge tre vertici nel grafo complementare  $\bar{G}$ . Quindi in termini di grafi il problema dato si può riformulare al modo seguente:

**PROPOSIZIONE 10.5** *Per ogni grafo  $G$  con 6 vertici,  $G$  o il suo complementare  $\bar{G}$  contiene un triangolo.*

**DIMOSTRAZIONE.** Sia  $v$  un vertice di  $G$ . Ogni vertice diverso da  $v$  o sarà collegato a  $v$  o non lo sarà, quindi  $v$  sarà adiacente o in  $G$  o in  $\bar{G}$  agli altri cinque vertici. Si può quindi supporre (fig. 10.37) senza perdita di generalità che ci siano tre vertici  $v_1, v_2$  e  $v_3$  in  $G$  adiacenti a  $v$ . Se tra questi ce ne sono due adiacenti tra loro, allora questi due sono vertici di un triangolo in  $G$  il cui terzo lato è  $v$ . Altrimenti (ossia se nessuno tra  $v_1, v_2$  e  $v_3$  è adiacente in  $G$ ), allora  $v_1, v_2$  e  $v_3$  formano un triangolo in  $\bar{G}$ .

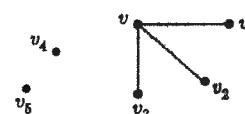


Figura 10.37.

#### La formula di Euler

Sia  $P$  un poliedro (ossia un solido limitato da poligoni). Per esempio sono poliedri i cosiddetti *solidi platonici*: il tetraedro, il cubo, l'ottaedro, il dodecaedro e l'icosaedro (fig. 10.38).

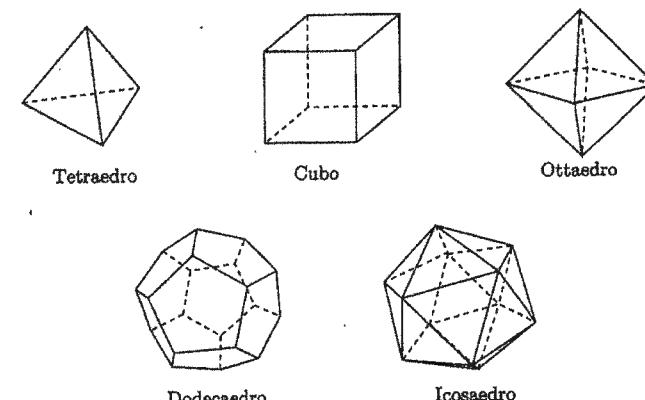


Figura 10.38. I solidi platonici.

Eulero trovò una importantissima relazione tra il numero  $F$  delle facce, dei vertici  $V$  e degli spigoli  $E$  di un qualunque poliedro semplice (ossia privo di buchi), data dalla celeberrima formula, detta per l'appunto *formula di Euler*,

$$V - E + F = 2.$$

Il numero  $V - E + F$  prende il nome di *caratteristica di Euler*: si indica generalmente con la lettera greca  $\chi$ . La formula di Euler dice quindi che la caratteristica di Euler  $\chi$  di ogni poliedro semplice è 2.

Ora questa stessa relazione sussiste tra il numero dei vertici, il numero degli archi e il numero delle facce (ossia le regioni limitate dagli archi, compresa la regione esterna infinita) di un grafo planare. Sia  $G$  un grafo finito, connesso, planare, disegnato sul piano senza incroci. Detto  $n$  il numero dei vertici,  $m$  il numero di archi e  $f$  il numero di facce si ha la relazione (detta ancora di Euler)

$$n - m + f = 2.$$

Il numero  $n - m + f$  è ancora la caratteristica di Euler. Il risultato precedente dice quindi che la caratteristica di Euler di un grafo finito connesso planare è 2. Consideriamo per esempio il grafo della figura 10.39:

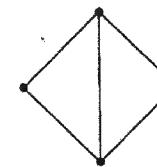


Figura 10.39.

Risulta  $n = 4, m = 5, f = 3$ , e  $n - m + f = 4 - 5 + 3 = 2$ .

Il motivo per cui la stessa formula vale per poliedri e grafi semplici planari è che ogni poliedro semplice si può trasformare in un grafo semplice, connesso planare

prendendo i vertici del poliedro come vertici del grafo, i lati del poliedro come archi del grafo: le facce del poliedro corrisponderanno in questo modo alle facce del grafo. Si veda la figura 10.40.

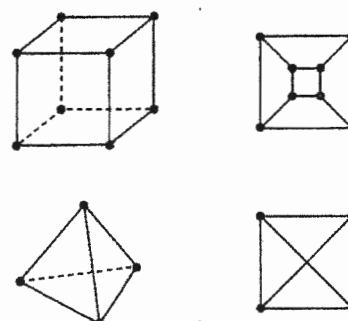


Figura 10.40.

**OSSERVAZIONE** Non ogni grafo semplice connesso e planare tuttavia è ottenibile da un poliedro in questo modo.

#### Il problema dei quattro colori

Una delle congetture più famose in matematica era la seguente:

Una qualunque carta geografica su una superficie piana (o su di una sfera) si può colorare con al più quattro colori, in modo che regioni adiacenti abbiano colori diversi.

Nel 1977 tale congettura è stata provata da K. Appel e W. Haken. Essi hanno dimostrato con l'aiuto del calcolatore che quattro colori sono sufficienti. Proprio per questo (che la dimostrazione è stata fatta con l'aiuto del calcolatore) alcuni matematici non la accettano: nonostante l'accusa di scarsa eleganza, non sono stati trovati errori. Alcuni perfezionamenti del teorema sono stati fatti successivamente.

Il problema dei quattro colori può essere espresso nel linguaggio della teoria dei grafi al modo seguente: si associa ad ogni regione della mappa un vertice di un grafo e si connettono due vertici se e solo se le due regioni corrispondenti hanno un confine in comune.

In questa formulazione il problema diventa: dato un grafo planare, i suoi vertici possono essere colorati con al massimo quattro colori in modo tale che due vertici adiacenti non abbiano mai lo stesso colore. Si usa dire che *ogni grafo planare è 4-colorabile*.

#### Il problema del commesso viaggiatore

Un commesso viaggiatore vuole visitare diverse città e rientrare al punto di partenza, in modo da minimizzare la distanza totale da percorrere. Il problema si traduce in un problema di teoria dei grafi rappresentando la rete di città come un grafo in cui le città

sono i nodi, le strade gli archi e le distanze i pesi sugli archi. È ovvia l'importanza di questo tipo di problemi nella teoria dei trasporti, nei circuiti elettrici, ecc.

Per la risoluzione di questo problema non esistono algoritmi efficienti: l'unico metodo è rappresentato dall'elencare tutti i possibili cammini sul grafo e successivamente scegliere quello migliore. La complessità di questa operazione è enorme: in un grafo con  $n$  vertici, nel caso peggiore (ossia nel caso in cui ogni vertice del grafo è collegato con tutti gli altri) i cammini sono  $n!$ , il che comporta che la complessità è esponenziale (tramite l'approssimazione di Stirling, cfr. Osservazione del par. 7 del cap. 6).

#### Il problema cinese del portalettere

Questo problema si chiama così perché è stato discusso dal matematico cinese Mei-Ko Kwan nel 1962. Un portalettere vuole consegnare tutte le lettere in modo da ridurre al minimo il percorso e poi ritornare al punto di partenza. Deve ovviamente percorrere *tutte le strade* del percorso che gli è stato affidato almeno una volta, ma desidererebbe evitare di percorrere troppe strade più di una volta.

Osserviamo che il problema cinese del portalettere differisce dal problema del commesso viaggiatore, dato che quest'ultimo deve solo visitare un certo numero di città e può scegliere le strade più convenienti per raggiungerle.

Ora, se si rappresenta la mappa della città dove il portalettere deve far le consegne con un grafo, il problema equivale alla determinazione di un ciclo di *lunghezza minima* che attraversa ogni arco *almeno* una volta. È chiaro che, se il grafo è euleriano, allora una soluzione al problema è data da un ciclo euleriano (che attraversa ogni arco esattamente una volta). Tuttavia è ben difficile che la rete stradale del portalettere soddisfi le condizioni richieste dal teorema di Eulero per possedere un ciclo euleriano. Si può dimostrare che questo ciclo di lunghezza minima che il portalettere cerca non passa mai per nessun arco per *più di due volte*. Quindi per ogni rete stradale esistono percorsi *ottimali* per il portalettere: si possono costruire aggiungendo al grafo della rete stradale opportuni archi in modo da farlo diventare euleriano.

#### Applicazioni alla sociologia o alla diffusione delle epidemie

Supponiamo che da certi studi di natura psicologica si riesca a capire quando una persona di un gruppo può influenzare il modo di pensare di altri membri del gruppo. Si può allora costruire un grafo con un vertice  $v_i$  per ogni persona del gruppo e un arco orientato  $(v_i, v_j)$  ogni volta che la persona  $v_i$  influenza la persona  $v_j$ . Ci si può chiedere quale sia il *minimo numero di persone* che possono diffondere un'idea all'intero gruppo o direttamente, oppure influenzando qualcuno che a sua volta può influenzare qualcun altro, e così via.

Uno stesso tipo di discorso si può fare con le epidemie: qual è il minimo numero di malati che possono creare un'epidemia in una popolazione.

#### Circuiti elettrici

Una ovvia applicazione si ha nei circuiti elettrici (si pensi alle leggi di Kirchoff).

#### Chimica

Ogni atomo di una struttura chimica si può rappresentare con un punto e legami atomici vengono rappresentati da archi.

# 11 Approfondimenti

*Or dissodo un terreno secco e duro.  
La vanga  
urta in pietre, in sterpaglia. Scavar devo  
profondo, come chi cerca un tesoro.*  
Umberto Saba, da LAVORO

Nel corso dei capitoli precedenti abbiamo introdotto alcuni concetti in modo informale, per non appesantire il discorso. Molti studenti potrebbero non essere soddisfatti di questo approccio: vorrebbero delle definizioni e risultati più formali e precisi. È quanto ci accingiamo a fare in questo capitolo, nel corso del quale verranno approfonditi, per il lettore interessato, alcuni argomenti. Più precisamente daremo la definizione formale dell'insieme  $\mathbb{Z}$  degli interi e dell'insieme  $\mathbb{Q}$  dei numeri razionali. Daremo alcune proprietà più generali relative agli anelli, parleremo di funzioni generatrici e termineremo con alcuni approfondimenti sui numeri primi.

## 1 LE OPERAZIONI IN $\mathbb{N}$

Come abbiamo visto, un'operazione binaria in un insieme  $S$  è un'applicazione da  $S \times S$  in  $S$ , ossia una legge che associa ad ogni coppia di elementi di  $S$  un ben determinato elemento di  $S$ .

Ebbene, gli assiomi di Peano (cfr. par. 3 del cap. 2) permettono di definire in  $\mathbb{N}$  due operazioni, di addizione e moltiplicazione, al modo seguente.

**DEFINIZIONE 11.1** Si definisce *somma* di due numeri naturali  $n$  ed  $m$  il numero naturale  $n + m$  dove

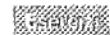
$$n + m \stackrel{\text{def}}{=} \begin{cases} \underbrace{\sigma(\sigma(\dots\sigma(n)))}_{m \text{ volte}} & \text{se } m > 0 \\ n & \text{se } m = 0. \end{cases}$$

Da questa definizione risulta ovviamente  $\sigma(n) = n + 1$ , dove  $1 = \sigma(0)$ .

**DEFINIZIONE 11.2** Si definisce *prodotto* di due numeri naturali  $n$  e  $m$  il numero naturale  $n \cdot m$  dove

$$n \cdot m \stackrel{\text{def}}{=} \begin{cases} \underbrace{n + n + \dots + n}_{m \text{ volte}} & \text{se } m > 0 \\ 0 & \text{se } m = 0. \end{cases}$$

Tali operazioni verificano tutte le ordinarie proprietà dell'aritmetica ordinaria (commutatività, associatività di addizione e moltiplicazione, proprietà distributive, esistenza di un elemento neutro rispetto all'addizione e uno neutro rispetto alla moltiplicazione, come indicato negli esercizi).



Si provi che l'addizione definita in  $\mathbb{N}$  (cfr. Definizione 11.1) è commutativa, associativa e che esiste un elemento neutro.

Si provi che la moltiplicazione definita in  $\mathbb{N}$  (cfr. Definizione 11.2) è commutativa e associativa, e che esiste un elemento neutro rispetto ad essa.

Si provi la validità della seguente legge distributiva:

$$a(b + c) = ab + ac.$$

## 2 I NUMERI INTERI COME CLASSI DI EQUIVALENZA

Sappiamo fin dai primi anni di scuola che l'insieme  $\mathbb{Z}$  dei numeri interi è costituito dai numeri  $0, \pm 1, \pm 2, \dots$ . Questa introduzione non è però soddisfacente: cosa è il simbolo — che interviene nella scrittura di un numero intero? Vorremmo poter definire gli interi sulla base di sole nozioni note. In ogni definizione devono apparire solamente concetti già definiti precedentemente e quindi noti. Per i numeri interi le nozioni *note* sulle quali baseremo la definizione sono i *numeri naturali*, il *prodotto cartesiano* di insiemi e la nozione di *relazione di equivalenza*.

Nel prodotto cartesiano  $\mathbb{N} \times \mathbb{N} = \{(a, b) | a, b \in \mathbb{N}\}$  si introduca la seguente relazione:

$$(2.1) \quad (a, b) \rho (a', b') \iff a + b' = b + a'.$$

Si invita lo studente a svolgere i seguenti passi, con l'aiuto della figura 11.1.

- Verificare che la relazione (2.1) è una relazione di equivalenza.
- Nell'insieme  $\mathbb{N} \times \mathbb{N}$  individuare le classi  $\overline{(a, b)}$  della partizione e darne un'interpretazione geometrica (cfr. fig. 11.1).
- Se come rappresentanti di ogni classe si scelgono coppie in cui almeno uno degli elementi è zero, provare che due coppie in cui il primo (o il secondo) elemento è zero sono equivalenti se e solo se sono uguali.

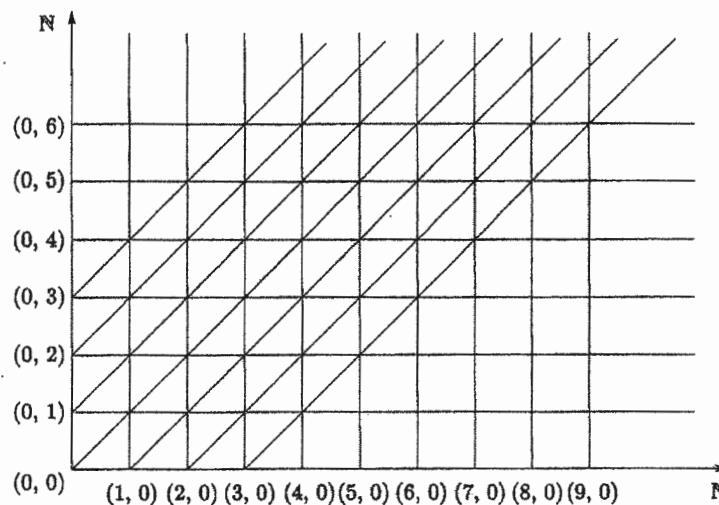


Figura 11.1.

- d) Provare che *ogni* classe è rappresentabile con uno dei seguenti rappresentanti privilegiati distinti:

$$\begin{aligned} & (0, 0) \\ & (1, 0), (2, 0), (3, 0), \dots, (n, 0), \dots \\ & (0, 1), (0, 2), (0, 3), \dots, (0, n), \dots \end{aligned}$$

Una volta che si sia provato che si tratta di una relazione di equivalenza, si può *passare al quoziente*. Ebbene, l'insieme  $\mathbb{Z}$  degli interi viene definito come

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/\rho.$$

Non è difficile controllare che  $\mathbb{Z}$  risulta decomposto nei seguenti sottoinsiemi:

$$\mathbb{Z} = \mathbb{Z}^+ \cup \{0\} \cup \mathbb{Z}^-$$

dove

$$\begin{aligned} \mathbb{Z}^+ &\stackrel{\text{def}}{=} \{(\overline{n}, 0) \mid n \in \mathbb{N}, n \neq 0\}, \\ 0 &\stackrel{\text{def}}{=} (\overline{0}, 0), \\ \mathbb{Z}^- &\stackrel{\text{def}}{=} \{(\overline{0}, n) \mid n \in \mathbb{N}, n \neq 0\}. \end{aligned}$$

Gli elementi di  $\mathbb{Z}^+$  prendono il nome di *interi positivi*, quelli di  $\mathbb{Z}^-$  di *interi negativi*;

Si noti che l'insieme  $\mathbb{Z}$  è un'estensione di  $\mathbb{N}$  nel senso che contiene al suo interno un sottoinsieme  $\mathbb{Z}^+ \cup \{0\}$  identificabile con  $\mathbb{N}$  mediante l'applicazione iniettiva da  $\mathbb{N}$  in  $\mathbb{Z}$  che associa ad ogni naturale  $n$  la classe  $(\overline{n}, 0)$ .

Il legame tra questa nuova definizione (nella quale ogni intero viene visto come una classe di equivalenza rispetto alla relazione di equivalenza (2.1)) e l'ordinaria scrittura dei numeri interi come  $0, \pm 1, \pm 2$ , ecc. è dato dalla seguente posizione, per ogni  $n \in \mathbb{N}$ :

$$\overline{(n, 0)} \stackrel{\text{def}}{=} n, \quad \overline{(0, 0)} \stackrel{\text{def}}{=} 0, \quad \overline{(0, n)} \stackrel{\text{def}}{=} -n.$$

Per maggiore chiarezza, possiamo scrivere la seguente tabella:

$(\mathbb{N} \times \mathbb{N})/\rho$	$\mathbb{Z}$
...	...
$(\overline{0}, 4)$	-4
$(\overline{0}, 3)$	-3
$(\overline{0}, 2)$	-2
$(\overline{0}, 1)$	-1
$(\overline{0}, 0)$	0
$(\overline{1}, 0)$	1
$(\overline{2}, 0)$	2
$(\overline{3}, 0)$	3
$(\overline{4}, 0)$	4
$(\overline{5}, 0)$	5
...	...

Una volta definito l'insieme  $\mathbb{Z}$  dei numeri interi come quoziente, occorre dargli una struttura algebrica, ossia introdurre due operazioni che permettano di fare di conto, come facciamo normalmente tra interi. Ebbene, definiamo le seguenti operazioni, di addizione e moltiplicazione rispettivamente:

$$(2.2) \quad \overline{(a, b)} + \overline{(c, d)} \stackrel{\text{def}}{=} \overline{(a+c, b+d)}$$

$$(2.3) \quad \overline{(a, b)} \cdot \overline{(c, d)} \stackrel{\text{def}}{=} \overline{(ac+bd, cd+ad)}.$$

C'è un problema. Chi ci assicura che queste operazioni siano *ben poste*? Cosa significa *essere ben poste*? Il problema è il seguente: abbiamo definito (cfr.(2.2) e (2.3))

$$\overline{(4, 7)} + \overline{(9, 3)} \stackrel{\text{def}}{=} \overline{(13, 10)}.$$

Cosa succede se nella classe  $\overline{(4, 7)}$  e nella classe  $\overline{(9, 3)}$  cambiamo rappresentante, ossia scegliamo un'altra coppia della classe, per esempio la coppia  $(1, 4)$  in  $\overline{(4, 7)}$  e la coppia  $(6, 0)$  in  $\overline{(9, 3)}$ ? Proviamo a fare

$$\overline{(1, 4)} + \overline{(6, 0)}.$$

Seguendo la (2.2) otteniamo la classe  $\overline{(7, 4)}$ : cosa dobbiamo pretendere? Che il risultato sia la stessa classe (attenzione, *classe*, non *coppia*) della classe  $\overline{(13, 10)}$ . E questo è effettivamente vero, perché  $(13, 10)$  è in relazione a  $(7, 4)$  essendo  $13+4=10+7$  e quindi  $\overline{(7, 4)} = \overline{(13, 10)}$  che è quanto chiedevamo. Analogamente per il prodotto:

$$\overline{(4, 7)} \cdot \overline{(9, 3)} = \overline{(57, 75)}, \quad \overline{(1, 4)} \cdot \overline{(6, 0)} = \overline{(6, 24)};$$

e  $\overline{(57, 75)} = \overline{(6, 24)}$  perché  $57+24=75+6=81$ .

L'avere controllato che le cose funzionano in questo caso non prova ovviamente che il teorema vale in generale: dobbiamo provarlo in generale, ossia che le definizioni date di addizione e moltiplicazione sono *ben poste*, nel senso che pur essendo definite attraverso i rappresentanti, sono indipendenti dai rappresentanti: in altri termini,

$$\begin{cases} \overline{(a,b)} = \overline{(a',b')} \\ \overline{(c,d)} = \overline{(c',d')} \end{cases} \implies \overline{(a+c, b+d)} = \overline{(a'+c', b'+d')}$$

e

$$\begin{cases} \overline{(a,b)} = \overline{(a',b')} \\ \overline{(c,d)} = \overline{(c',d')} \end{cases} \implies \overline{(ac+bd, cb+ad)} = \overline{(a'c'+b'd', c'b'+a'd')}.$$

Rimandiamo agli esercizi la dimostrazione che in generale addizione e moltiplicazione definite sono ben poste.

### Esercizi

- 1 Si provi che le operazioni di addizione e moltiplicazione definite in  $\mathbb{Z}$  sono *ben poste*.
- 2 Quale numero intero rappresenta la classe  $\overline{(4,5)}$ ? E la classe  $\overline{(11,8)}$ ?
- 3 Quale classe è  $\overline{(4,5)} + \overline{(11,8)}$ ? Verificarlo con la ordinaria simbologia.
- 4 Provare che l'opposto della classe  $\overline{(a,b)}$  è la classe  $\overline{(b,a)}$ .
- 5 Provare che  $\mathbb{Z}$  con le operazioni definite è un anello commutativo con unità.
- 6 Si provi che in  $\mathbb{Z}$  valgono le seguenti leggi di cancellazione:

$$\begin{aligned} ac = bc, \quad c \neq 0 &\implies a = b \\ ca = cb, \quad c \neq 0 &\implies a = b. \end{aligned}$$

### 3 I NUMERI RAZIONALI

Finora abbiamo parlato informalmente dei numeri razionali: tutti d'altra parte li conoscono, come quei numeri che sono rapporto di interi: per esempio

$$\frac{3}{5}, \quad \frac{30}{7}, \quad -\frac{4}{5}, \quad 9, \quad \frac{1}{12}, \quad \text{ecc.}$$

È arrivato però il momento, come abbiamo fatto per gli interi, di darne una definizione più formale.

Sappiamo che l'esigenza di introdurre nuovi numeri, da "aggiungere" agli interi, sorge quando si voglia risolvere un'equazione del tipo

$$5x = 12$$

che chiaramente non ha soluzione in  $\mathbb{Z}$ . I numeri razionali sono esattamente le soluzioni di un'equazione del tipo

$$ax = b, \quad a, b \in \mathbb{Z}, \quad a \neq 0.$$

Nel dare la definizione formale dei numeri razionali ci dovremo servire delle sole nozioni già acquisite, e quindi delle nozioni di numeri interi, con le loro operazioni e della nozione di relazione di equivalenza.

Si consideri il prodotto cartesiano  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ , ossia l'insieme delle coppie ordinate di interi, in cui il secondo elemento della coppia è diverso da zero. Si introduca in tale insieme la seguente relazione:

$$(3.1) \quad (a,b) \rho (c,d) \iff ad = bc.$$

Si tratta di una relazione di equivalenza (cfr. eserc. 10).

Ebbene, poniamo

$$\mathbb{Q} \stackrel{\text{def}}{=} (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})/\rho$$

Gli elementi di  $\mathbb{Q}$  sono quindi le classi di equivalenza, che indicheremo con

$$\overline{(a,b)}.$$

La figura 11.2 mostra alcuni elementi di  $\mathbb{Q}$ , ossia alcune classi di equivalenza in  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ .

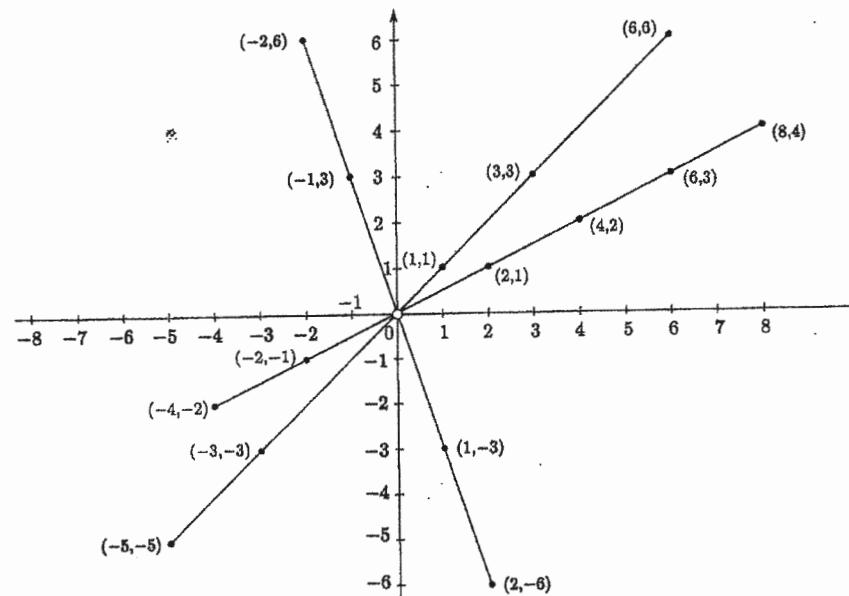


Figura 11.2.

Introduciamo in  $\mathbb{Q}$  le seguenti operazioni:

$$\overline{(a,b)} + \overline{(c,d)} \stackrel{\text{def}}{=} \overline{(ad+bc, bd)}$$

$$\overline{(a,b)} \cdot \overline{(c,d)} \stackrel{\text{def}}{=} \overline{(ac, bd)}$$

Osserviamo innanzitutto che le coppie  $(ad+bc, bd)$  e  $(ac, bd)$  stanno entrambe in  $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ , dato che in  $\mathbb{Z}$  non ci sono divisori dello zero e quindi  $bd \neq 0$ . Resta da provare che tali definizioni sono *ben poste*, ossia che, pur essendo definite attraverso dei rappresentanti delle classi, non dipendono da questi. Si veda l'esercizio 11.

Le classi

$$0 \stackrel{\text{def}}{=} \overline{(0,1)} = \overline{(0,b)}$$

$$1 \stackrel{\text{def}}{=} \overline{(1,1)} = \overline{(a,a)}$$

sono *elementi neutri rispettivamente per l'addizione e per la moltiplicazione*. Rispetto a queste operazioni,  $\mathbb{Q}$  è un anello commutativo con unità. Vale una proprietà ulteriore. Risulta

$$\overline{(a,b)} \cdot \overline{(b,a)} = \overline{(ab, ba)} = \overline{(1,1)}, \quad \forall \overline{(a,b)}, \text{ tale che } a \neq 0, b \neq 0.$$

Si noti che  $(b,a)$  sta in  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  perché si è supposto  $a \neq 0$ . L'elemento  $\overline{(b,a)}$  prende il nome di *inverso* dell'elemento  $\overline{(a,b)}$ . Sappiamo che un anello commutativo con unità in cui ogni elemento non nullo ammette inverso moltiplicativo prende il nome di *campo* (cfr. definizione 5.4). Abbiamo così provato il seguente risultato.

**PROPOSIZIONE 11.1** *L'insieme  $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})/\varrho$  con le operazioni definite sopra è un campo.*

Vogliamo ora mostrare il seguente ulteriore risultato.

**PROPOSIZIONE 11.2** *Il campo  $\mathbb{Q}$  è un'estensione di  $\mathbb{Z}$ . Inoltre ogni elemento di  $\mathbb{Q}$  è della forma  $uv^{-1}$ , con  $u, v \in \mathbb{Z}$ ,  $v \neq 0$ .*

**DIMOSTRAZIONE.** Dobbiamo trovare dentro  $\mathbb{Q}$  una *copia* di  $\mathbb{Z}$ . Basta a tal fine notare che l'applicazione  $\varphi : \mathbb{Z} \rightarrow \mathbb{Q}$

$$a \mapsto \overline{(a,1)}$$

è iniettiva (si provi). Inoltre il trasformato mediante  $\varphi$  della somma di due elementi di  $\mathbb{Z}$  è la somma (in  $\mathbb{Q}$ ) dei trasformati, e così per il prodotto. Questo ci garantisce che l'immagine di  $\mathbb{Z}$  in  $\mathbb{Q}$  è la *copia* di  $\mathbb{Z}$  che cercavamo dentro  $\mathbb{Q}$ .

Infine, ogni elemento  $\overline{(a,b)} \in \mathbb{Q}$ , si può scrivere nella forma

$$\overline{(a,b)} = \overline{(a,1)} \cdot \overline{(1,b)},$$

dove  $\overline{(a,1)}$  e  $\overline{(1,b)}$  sono identificabili mediante la  $\varphi$  a elementi di  $\mathbb{Z}$  e quindi  $\overline{(1,b)}$  è l'inverso di un elemento di  $\mathbb{Z}$ . Ogni elemento di  $\mathbb{Q}$  è quindi della forma  $uv^{-1}$ ,  $u, v \in \mathbb{Z}$ ,  $v \neq 0$ .  $\diamond$

Dato che ogni elemento di  $\mathbb{Q}$  si può scrivere nella forma  $uv^{-1}$ ,  $u, v \in \mathbb{Z}$ ,  $v \neq 0$ , si dice che  $\mathbb{Q}$  è *campo dei quozienti* di  $\mathbb{Z}$ .

Siamo così arrivati alla ordinaria rappresentazione dei numeri razionali come quozienti di interi, mediante l'identificazione della classe  $\overline{(a,b)}$  con il numero  $\frac{a}{b}$ .



Provare che la relazione (3.1) definita su  $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$  è una relazione di equivalenza.

Siano  $(a,b)\varrho(a',b')$  e  $(c,d)\varrho(c',d')$ . Provare che  $(ad+bc, bd)\varrho(a'd'+b'c', b'd')$ , ossia  $(ad+bc)b'd' = bd(a'd'+b'c')$ .

#### ■ 4 GENERALITÀ SUGLI ANELLI E ALCUNE CLASSI DI ANELLI

Abbiamo visto che in  $\mathbb{Z}$  le nozioni di elemento irriducibile e di elemento primo coincidono e che vale il Teorema Fondamentale dell'Aritmetica, che dice che ogni numero intero non nullo e non invertibile si scrive in modo unico come prodotto di irriducibili (o numeri primi).

Possiamo generalizzare questo teorema a una vasta classe di anelli.

**DEFINIZIONE 11.3** Un *dominio a fattorizzazione unica* è un dominio di integrità  $R$  in cui ogni elemento non nullo e non invertibile si può scrivere come prodotto di elementi irriducibili di  $R$  e questa fattorizzazione è unica nel senso che se  $a = p_1 \cdot p_2 \cdots p_n$  e  $a = q_1 \cdot q_2 \cdots q_m$ ,  $p_i, q_j$  irriducibili, allora  $m = n$  ed esiste una corrispondenza biunivoca  $\varphi : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, m\}$  tale che per ogni  $i = 1, 2, \dots, n$   $p_i$  è associato a  $q_{\varphi(i)}$ . ■

#### Esempi di domini a fattorizzazione unica

1. L'anello  $(\mathbb{Z}, +, \cdot)$ .
2. L'anello degli interi di Gauss, ossia il sottoanello di  $\mathbb{C}$   $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$  rispetto alle ordinarie operazioni dei complessi.
3. Ogni campo. Infatti ogni elemento non nullo di un campo è invertibile, quindi non ci sono elementi irriducibili.
4. Se  $R$  è un dominio a fattorizzazione unica, allora anche l'anello  $R[x]$  dei polinomi a coefficienti in  $R$  è a fattorizzazione unica. Quindi  $\mathbb{Z}[x]$  è a fattorizzazione unica,  $K[x_1, x_2, \dots, x_n]$  ( $K$  campo) è a fattorizzazione unica.

**OSSERVAZIONE** Si può dimostrare che nei domini a fattorizzazione unica le nozioni di irriducibile e di primo coincidono. Quindi ogni anello in cui esistono irriducibili che non sono primi non è a fattorizzazione unica. Di tali anelli siamo già venuti a conoscenza (cfr. es. 8.12). Li riprendiamo nell'esempio che segue.

#### Esempi di anelli che non sono a fattorizzazione unica

Sia  $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ . Si tratta di un sottoinsieme del campo dei numeri complessi: rispetto alle stesse operazioni del campo complesso, cioè

$$(a + b\sqrt{-5}) + (c + d\sqrt{-5}) = a + c + (b + d)\sqrt{-5} \in R$$

e

$$(a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) = ac - 5bd + (ad + bc)\sqrt{-5} \in R$$

$\mathbb{Z}[\sqrt{-5}]$  è chiuso e non è difficile verificare che si tratta di un dominio di integrità.  $\mathbb{Z}[\sqrt{-5}]$  non è a fattorizzazione unica, perché

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

sono due fattorizzazioni diverse in irriducibili. Infatti, valgono le seguenti osservazioni.

- Nessuno dei fattori è invertibile. Infatti gli elementi  $a + b\sqrt{-5}$  invertibili hanno norma uguale ad 1, cioè  $N(a + b\sqrt{-5}) = a^2 + 5b^2 = 1$ . Ora, nessuno di quei fattori può avere norma 1.
- Ciascuno dei fattori è irriducibile. Supponiamo  $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ . Passando alle norme, si ha  $4 = (a^2 + 5b^2)(c^2 + 5d^2)$ : questa è una relazione in  $\mathbb{N}$  dove vale il Teorema di Fattorizzazione Unica, quindi non potendo nessuno dei due fattori essere 1, dovrebbero essere uguali a 2, ma questo è assurdo.
- Il numero 2 non è associato né a  $1 + \sqrt{-5}$  né a  $1 - \sqrt{-5}$ , e così 3 non è associato né a  $1 + \sqrt{-5}$  né a  $1 - \sqrt{-5}$ . Quindi le due fattorizzazioni sono effettivamente diverse.
- Il numero 2 non è primo: infatti 2 divide il prodotto  $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ , ma non divide nessuno dei due fattori. Questo prova l'esistenza in  $\mathbb{Z}[\sqrt{-5}]$  di elementi irriducibili non primi.

**OSSERVAZIONE** In generale, sia  $t \in \mathbb{Z}$  un intero dispari  $\leq -3$ . Allora  $\mathbb{Z}[\sqrt{t}]$  non è un dominio a fattorizzazione unica. Infatti dalla  $(1 + \sqrt{t})(1 - \sqrt{t}) = 1 - t$  e dal fatto che  $1 - t$  è un intero pari  $\geq 4$ , passando alle norme, si vede che 2 è irriducibile, ma non è primo, perché divide il prodotto  $(1 + \sqrt{t})(1 - \sqrt{t})$  ma non divide né  $1 + \sqrt{t}$  né  $1 - \sqrt{t}$ . Quindi  $1 - t$  ammetterà due fattorizzazioni diverse in irriducibili.

## 5 FUNZIONI GENERATRICI

Sia data una successione  $\{a_n\}_{n \in \mathbb{N}}$ . Per studiarla è conveniente pensare i termini della successione come i coefficienti della seguente somma infinita in termini di un parametro  $x$

$$f(x) = a_0 + a_1x + a_2x^2 + \dots = \sum_{k=0}^{\infty} a_k x^k.$$

Tale somma prende il nome di serie di potenze nella variabile  $x$ .

Una serie così definita a partire da una successione  $\{a_n\}_{n \in \mathbb{N}}$  prende il nome di funzione generatrice della successione. Il vantaggio di interpretare una successione come funzione generatrice è che in questo modo raccogliamo in un unico oggetto (la funzione generatrice) gli infiniti termini della successione.

Un'osservazione semplice ma importante è la seguente proprietà di traslazione: se  $f(x) = a_0 + a_1x + a_2x^2 + \dots = \sum_{k=0}^{\infty} a_k x^k$  è la funzione generatrice della successione  $\{a_n\}_{n \in \mathbb{N}}$ , allora  $x^n f(x)$  è la funzione generatrice della successione  $\underbrace{0, 0, \dots, 0}_n, a_0, a_1, a_2, \dots$  Basta infatti osservare che

$$x^n \sum_{k=0}^{\infty} a_k x^k = \sum_{k=n}^{\infty} a_{k-n} x^k.$$

Data una serie di potenze, non è detto che essa converga, ossia che sia esprimibile come una espressione che non faccia intervenire il simbolo di sommatoria infinita. In certi casi questo succede.

### Esempio 11.1

Se  $\{a_n\}$  è la successione costante 1, 1, 1, ..., la sua funzione generatrice è

$$f(x) = \sum_{k=0}^{\infty} x^k = 1 + x + x^2 + x^3 + \dots$$

e questa serie formale *uguaglia* la funzione  $\frac{1}{1-x}$ . Infatti, per l'osservazione appena fatta,  $xf(x)$  è funzione generatrice della successione 0, 1, 1, 1, ..., per cui

$$xf(x) = \sum_{k=1}^{\infty} x^k = x + x^2 + x^3 + \dots$$

da cui  $f(x) - xf(x) = 1$  e quindi  $(1-x)f(x) = 1$  per cui

$$f(x) = \frac{1}{1-x} = 1 + x + x^2 + \dots$$

### Esempio 11.2

Partiamo dalla successione di Fibonacci che, come si è visto, è definita ricorsivamente al modo seguente:

$$a_0 = 0, \quad a_1 = 1, \quad a_n = a_{n-1} + a_{n-2}.$$

Vogliamo determinare la sua funzione generatrice  $f(x) = \sum_{n=0}^{\infty} a_n x^n$ . Dalle condizioni iniziali  $a_0 = 0, a_1 = 1$  e dalla relazione ricorsiva si ha

$$\begin{aligned} f(x) &= 0 + x + \sum_{n \geq 2} a_n x^n = x + \sum_{n \geq 2} (a_{n-1} + a_{n-2}) x^n = \\ &= x + \sum_{n \geq 2} a_{n-1} x^n + \sum_{n \geq 2} a_{n-2} x^n = x + x \sum_{n \geq 2} a_{n-1} x^{n-1} + x^2 \sum_{n \geq 2} a_{n-2} x^{n-2} = \\ &= x + x(f(x) - a_0) + x^2 f(x) = x + xf(x) + x^2 f(x) \end{aligned}$$

da cui

$$f(x) = \frac{x}{1 - x - x^2}.$$

L'avere espresso  $f(x)$  in forma chiusa ci permetterà di determinare una formula chiusa per la successione di Fibonacci, ottenendo così un metodo alternativo a quello del polinomio caratteristico che abbiamo visto a suo tempo (cfr. (4.10) del cap. 2).

Come si fa? Vogliamo trovare una formula chiusa per l' $n$ -esimo numero di Fibonacci  $a_n$  a partire dall'espressione  $\frac{x}{1 - x - x^2}$  della funzione generatrice.

Ci serviranno alcuni risultati. Come abbiamo visto, se  $f(x) = \sum_{n=0}^{\infty} x^n$ , si ha

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

da cui si deriva facilmente che

$$(5.1) \quad \sum_{n=0}^{\infty} ab^n x^n = \frac{a}{1-bx}.$$

Partiamo dalla

$$f(x) = \frac{x}{1-x-x^2}.$$

Le radici dell'equazione  $x^2 + x - 1 = 0$  sono gli opposti di  $\Phi$  (numero aureo) e di  $\widehat{\Phi}$ . Quindi

$$f(x) = \frac{x}{1-x-x^2} = \frac{-x}{(x+\Phi)(x+\widehat{\Phi})} = \frac{x}{(1-\widehat{\Phi}x)(1-\Phi x)}$$

Cerchiamo ora di scrivere questa frazione come somma di due frazioni con denominatore rispettivamente  $1-\Phi x$  e  $1-\widehat{\Phi}x$ , ossia

$$f(x) = \frac{x}{(1-\widehat{\Phi}x)(1-\Phi x)} = \frac{a}{1-\Phi x} + \frac{b}{1-\widehat{\Phi}x}.$$

Dalla  $a(1-\widehat{\Phi}x) + b(1-\Phi x) = x$  si ottiene

$$(a\widehat{\Phi} + b\Phi - 1)x + a + b = 0$$

ossia il polinomio di primo grado in  $x$ ,  $(a\widehat{\Phi} + b\Phi - 1)x + a + b$  deve essere il polinomio nullo, cioè il polinomio che ha tutti i coefficienti uguali a zero. Basta allora risolvere il seguente sistema lineare in  $a$  e  $b$ :

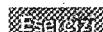
$$\begin{cases} a + b = 0 \\ a\widehat{\Phi} + b\Phi - 1 = 0 \end{cases}$$

È facile vedere che il sistema ammette la soluzione  $a = -\frac{1}{\sqrt{5}} = -b$ , da cui in base alla (5.1)

$$f(x) = \frac{1}{\sqrt{5}} \sum_{k=0}^{\infty} (\Phi^k - \widehat{\Phi}^k) x^k$$

e siamo così arrivati alla ben nota formula chiusa per il  $k$ -esimo numero di Fibonacci  $a_k$ :

$$a_k = \frac{1}{\sqrt{5}} \left[ \left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k \right]$$



11 Sia  $n$  un intero positivo. Si consideri la sequenza  $a_k = \binom{n}{k}$ ,  $k = 0, \dots, n$ . Determinare la funzione generatrice della  $a_0, a_1, a_2, \dots, a_n$ .

## 6 APPROFONDIMENTI SUI NUMERI PRIMI

Partiamo dalla seguente funzione di una variabile reale  $s$ , definita da Eulero nel 1740, la cosiddetta *funzione zeta*:

$$(6.1) \quad \zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots$$

C'è un'altra rappresentazione della funzione  $\zeta$ , che Eulero stesso provò nel 1749, che fa intervenire una produttoria anziché una sommatoria:

$$(6.2) \quad \zeta(s) = \prod_p (1 - \frac{1}{p^s})^{-1},$$

dove la produttoria è estesa a tutti i *numeri primi*  $p$ , in ordine crescente.

Questa rappresentazione, che comunemente si chiama *rappresentazione prodotto*, probabilmente è quella che rende la funzione  $\zeta$  così importante.

Perché questa uguaglianza tra due espressioni che apparentemente sono slegate (nella prima intervengono *tutti i numeri naturali*, mentre nell'altra intervengono i *numeri primi*)? Deriva dalla seguente osservazione:

- Ogni fattore  $(1 - \frac{1}{p^s})^{-1}$  della produttoria uguaglia la serie

$$1 + \frac{1}{p^s} + \frac{1}{(p^s)^2} + \frac{1}{(p^s)^3} + \dots$$

che è una serie geometrica di ragione  $q = \frac{1}{p^s}$  e pertanto la somma è  $\frac{1}{1-q}$ .

- Moltiplicando i vari fattori della (6.2) si ottiene una somma di termini della forma

$$(6.3) \quad \frac{1}{(p_1^s)^{h_1} (p_2^s)^{h_2} \dots (p_t^s)^{h_t}}$$

dove i  $p_i$  sono primi distinti. Quindi

$$(6.4) \quad \prod_p (1 - \frac{1}{p^s})^{-1} = \sum \frac{1}{(p_1^{h_1} p_2^{h_2} \dots p_t^{h_t})^s}$$

dove la somma è estesa al variare dei  $p_i$  tra tutti i primi, di tutti gli esponenti  $h_i$  in  $\mathbb{N}$ , e di  $t \in \mathbb{N}$ . Ma allora, *stante il Teorema Fondamentale dell'Aritmetica*, i denominatori che compaiono nelle frazioni del secondo membro della (6.4) rappresentano tutti e soli i numeri naturali  $n$  elevati alla potenza  $s$ -esima. In definitiva

$$\prod_p (1 - \frac{1}{p^s})^{-1} = \sum \frac{1}{(p_1^{h_1} p_2^{h_2} \dots p_t^{h_t})^s} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

che è quanto volevamo provare.



Riemann nel 1859 ha considerato la funzione  $\zeta$  come funzione di una variabile complessa  $s$  e ha provato (ma noi ce ne asterremo) alcune proprietà della funzione  $\zeta(s)$ , tra le quali che la funzione  $\zeta$  è definita e converge nell'intervallo reale aperto  $(1, \infty)$  e risulta che

$$(6.5) \quad \lim_{s \rightarrow 1} \zeta(s) = \infty.$$

Ora, questa proprietà e i due diversi modi di scrivere la funzione  $\zeta$  ci permettono di dimostrare che i numeri primi sono infiniti. Supponiamo l'insieme dei numeri primi finito. Allora chiaramente l'espressione (6.2) per  $s = 1$  sarebbe finita, contraddicendo quanto appena detto in (6.5). Ancora, Riemann ha stabilito un legame tra la distribuzione degli zeri della funzione  $\zeta$  nel piano complesso e il numero  $\pi(n)$  di primi minori di  $n$ .



## Esercizi di elementi di matematica

In questa appendice si vogliono rinfrescare alcune nozioni che tutti dovrebbero già conoscere dalle scuole superiori. Vengono raccolti una serie di esercizi che sono stati assegnati durante il corso di Elementi di Matematica della laurea in Informatica, corso propedeutico ad ogni corso di matematica. Il materiale presente in questa appendice *non* esaurisce certamente il bagaglio che uno studente deve sapere. Si invitano gli studenti a riprendere i loro testi di matematica delle scuole superiori e fare (rifare) tutti gli esercizi. Gli esercizi verranno suddivisi per argomento.

### Numeri (naturali, interi, razionali e reali) e loro proprietà

- Decidere se il numero  $2^4 \cdot 3^6 \cdot 5^4$  è o no il quadrato di un numero intero. Se sì, dire di quale numero intero è il quadrato.
- Scrivere come prodotto di potenze di numeri primi distinti il numero  $8^6 \cdot 15^9 \cdot 6^5 \cdot 48^8$ .
- Quanto vale il quadrato di  $3^{10}$ ? e la metà di  $8^{30}$ ? Quanto vale  $\frac{-2^6}{(-4)^8}$ ? e  $\frac{(-2)^6}{(-4)^{-3}}$ ?
- Quanto vale il quadrato di  $5^{15}$ ? e la metà di  $4^{30}$ ? Quanto vale  $\frac{-2^8}{(-4)^6}$ ? e  $\frac{(-2)^5}{(-4)^{-4}}$ ?
- Determinare la metà di  $26^{15}$ .
- Determinare il più piccolo intero positivo *pari* che è divisibile per 3, 9 e 11.
- Disporre in ordine crescente i seguenti numeri:  
 $-|-4|, |-2| + |2|, |2| - |-2|, 0, |-4|, -4, -2 + |-2|$   
 individuando anche eventuali coincidenze.
- Disporre in ordine crescente i seguenti numeri:  
 $-|3.5|, |-3.5|, -3.5, -\frac{8}{3}, 2^{3^2}, -2^{3^2}, (-2)^{3^2}$   
 individuando anche eventuali coincidenze.

$$-|3.5|, |-3.5|, -3.5, -\frac{8}{3}, 2^{3^2}, -2^{3^2}, (-2)^{3^2}$$

Scrivere il numero  $8^3 \cdot 10^4 \cdot 6^2 \cdot 12^4$  sotto forma di prodotto di potenze di numeri primi distinti.

Determinare la metà di  $28^{28}$ .

Scrivere il numero  $12^4 \cdot 6^2 \cdot 32^2 \cdot 14^3$  sotto forma di prodotto di potenze di numeri primi.

Calcolare  $(-3)^4 \cdot (-3)^2$ .

Calcolare  $(-3)^{-3} \cdot (-3)^5$ .

Calcolare  $\frac{(-3)^4}{(-3)^8}$ .

Determinare il più piccolo intero positivo che è divisibile per 4, 25, 6, 15.

Calcolare

$$(-2)^{3^2}, \quad (-2)^{2^3}, \quad ((-2)^3)^2, \quad ((-2)^2)^3, \quad (-2)^{2 \cdot 3}, \quad (-2)^3 \cdot (-2)^2$$

scrivendo esplicitamente quali sono uguali, e in base a quale proprietà delle potenze.

Disporre in ordine crescente i seguenti numeri:

$$2^{3^4}, \quad 2^{4^3}, \quad (2^4)^3, \quad (2^3)^4, \quad ((-2)^3)^4, \quad ((-2)^4)^3, \quad (-2)^{3^4}, \quad (-2)^{4^3}, \quad -(2^3)^4.$$

Ci sono alcuni di questi numeri che coincidono? Quanti e quali di questi numeri sono negativi?

Disporre in ordine crescente i seguenti numeri:

$$(3^5)^2, \quad ((-3)^5)^2, \quad -(3^5)^2, \quad 3^{5^2}, \quad (-3)^{5^2}, \quad -3^{5^2}, \quad 3^{2^5}, \quad (-3)^{2^5}, \quad -3^{2^5}$$

individuando anche eventuali coincidenze.

N.B. Non si chiede di calcolare effettivamente i numeri corrispondenti alle varie potenze.

Scrivere il numero  $6^3 \cdot 10^4 \cdot 9^3 \cdot 15^3$  sotto forma di prodotto di potenze di 2, 3 e 5.

Calcolare

$$\left(\frac{3}{4} - \frac{1}{2}\right)^2 : \left(-\frac{1}{3} + \frac{3}{4}\right)^2 - \left(1 - \frac{2}{3}\right)^2 : \left(3 - \frac{7}{3}\right)^2.$$

Calcolare

$$\left\{ \left[ \left(\frac{1}{8} + \frac{3}{5}\right) \left(\frac{4}{3} + \frac{3}{4}\right) : \frac{29}{3} - \frac{21}{32} \right]^2 - \left(-\frac{1}{2}\right)^4 \right\} \cdot \left(-\frac{16}{3}\right).$$

Cosa si può dire dei numeri interi  $a, b, c$  se  $abc = 0$ ?

Cosa si può dire dei numeri interi  $a, b, c$  se  $abc \neq 0$ ?

Cosa si può dire dei numeri interi  $a$  e  $b$  entrambi diversi da zero se sappiamo che  $(a^2 + b^2)(a^2 - b^2) = 0$ ?

Dare almeno un esempio di due interi  $a$  e  $b$  che verificano la predetta relazione e un esempio di due interi che non la verificano.

Cosa si può dire dei numeri interi  $a, b, c$  se  $\frac{a^2+b^2}{c} = 0$ ?

Cosa si può dire dei numeri interi  $a, b$  se  $a^2 - b^2 = 0$ ?

Cosa si può dire dei numeri interi  $a, b$  se  $(a+b)(a-2b) = 0$ ? Dare un esempio (se esiste) di due interi che verificano questa condizione.

Cosa si può dire dei numeri interi  $a, b, c$  se  $(a-b)(b-c)(c-a) = 0$ ?

Siano  $a$  e  $b$  due numeri reali con  $a > b$ . Che legame ci sarà tra  $-a$  e  $-b$ ? e tra  $a-3$  e  $b-3$ ? e tra  $\frac{a}{3}$  e  $\frac{b}{3}$ ?

### Fattorizzazione e prodotti notevoli

Scrivere, se possibile, come prodotto di due fattori, l'espressione  $2x^5 - x^3 + 6x^2 - 3$ .

Fattorizzare l'espressione  $m^2 + 2mn + n^2 - m - n$  come prodotto di più fattori, se possibile.

Scrivere, se possibile, come prodotto di due fattori, l'espressione  $7x^2 + 2x - 35xy - 10y$ .

Scrivere, se possibile, come prodotto di due fattori, l'espressione  $25a^4b^2 - 16 - 24c^4 - 9c^8$ .

Scrivere, se possibile, come prodotto di due fattori, la seguente espressione  $a(x^2 + 1) - x(a^2 + 1)$ .

Scrivere, se possibile, come prodotto di due fattori, l'espressione  $x^3y^3 + 3x^3 - 3y^3 - 9$ .

### Espressioni razionali

Semplificare l'espressione  $(a-b)(a+b)(a^2+b^2)(a^4+b^4) - a^8$ .

Semplificare l'espressione  $(x+y)(x^2 - xy + y^2) + (x-y)(x^2 + xy + y^2)$ .

Calcolare  $\frac{1}{ab+a^2} - \frac{2b}{ab^2-a^3} - \frac{1}{b^2-ab} + \frac{a+b}{ab^2-a^2b}$ .

Calcolare  $\frac{\frac{1}{2}a^2+20ab+25b^2}{a+5b}$ .

Calcolare  $\frac{a^3-b^3}{a^2-b^2} : \frac{a^2+ab+b^2}{a^4-b^4}$  per  $a = -\frac{1}{2}$ ,  $b = \frac{1}{4}$ .

- 1) Semplificare l'espressione  $\frac{(a+b)^2 - c^2}{c-a-b}$ .
- 2) Svolgere le operazioni semplificando il più possibile  $\frac{a+b}{b} - \frac{a-b}{a}$ .
- 3) Semplificare quanto più è possibile la  $\frac{y-\frac{x^2}{y}}{1+\frac{x^2-y^2}{x^2}}$ .
- 4) Semplificare l'espressione  $\frac{x^2+y^2}{2xy} - \frac{x+y}{x} - \frac{x-y}{y} + \frac{x}{2y}$ .
- Passaggio da decimali finiti e decimali infiniti periodici a frazioni e viceversa**
- 5) Scrivere sotto forma di frazione il numero  $1,2\overline{7}$ .
- 6) Scrivere sotto forma di frazione il numero  $3,0\overline{27}$ .
- 7) Scrivere sotto forma di frazione il numero  $2,0\overline{36}$ .
- Insiemi**
- 8) Siano  $A = \{x \in \mathbb{N} \mid x^3 - 1 \geq 0\}$ ,  $B = \{x \in \mathbb{Z} \mid \text{divisori di } 10\}$  e  $C = (-4, 5) \cap \mathbb{Z}$ . Determinare esplicitamente  $A$ ,  $B$  e  $C$ . N.B. Dati due numeri reali  $a$  e  $b$ ,  $a < b$ , con  $(a, b)$  si intende l'insieme dei numeri reali  $x$  tali che  $a < x < b$ .
- 9) Siano  $A = \{-5, -4, -3, 3, 4, 5\}$  e  $B = \{n \in \mathbb{N} \mid n^2 - 16 < 0\}$ . Determinare esplicitamente  $B$ ,  $A \cap B$  e  $A \cup B$ .
- 10) Siano  $A = \{x \in \mathbb{Z} \mid |x| < 3\}$ ,  $B = \{x \in \mathbb{N} \mid x^2 < 10\}$ . Determinare esplicitamente  $A$ ,  $B$ ,  $A \cap B$  e  $A \cup B$ .
- 11) Siano  $A = \{x \in \mathbb{Z} \mid x^2 \leq 2x - 1\}$ ,  $B = \{x \in \mathbb{Q} \mid x^2 = 2\}$ ,  $C = \{x \in \mathbb{Z} \mid x^2 \geq -2x - 1\}$ . Determinare esplicitamente  $A$ ,  $B$ ,  $C$ ,  $A \cap B$  e  $A \cup B$ ,  $A \cap C$  e  $A \cup C$ ,  $B \cap C$  e  $B \cup C$ .
- 12) Siano  $A = \{1, 2, 3, 4\}$  e  $B = \{5, 6\}$ . Quanti elementi ha il prodotto cartesiano  $A \times B$ ? Determinare i suoi elementi. Scrivere a vostro piacere una relazione da  $A$  a  $B$ , e decidere se si tratta di una funzione da  $A$  a  $B$ .
- Polinomi e radici di polinomi. Equazioni razionali. Divisione tra polinomi**
- 13) Determinare le soluzioni dell'equazione in  $x$ :  $(x-a)^3 - a^3 = (x+2a)^2 - (b-a)(b+a)$ .
- 14) Risolvere la seguente equazione  $\frac{1}{2x} = \frac{2x}{5}$ .
- 15) Determinare (se esistono) tutte le radici razionali del polinomio  $4x^4 - 3x^3 + 2$ .
- 16) Determinare quoziente e resto della divisione in  $\mathbb{Q}[x]$  del polinomio  $f(x) = x^4 + 3x - a$  per  $g(x) = x^2 + 3$ . Decidere se esistono dei valori del parametro  $a \in \mathbb{Q}$  per i quali il polinomio  $f(x)$  è divisibile per  $g(x)$ .

- 17) Determinare (se esistono) tutte le radici *razionali* dell'equazione  $3x^6 - 4x^3 + x + 1 = 0$ .
- 18) Determinare quoziente e resto della divisione in  $\mathbb{Q}[x]$  del polinomio  $f(x) = x^4 + 3x^3 - 3$  per  $g(x) = x^2 - 1$ . Decidere se il polinomio  $f(x)$  è divisibile per  $g(x)$ .
- 19) Determinare tutti i numeri  $x$  che soddisfano l'equazione  $(2x-1)(x-3) = (3x-1)(x-\frac{1}{2})$ .
- 20) Risolvere l'equazione in  $x$ :  $(x-1)(x+4) = (2x+1)(x-1)$ .
- 21) Determinare tutte le radici *razionali* dell'equazione  $(x^2+1)(x+\frac{3}{4})(x-2)(x+7)(x^2-3) = 0$ . Quali tra queste sono numeri interi? Quali sono numeri naturali?
- 22) Per quali valori del parametro reale  $a$  l'equazione  $(a^2-1)x = 1$  non ammette soluzioni?
- 23) Determinare tutte le radici *interne* del polinomio  $x^4 - 16$ .
- 24) Determinare tutte le radici *razionali* dell'equazione  $(x^2+6)(x+\frac{2}{3})(x+5)(x+10)(x^2-5) = 0$ . Quali tra queste sono numeri interi? Quali sono numeri naturali?
- 25) Risolvere l'equazione  $(x-1)(1 - \frac{3}{x-1}) = \frac{9-x^2}{1-x}$ .
- 26) Scrivere un polinomio di secondo grado che sia privo di radici reali.
- 27) Determinare tutte le soluzioni della seguente equazione in  $x$ :
- $$(3x-2)(x+1) = (2-3x)(x+5).$$
- 28) Determinare tutte le radici *razionali* dell'equazione  $(x^3-1)(x^2+3)(x^2-8)(x^4-16) = 0$ . Quali tra queste sono numeri interi? Quali sono numeri naturali?
- 29) Per quali valori del parametro reale  $k$  l'equazione  $(k^2+1)x = 8$  non ammette soluzioni?
- 30) Determinare tutte le soluzioni della seguente equazione in  $x$ :
- $$(x+3)(x-1) = (-x+2)(3+x).$$
- 31) Determinare tutti i numeri  $x$  che soddisfano l'equazione  $(3x-1)(x-5) = (2x-3)(x-\frac{1}{3})$ .
- 32) Risolvere la seguente equazione in  $x$ :  $\frac{1}{x+1} = 1 - \frac{x}{x+4}$ .
- 33) Per quali valori del parametro reale  $a$  l'equazione  $x^2 + ax - 1 = 0$  possiede radici reali?
- 34) Quanti sono i *numeri naturali* diversi da zero che soddisfano la condizione che il loro quadruplo diminuito del loro terzo è un numero naturale  $< 5$ ? Quanti sono gli *intervi* che verificano questa condizione?

**Equazioni con modulo e disequazioni**

- Ⓐ Risolvere l'equazione (con modulo)  $|x + 3| + |x - 5| = 9$ .
- Ⓑ Risolvere l'equazione  $|x + 2| + |x - 3| = 6$ .
- Ⓒ Risolvere la seguente disequazione:  $x^2 - x + 8 > 0$ .
- Ⓓ Risolvere la seguente equazione:

$$(x + 1)^2 = 3|x + 1|.$$

- Ⓔ Risolvere la disequazione  $\frac{x+4}{x-3} < 1$ .
- Ⓕ Risolvere la disequazione  $\frac{(x^2-3x+1)}{x^2} \leq 0$ .

**Logaritmi e radicali**

- Ⓖ Determinare tutte le soluzioni (se esistono) della seguente equazione logaritmica:

$$\log_2(x - 2) + \log_2(2x - 3) - 2\log_2 x = 0.$$

- Ⓗ Risolvere l'equazione logaritmica  $\log_2(x + 3) = 2\log_2 x - 2$ .
- Ⓘ Determinare tutti i valori di  $x$  in  $\mathbb{R}$  per cui è definita  $\sqrt[4]{\frac{x+5}{x+4}}$ .
- Ⓛ Determinare tutti gli  $x \in \mathbb{R}$  tali che  $\log(x - 1) + \log(x + 1) = \log 5$ .
- Ⓜ Determinare tutti i valori di  $x$  in  $\mathbb{R}$  per cui è definita  $\sqrt[8]{\frac{x+1}{x+5}}$ .
- Ⓝ Determinare tutti gli  $x$  tali che
  - a. Sia definito  $\log_{10}(x^2 - 1)$ .
  - b. Risulti  $\log_{10}(x^2 - 1) = 1$ .

**Bibliografia**

- [1] M.W. BALDONI, C. CILIBERTO, G.M. PIACENTINI CATTANEO, *Aritmetica, Crittografia e Codici*. Springer Unitext (2006).
- [2] B. BOLLOBAS, *Graph Theory. An Introductory Course*. Springer-Verlag Graduate texts in Mathematics (1979).
- [3] D.M. BURTON, *Elementary Number Theory*. Allyn & Bacon, Boston (1980).
- [4] L.R. FOULDS, *Graph Theory Applications*. Springer New York (1994).
- [5] R.H. GRIMALDI, *Discrete and Combinatorial Mathematics. An applied Introduction*. Addison Wesley (1994).
- [6] R.H. GRAHAM, D.E. KNUTH, O. PATASHNIK, *Concrete Mathematics*. Addison-Wesley Publishing Company, second edition (1994).
- [7] F. HARARY, *Graph Theory*. Addison-Wesley Publishing Company (1972).
- [8] I.N. HERSTEIN, *Algebra*. Editori Riuniti (1982).
- [9] K. KALMANSON, *An introduction to Discrete Mathematics and its Applications*. Addison-Wesley Publishing Company (1986).
- [10] R.J. MCELIECE, R.B. ASH, C. ASH, *Introduction to Discrete Mathematics*. McGraw-Hill International Editions, Computer Science Series (1989).
- [11] D.E. KNUTH, *The art of Computer Programming*, Vols 1,2. Addison-Wesley, (1974, 1981).
- [12] G.M. PIACENTINI CATTANEO, *Algebra. Un approccio algoritmico*. Decibel Zanichelli (2006).
- [13] P.V. O'NEIL, *Ulam's Conjecture and Graph Reconstructions*, "American Mathematical Monthly", vol 77, n.1, 35-43 (1970).
- [14] K.H. ROSEN, *Discrete Mathematics and its applications*. McGraw Hill (1995).
- [15] H.N.V. TEMPERLEY, *Graph Theory and Applications*. Ellis Horwood Series Mathematics and its applications (1981).
- [16] C. VANDEN EYNDEN, *Elementary Number Theory*. Birkhäuser Mathematics Series McGraw-Hill (1987).

# Soluzioni degli esercizi

## SOLUZIONI RELATIVE AL CAPITOLO 1

Proviamo la prima.  $x \in C(A \cap B) \iff x \notin A \cap B \iff [x \notin A \text{ oppure } x \notin B] \iff [x \in CA \text{ oppure } x \in CB] \iff x \in CA \cup CB$ .

$B \cup C = \{11, 12, 13, 14, 15, 16, 17\}$ , quindi  $A \cap (B \cup C) = \{11, 12, 13, 14, 15\}$ .  
 $A \cap B = \{12, 13, 14, 15\}$ , quindi  $(A \cap B) \cup C = \{11, 12, 13, 14, 15\}$ .  
I due insiemi sono pertanto uguali.

Non vale per ogni scelta di  $A, B, C$ : per esempio, se si prende  $A = B$  e  $C$  contenente propriamente  $A$ ,  $A \cap (B \cup C) = A$ , mentre  $(A \cap B) \cup C = C$ .

- a.  $A = \{11, 33, 55, 77, 99\}$ .
- b.  $A = \{1, -5\}$ .
- c.  $A = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}$ .

Sono tutti diversi: infatti  $A$  è l'insieme vuoto (non possiede nessun elemento);  $B$  e  $C$  contengono entrambi un elemento, ma si tratta di elementi diversi.

$A = C = \emptyset$ ;  $B = \{0\}$ ;  $D = \{-1, -2\}$ .

$A \subseteq C$  ( $A$  coincide con  $C$ , ma si può sempre scrivere  $A \subseteq C$ , dato che questa relazione include l'uguaglianza),  $C \subseteq A$ ,  $A \subset B$ ,  $A \subset D$ ,  $C \subset B$ ,  $C \subset D$ .

- a.  $A = \{-5, -4, -3, -2, -1, 0, 1, 2\}$ ,  $B = \{-1, 0, 1, 2\}$ : risulta  $A \supset B$  e quindi  $A \cup B = A$ ,  $A \cap B = B$ .
- b.  $A = \{-1, 0, 1, 2, 3, 4, 5\}$ ;  $B = \{x = 3h \mid h \in \mathbb{Z}\}$ . Quindi  $A \cup B = \{-1, 2, 4, 5, 3h, h \in \mathbb{Z}\}$ ;  $A \cap B = \{0, 3\}$ .
- c.  $A = \emptyset$ ,  $B = \{0, 1, 2\}$ . Quindi  $A \cup B = B$ ,  $A \cap B = \emptyset$ .

- a.  $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ ;  
 $|A| = 3$ ,  $|\mathcal{P}(A)| = 2^3 = 8$ .
- b.  $A = \{0, 1, 2\}$ ;  $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$ .  
 $|A| = 3$ ,  $|\mathcal{P}(A)| = 2^3 = 8$ .
- c.  $\mathcal{P}(A) = \{\emptyset, \{-1\}, \{3\}, \{5\}, \{4\}, \{-1, 3\}, \{-1, 5\}, \{-1, 4\}, \{3, 5\}, \{3, 4\}, \{5, 4\}, \{-1, 3, 5\}, \{-1, 3, 4\}, \{-1, 5, 4\}, \{3, 5, 4\}, \{-1, 3, 5, 4\}\}$   
 $|A| = 4$ ,  $|\mathcal{P}(A)| = 2^4 = 16$ .

$B = \{-1, 0, 1, 2, 3\}$ ;  $C = \{0, 6, 12, 18\}$ .

$$A \times A = \{(t, t), (t, u), (t, v), (u, t), (u, u), (u, v), (v, t), (v, u), (v, v)\};$$

$$B \times C = \{(-1, 0), (-1, 6), (-1, 12), (-1, 18), (0, 0), (0, 6), \dots, (3, 0), (3, 6), (3, 12), (3, 18)\}.$$

Esistono interi che non sono somma di due quadrati.

La negazione di questa proposizione è: dati comunque due interi  $a$  e  $b$ , risulta  $(a + b)(a - 2b) \neq 0$ .  
In altre parole, dati comunque due interi  $a$  e  $b$ ,  $a$  è diverso da  $-b$  e  $a \neq 2b$ .

Ci sono mesi in cui nessuno studente legge libri ossia ci sono mesi in cui ogni studente non legge nemmeno un libro.

C'è almeno uno studente in quest'aula che a febbraio non supererà nessun esame.

Ogni giorno o non piove o non c'è il sole. (In altre parole, tutti i giorni in cui piove non c'è il sole, oppure ogni giorno in cui c'è il sole non piove).

Ricordarsi che la negazione di una proposizione del tipo  $\exists x \mid p$  è la proposizione  $\forall x \neg p$ . Nel nostro caso sia  $p$  la proposizione: piove e sia  $q$  la proposizione c'è il sole e sia  $g$  una variabile che denota i giorni. Allora la frase iniziale si può scrivere al modo seguente:  $\exists g \mid (p \wedge q)$ . La negazione sarà quindi:  $\forall g \neg(p \wedge q)$ . Ricordando che  $\neg(p \wedge q) = \neg p \vee \neg q$ , la precedente proposizione si può scrivere come  $\forall g (\neg p \vee \neg q)$  che corrisponde esattamente a quello che abbiamo scritto a parole.

Condizione sufficiente per  $q$  è  $p$  (ma non necessaria), oppure condizione necessaria per  $p$  è  $q$ .

L'essere maggiorenne ( $q$ ) è condizione necessaria per votare ( $p$ ).  
 $p$  (l'esercitare il diritto di voto) è condizione sufficiente per  $q$  (essere maggiorenne).

$q$  è necessaria per  $p$ ,  $p$  è sufficiente per  $q$ .

Si deduce dalla seguente tavola di verità:

$p$	$q$	$p \Leftrightarrow q$	$\neg(p \Leftrightarrow q)$	$(p \vee q) \wedge \neg(p \wedge q)$	$\neg(p \Leftrightarrow q) \Leftrightarrow ((p \vee q) \wedge \neg(p \wedge q))$
T	T	T	F	F	T
T	F	F	T	T	T
F	T	F	T	T	T
F	F	T	F	F	T

- a.  $\exists x (p(x) \wedge q(x))$ .
- b.  $\exists x (p(x) \wedge \neg q(x))$ .
- c.  $\forall x (p(x) \vee q(x))$ .
- d.  $\forall x (\neg p(x) \wedge \neg q(x)) = \forall x \neg(p(x) \vee q(x))$ .

Raccogliamo nella tabella che segue le varie possibilità:

A	T	F	F	F
B	F	T	F	F
C	F	F	T	F
D	F	F	F	T

La seconda colonna rappresenta la situazione in cui è Antonio ad aver detto la verità e tutti gli altri hanno mentito, la terza colonna rappresenta il caso in cui è Bruno ad aver detto la verità e tutti gli altri hanno mentito, e così via.

1. La seconda colonna non può sussistere, perché porterebbe ad incolpare due bambini, mentre il responsabile è uno solo. Infatti dalla risposta di Davide, che mente, si deduce che Carla ha detto la verità, quindi il colpevole è Davide. Ma dalla risposta di Antonio (che dice la verità) si trae che il colpevole è Carla.
2. La terza colonna non può sussistere: infatti si arriva ad un assurdo: da un lato non è stato Davide (perché Carla non dice la verità), dall'altro, dato che Davide mente, Carla non ha mentito, quindi il colpevole è Davide.
3. Anche la quarta colonna non si può verificare: infatti dalla risposta di Bruno (che mente) si trae che il colpevole è Bruno, mentre dalla risposta di Carla (che dice la verità) si trae che il colpevole è Davide.
4. L'ultima colonna è quella che porta alla individuazione del vero colpevole: dato che Bruno mente e dice di non essere colpevole, segue che il colpevole è proprio Bruno (si noti che non restano individuati altri colpevoli).

● No, perché non è un sottoinsieme di  $\mathbb{N} \times \mathbb{N}$ , dato che il secondo elemento della coppia non è sempre un elemento di  $\mathbb{N}$ .

● Sì, perché primo e secondo elemento della coppia sono elementi di  $\mathbb{R}$  (di cui il primo sempre maggiore o uguale a zero).

● Per provare che  $f$  è suriettiva dobbiamo provare che per ogni  $r \in \mathbb{R}$  esiste  $\bar{x} \in \mathbb{R}$  tale che  $r = \bar{x}^5 + 3\bar{x}^4 - 2\bar{x}^3 + \bar{x} + 1$ . Basta allora considerare il polinomio  $x^5 + 3x^4 - 2x^3 + x + 1 - r$ : sappiamo che ammette una radice in  $\mathbb{R}$  (trattandosi di un polinomio di grado dispari) per cui esisterà  $\bar{x}$  tale che  $\bar{x}^5 + 3\bar{x}^4 - 2\bar{x}^3 + \bar{x} + 1 - r = 0$ .  $\bar{x}$  è tale che  $r = f(\bar{x})$ , quindi  $f$  è suriettiva.

- a.  $a \in f(X) \cup f(Y) \iff a \in f(X) \text{ o } a \in f(Y) \iff [a = f(x) \text{ per qualche } x \in X \text{ o } a = f(y) \text{ per qualche } y \in Y] \iff a = f(t) \text{ per qualche } t \in X \cup Y \iff a \in f(X \cup Y)$ .
- b.  $a \in f(X \cap Y) \iff a = f(c) \text{ per qualche } c \in X \cap Y$ . Quindi  $a \in f(X) \text{ e } a \in f(Y)$ , cioè  $a \in f(X) \cap f(Y)$ . L'altra inclusione non vale sempre. Per esempio, sia  $f(x) = \sin x : \mathbb{R} \rightarrow \mathbb{R}$ . Sia  $X = [0, \pi/2] = \{x \in \mathbb{R} \mid 0 \leq x \leq \frac{\pi}{2}\}$ ,  $Y = [\pi/2, \pi] = \{x \in \mathbb{R} \mid \frac{\pi}{2} \leq x \leq \pi\}$ . Risulta  $f(X \cap Y) = f(\pi/2) = 1$ . Dato che  $f(X) = f(Y) = [0, 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$  si ha  $f(X) \cap f(Y) = [0, 1] \supset f(X \cap Y)$ . L'uguaglianza  $f(X \cap Y) = f(X) \cap f(Y)$  vale se e solo se  $f$  è iniettiva.
- c.  $a \in f^{-1}(X' \cup Y') \iff f(a) \in X' \cup Y' \iff [f(a) \in X' \text{ o } f(a) \in Y'] \iff [a \in f^{-1}(X') \text{ o } a \in f^{-1}(Y')] \iff a \in f^{-1}(X') \cup f^{-1}(Y')$ .
- d. Analoga.

- a. È una relazione da  $Z$  in  $\mathbb{N}$  dato che è un s.i. di  $Z \times \mathbb{N}$  (infatti per ogni  $a \in Z$   $3(a-1)^2 \in \mathbb{N}$ ).
- b. È una funzione perché per ogni  $a \in Z$  esiste una e una sola immagine.
- c.  $f(0) = 3$  e  $f(2) = 3$ .
- d. Per determinare la controimmagine di 0 si devono determinare gli  $a \in Z$  tali che  $3(a-1)^2 = 0$ , ossia la controimmagine di 0 è 1. Per determinare la controimmagine di  $\{30\}$  si devono determinare gli  $a \in Z$  tali che  $30 = 3(a-1)^2$  ossia risolvere in  $a$  la  $10 = (a-1)^2$ : dato che 10 non è il quadrato di nessun numero intero, la controimmagine di 30 è l'insieme vuoto. La controimmagine di 108 è  $\{-5, 7\}$ .
- e. Non è iniettiva (v. punto c), ci sono elementi distinti del dominio che hanno la stessa immagine.
- f. Non è suriettiva, perché per esempio 30 non appartiene all'immagine (v. punto d).

● Si ha:  $B = \{0, 1, 2, 3\}$ .

- a. Non è una funzione da  $A$  in  $B$ , poiché l'immagine di  $d$  non appartiene al codominio.
- b. Non è una funzione da  $A$ , poiché l'immagine di  $d$  non è definita.
- c. È una funzione, ma non è né iniettiva né suriettiva (non è iniettiva perché l'immagine di  $a$  è uguale all'immagine di  $d$ ; non è suriettiva perché 3 non è immagine di nessun elemento).
- a. È una funzione da  $A$  in  $A$  dato che ad ogni elemento di  $A$  corrisponde uno e un solo elemento di  $A$ .
- b.  $f(3) = 4$ .
- c.  $f^{-1}(\{2\}) = \emptyset$ ,  $f^{-1}(\{1\}) = \{1, 2, 5\}$ .
- d. Non è iniettiva dato che per esempio 1 e 2 hanno la stessa immagine.
- e. Non è suriettiva, dato che ci sono elementi (come per esempio 2) che non hanno nessuna controimmagine, ossia l'immagine di  $f$  non coincide con tutto il codominio.

●  $(f \circ g)(x) = 2x^2$  e  $(g \circ f)(x) = 4x^2$ .

● Si tratta di provare che  $\forall x \in A$   $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$ . Infatti,  $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$  e  $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$ .

●  $\Phi_1$  biiettiva;  $\Phi_2$  iniettiva, non suriettiva;  $\Phi_3$  iniettiva, non suriettiva;  $\Phi_4$  biiettiva;  $\Phi_5$  non è una funzione, perché  $\phi_5(0)$  non appartiene a  $\mathbb{R}_+$ ;  $\Phi_6$  biiettiva;  $\Phi_7$  iniettiva, non suriettiva.

● I tipi di relazione d'ordine parziale su  $X$  sono i seguenti:



Corrispondentemente, il numero complessivo di relazioni d'ordine parziale su  $X$  è  $1 + 6 + 6 + 3 + 3 = 19$ . Di queste, 6 sono relazioni d'ordine totale (quelle corrispondenti al terzo tipo).

- a. Chiaramente un insieme si può porre in corrispondenza biunivoca con se stesso mediante l'applicazione identica (quella che associa ad ogni elemento se stesso): quindi vale la proprietà riflessiva.  
Se  $A$  si può mettere in corrispondenza biunivoca con  $B$  mediante la corrispondenza biunivoca  $f$ , allora  $B$  si potrà mettere in corrispondenza biunivoca con  $A$  (mediante l'inversa della  $f$ , che è ancora biunivoca): quindi vale la proprietà simmetrica.  
Infine, se esiste una corrispondenza biunivoca  $f$  tra  $A$  e  $B$  e una corrispondenza biunivoca  $g$  tra  $B$  e  $C$ , allora la  $g \circ f$  è una corrispondenza ancora biunivoca (controllare!) tra  $A$  e  $C$  e pertanto vale la proprietà transitiva.  
Ogni classe di equivalenza è costituita di tutti i sottoinsiemi di  $X$  che hanno lo stesso numero di elementi, ossia la stessa potenza o cardinalità. L'insieme quoziente  $\mathcal{P}(X)/\sim$  è l'insieme di tutte le cardinalità. Le cardinalità finite sono costituite dai numeri naturali  $0, 1, 2, \dots$ , poi ci sarà la cardinalità del numerabile, la cardinalità del continuo, e via via le cardinalità crescenti (cfr. cap.4).
- b. Se  $X$  ha  $n$  elementi,  $\mathcal{P}(X)/\sim$  ha  $n+1$  elementi, corrispondenti alle cardinalità 0 (quella dell'insieme vuoto), la cardinalità 1 (corrispondente alla cardinalità 1 di tutti gli insiemi con un solo elemento), e infine la cardinalità  $n$  che è la cardinalità di tutto  $X$ .

Chiaramente  $m \sim m$  perché  $|m| = |m|$  (proprietà riflessiva).

Proprietà simmetrica:  $m\rho n \iff |m| = |n| \iff |n| = |m| \iff n\rho m$ .

Proprietà transitiva: supponiamo  $m\rho n$  e  $n\rho p$ . Allora dalle  $m\rho n \iff |m| = |n|$  e  $n\rho p \iff |n| = |p|$  segue (per la proprietà transitiva della uguaglianza) che  $|m| = |p|$  ossia  $n\rho p$ .

La classe di equivalenza  $\bar{n}$  di ogni intero  $n \neq 0$  è costituita dai due interi  $\pm n$ . La classe di equivalenza dello 0 è costituita dal solo 0. Ogni classe può essere etichettata con l'intero positivo  $|n|$  corrispondente. Quindi si può stabilire una corrispondenza biunivoca (verificare che è effettivamente biunivoca)  $f$  tra  $\mathbb{Z}/\rho$  e  $\mathbb{N}$  ponendo per ogni  $\bar{n} \in \mathbb{Z}/\rho$

$$f(\bar{n}) = |n| \in \mathbb{N}.$$

Il fatto che si tratti di una relazione di equivalenza deriva dal fatto che la relazione è definita attraverso l'uguaglianza dei numeri  $x^2 + y^2$  e  $\bar{x}^2 + \bar{y}^2$ , e per queste uguaglianze valgono le proprietà riflessiva, simmetrica e transitiva.

Geometricamente le classi di equivalenza sono circonferenze del piano  $\mathbb{R}^2$  di centro l'origine (che hanno equazione  $x^2 + y^2 = r^2$ ); l'origine (che è una classe a sé) si può pensare come circonferenza di raggio zero. Ogni tale circonferenza è individuata dal suo raggio, che è un intero maggiore o uguale a zero. Pertanto possiamo definire la seguente corrispondenza

$$\begin{array}{ccc} \mathbb{R}^2/\rho & \longrightarrow & \mathbb{R}^{\geq 0} = \{x \in \mathbb{R}, x \geq 0\} \\ \text{circonferenza} & \longrightarrow & \text{raggio della circonferenza} \end{array}$$

Chiaramente si tratta di un corrispondenza biunivoca (provare!). Il quoziente è pertanto in corrispondenza biunivoca con i reali maggiori o uguali a zero.

Si tratta della relazione di congruenza modulo un intero  $n$ .

È riflessiva:  $x \sim x \forall x \in \mathbb{R}$  perché  $x - x = 0 \in \mathbb{Z}$ .

È simmetrica:  $\forall x, y \in \mathbb{Z}$  se  $x \sim y$  vuol dire che  $x - y = a \in \mathbb{Z}$ . Allora  $y - x = -a \in \mathbb{Z}$  ossia  $y \sim x$ .

È transitiva:  $\forall x, y, z \in \mathbb{R}$  se  $x \sim y$  e  $y \sim z$ , allora  $x - y = a \in \mathbb{Z}$ ,  $y - z = b \in \mathbb{Z}$  da cui (sommando membro a membro)  $x - z = a + b \in \mathbb{Z}$ .

Si tratta quindi di una relazione di equivalenza. Stiamo identificando in  $\mathbb{R}$  numeri reali che differiscono per un intero. Come rappresentante di ogni classe possiamo scegliere un intero che appartiene all'intervallo  $[0, 1) = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ . Quindi  $\mathbb{R}/\sim$  è identificabile con  $[0, 1)$ .

$\rho$  è riflessiva, infatti la differenza tra il prezzo di un articolo e il prezzo dello stesso articolo è 0 (che è meno di un euro); se il prezzo dell'articolo  $x$  e il prezzo dell'articolo  $y$  differiscono per meno di un euro, allora evidentemente anche il prezzo dell'articolo  $x$  e il prezzo dell'articolo  $y$  differiscono per meno di un euro, quindi  $\rho$  è simmetrica. Se l'articolo  $x$  costa 1 euro e 10 centesimi, l'articolo  $y$  costa 2 euro e l'articolo  $z$  costa 2 euro e 50 centesimi, allora evidentemente  $x\rho y$  e  $y\rho z$  ma  $x$  non è in relazione con  $z$ : quindi la relazione non è transitiva.

a.  $\rho$  è una relazione d'ordine: riflessiva: se  $b \in \mathcal{P}(A)$  allora  $b \subseteq b$ . Antisimmetrica: se  $b \in \mathcal{P}(A)$  e  $c \in \mathcal{P}(A)$  allora  $b \subset c$  e  $c \subset b$  ma questo significa esattamente  $b = c$ . Transitiva: se  $b \subset c$  e  $c \subset d$  (da cui  $b \subset d$ ) allora ciò significa  $b \subseteq c$  e  $c \subseteq d$  ma questo implica chiaramente  $b \subseteq d$  ovvero  $b \subset d$ .

b. Il sottoinsieme di  $\mathcal{P}(A) \times \mathcal{P}(A)$  che rappresenta la relazione è costituito dalle coppie in cui il primo elemento della coppia è un sottoinsieme contenuto nel secondo elemento della coppia.

- a. È simmetrica ma non è né riflessiva né transitiva (se  $r$  non è parallela a  $s$  e  $s$  non è parallela a  $t$ ,  $r$  può essere parallela a  $t$ ).  
 b. È di equivalenza.  
 c. È solo simmetrica.  
 d. È riflessiva e transitiva ma non simmetrica.  
 e. Non è riflessiva, perché non tutte le rette del piano passano per  $x$ .

• Si tratta di una relazione di equivalenza (si osservi che  $\frac{1}{(a+1)^2}$  è definita solo per  $a \neq -1$ , quindi in  $\mathbb{Q} \setminus \{-1\}$  la relazione è definita).

Ora,

$$\begin{aligned} \frac{1}{(a+1)^2} = \frac{1}{(b+1)^2} &\iff (a+1)^2 = (b+1)^2 \iff \\ &\iff \begin{cases} a+1 = b+1 \iff a = b \\ a+1 = -(b+1) \iff b = -a-2 \end{cases} \end{aligned}$$

Ogni classe è quindi  $[a] = \{a, -a-2\}$ .

Il quoziente è in corrispondenza biunivoca con  $(-1, \infty) \cap \mathbb{Q}$ .

- a. La relazione non è riflessiva: infatti non è vero che per ogni  $x \in A$  si ha  $x \sim x$ . Per  $x = 0$  la condizione non è verificata.  
 b. Poniamo  $S = \mathbb{Z} \setminus \{0\}$ . In questo caso la relazione è di equivalenza.  
 Riflessiva:  $\forall s \in S$   $s \sim s$  perché  $s^2 > 0$ .  
 Simmetrica: se  $s \sim t$ , ossia  $st > 0$ , allora  $ts > 0$  e quindi  $t \sim s$ .  
 Transitiva: se  $s \sim t$ ,  $t \sim u$ , allora  $st > 0$ ,  $tu > 0$ , il che significa che  $s$  e  $t$  sono concordi (o entrambi positivi, o entrambi negativi) e anche  $t$  ed  $u$  sono concordi, da cui  $s$  e  $u$  sono concordi, cioè  $s \sim u$ .  
 c. Dato un intero  $a$  diverso da zero, ossia appartenente a  $S$ ,

$$[a] = \{x \in S \mid x \sim a\} = \{x \in S \mid xa > 0\}$$

quindi la classe  $[a]$  consiste di tutti gli elementi di  $S$  di segno concorde ad  $a$ : se  $a > 0$  la classe  $[a]$  consiste di tutti gli interi positivi, se  $a$  è negativo,  $[a]$  consiste di tutti gli interi negativi. In definitiva,  $S/\sim$  consiste di due classi.

• Non è riflessiva: infatti  $m\rho m$  significa  $m = m \cdot 2^k$  per qualche  $k \in \mathbb{Z}$  dispari e questo è evidentemente falso.

È simmetrica: infatti se  $m\rho n$ , allora  $m = n \cdot 2^k$  per qualche  $k$  dispari in  $\mathbb{Z}$ . Allora  $n = m \cdot 2^{-k}$  e  $-k$  è ancora intero e dispari.

Non è transitiva: basta dare un controsenso.  $6\rho 3$  (perché  $6 = 3 \cdot 2^1$ ),  $3\rho 6$  (perché  $3 = 6 \cdot 2^{-1}$ ), ma 6 non è in relazione con 6.

Non è antisimmetrica: dal punto precedente,  $3\rho 6$ ,  $6\rho 3$  ma  $3 \neq 6$ .

Non è quindi né una relazione di equivalenza, né una relazione d'ordine.

• È riflessiva: infatti per ogni  $m \in \mathbb{N}$   $m\rho m$  perché  $m = m \cdot 2^0$  e 0 è un intero pari.

È simmetrica: infatti se  $m\rho n$ , allora  $m = n \cdot 2^k$  per qualche  $k$  pari in  $\mathbb{Z}$ . Allora  $n = m \cdot 2^{-k}$  e  $-k$  è ancora intero e pari.

È transitiva: per ogni  $m, n, r \in \mathbb{N}$  se  $m\rho n$  e  $n\rho r$  si ha  $m = n \cdot 2^h$  con  $h$  intero pari,  $n = r \cdot 2^k$  con  $k$  intero pari. Quindi  $m = r \cdot 2^{h+k}$  e  $h+k$  è ancora un intero pari, da cui  $m\rho r$ .

Non è antisimmetrica. Basta dare un controsenso:  $12\rho 3$  perché  $12 = 3 \cdot 2^2$ ,  $3\rho 12$  perché  $3 = 12 \cdot 2^{-2}$ , ma  $3 \neq 12$ .

È una relazione di equivalenza, non è una relazione d'ordine.

L'unica classe di equivalenza finita è la classe dello 0 che consiste nel solo elemento 0. Tutte le altre sono infinite: per esempio

$$\begin{aligned}[1] &= \{n \in \mathbb{N} \mid n = 1 \cdot 2^h, \text{ per qualche } h \text{ pari in } \mathbb{Z}\} = \{2^h, h \text{ pari } \in \mathbb{N}\} = \\ &= \{1, 2^2, 2^4, 2^6, \dots\}\end{aligned}$$

$$\begin{aligned}[2] &= \{n \in \mathbb{N} \mid n = 2 \cdot 2^h, \text{ per qualche } h \text{ pari in } \mathbb{Z}\} = \{2^{h+1}, h \text{ pari } \in \mathbb{N}\} = \\ &= \{2, 2^3, 2^5, 2^7, \dots\}\end{aligned}$$

$$\begin{aligned}[3] &= \{n \in \mathbb{N} \mid n = 3 \cdot 2^h, \text{ per qualche } h \text{ pari in } \mathbb{Z}\} = \{3 \cdot 2^h, h \text{ pari } \in \mathbb{N}\} = \\ &= \{3, 12, 48, \dots\}\end{aligned}$$

$$[4] = [1], \quad [5] = \{5, 20, 80, \dots\}, \quad [6] = \{6, 24, \dots \text{ecc.}\}$$

Proseguite voi. Controllate che siano davvero una partizione di  $\mathbb{N}$ .

- È riflessiva. Non è simmetrica, perché  $(a, c) \in R$  ma  $(c, a) \notin R$ . Non è antisimmetrica, perché  $(b, d) \in R$ ,  $(d, b) \in R$ , ma  $b \neq d$ . È transitiva. Non è di equivalenza poiché non simmetrica.

Aggiungendo la coppia  $(c, a)$  si ottiene però una relazione di equivalenza  $\sigma$  (la relazione di equivalenza associata alla partizione  $\{\{a, c\}, \{b, d\}, \{e\}\}$ ).  $\sigma$  ha 3 classi di equivalenza:  $\{a, c\}$ ,  $\{b, d\}$ ,  $\{e\}$ ; le prime due classi hanno 2 elementi e la terza classe ha un elemento. L'insieme quoziante è  $\{\{a, c\}, \{b, d\}, \{e\}\}$ .

- $R$  è riflessiva, perché ogni stringa bit ha ovviamente lo stesso numero di 1 di se stessa.  $R$  è simmetrica, perché se  $x$  ha lo stesso numero di 1 della stringa bit  $y$ , allora  $y$  ha lo stesso numero di 1 della stringa bit  $x$ . È transitiva, perché se  $x$  ha lo stesso numero di 1 della stringa bit  $y$ , e  $y$  ha lo stesso numero di 1 della stringa bit  $z$ , allora  $x$  ha lo stesso numero di 1 della stringa bit  $z$ .

- a. No. Per esempio,  $1\rho 3$  e  $3\rho 5$  ma non è vero che  $1\rho 5$ .  
 b. Sì, infatti  $a\rho b$  se e solo se  $a + b$  è multiplo di 4, se e solo se  $b + a$  è multiplo di 4, se e solo se  $b\rho a$ .  
 c. No. Per esempio, non è vero che  $1\rho 1$ .  
 d.  $a\rho 3$  se e solo se  $a + 3$  è multiplo di 4, cioè  $a + 3 = 4h$ , per qualche  $h \in \mathbb{Z}$ , se e solo se  $a = -3 + 4h$ , per qualche  $h \in \mathbb{Z}$ , se e solo se  $a$  è congruo a 1 modulo 4. L'insieme è quindi infinito.

- a. No. Per esempio,  $1\rho 5$  e  $5\rho 7$  ma non è vero che  $1\rho 7$ .  
 b. Sì, infatti  $a\rho b$  se e solo se  $a + b$  è multiplo di 6, se e solo se  $b + a$  è multiplo di 6, se e solo se  $b\rho a$ .  
 c. No. Per esempio, non è vero che  $1\rho 1$ .  
 d.  $a\rho 3$  se e solo se  $a + 3$  è multiplo di 6, cioè  $a + 3 = 6h$ , per qualche  $h \in \mathbb{Z}$ , se e solo se  $a = -3 + 6h$ , per qualche  $h \in \mathbb{Z}$ , se e solo se  $a$  è congruo a 3 modulo 6. L'insieme è quindi infinito.

- $R = \{(1, 18), (2, 9), (3, 6), (6, 3), (9, 2), (18, 1)\}$ .  $R$  è quindi finito.  
 La relazione è simmetrica, ma non transitiva, non riflessiva, e non antisimmetrica.

- a.  $\rho$  è una relazione da  $\mathbb{N}^+$  in  $\mathbb{N}^+$  perché consiste del sottoinsieme di  $\mathbb{N}^+ \times \mathbb{N}^+$  costituito dalle coppie  $(m, n)$  ( $m, n \in \mathbb{N}^+$ ) tali che esista un  $k \in \mathbb{Z}$  tale che  $m = 2^k \cdot n$ . Quindi dati comunque due numeri naturali  $m$  e  $n$  è possibile stabilire se sono o non sono in relazione: per esempio  $3\rho 6$ , perché  $3 = 2^{-1}6$ ,  $20\rho 5$  perché  $20 = 2^2 \cdot 5$ .  $\rho$  sarà

quindi il sottoinsieme di  $\mathbb{N}^+ \times \mathbb{N}^+$  costituito dalle coppie  $(m, n)$ , dove  $m, n \in \mathbb{N}^+$  e  $m = 2^r n$  oppure  $n = 2^s m$  per qualche  $r, s \in \mathbb{N}$ .

Non è una funzione, perché per esempio 3 compare come primo elemento di più di una coppia (per esempio di  $(3, 6)$  e di  $(3, 12)$ ).

- b. Da quanto detto nel punto precedente segue chiaramente che la relazione è sia riflessiva sia simmetrica. È anche transitiva, dato che se  $m\rho n$  e  $n\rho p$  significa che esistono  $h, k \in \mathbb{Z}$  tali che  $\frac{m}{n} = 2^h$  e  $\frac{n}{p} = 2^k$ , da cui  $\frac{m}{p} = \frac{m}{n} \cdot \frac{n}{p} = 2^h \cdot 2^{-k} = 2^{h-k}$  e  $h - k$  sta in  $\mathbb{Z}$  per cui  $m\rho p$ . Quindi si tratta di una relazione di equivalenza.

Non è antisimmetrica: per esempio,  $1\rho 8$ ,  $8\rho 1$  ma  $1 \neq 8$ .

- c. Le classi di equivalenza sono:

$$[1] = \{2^h, h \in \mathbb{N}\}$$

$$[3] = \{3 \cdot 2^h, h \in \mathbb{N}\} = [6] = [12] = [24] = \dots$$

$$[5] = \{5 \cdot 2^h, h \in \mathbb{N}\}$$

...

In generale sono in corrispondenza biunivoca con tutti i numeri naturali dispari. Quindi l'insieme quoziante  $\mathbb{N}^+/\rho$  è in corrispondenza biunivoca con i numeri dispari. Ogni classe di equivalenza è costituita da infiniti elementi.

- a. Tutti gli elementi della classe  $[P]$  hanno la stessa immagine mediante la proiezione  $\pi$ , per cui

$$[P] = [Q] \iff P \rho_\pi Q \iff \pi(P) = \pi(Q) \iff \Psi([P]) = \Psi([Q]).$$

Questo dimostra al tempo stesso che la  $\Psi$  è ben definita ed è iniettiva.

- b.  $\Psi$  è suriettiva: si tratta di provare che  $\forall P' \in C$  esiste una classe  $[P]$  tale che  $\Psi([P]) = P'$ . Basta prendere la generatrice del cilindro passante per  $P'$ : questa intersecherà l'elica in vari punti, ciascuno dei quali si proietta in  $P'$ .

## SOLUZIONI RELATIVE AL CAPITOLO 2

$$\sum_{k=0}^9 (-1)^k \frac{1}{k+1} = \sum_{k=1}^{10} (-1)^{k+1} \frac{1}{k}.$$

$$\sum_{i=1}^2 \sum_{j=1}^3 (i+j) = \sum_{i=1}^2 [(i+1) + (i+2) + (i+3)] = \sum_{i=1}^2 (3i+6) = (3+6) + (3 \cdot 2 + 6) = 21.$$

$$\sum_{i=1}^n \sum_{j=1}^m a_{i,j} = \sum_{i=1}^n (\sum_{j=1}^m a_{i,j}) = \sum_{i=1}^n (a_{i,1} + a_{i,2} + \dots + a_{i,m}) = (a_{1,1} + a_{1,2} + \dots + a_{1,m}) + (a_{2,1} + a_{2,2} + \dots + a_{2,m}) + \dots + (a_{n,1} + a_{n,2} + \dots + a_{n,m}).$$

$$\sum_{j=1}^m \sum_{i=1}^n a_{i,j} = \sum_{j=1}^m (a_{1,j} + a_{2,j} + \dots + a_{n,j}) = (a_{1,1} + a_{2,1} + \dots + a_{n,1}) + (a_{1,2} + a_{2,2} + \dots + a_{n,2}) + \dots + (a_{1,m} + a_{2,m} + \dots + a_{n,m}).$$

Utilizzando le proprietà associativa e commutativa dei numeri si vede che le due espressioni sono uguali.

a.  $a_{10} = \frac{1}{3+10} = \frac{1}{13}$  e  $b_{10} = 10^2 + 2 = 102$ .

b. Per esprimere con il simbolo di sommatoria  $a_0 + a_2 + a_4 + \dots + a_{28}$ , basta scrivere:

$$\sum_{k=0}^{14} a_{2k}, \text{ ossia } \sum_{k=0}^{14} \frac{1}{3+2k}.$$

a.  $a_{10} = \frac{1}{101}$  e  $b_{10} = 35$ .

b. Per esprimere con il simbolo di sommatoria  $a_0 + a_2 + a_4 + \dots + a_{28}$ , basta scrivere:

$$\sum_{k=0}^{14} a_{2k}, \text{ ossia } \sum_{k=0}^{14} \frac{1}{(2k)^2 + 1}.$$

Si tratta di stabilire che legame c'è tra  $i$  e  $j$ : si ha  $i = j + 4$ . Infatti per  $i = 4$  si ha  $j = 0$ , mentre per  $i = 8$ ,  $j = 4$ . In definitiva,

$$b_j = \frac{3^{j+4+1}}{5(j+4)} = \frac{3^{j+5}}{5j+20}.$$

Infatti  $b_0 = a_4 = \frac{3^5}{20}$ ,  $b_1 = a_5 = \frac{3^6}{28}$ , ecc.

Dovremo provare:

- La base dell'induzione:  $P(1)$  è verificata perché per  $n = 1$  entrambi i membri di (3.1) si riducono a  $2^3$ .
- Il passo induttivo: per ogni  $n$  supposta vera  $P(n-1)$ , dimostriamo  $P(n)$ . La  $P(n-1)$  (che stiamo supponendo vera) è:

$$(*) \quad \underbrace{2^3 + 4^3 + 6^3 + \dots + (2(n-1))^3}_{n-1 \text{ addendi}} = 2(n-1)^2 n^2$$

Aggiungendo ad ambo i membri della (\*) il termine  $(2n)^3$  si ha

$$\begin{aligned} 2^3 + 4^3 + 6^3 + \dots + (2(n-1))^3 + (2n)^3 &= 2(n-1)^2 n^2 + (2n)^3 \\ &= 2n^2[(n-1)^2 + 4n] \\ &= 2n^2(n+1)^2 \end{aligned}$$

che è esattamente  $P(n)$ .

Supponiamo per assurdo che esista un  $a \in \mathbb{N}$  tale che  $0 < a < 1$ . Allora l'insieme  $T = \{a \in \mathbb{N} \mid 0 < a < 1\}$  è non vuoto e pertanto possiede minimo  $m$ . Moltiplicando per  $m > 0$  ogni membro della  $0 < m < 1$  si ottiene  $0 < m^2 < m < 1$  che contraddice la minimalità di  $m$ .

Per induzione su  $n$ . Per  $n = 0$  si ha  $1 = 1$ , quindi la base dell'induzione è vera. Supponendo vera la  $\sum_{k=0}^{n-1} (4k+1) = (2(n-1)+1)n$ , dimostriamolo per  $n$ .  $\sum_{k=0}^n (4k+1) = \sum_{k=0}^{n-1} (4k+1) + 4n+1 = 2n^2 + 3n + 1 = (2n+1)(n+1)$ . Quindi la proposizione è vera per ogni  $n$ .

Per  $n = 1$  è vera.

Supponiamo vera la  $1^2 + 2^2 + 3^2 + \dots + (n-1)^2 = ((n-1)n(2(n-1)+1))/6$  e dimostriamola per  $n$ .  $1^2 + 2^2 + 3^2 + \dots + n^2 = ((n-1)n(2(n-1)+1))/6 + n^2 = (n(n+1)(2n+1))/6$ . Quindi la formula è vera per ogni  $n$ .

Per  $n = 1$  si ottiene  $5 = 5$ , e la base dimostrata.

Supponiamo l'uguaglianza vera per  $n$ , e dimostriamola per  $n+1$ . Dobbiamo cioè dimostrare:

$$1 + 4 + 7 + \dots + (3n+1) + (3(n+1)+1) = \frac{3(n+1)^2 + 5(n+1) + 2}{2}.$$

Usando l'ipotesi induttiva, il primo membro diventa:

$$1 + 4 + 7 + \dots + (3n+1) + (3(n+1)+1) = \frac{3n^2 + 5n + 2}{2} + (3(n+1)+1) = \frac{3n^2 + 11n + 10}{2}.$$

e semplici calcoli mostrano che la tesi è verificata.

Per  $n = 1$  si ottiene  $7 = 7$ , e la base è dimostrata.

Supponiamo l'uguaglianza vera per  $n$ , e dimostriamola per  $n+1$ . Dobbiamo cioè dimostrare:

$$2 + 5 + 8 + \dots + (3n+2) + (3(n+1)+2) = \frac{3(n+1)^2 + 7(n+1) + 4}{2}.$$

Usando l'ipotesi induttiva, il primo membro diventa:

$$2 + 5 + 8 + \dots + (3n+2) + (3(n+1)+2) = \frac{3n^2 + 7n + 4}{2} + (3(n+1)+2) = \frac{3n^2 + 13n + 14}{2}$$

e semplici calcoli mostrano che la tesi è verificata.

Per induzione su  $n = |X|$ . Se  $n = 1$ , il numero di sottoinsiemi di  $X$  è 2, quindi la formula vale. Supponiamo vero che ogni insieme  $X$  con  $n-1$  elementi abbia  $2^{n-1}$  sottoinsiemi e dimostriamolo se  $|X| = n$ . Fissiamo un elemento  $x \in X$ . L'insieme  $X \setminus \{x\}$  possiede  $n-1$  elementi, e quindi possiede  $2^{n-1}$  sottoinsiemi. Per ottenere i sottoinsiemi di  $X$  si devono aggiungere a questi  $2^{n-1}$  sottoinsiemi quegli altri  $2^{n-1}$  che si ottengono da quelli aggiungendo l'elemento  $x$ . In tutto si hanno allora  $2^{n-1} + 2^{n-1} = 2^n$  sottoinsiemi.

Il passo induttivo (che invece deve valere per ogni  $n$ ) non vale per  $n = 2$ . In questo caso infatti l'intersezione dei due insiemi con  $n-1$  elementi è vuota.

Per induzione sul numero  $n$  di tutte le rette. Se  $n = 1$  è ovvio che bastano due colori. Supponiamo quindi di avere provato che è possibile colorare con due soli colori le regioni formate da meno di  $n$  rette, e dimostriamolo nel caso in cui si aggiunga la  $n$ -esima retta,  $r$ . Dividiamo le regioni in due gruppi, a seconda del lato in cui si trovano rispetto alla  $r$ . Basta allora lasciare invariata la colorazione di tutte le regioni che si trovano da una delle due parti e scambiare invece il colore di quelle che si trovano dall'altra parte. Dobbiamo verificare che si tratta di una "buona" colorazione: infatti, se due regioni confinanti si trovano dalla stessa parte della  $r$ , avranno colorazioni diverse (avevano colorazioni diverse prima dell'aggiunzione della  $r$ , e ora o manterranno i loro colori, o questi saranno invertiti, ma comunque saranno diversi). Se le due regioni si trovano da lati opposti rispetto alla  $r$ , i loro colori saranno diversi, perché il colore di una delle due è stato invertito.

Sia  $q+1$  il più piccolo intero positivo tale che  $b(q+1) > a$  (tale minimo esiste sicuramente, considerando l'insieme [non vuoto!]  $T = \{x \in \mathbb{N} \mid bx > a\}$ ). Sarà pertanto  $bq \leq a < b(q+1)$ , da cui  $0 \leq a - bq < b$ . Posto  $r = a - bq$ , si ha  $a = bq + r$ ,  $0 \leq r < b$ .

- a. L'incasso totale è dato da  $1+2+3+\dots+100$  euro. Ora, questa quantità corrisponde ad un incasso di

$$\frac{100 \cdot (100+1)}{2} = \frac{10100}{2} = 5050 \text{ euro.}$$

- b. I biglietti gratuiti (cioè i biglietti che sono multipli di 5 compresi tra 1 e 100) costano

$$5(1+2+\dots+20) = 5 \frac{20(1+20)}{2} = 5 \cdot 210 = 1050 \text{ euro.}$$

In definitiva la seconda lotteria incassa  $5050 - 1050 = 4000$  euro.

- Per  $n = 1$  la  $f_1 > ((1 + \sqrt{5})/2)^{-1}$  è vera. Posto  $\alpha = (1 + \sqrt{5})/2$ , supponiamo vera la  $f_m > \alpha^{m-2}$  per ogni  $m < n$  e dimostriamola per  $n$ . Si ha  $f_n = f_{n-1} + f_{n-2} > \alpha^{n-3} + \alpha^{n-4} = \alpha^{n-4}(\alpha + 1) = \alpha^{n-4}\alpha^2 = \alpha^{n-2}$ .

- L'equazione caratteristica è  $x^2 - x - 2$ , con radici (distinte)  $-1$  e  $2$ . La soluzione generale è quindi  $a_n = c_1 2^n + c_2 (-1)^n$ . Sostituendo i valori iniziali si ottiene  $-4 = c_1 + c_2$  e  $7 = 2c_1 - c_2$ , da cui si ricava  $c_1 = 1$  e  $c_2 = -5$ .

- La soluzione è quindi  $a_n = 2^n - 5 \cdot (-1)^n$ , da cui si ricavano  $a_8 = 2^8 - 5 = 251$  e  $a_9 = 2^9 + 5 = 517$ .

- L'equazione caratteristica è  $x^2 + x - 2$ , con radici (distinte)  $1$  e  $-2$ . La soluzione generale è quindi  $a_n = c_1 1^n + c_2 (-2)^n$ . Sostituendo i valori iniziali si ottiene  $5 = c_1 + c_2$  e  $2 = c_1 - 2c_2$ , da cui si ricava  $c_1 = 4$  e  $c_2 = 1$ .

- La soluzione è quindi  $a_n = 4 \cdot 1^n + (-2)^n$  da cui si ricavano  $a_8 = 4 + 2^8 = 260$  e  $a_9 = 4 - 2^9 = -508$ .

- L'equazione caratteristica è  $x^2 - x - 2$ , con radici (distinte)  $-1$  e  $2$ . La soluzione generale è quindi  $a_n = c_1 2^n + c_2 (-1)^n$ . Sostituendo i valori iniziali si ottiene  $-3 = c_1 + c_2$  e  $6 = 2c_1 - c_2$ , da cui si ricava  $c_1 = 1$  e  $c_2 = -4$ .

- La soluzione è quindi  $a_n = 2^n - 4 \cdot (-1)^n$ , da cui si ricavano  $a_8 = 2^8 - 4 = 252$  e  $a_9 = 2^9 + 4 = 516$ .

- L'equazione caratteristica è  $x^2 + x - 2$ , con radici (distinte)  $1$  e  $-2$ . La soluzione generale è quindi  $a_n = c_1 1^n + c_2 (-2)^n$ . Sostituendo i valori iniziali si ottiene  $6 = c_1 + c_2$  e  $3 = c_1 - 2c_2$ , da cui si ricava  $c_1 = 5$  e  $c_2 = 1$ .

- La soluzione è quindi  $a_n = 5 \cdot 1^n + (-2)^n$  da cui si ricavano  $a_8 = 5 + 2^8 = 261$  e  $a_9 = 5 - 2^9 = -507$ .

- Equazione caratteristica:  $x^2 - 6x + 8 = 0$ , che ammette come radici:  $r_1 = 2$ ,  $r_2 = 4$ . Le radici sono distinte, quindi  $a_n = c_1 2^n + c_2 4^n$ .

Per  $n = 0$  si ha  $c_1 + c_2 = 0$ , per  $n = 1$  si ha  $2c_1 + 4c_2 = 1$ . Risolvendo il sistema

$$\begin{cases} c_1 + c_2 = 0 \\ 2c_1 + 4c_2 = 1 \end{cases}$$

si ottiene la soluzione  $(c_1, c_2) = (-\frac{1}{2}, \frac{1}{2})$ . Quindi  $a_n = -\frac{1}{2}2^n + \frac{1}{2}4^n$ .

- Equazione caratteristica:  $x^2 + 2x - 15 = 0$ , che ammette come radici:  $r_1 = 3$ ,  $r_2 = -5$ . Le radici sono distinte, quindi

$$a_n = c_1 3^n + c_2 (-5)^n.$$

Per  $n = 0$  si ha  $c_1 + c_2 = 0$ , per  $n = 1$  si ha  $3c_1 + (-5)c_2 = 1$ . Risolvendo il sistema

$$\begin{cases} c_1 + c_2 = 0 \\ 3c_1 - 5c_2 = 1 \end{cases}$$

si ottiene la soluzione  $(c_1, c_2) = (\frac{1}{8}, -\frac{1}{8})$ . Quindi  $a_n = \frac{1}{8}3^n - \frac{1}{8}(-5)^n$ .

- L'equazione caratteristica è  $r^2 - 9r + 20 = 0$ , da cui  $r_1 = 5$ ,  $r_2 = 4$  (distinte). La soluzione generale è pertanto:  $a_n = c_1 \cdot 5^n + c_2 \cdot 4^n$ .

Imponendo le condizioni iniziali, si ottiene:  $1 = a_0 = c_1 + c_2$ ,  $1 = a_1 = 5c_1 + 4c_2$ , da cui si ricava  $c_2 = 4$  e  $c_1 = -3$ , per cui la soluzione è:  $a_n = (-3) \cdot 5^n + 4 \cdot 4^n$ .

- a. Applicando la condizione  $a_{n+1} = a_n + 6a_{n-1}$  per  $n = 3$  si ottiene  $a_4 = 11 + 6 \cdot 17 = 113$ . Altrimenti, si può applicare la formula ottenuta rispondendo al punto b).

- b. Equazione caratteristica  $x^2 - x - 6 = 0$  con radici (distinte)  $x = 3$  e  $x = -2$ . La formula chiusa è quindi del tipo  $a_n = c_1 3^n + c_2 (-2)^n$ .

Applicando le condizioni iniziali si ottiene  $a_2 = 17 = c_1 3^2 + c_2 (-2)^2 = 9c_1 + 4c_2$  e  $a_3 = 11 = c_1 3^3 + c_2 (-2)^3 = 27c_1 - 8c_2$  da cui si ricava  $c_1 = 1$  e  $c_2 = 2$ . La formula chiusa è quindi  $a_n = 3^n + 2(-2)^n$ , da cui si poteva ricavare  $a_4 = 81 + 2 \cdot 16 = 113$ .

N.B. Fare attenzione ai segni e all'uso delle parentesi!

- In ciascuno dei casi, se esiste una successione, questa deve avere equazione caratteristica  $r^2 + r - 6 = 0$ ; radici  $r = 2$ ,  $r = -3$  (distinte), quindi la formula chiusa dovrebbe essere del tipo  $a_n = c_1 (-3)^n + c_2 2^n$ .

Nel caso a. si ricava  $a_0 = 1 = c_1 + c_2$ . Siccome esistono infiniti valori di  $c_1$  e  $c_2$  che soddisfano a questa uguaglianza, esistono infinite successioni che soddisfano a.

Nel caso b. si ricava  $a_0 = 1 = c_1 + c_2$ ,  $a_1 = 12 = -3c_1 + 2c_2$ , da cui necessariamente  $c_1 = -2$  e  $c_2 = 3$ . Quindi esiste un'unica successione che soddisfa b., cioè la successione data dalla formula  $a_n = -2(-3)^n + 3 \cdot 2^n$ .

Se una successione soddisfa le condizioni date nel caso c., soddisfa anche tutte le condizioni date nel caso b., quindi, se esiste, tale successione è quella trovata in b.:  $a_n = -2(-3)^n + 3 \cdot 2^n$ . Questa successione soddisfa anche alla quarta condizione  $a_4 = -114$ , quindi è l'unica successione che soddisfa le condizioni date in c.

Se una successione soddisfa le condizioni date nel caso d., soddisfa anche tutte le condizioni date nel caso b., quindi, se esiste, tale successione è quella trovata in b.:  $a_n = -2(-3)^n + 3 \cdot 2^n$ . Questa successione, però, non soddisfa la quarta condizione  $a_4 = 210$ , quindi non esiste nessuna successione che soddisfi le condizioni date in d.

- a.  $A(1, 3) = A(0, A(1, 2)) = A(1, 2) + 1 = A(0, A(1, 1)) + 1 = A(1, 1) + 1 + 1 = A(0, A(1, 0)) + 2 = A(1, 0) + 3 = A(0, 1) + 3 = 1 + 1 + 3 = 5$  da cui  $A(1, 4) = A(0, A(1, 3)) = A(1, 3) + 1 = 5 + 1 = 6$ .

- b.  $A(2, 2) = 7$ .

- c.  $A(3, 2) = 29$ .

- d.  $A(1, n) = A(0, A(1, n-1)) = A(1, n-1) + 1 = A(0, A(1, n-2)) + 1 = A(1, n-2) + 2 = \dots = A(1, 0) + n = A(0, 1) + n = n + 2$ .

- e.  $A(2, n) = A(1, A(2, n-1)) = A(2, n-1) + 2 = A(1, A(2, n-2)) + 2 = A(2, n-2) + 4 = \dots = A(2, 0) + 2n = A(1, 1) + 2n = 2n + 3$ .

- f.  $a_1 = 5a_0 + 2 = 5 \cdot 2 + 2$

$$a_2 = 5a_1 + 2 = 5(5 \cdot 2 + 2) + 2 = 5^2 2 + 5 \cdot 2 + 2$$

$$a_3 = 5a_2 + 2 = 5(5^2 2 + 5 \cdot 2 + 2) + 2 = 5^3 2 + 5^2 \cdot 2 + 5 \cdot 2 + 2 = (5^3 + 5^2 + 5 + 1)2$$

.....  
 $a_n = (5^n + 5^{n-1} + 5^{n-2} + \dots + 5 + 1)2$   
 Ricordando che  $5^n + 5^{n-1} + 5^{n-2} + \dots + 5 + 1 = \frac{5^{n+1}-1}{4}$  abbiamo la formula generale

$$a_n = \frac{5^{n+1}-1}{2}$$

Per determinare a quale mese le azioni raggiungeranno 1562 euro, dobbiamo determinare il valore  $n$  tale che

$$\frac{5^{n+1}-1}{2} = 1562, \text{ ossia } 5^{n+1} = 3125$$

Osservando che  $3125 = 5^5$ , ne segue che le azioni  $a$  raggiungeranno il valore di 1562 euro dopo 4 mesi.

La formula risolutiva per le seconde azioni è invece ovviamente  $b_n = n + 2$ , per cui le seconde azioni raggiungeranno il valore di 1562 euro dopo 1560 mesi (= 130 anni!!).

### SOLUZIONI RELATIVE AL CAPITOLO 3

1) Risulta  $0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$ , da cui  $(-a) \cdot b = -(a \cdot b)$ .  
 $(-a)(-b) = (\text{per il punto 2 della proposizione 3.1}) = -(a(-b)) = -(-(ab)) = ab$ .

2) Sia  $S = \{xa + yb \mid x, y \in \mathbb{Z}, xa + yb > 0\} \subseteq \mathbb{N}$ .  $S$  è sicuramente non vuoto, perché  $a$  e  $b$  non sono entrambi nulli e quindi, se per esempio  $a$  è diverso da zero, sarà certamente  $a > 0$  o  $-a > 0$  e quindi  $a$  o  $-a$  starà in  $S$ . Esisterà pertanto un minimo: sia esso  $d = x_0a + y_0b$ . Proveremo che  $d$  è un massimo comun divisore di  $a$  e  $b$ . La (ii) è ovviamente verificata. Per provare che  $d \mid a$  e  $d \mid b$ , dividiamo  $a$  per  $d$ : si ha  $a = dq + r$ , con  $0 \leq r < d$ . Ora,  $0 \leq r = a - dq = a(x_0a + y_0b)q = (1 - x_0)a + (-y_0q)b < d$ ; per non contraddirre la minimalità di  $d$ , deve essere  $r = 0$ , e quindi  $d \mid a$ . Analogamente si prova che  $d \mid b$ . Abbiamo dimostrato in questo modo contemporaneamente l'esistenza del  $\text{MCD}(a, b)$  e la sua scrittura nella forma  $d = sa + tb$ .

3)  $\text{MCD}(a, b) = \frac{ab}{\text{lcm}(a, b)} = \frac{2^5 \cdot 3^4 \cdot 7^2 \cdot 11^4 \cdot 13^2}{2^3 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13^2} = 2^2 \cdot 3^2 \cdot 7 \cdot 11^3$ .

4) Basta scegliere  $a = f_{n+2}$ ,  $b = f_{n+1}$ , rispettivamente l' $(n+2)$ -esimo e l' $(n+1)$ -esimo numero di Fibonacci. Infatti

$$\begin{aligned} f_{n+2} &= f_{n+1} \cdot 1 + f_n & 0 < f_n < f_{n+1} \\ f_{n+1} &= f_n \cdot 1 + f_{n-1} & 0 < f_{n-1} < f_n \\ f_n &= f_{n-1} \cdot 1 + f_{n-2} & 0 < f_{n-2} < f_{n-1} \\ f_{n-1} &= f_{n-2} \cdot 1 + f_{n-3} & 0 < f_{n-3} < f_{n-2} \\ &\dots \\ f_4 &= f_3 \cdot 1 + f_2 & 0 < f_2 < f_3 \\ f_3 &= f_2 \cdot 2 + 0 \end{aligned}$$

sono esattamente  $n$  divisioni ( $f_{n-k}$  è diverso da zero fin quando  $k = n-1$ ).

- a. 6. b. 17. c. 1.

5)  $385 = 5 \cdot 7 \cdot 11$ ,  $33 = 11 \cdot 3$ ,  $143 = 11 \cdot 13$ . Quindi  $\text{MCD}(385, 33) = 11$  che divide il termine noto 143. La a) è quindi risolubile. Invece 11 non divide 105, quindi la b) non è risolubile.  
 La a) è equivalente (dividendo primo e secondo membro per 11) alla  $35x + 3y = 13$ .

Mediante l'algoritmo euclideo delle divisioni successive si ha:

$$35 = 3 \cdot 11 + 2 \quad 3 = 2 \cdot 1 + 1$$

da cui si ricava  $1 = 35 \cdot (-1) + 3 \cdot 12$ , e quindi  $13 = 35 \cdot (-13) + 3 \cdot 156$ . Una soluzione è quindi  $(\bar{x}, \bar{y}) = (-13, 156)$ . Tutte le soluzioni si ottengono aggiungendo a questa le soluzioni dell'equazione omogenea associata  $35x + 3y = 0$ , che sono tutte e sole le coppie  $(-3t, 35t)$  al variare di  $t \in \mathbb{Z}$ . In definitiva, tutte e sole le soluzioni di a) sono  $(-13 - 3t, 156 + 35t)$ , al variare di  $t \in \mathbb{Z}$ .

6)  $\text{MCD}(153, 45) = 9$ . Ora, 9 divide 18, mentre 9 non divide 10, quindi la prima equazione ammette soluzioni intere, mentre la seconda no. La prima è equivalente (dividendo tutti gli addendi per 9) a  $17x + 5y = 2$ .

Esprimendo il  $\text{MCD}(17, 5) = 1$  mediante l'identità di Bézout come combinazione di 17 e di 5, si ottiene  $1 = 17 \cdot (-2) + 5 \cdot 7$  da cui si ricava (moltiplicando ogni addendo per 2)  $2 = 17 \cdot (-4) + 5 \cdot 14$ .

Dunque una soluzione dell'equazione è data dalla coppia  $(\bar{x}, \bar{y}) = (-4, 14)$ . Tutte le soluzioni si ottengono aggiungendo alla soluzione data la soluzione generale dell'equazione omogenea associata, ossia  $(5t, -17t)$ , al variare di  $t \in \mathbb{Z}$ . Tutte e sole le soluzioni dell'equazione sono pertanto  $(-4 + 5t, 14 - 17t)$ , al variare di  $t \in \mathbb{Z}$ .

7) Mediante l'algoritmo delle divisioni successive si ottiene:

$$\begin{aligned} 819 &= 221 \cdot 3 + 156 \\ 221 &= 156 + 65 \\ 156 &= 65 \cdot 2 + 26 \\ 65 &= 26 \cdot 2 + 13 \\ 26 &= 13 \cdot 2. \end{aligned}$$

Il  $\text{MCD}(819, 221)$  è dunque 13. Siccome 13 divide 26 e non divide 28, (a) ha soluzione, mentre (b) non ha soluzione.

Per trovare una soluzione, si ricava:

$$\begin{aligned} 156 &= (1, 0) + (0, 1)(-3) = (1, -3) \\ 65 &= (0, 1) + (1, -3)(-1) = (-1, 4) \\ 26 &= (1, -3) + (-1, 4)(-2) = (3, -11) \\ 13 &= (-1, 4) + (3, -11)(-2) = (-7, 26). \end{aligned}$$

Quindi  $13 = 819 \cdot (-7) + 221 \cdot 26$  da cui, moltiplicando per 2:  $26 = 819 \cdot (-14) + 221 \cdot 52$  e una scelta possibile è  $\bar{x} = -14$ ,  $\bar{y} = 52$ .

Una volta trovata una soluzione, tutte le altre sono

$$(-14 + 221 \cdot \frac{t}{13}, 52 - 819 \cdot \frac{t}{13}) = (-14 + 17t, 52 - 63t), \quad t \in \mathbb{Z}.$$

8)  $85 = 17 \cdot 5$ ,  $51 = 17 \cdot 3$ . Quindi  $\text{MCD}(85, 51) = 17$  che divide 68 ( $68 = 17 \cdot 4$ ) ma non divide 78. Quindi la prima non è risolubile, mentre la seconda lo è. Dividendo entrambi i membri dell'equazione per 17 si ottiene  $5x + 3y = 4$ .

Con l'algoritmo euclideo si ha:

$$5 = 3 \cdot 1 + 2 \quad 3 = 2 \cdot 1 + 1$$

da cui  $1 = 5(-1) + 3 \cdot 2$ . Moltiplicando tutto per 4 si ha  $5(-4) + 3 \cdot 8 = 4$  ossia la coppia  $(-4, 8)$  è soluzione dell'equazione.

N.B. Allo stesso risultato si perveniva anche se non avessimo diviso per 17. In questo caso infatti

$$85 = 51 \cdot 1 + 34, \quad 51 = 34 \cdot 1 + 17$$

da cui  $17 = 85(-1) + 51 \cdot 2$ . Quindi, dato che  $78 = 17 \cdot 4$ , una soluzione dell'equazione è data da  $(-4, 8)$ .

Tutte le altre si ottengono aggiungendo tutte le soluzioni dell'equazione omogenea associata, ossia  $85x + 51y = 0$  che conviene scrivere come  $5x + 3y = 0$ , le cui soluzioni sono  $(-3t, 5t)$  al variare di  $t \in \mathbb{Z}$ . In definitiva tutte e sole le soluzioni dell'equazione originaria sono  $(-4 - 3t, 8 + 5t)$ ,  $t \in \mathbb{Z}$ .

N.B. Se avessimo lasciato  $85x + 51y = 0$ , anziché dividere per 17, le soluzioni sarebbero state del tipo  $(-51\frac{t}{17}, 85\frac{t}{17})$  cioè  $(-51\frac{t}{17}, 85\frac{t}{17}) = (-3t, 5t)$ ,  $t \in \mathbb{Z}$ , ritrovando (ovviamente) il risultato precedente.

Si consideri l'equazione diofantea

$$8747x + 8717y = 120.$$

Dato che  $8747 - 8717 = 30$ , la equazione ammette la soluzione  $(4, -4)$ . Allora, in virtù della proposizione 3.6, il MCD  $(8747, 8717)$  divide certamente il termine noto 120. Potete controllare che in effetti, con l'algoritmo euclideo delle divisioni successive,  $\text{MCD}(8747, 8717) = 1$ .

$2^{14} = (2^7 - 1)(2^7 + 1) = 127 \cdot 129 = 127 \cdot 3 \cdot 43$  e tutti i fattori sono primi.

## SOLUZIONI RELATIVE AL CAPITOLO 4

Basta osservare che  $\mathbb{N}$  contiene gli interi pari, che sono in corrispondenza biunivoca con  $\mathbb{N}$  (tramite la  $f(n) = 2n$ ).

Dimostriamo solo il punto b. Dato  $r \in \mathbb{R}$ , la sua classe di equivalenza è data da  $[r] = \{x \in \mathbb{R} \mid x = r + q, q \in \mathbb{Q}\} = r + \mathbb{Q}$ . In particolare, se  $r \in \mathbb{Q}$  la sua classe di equivalenza è  $\mathbb{Q}$ . Tutte le classi di equivalenza hanno la stessa cardinalità, che è la cardinalità del numerabile, perché sono tutte equipotenti alla classe  $\mathbb{Q}$ . Se l'insieme  $\mathbb{R}/\varrho$  fosse numerabile,  $\mathbb{R}$  sarebbe numerabile anch'esso, come unione di una infinità numerabile di insiemi numerabili (le sue classi).

Ovviamente il primo giorno ha cinque possibilità di scelta, il secondo giorno ne ha quattro, il terzo ne ha tre, e così via fino all'ultimo giorno, in cui ha un'unica possibilità. In totale il numero di possibili scelte è  $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ .

Ci sono  $10 \cdot 10 \cdot 10$  possibili numeri a quattro cifre. Ci sono  $26 \cdot 26 \cdot 26$  possibili modi di utilizzare tre lettere. In tutto quindi il numero di targhe che si possono ottenere è  $10^4 \cdot 26^3 = 17576 \cdot 10^4$ .

$$26 \cdot 1 \cdot 1 \cdot 26 \cdot 26.$$

Una funzione è individuata non appena si conoscono le immagini dei 3 elementi del dominio  $A$ . In quanti modi si possono scegliere tre elementi (eventualmente ripetuti) in un insieme con due elementi? Si tratta del numero di disposizioni con ripetizione di 2 elementi di classe 3, ossia  $2^3$ . Il numero richiesto è pertanto  $2^3$ . Le funzioni da  $A$  a  $B$  sono le seguenti:

$$\begin{array}{llll} f_1: & a_1 \rightarrow b_1 & f_2: & a_1 \rightarrow b_1 \\ & a_2 \rightarrow b_1 & f_2: & a_2 \rightarrow b_1 \\ & a_3 \rightarrow b_1 & f_3: & a_2 \rightarrow b_2 \\ & & f_3: & a_2 \rightarrow b_2 \\ & & & a_3 \rightarrow b_1 \\ \\ f_5: & a_1 \rightarrow b_2 & f_6: & a_1 \rightarrow b_2 \\ & a_2 \rightarrow b_2 & f_6: & a_2 \rightarrow b_2 \\ & a_3 \rightarrow b_2 & f_7: & a_2 \rightarrow b_1 \\ & & f_7: & a_2 \rightarrow b_1 \\ & & & a_3 \rightarrow b_2 \\ & & f_8: & a_2 \rightarrow b_2 \\ & & f_8: & a_3 \rightarrow b_2. \end{array}$$

$m^n$ : infatti per ciascuno degli  $n$  elementi di  $A$  ci sono  $m$  scelte per la sua immagine, quindi ....

Un sottoinsieme è individuato decidendo, per ciascuno dei dodici elementi dell'insieme, se appartiene o non al sottoinsieme. Per ogni elemento ci sono quindi 2 possibilità: appartiene o non appartiene. In definitiva, le possibilità totali sono  $2^{12}$ .

La cosa non ci stupisce, perché abbiamo dimostrato per induzione su  $n$  che il numero di sottoinsiemi di un insieme con  $n$  elementi è proprio  $2^n$ .

Quello che si siede al primo posto può essere scelto arbitrariamente (10 in tutto fra ragazzi e ragazze), cioè 10 possibilità. Fissato il primo, il secondo deve essere di sesso opposto, quindi può essere scelto fra 5. Il terzo deve essere del sesso del primo, quindi può essere scelto in 4 modi, e così via.

In tutto le possibilità sono quindi  $10 \cdot 5 \cdot 4 \cdot 4 \cdot 3 \cdot 3 \cdot 2 \cdot 2 \cdot 1 \cdot 1 = 2 \cdot 5! \cdot 5!$ .

L'esercizio si può risolvere più brevemente se si osserva che la disposizione dei 10 ragazzi e ragazze è determinata dalla disposizione di tutti i ragazzi ( $5!$  possibilità), dalla disposizione di tutte le ragazze ( $5!$  possibilità), e dalla scelta di chi sta seduto al primo posto (2 possibilità, maschio o femmina). Siccome queste scelte sono tutte indipendenti l'una dall'altra, si hanno in tutto  $5! \cdot 5! \cdot 2$  possibilità.

$$7!.$$

$n!$ . Le iniettive sono anche suriettive in questo caso.

Ancora  $n!$ .

$m(m-1)(m-2) \cdots (m-n+1)$ . Si tratta del numero di disposizioni semplici di  $m$  elementi di classe  $n$ .

$${9 \choose 4} = 126.$$

Si parta dall'identità  $(n+1)/(k(n-k+1)) = 1/k + 1/(n-k+1)$ . Moltiplicando ambo i membri per  $n!/(k-1)!(n-k)!$  si ottiene

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

$$\text{cioè } {n+1 \choose k} = {n \choose k} + {n \choose k-1}.$$

$${8 \choose 6} = 7! = 5040.$$

Le possibilità sono  $6! \cdot 6! \cdot 2$ .

$f(a_1)$  può essere scelto in 3 modi, così pure  $f(a_2)$ ,  $f(a_4)$  e  $f(a_5)$ . Le scelte sono indipendenti l'una dall'altra, quindi in tutto si hanno  $3^4 = 81$  funzioni.

$${10 \choose 7} = 120.$$

$$3 \cdot 2^5 = 96.$$

● Dal numero totale  $3 \cdot 2^5$  si devono sottrarre le seguenti configurazioni: quelle in cui sono presenti solo votazioni 28 e 29, che sono in tutto  $2 \cdot 1 \cdot 1 \cdot 1$ ; quelle in cui sono presenti solo votazioni 28 e 30, che sono in tutto  $2 \cdot 1 \cdot 1 \cdot 1$ ; quelle in cui sono presenti solo votazioni 29 e 30, che sono in tutto  $2 \cdot 1 \cdot 1 \cdot 1$ . Quindi il numero richiesto è  $3 \cdot 2^5 - 6 = 90$ .

$$\text{● } \frac{10!}{2!2!3!} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4!}{4 \cdot 3 \cdot 2} = 151\,200.$$

- a. Con 20 euro può comprare 4 CD a 5 euro l'uno, quindi può effettuare  $\binom{7}{4} = 35$  scelte.  
 b. Se vuole spendere esattamente 20 euro, deve scegliere se comprare 5 CD a 4 euro, oppure 4 CD a 5 euro (non ci sono altre possibilità per ottenere una spesa di esattamente 20 euro). Nel primo caso, può effettuare  $\binom{8}{5} = 56$  scelte; nel secondo caso, può effettuare  $\binom{7}{4} = 35$  scelte.  
 Le possibili scelte sono quindi in tutto  $56 + 35 = 91$ .

● Dobbiamo contare tutte le possibili quintuple costituite dai due elementi  $c$  (camicie) e  $p$  (pantaloni). Le possibili quintuple sono in tutto  $2^5$ .

● Si tratta di contare le combinazioni con ripetizioni di  $n = 2$  oggetti a 5 a 5. In tutto sono

$$\binom{n+k-1}{k} = \binom{6}{5} = 6.$$

Sono le seguenti:

$$|xxxxx, \quad x|xxxx, \quad xx|xxx, \quad xxx|xx, \quad xxxx|x, \quad xxxxx|$$

● Il numero di funzioni iniettive da un insieme con  $n$  elementi ad un insieme con  $m$  elementi è  $m(m-1)(m-2)\cdots(m-n+1)$ . Nel nostro caso, essendo  $n=5$  tale numero è  $m(m-1)(m-2)(m-3)$ . Quindi dobbiamo imporre

$$m(m-1)(m-2)(m-3) = 840.$$

Ora,  $840 = 2^3 \cdot 3 \cdot 5 \cdot 7$ : necessariamente risulta  $m=7$ ,  $m-1=2 \cdot 3=6$ ,  $m-2=5$ ,  $m-3=4$ . Quindi la cardinalità di  $B$  è 7.

Nel secondo caso,  $1680 = m(m-1)(m-2)(m-3)$ : dato che  $1680 = 2^4 \cdot 3 \cdot 5 \cdot 7$ , l'unico modo per esprimere 1680 come prodotto di quattro interi che differiscono per una unità è prendendo  $m=8$  (da cui  $m-1=7$ ,  $m-2=2 \cdot 3=6$ ,  $m-3=5$ ).

● La prima cifra può essere 2 o 4 (non può essere 0, altrimenti il numero avrebbe 2 cifre e non 3 come richiesto), cioè può assumere 2 valori. La seconda può assumere i valori 0, 2, 4, 6, 8 ma si deve escludere il valore della prima posizione, quindi per la seconda posizione ci sono 4 scelte. Per la terza posizione le possibilità sono 0, 2, 4, 6, 8 ma se ne devono escludere due (quelle delle prime due posizioni: quindi le scelte possibili per la terza posizione sono 3. In definitiva, il numero di interi positivi richiesti è  $2 \cdot 4 \cdot 3 = 24$ .

● Il problema corrisponde a determinare in quanti modi si possono disporre 50 carte identiche in 4 pile, in modo tale che in ogni pila ci sia almeno una carta. Togliamo una carta da ogni pila. In tutto abbiamo tolto 4 carte, quindi il problema ora diventa quello di determinare in quanti modi si possono disporre 46 carte in 4 pile (*eventualmente vuote*). Se attribuiamo ad ogni carta il numero 1, 2, 3 o 4 a seconda che la mettiamo nella prima, nella

seconda o nella terza pila, il problema diventa: in quanti modi possiamo numerare 46 carte con i numeri 1, 2, 3, 4? Si tratta delle combinazioni con ripetizioni di 4 elementi di classe 46. Sappiamo essere in numero di

$$\binom{4+46-1}{46} = \binom{49}{46} = 18424.$$

- a. Aldo può scegliere fra 6 liste; una volta scelta la lista per cui votare, deve scegliere 3 candidati fra i 10 proposti, cioè  $\binom{10}{3} = 120$ . Il voto può essere dunque espresso in  $6 \cdot 120 = 720$  modi.  
 b. Una volta scelta la lista, Giovanni può non esprimere nessuna preferenza, esprimere una sola ( $\binom{10}{1} = 10$  possibilità), esprimere due ( $\binom{10}{2} = 45$  possibilità), oppure esprimere tre ( $\binom{10}{3} = 120$  possibilità). Le possibilità sono quindi in totale  $6 \cdot (1 + 10 + 45 + 120) = 6 \cdot 176 = 1056$ .  
 c. Nel primo caso si hanno  $4 \cdot \binom{8}{3} + 2 \cdot \binom{10}{3} = 4 \cdot 56 + 2 \cdot 120 = 224 + 240 = 464$  possibilità. Nel secondo caso le possibilità sono

$$4 \left[ \binom{8}{0} + \binom{8}{1} + \binom{8}{2} + \binom{8}{3} \right] + 2 \left[ \binom{10}{0} + \binom{10}{1} + \binom{10}{2} + \binom{10}{3} \right] = \\ = 4 \cdot (1 + 8 + 28 + 56) + 2(1 + 10 + 45 + 120) = 372 + 352 = 724.$$

● La fattorizzazione in primi di 210 è  $210 = 2 \cdot 3 \cdot 5 \cdot 7$ .

Primo fattore	Secondo fattore	Possibili fattorizzazioni
2	$3 \cdot 5 \cdot 7$	$= 2 \cdot 105$
3	$2 \cdot 5 \cdot 7$	$= 3 \cdot 70$
5	$2 \cdot 3 \cdot 7$	$= 5 \cdot 42$
7	$2 \cdot 3 \cdot 5$	$= 7 \cdot 30$
$2 \cdot 3$	$5 \cdot 7$	$= 6 \cdot 35$
$2 \cdot 5$	$3 \cdot 7$	$= 10 \cdot 21$
$2 \cdot 7$	$3 \cdot 5$	$= 14 \cdot 15$

Il problema equivale a determinare in quanti modi si possono distribuire 4 oggetti (ossia i numeri 2, 3, 5, 7) in due contenitori identici (il primo e il secondo fattore del prodotto), in modo tale che nessuno dei due contenitori resti vuoto.

In generale, il numero di modi in cui si possono distribuire  $m$  oggetti in  $n$  ( $m \geq n$ ) contenitori identici è dato dalla formula

$$\frac{1}{n!} \sum_{k=0}^n (-1)^k \binom{n}{n-k} (n-k)^m.$$

Tale quantità si denota con  $S(m, n)$  e si chiama numero di Stirling del secondo tipo. Si può verificare che vale la seguente relazione (cfr.[5] pagg. 263-265):

$$S(m+1, n) = S(m, n-1) + nS(m, n).$$

Nel nostro caso il numero richiesto è  $S(4, 2) = S(3, 1) + 2S(3, 2) = 1 + 2 \cdot 3 = 7$ .

- Le targhe del primo tipo (ossia tre lettere seguite da due cifre) sono in tutto (regola del prodotto)  $N_1 = 26 \cdot 26 \cdot 26 \cdot 10 \cdot 10$ . Le targhe del secondo tipo (ossia quattro lettere seguite da 1 cifra) sono  $N_2 = 26 \cdot 26 \cdot 26 \cdot 26 \cdot 10$ . In definitiva, tutte le possibili targhe sono in numero di  $N_1 + N_2$  (regola della somma) perché ogni targa può essere del primo tipo o del secondo ma non di entrambi. Quindi il numero totale è 6 327 360.

Tutti gli interi di 4 cifre sono  $9 \cdot 10^3 = 9000$  (infatti la prima cifra non può essere lo zero, altrimenti si tratterebbe di un numero con 3 cifre e non di 4, tutte le altre possono essere scelte tra 10 possibilità). Da questi si devono eliminare i numeri che non hanno *nessuna cifra dispari*, ossia i numeri di 4 cifre che hanno solo cifre pari: le cifre pari sono in numero di 5, quindi i numeri con sole cifre pari sono in numero di  $4 \cdot 5^3$  (ancora per il motivo che la prima cifra può essere scelta solo tra 2, 4, 6, 8). In definitiva il numero richiesto è

$$9000 - 500 = 8500.$$

Per  $f(3)$  abbiamo 6 scelte, (4, 5, 6, 7, 8, 9), per  $f(4)$  abbiamo 5 scelte, (5, 6, 7, 8, 9), per  $f(5)$  abbiamo 4 scelte, (6, 7, 8, 9); siccome le scelte sono indipendenti, le possibilità totali sono  $6 \cdot 5 \cdot 4 = 120$ .

Per  $f(3)$  abbiamo 5 scelte (3, 4, 5, 6, 7), per  $f(4)$  abbiamo 4 scelte (4, 5, 6, 7), per  $f(5)$  abbiamo 3 scelte (5, 6, 7), per  $f(6)$  abbiamo 2 scelte (6, 7); siccome le scelte sono indipendenti, le possibilità totali sono  $5 \cdot 4 \cdot 3 \cdot 2 = 120$ .

a.  $\binom{40}{2}$ .

b. Per ciascun valore le possibilità sono  $\binom{4}{2} = 6$ ; siccome i valori delle carte sono 10, le possibilità in tutto sono  $10 \cdot 6 = 60$ . Il ragionamento da fare è il seguente: fissiamo uno dei 10 valori, per esempio 3. Si possono prendere a due a due in  $\binom{4}{2}$  modi (cioè in 6 modi): se indichiamo con  $C, Q, P, F$  i 4 semi (cuori, quadri, picche e fiori) avremo le seguenti possibilità:  $CQ, CP, CF, QP, QF, PF$ . Il numero di possibilità di prendere due 3 nel mazzo è quindi 6. Ma dato che i valori sono 10 (da 1 a 10), per sapere in quanti modi si possono prendere 2 carte con uno stesso valore dal mazzo dovremo moltiplicare il valore 6 per 10, ottenendo 60 come risultato. Quindi 60 rappresenta il numero richiesto.

a.  $\binom{40}{3}$ .

b. Per ciascun valore le possibilità sono  $\binom{4}{3} = 4$ ; siccome i valori delle carte sono 10, le possibilità in tutto sono  $10 \cdot 4 = 40$ .

$A \times B$  ha  $4 \cdot 2 = 8$  elementi;  $C = \{3, 4\}$  ha 2 elementi, quindi le funzioni sono in tutto  $2^8$ .

$A$  ha 3 elementi;  $C = \{5, 6\}$  ha 2 elementi, quindi  $B \times C$  ha  $2 \cdot 2 = 4$  elementi, quindi le funzioni sono in tutto  $4^3$ .

$A \times B$  ha  $3 \times 3 = 9$  elementi;  $C = \{3, 4\}$  ha 2 elementi, quindi le funzioni sono in tutto  $2^9$ .

$A$  ha 3 elementi;  $C = \{5, 6\}$  ha 2 elementi, quindi  $B \times C$  ha  $3 \times 2 = 6$  elementi, quindi le funzioni sono in tutto  $6^3$ .

a.  $\binom{32}{5} = 201\,376$ .

b. Per ciascun seme le possibilità sono  $\binom{8}{5} = 56$ ; siccome i semi sono 4, le possibilità in tutto sono  $4 \cdot 56 = 224$ .

OSSERVAZIONE Per chi ha fatto o farà calcolo delle probabilità, il rapporto fra il secondo risultato ed il primo ( $\frac{224}{201\,376} = \frac{1}{899}$ ) rappresenta la probabilità di ottenere colore pescando 5 carte da un mazzo di 32.

a.  $\binom{28}{5} = 98\,280$ .

b. Per ciascun seme le possibilità sono  $\binom{7}{5} = 21$ ; siccome i semi sono 4, le possibilità in tutto sono  $4 \cdot 21 = 84$ .

OSSERVAZIONE Per chi ha fatto o farà calcolo delle probabilità, il rapporto fra il secondo risultato ed il primo, ossia  $\frac{84}{98280} = \frac{1}{1170}$ , rappresenta la probabilità di ottenere colore pescando 5 carte da un mazzo di 32.

a. I detti numeri sono del tipo  $3^a 5^b 7^c 11^d$ , con  $0 \leq a, b, c, d < 10$ . Essendoci 10 possibilità per la scelta di ciascun valore di  $a, b, c, d$ , ed essendo queste scelte indipendenti fra loro, vi sono in tutto  $10^4 = 10\,000$  possibilità.

b. Si tratta di scegliere quattro numeri distinti fra 10, quindi  $10 \cdot 9 \cdot 8 \cdot 7 = 5040$ .

c. Ai numeri precedenti bisogna aggiungere i loro opposti, quindi le possibilità sono in tutto, rispettivamente, 20 000 e 10 080.

a.  $\binom{12}{9} = 220$ .

b. La prima scelta può farla in  $\binom{6}{4} = 15$  modi, la seconda in  $\binom{6}{5} = 6$  modi. Le scelte sono indipendenti, quindi per la regola del prodotto il numero totale di scelte è

$$\binom{6}{4} \cdot \binom{6}{5} = 15 \cdot 6 = 90.$$

Procediamo per induzione su  $n$ . Per  $n = 1$  si ha  $|A_1| = |A_1|$ . Per  $n = 2$ ,  $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$  e quindi  $|A_1 \cup A_2| \leq |A_1| + |A_2|$ . La base dell'induzione è quindi provata. Supponiamo di avere provato che la proposizione è vera per  $n - 1$  insiemi, ossia che

$$|A_1 \cup A_2 \cup \dots \cup A_{n-1}| \leq |A_1| + |A_2| + \dots + |A_{n-1}|.$$

Allora

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= |(A_1 \cup A_2 \cup \dots \cup A_{n-1}) \cup A_n| \leq \\ &\leq |A_1 \cup A_2 \cup \dots \cup A_{n-1}| + |A_n| \leq \end{aligned}$$

per l'ipotesi induttiva

$$\leq (|A_1| + |A_2| + \dots + |A_{n-1}|) + |A_n| = |A_1| + |A_2| + \dots + |A_{n-1}| + |A_n|.$$

Poniamo:

$U = \{\text{studenti del primo anno di Informatica}\}$ ,  $A = \{\text{maschi}\}$ ,  $B = \{\text{studenti biondi}\}$ ,  $C = \{\text{maschi biondi}\}$ . Allora  $CA = \{\text{femmine}\}$ ,  $A \cap B = \{\text{maschi biondi}\}$ ,  $CA \cap B = \{\text{femmine bionde}\}$ ,  $CA \cap CB = \{\text{femmine brune}\}$ .

Dato che  $CA \cap CB = C(A \cap B)$ , basta determinare  $A \cup B$ . Si ha

$$|A \cup B| = |A| + |B| - |A \cap B| = 80 + 20 - 9 = 91.$$

Quindi le femmine brune sono 9.

Indicati con  $A$  l'insieme delle donne troppo scure, con  $B$  l'insieme delle donne troppo chiare, con  $C$  l'insieme delle donne troppo strette, si ha:

$$|A| = 8, \quad |B| = 6, \quad |C| = 12, \quad |A \cap C| = 6, \quad |B \cap C| = 5, \quad |A \cap B| = 0.$$

Si ha quindi  $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap C| - |B \cap C|$  da cui

$$|A \cup B \cup C| = 8 + 6 + 12 - 6 - 5 = 15.$$

Le donne che possono andar bene sono in definitiva 25-15=10. Speriamo che una di queste sia di suo gradimento!

## SOLUZIONI RELATIVE AL CAPITOLO 5

Si ha  $3546 \equiv 6 \pmod{10}$ , e inoltre  $6^2 \equiv 6 \pmod{10}$  e quindi  $6^k \equiv 6 \pmod{10}$  per ogni  $k > 0$ . Ne segue che

$$3546^{2007} \equiv 6 \pmod{10}.$$

Dato che  $\text{MCD}(3, 5) = 1$ , possiamo utilizzare il Corollario del Piccolo Teorema di Fermat che ci garantisce che  $5^{3-1} \equiv 1 \pmod{3}$ . In realtà per vedere che  $5^2 = 25$  è congruo ad 1 modulo 3 non serve nemmeno scomodare il Corollario del Piccolo Teorema di Fermat. Una volta acquisito questo fatto, si ha:

$$5^{427} = 5^{213 \cdot 2 + 1} = (5^2)^{213} \cdot 5 \equiv 1 \cdot 5 = 5.$$

Il resto cercato è 5.

Si tratta di calcolare  $2459^{547} \pmod{10}$ . Ora,  $2459 \equiv 9 \pmod{10}$ . Inoltre  $9 \equiv -1 \pmod{10}$  e quindi 9 elevato ad un numero pari è congruente ad 1, mentre elevato ad un numero dispari è congruente a -1, ossia 9. Nel nostro caso l'esponente è dispari, quindi l'ultima cifra del numero richiesto è 9.

$1000 \equiv 6 \pmod{7}$ . Ora,  $\text{MCD}(6, 7) = 1$ , quindi possiamo applicare il Corollario del Piccolo Teorema di Fermat, secondo cui se  $p$  è primo e  $(a, p) = 1$ , allora  $a^{p-1} \equiv 1 \pmod{p}$ . Quindi nel nostro caso  $6^6 \equiv 1 \pmod{7}$ . Ma allora

$$6^{2000} = 6^{6 \cdot 333 + 2} = (6^6)^{333} \cdot 6^2 \equiv 1 \cdot 6^2 = 36 \equiv 1 \cdot 1 = 1 \pmod{7}.$$

In definitiva, il numero  $1000^{2000}$  sta nella classe  $\bar{1}$  di  $\mathbb{Z}_7$ .

Ancora più semplicemente, si poteva procedere osservando che  $6^2 \equiv 1 \pmod{7}$ , da cui

$$6^{2000} = 6^{2 \cdot 1000} = (6^2)^{1000} \equiv 1 \pmod{7}.$$

Supposto per assurdo che due delle soluzioni (4.1) siano congruenti modulo  $n$ , cioè  $x_0 + k_1 \cdot \frac{n}{d} \equiv x_0 + k_2 \cdot \frac{n}{d} \pmod{n}$  con  $k_1, k_2 \in \mathbb{Z}$  e  $0 \leq k_1 < k_2 \leq d-1$ , si avrebbe  $k_1 \cdot \frac{n}{d} \equiv k_2 \cdot \frac{n}{d} \pmod{n}$  da cui, dividendo per  $n/d$  (che è il  $\text{MCD}(n/d, n)$ ),  $k_1 \equiv k_2 \pmod{n/(n/d)}$  e quindi  $k_1 \equiv k_2 \pmod{d}$  che è assurdo perché  $0 < k_2 - k_1 < d$ .

Per provare che ogni soluzione del tipo  $x_0 + k \cdot (n/d)$ , al variare di  $k$  in  $\mathbb{Z}$  è congruente ad una delle (4.1), basta dividere  $k$  per  $d$ :  $k = dq + r$ , con  $0 \leq r \leq d-1$ , da cui

$$x_0 + k \cdot \frac{n}{d} = x_0 + (dq + r) \frac{n}{d} = x_0 + qn + \frac{n}{d}r \equiv x_0 + \frac{n}{d}r, \quad 0 \leq r \leq d-1.$$

La congruenza è equivalente alla  $8x \equiv 16 \pmod{20}$  che è compatibile perché  $(8, 20) = 4|16$ . Una soluzione è ovviamente data da  $x_0 = 2$ ; le altre sono  $x_1 = 2 + \frac{20}{4} = 2 + 5 = 7$ ,  $x_2 = 2 + 2 \cdot 5 = 12$ ,  $x_3 = 2 + 3 \cdot 5 = 17$ .

Si ha:  $1500 = 2^2 \cdot 3 \cdot 5^3$ ,  $336 = 2^4 \cdot 3 \cdot 7$ . Se vogliamo che ci siano 12 soluzioni non congrue tra loro modulo 1500 innanzitutto osserviamo che 12 deve essere il  $\text{MCD}(a, 1500)$  e che 12 divide 336: effettivamente 12 divide 336. Dobbiamo allora scegliere un  $a \in \mathbb{Z}$  tale che  $(a, 2^2 \cdot 3 \cdot 5^3)$  sia uguale a 12. Per esempio possiamo prendere  $a = 12$ , oppure  $a = 132 = 12 \cdot 11$ , ecc.

Perché la congruenza ammetta soluzioni, il  $\text{MCD}(a, 20)$  deve essere un divisore di 6, ossia deve appartenere a  $\{1, 2, 3, 6\}$ . Non può essere né 3 né 6, dato che 3 e 6 non dividono 20, quindi deve essere 1 o 2. Dato che  $20 = 2^2 \cdot 5$ , i valori di  $a$  per i quali il  $\text{MCD}(a, 20)$  è 1 sono  $a = 1, 3, 7, 9, 11, 13, 17, 19$ .

I valori di  $a$  per i quali  $\text{MCD}(a, 20) = 2$  sono  $a = 2, 6, 14, 18$ .

Le soluzioni sono quindi:

- $x \equiv 6 \pmod{20} \quad x = 6 + 20h, h \in \mathbb{Z}$
- $3x \equiv 6 \pmod{20} \iff x \equiv 2 \pmod{20} \implies x = 2 + 20h, h \in \mathbb{Z}$
- $7x \equiv 6 \pmod{20} \quad x = -2 + h20 = 18 + 20h, h \in \mathbb{Z}$
- $9x \equiv 6 \pmod{20} \iff 3x \equiv 2 \pmod{20} \implies x = 14 + 20h, h \in \mathbb{Z}$
- $11x \equiv 6 \pmod{20} \quad x = 6 + 20h, h \in \mathbb{Z}$
- $13x \equiv 6 \pmod{20} \quad x = 2 + 20h, h \in \mathbb{Z}$
- $17x \equiv 6 \pmod{20} \quad x = -2 + h20 = 18 + 20h, h \in \mathbb{Z}$
- $19x \equiv 6 \pmod{20} \quad x = -6 + h20 = 14 + 20h, h \in \mathbb{Z}$
- $2x \equiv 6 \pmod{20} \iff x \equiv 3 \pmod{10}, x = 3 + 10h, h \in \mathbb{Z}$
- $6x \equiv 6 \pmod{20} \iff x \equiv 1 \pmod{10}, x = 1 + 10h, h \in \mathbb{Z}$
- $14x \equiv 6 \pmod{20} \iff -6x \equiv 6 \pmod{20}, x = 9 + 10h, h \in \mathbb{Z}$
- $18x \equiv 6 \pmod{20} \iff -x \equiv 3 \pmod{10}, x = 7 + 10h, h \in \mathbb{Z}$ .

La soluzione è  $\bar{x} = N_1 \bar{x}_1 + N_2 \bar{x}_2 + \dots + N_s \bar{x}_s$  dove, per ogni  $k = 1, \dots, s$ ,  $\bar{x}_k$  è tale che  $a_k N_k \bar{x}_k \equiv b_k \pmod{n_k}$ .

$$\bar{x} \equiv 2009^{1982} \pmod{75} \iff \begin{cases} x \equiv 2009^{1982} \pmod{3} \\ x \equiv 2009^{1982} \pmod{25} \end{cases}$$

Ora,  $2009 \equiv 2 \pmod{3}$ , da cui (dato che  $2^2 \equiv 1 \pmod{3}$ )  $2009^{1982} \pmod{75} \equiv 2^{2 \cdot 991} \equiv 1 \pmod{3}$

$2009 \equiv 9 \pmod{25}$ ,  $(9, 25) = 1$ , e quindi  $9^{20} \equiv 1 \pmod{25}$  da cui  $9^{1982} = 9^{20 \cdot 99+2} \equiv 9^2 = 81 \equiv 6 \pmod{25}$ .

Si tratta allora di risolvere il seguente sistema di congruenze:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 6 \pmod{25} \end{cases}$$

le cui soluzioni sono  $31 + h75, h \in \mathbb{Z}$ . In definitiva  $2009^{1982} \equiv 31 \pmod{75}$ .

$32^{511} \equiv 2^{511} \pmod{4}$ . Dato che (in virtù del Corollario del Piccolo Teorema di Fermat)  $2^4 \equiv 1 \pmod{5}$ , ne segue che

$$32^{511} \equiv 2^{511} = 2^{4 \cdot 127 + 3} = (2^4)^{127} \cdot 2^3 \equiv 2^3 \equiv 3 \pmod{5}.$$

Il sistema è quindi equivalente al seguente:

$$\begin{cases} x \equiv 3 \pmod{5} \\ 3x \equiv 1 \pmod{4} \\ x \equiv 7 \pmod{11} \end{cases} \quad \text{ossia} \quad \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 3 \pmod{4} \\ x \equiv 7 \pmod{11} \end{cases}$$

Dobbiamo risolvere le seguenti tre congruenze:

$$44x_1 \equiv 3 \pmod{5}, \quad 55x_2 \equiv 3 \pmod{4}, \quad 20x_3 \equiv 7 \pmod{11}$$

che hanno soluzioni rispettivamente  $\bar{x}_1 = 2$ ,  $\bar{x}_2 = 1$ ,  $\bar{x}_3 = 2$ . Una soluzione del sistema originario è quindi:  $\bar{x} = 44 \cdot 2 + 55 \cdot 1 + 20 \cdot 2 \equiv 183$ . Tutte e sole le soluzioni sono del tipo  $183 + h \cdot 220, h \in \mathbb{Z}$ .

a. Il sistema è equivalente a

$$\begin{cases} x \equiv 2 \pmod{9} \\ x \equiv 3 \pmod{7} \\ x \equiv 3 \pmod{5}. \end{cases}$$

dato che ogni congruenza del sistema è risolubile e i moduli sono a due a due coprimi, in base al Teorema Cinese dei Resti, il sistema ammette soluzione (unica modulo  $9 \cdot 7 \cdot 5 = 315$ ).

b. Posto  $N = 315$ ,  $N_1 = \frac{315}{9} = 35$ ,  $N_2 = \frac{315}{7} = 45$ ,  $N_3 = \frac{315}{5} = 63$ , risolviamo le tre congruenze

$$35x_1 \equiv 2 \pmod{9} \quad \text{che ha soluzione } x_1 = 7;$$

$$45x_2 \equiv 3 \pmod{7} \quad \text{che ha soluzione } x_2 = 1;$$

$$63x_3 \equiv 3 \pmod{5} \quad \text{che ha soluzione } x_3 = 1;$$

In definitiva una soluzione del sistema è

$$\bar{x} = 35 \cdot 7 + 45 \cdot 1 + 63 \cdot 1 = 353 \equiv 38$$

Tutte le soluzioni del sistema sono:  $38 + h \cdot 315$ ,  $h \in \mathbb{Z}$ .

c. Qualunque valore intero si attribuisca ad  $a$  il sistema sarà sempre compatibile, in virtù del Teorema Cinese dei Resti, perché la congruenza ammette soluzione e il nuovo sistema ha ancora i moduli a due a due coprimi, dato che 11 è coprimo con 9, con 7 e con 5.

a.  $x = 323 + 420k$ ,  $k \in \mathbb{Z}$ .

b.  $x = 323 + 60k$ ,  $k \in \mathbb{Z}$ , cioè  $x = 23 + 60k$ .

a. Il sistema è equivalente al sistema

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 5 \pmod{7} \\ 3x \equiv 235^{146} \pmod{16} \end{cases}$$

Ciascuna delle congruenze del sistema è risolubile perché in ciascuna delle congruenze il MCD tra il coefficiente della  $x$  e il modulo è 1, che divide il termine noto, qualunque esso sia. Inoltre i moduli sono a due a due coprimi, pertanto in virtù del Teorema Cinese dei Resti il sistema è risolubile e la soluzione è unica modulo  $N = 3 \cdot 7 \cdot 16 = 336$ .

b. Possiamo ora a risolvere il sistema. Innanzitutto calcoliamo  $235^{146} \pmod{16}$ .  $235 \equiv 11 \pmod{16}$ . Quindi  $235^{146} \equiv 11^{146} \pmod{16}$ . Ora, in virtù del Teorema di Eulero, che si può utilizzare dato che  $\text{MCD}(11, 16) = 1$ ,  $11^{\varphi(16)} \equiv 1 \pmod{16}$ , cioè  $11^8 \equiv 1 \pmod{16}$ , da cui  $11^{146} = 11^{8 \cdot 18 + 2} = (11^8)^{18} \cdot 11^2 \equiv 1 \cdot 11^2 \equiv 9 \pmod{16}$ . Il sistema diventa quindi

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 5 \pmod{7} \\ 3x \equiv 9 \pmod{16} \end{cases}$$

Possiamo dividere per 3 (che è coprimo con 16) l'ultima congruenza, ottenendo così

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 5 \pmod{7} \\ x \equiv 3 \pmod{16} \end{cases}$$

Posto  $N_1 = \frac{N}{3} = 112$ ,  $N_2 = \frac{N}{7} = 48$ ,  $N_3 = \frac{N}{16} = 21$ , risolviamo singolarmente le seguenti tre congruenze:

$$112x_1 \equiv 1 \pmod{3}, \quad \text{cioè } x_1 \equiv 1 \pmod{3};$$

$$48x_2 \equiv 5 \pmod{7} \quad \text{cioè } x_2 \equiv 2 \pmod{7};$$

$$21x_3 \equiv 3 \pmod{16} \quad \text{cioè } 5x_3 \equiv 3 \pmod{16}$$

che fornisce  $x_3 \equiv 7 \pmod{16}$ .

Una soluzione del sistema è quindi

$$\bar{x} = 112 \cdot 1 + 48 \cdot 2 + 21 \cdot 7 = 355 \equiv 19 \pmod{336}.$$

Tutte le soluzioni del sistema sono:  $19 + h \cdot 336$  al variare di  $h \in \mathbb{Z}$ .

c. Le soluzioni comprese nell'intervallo  $[0, 1000]$  sono tre: 19, 355, 691.

• Sia  $n = rs$ ,  $(r, s) = 1$ . I numeri  $m$  tali che  $0 \leq m < n$  si possono (cfr. proposizione 5.9) rappresentare come coppie del tipo  $(m \pmod{r}, m \pmod{s})$  e si ha (si provi!)

$$(m, rs) = 1 \iff (m \pmod{r}, r) = 1 \quad \text{e} \quad (m \pmod{s}, s) = 1.$$

Il numero totale  $\varphi(rs)$  degli  $m \pmod{rs}$  coprimi con  $rs$  è quindi  $\varphi(r) \cdot \varphi(s)$ , perché gli elementi  $\pmod{r}$  coprimi con  $r$  nel primo elemento della coppia sono in numero di  $\varphi(r)$  e quelli  $\pmod{s}$  coprimi con  $s$  nel secondo elemento della coppia sono in numero di  $\varphi(s)$ .

• Basta dare un controsenso: sia  $r = 6$ ,  $s = 4$ . Allora  $\varphi(6) = 2$ ,  $\varphi(4) = 2$ , mentre  $\varphi(24) = 8 \neq \varphi(6) \cdot \varphi(4)$ . Si noti che invece  $\varphi(24) = \varphi(8)\varphi(3)$ .

• Ammettono inverso solo le classi  $\bar{a}$  tali che  $\text{MCD}(a, n) = 1$ . Quindi sono invertibili solo:

in  $\mathbb{Z}_8 : \bar{1}, \bar{3}, \bar{5}, \bar{7}$ ;

in  $\mathbb{Z}_{10} : \bar{1}, \bar{3}, \bar{7}, \bar{9}$ ;

in  $\mathbb{Z}_{20} : \bar{1}, \bar{3}, \bar{7}, \bar{9}, \bar{11}, \bar{13}, \bar{17}, \bar{19}$ .

Per trovare le classi inverse delle varie classi  $\bar{a}$  che siano invertibili in  $\mathbb{Z}_n$  occorre risolvere la congruenza  $ax \equiv 1 \pmod{n}$  che è risolubile (e ammette una e una sola soluzione, perché  $\text{MCD}(a, n) = 1$ ). Quindi le classi inverse (nell'ordine dato) sono:

$\bar{1}, \bar{3}, \bar{5}, \bar{7}$  in  $(\mathbb{Z}_8, +)$ ,

$\bar{1}, \bar{7}, \bar{3}, \bar{9}$  in  $(\mathbb{Z}_{10}, +)$ ,

$\bar{1}, \bar{7}, \bar{3}, \bar{9}, \bar{11}, \bar{17}, \bar{13}, \bar{19}$  in  $(\mathbb{Z}_{20}, +)$ .

• In tutti e tre i casi si può utilizzare il Teorema di Eulero, perché  $(2, 5) = (2, 7) = (2, 11) = 1$ . Allora  $2^{877} \equiv (2^4)^{109} \cdot 2 \equiv 2 \pmod{5}$  e analogamente  $2^{877} \equiv 4 \pmod{7}$  e  $2^{877} \equiv 7 \pmod{11}$ .

•  $385 = 5 \cdot 7 \cdot 11$ . Quindi per risolvere il problema basta trovare un  $x$  tale che

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{7} \\ x \equiv 7 \pmod{11} \end{cases}$$

Risolvendo il sistema al solito modo si trova che  $x \equiv 172 \pmod{385}$ .

- a. Poiché 8191 e 11953 sono primi distinti, quindi relativamente primi,

$$\varphi(n) = \varphi(8191)\varphi(11953) = 8190 \cdot 11952 = 2 \cdot 5 \cdot 3^2 \cdot 7 \cdot 13 \cdot 2^4 \cdot 3^2 \cdot 83.$$

$e = 913 = 11 \cdot 83$ , quindi, in questo caso,  $(\varphi(n), e) = 83$ .

- b.  $\varphi(n)$  è calcolata al punto precedente,  $e = 1111 = 11 \cdot 101$ , quindi, in questo caso,  $(\varphi(n), e) = 1$ .

- c. Poiché 11971 e 11953 sono primi distinti, quindi relativamente primi,

$$\varphi(n) = \varphi(11971)\varphi(11953) = 11970 \cdot 11952 = 2 \cdot 5 \cdot 3^2 \cdot 7 \cdot 19 \cdot 2^4 \cdot 3^2 \cdot 83.$$

$e = 17 \cdot 23$ , quindi, in questo caso,  $(\varphi(n), e) = 1$ .

- d.  $\varphi(n)$  è calcolata al punto precedente,  $e = 195 = 5 \cdot 3 \cdot 13$ , quindi, in questo caso,  $(\varphi(n), e) = 15$ .

- e.  $59049 = 3^{10}$ , da cui 59049 e 11953 sono coprimi quindi

$$\varphi(n) = \varphi(59049) \cdot \varphi(11953) = 3^9 \cdot 2 \cdot 2^4 \cdot 3^2 \cdot 83.$$

Dato che 139 è primo,  $(\varphi(n), e) = 1$ .

- a. Con il metodo di fattorizzazione di Fermat (in cinque passi) si ottiene  $81217 = 241 \cdot 337$  e questi due numeri sono primi.  
 b. 5719 è divisibile per 7, da cui  $5719 = 7 \cdot 817$ . Con il metodo di fattorizzazione di Fermat per 817:  $k = 29$ .

$$k^2 - 817 = 841 - 817 = 24, \text{ non quadrato}$$

$$(k+1)^2 - 817 = 900 - 817 = 83, \text{ non quadrato}$$

$$(k+2)^2 - 817 = 961 - 817 = 144 = 12^2$$

per cui  $817 = (31-12)(31+12) = 19 \cdot 43$  (fattorizzazione in primi). La fattorizzazione in primi di 5719 è quindi  $5719 = 7 \cdot 19 \cdot 43$ .

- c.  $33792 = 2^{10} \cdot 3 \cdot 11$ .

8999919 = 9 · 999991.

Con il metodo di fattorizzazione di Fermat:  $1000000 - 999991 = 9 = 3^2$ , quindi  $999991 = 1000^2 - 3^2 = 997 \cdot 1003$ .

997 è primo poiché non ha divisori primi < 34.

Applicando ancora il metodo di fattorizzazione di Fermat,

$$34^2 - 1003 = 153 \text{ non è un quadrato perfetto;}$$

$$35^2 - 1003 = 222 \text{ non è un quadrato perfetto;}$$

$$36^2 - 1003 = 293 \text{ non è un quadrato perfetto;}$$

$$37^2 - 1003 = 366 \text{ non è un quadrato perfetto;}$$

$$38^2 - 1003 = 441 = 21^2,$$

quindi  $1003 = (38+21)(38-21) = 59 \cdot 17$ , entrambi numeri primi.

In conclusione,  $8999919 = 3^2 \cdot 17 \cdot 59 \cdot 997$ .

4999955 = 5 · 999991.

In conclusione, (v. esercizio precedente)  $8999919 = 5 \cdot 17 \cdot 59 \cdot 997$ .

- a. Non è un campo perché 5719 non è un numero primo, essendo  $5719 = 7 \cdot 19 \cdot 43$ .

- b.  $38 = 19 \cdot 2$  non è coprimo con 5719, quindi  $\bar{38}$  non è invertibile, come anche  $\bar{14}$ . L'unica classe invertibile è pertanto  $\bar{2}$ . Per trovare la sua inversa si deve risolvere la congruenza  $2x \equiv 1 \pmod{5719}$ . Dalla  $5719 = 2 \cdot 2859 + 1$  si deduce  $1 = 5719 + 2 \cdot (-2859)$  che ci dice che la classe inversa della classe  $\bar{2}$  è la classe  $\bar{-2859}$  ossia la 2860.

- Il messaggio verrà inviato elevando  $M$  alla potenza  $e_B$  e riducendola modulo  $n_B$ . Bob riceverà quindi il messaggio  $M' = 30$ : infatti  $M' = 4^7 \pmod{221} \equiv 30 \pmod{221}$ . Per decodificarlo, Bob ha a disposizione la sua chiave segreta, che è il numero  $d_B$  soluzione della congruenza  $e_B d_B \equiv 1 \pmod{\varphi(n_B)}$ . Si è visto che il segreto per la determinazione di  $d_B$  è la conoscenza della fattorizzazione di  $n_B$ , che lui solo conosce. Ora, Bob aveva scelto  $n_B = 221$  come prodotto dei due fattori primi 13 e 17, quindi  $\varphi(221) = \varphi(13)\varphi(17) = 12 \cdot 16 = 192$  da cui  $d_B = 55$ . Per decifrare il messaggio ricevuto, Bob deve elevare  $M'$  alla potenza  $d_B$  e ridurlo modulo 221. Facendo qualche riduzione che omettiamo, ma che è fattibile abbastanza rapidamente con i metodi del paragrafo 9, Bob riesce a leggere il messaggio originario  $30^{55} \pmod{221} \equiv 4 = M$ .

- a.  $n_A = 247 = 13 \cdot 19$ ,  $\varphi(n_A) = 12 \cdot 18$  e  $\text{MCD}(7, 12) = \text{MCD}(7, 18) = 1$ .  
 $n_B = 253 = 23 \cdot 11$ ,  $\varphi(n_B) = 22 \cdot 10$  e  $\text{MCD}(3, 22) = \text{MCD}(3, 10) = 1$ .  
 b. Alice calcolerà  $30^3$  e lo ridurrà modulo 253. Il messaggio che Bob riceverà è quindi  $30^3 \pmod{253} = (30^2) \cdot 30 \equiv 141 \cdot 30 \equiv 182 \pmod{253}$ .  
 c. La chiave segreta di Bob è la soluzione della congruenza  $3x \equiv 1 \pmod{\varphi(253)}$  cioè  $3x \equiv 1 \pmod{220}$  che è 147. Per decifrare il messaggio ricevuto Bob eleverà 182 a 147 e ridurrà il risultato modulo 253, ottenendo così 30.

- Il numero 503 è primo poiché non ha fattori primi minori di radice di 503; ovvero, poiché non è divisibile per nessuno dei seguenti primi: 2, 3, 5, 7, 11, 13, 17, 23. Il numero 607 è primo poiché non ha fattori primi minori di radice di 607; ovvero, poiché non è divisibile per nessuno dei seguenti primi: 2, 3, 5, 7, 11, 13, 17, 23.

Il numero 701 è primo poiché non ha fattori primi minori di radice di 701; ovvero, poiché non è divisibile per nessuno dei seguenti primi: 2, 3, 5, 7, 11, 13, 17, 23.

Ogni scelta di  $n = pq$ , con  $p$  e  $q$  primi è accettabile;  $e$  va poi scelto in modo che  $(\phi(p), e) = 1$  e  $(\phi(q), e) = 1$ ; ovvero  $(p-1, e) = 1$  e  $(q-1, e) = 1$ .

La scelta più conveniente per  $n$  è comunque  $n = 503 \cdot 701 = 352\,603$ , poiché trovarne la fattorizzazione è più difficile. Infatti sono necessari 9 tentativi con il metodo di fattorizzazione di Fermat:

$$594^2 - 352\,603 \text{ non è un quadrato perfetto}$$

$$\dots$$

$$602^2 - 352\,603 = 99^2.$$

Se invece, per esempio, si scegliesse  $n = 503 \cdot 607 = 305\,321$ , per trovare la fattorizzazione di 305 321 ad un estraneo basterebbero tre soli tentativi! Infatti:

$$553^2 - 305\,321 \text{ non è un quadrato perfetto}$$

$$554^2 - 305\,321 \text{ non è un quadrato perfetto}$$

$$555^2 - 305\,321 = 2704 = 52^2.$$

- Il messaggio verrà inviato come  $8^{13} \pmod{46}$ . Per determinare tale numero, conviene scrivere 13 in base 2:  $13 = (1101)_2$ . C'è un metodo alternativo (ma sostanzialmente equivalente) a quello del paragrafo 9. Il numero 1101 in base 2 ha 4 cifre: scriviamo pertanto tre ( $=4-1$ ) lettere  $E$ :

$E\ E\ E$

e inseriamo tra loro una  $M$  a partire da sinistra per ogni cifra 1 che compare nella scrittura in base 2 di 13. Si avrà quindi:

**MEMEEM.**

Se diamo alla lettera  $E$  il significato di elevamento al quadrato e alla lettera  $M$  il significato di moltiplicazione per 8, sappiamo esattamente il tipo di operazioni che dobbiamo fare:

$$\begin{aligned} 8^{13} &= ((8^2 \cdot 8)^2)^2 \cdot 8 = ((64 \cdot 8)^2)^2 \\ &= ((144)^2)^2 \cdot 8 \equiv \dots \equiv 18 \pmod{46}. \end{aligned}$$

Il messaggio in codice è quindi 18.

L'utente  $B$ , per decifrare il messaggio, utilizzerà la sua chiave segreta, che è la soluzione  $d_B$  della congruenza  $e_B x \equiv 1 \pmod{\varphi(n_B)}$  che lui solo conosce, perché lui solo conosce la fattorizzazione di  $n_B$ . Nel nostro caso  $\varphi(46) = 22$  e la congruenza è  $13x \equiv 1 \pmod{22}$  cioè  $d_B = -5 \equiv 17 \pmod{22}$ . A questo punto  $B$  calcola  $18^{17} \cdot 17 = (10001)_2$ , quindi  $18^{17} = (((18^2)^2)^2)^2 \cdot 18 \pmod{46} \equiv \dots \equiv 8 \pmod{46}$  (che è il messaggio originario!!!!!!).

Essendo  $77 = 11 \cdot 7$ , la chiave segreta di Alice è  $d_A = 37$ . Alice ha pertanto autenticato la propria firma elevando 70 alla potenza  $d_A$ :  $70^{37} \equiv 49 \pmod{77}$ .

Bob verifica l'autenticità della firma elevando 49 alla potenza  $e_A = 13$ :  $49^{13} \equiv 70 \pmod{77}$  e in tal modo è sicuro che il messaggio proviene da Alice.

## SOLUZIONI RELATIVE AL CAPITOLO 6

Sia  $a$  un elemento non nullo di  $\mathbb{K}$  e sia  $b$  un elemento di  $\mathbb{K}$  tale che  $ab = 0$ . Dobbiamo provare che  $b = 0$ . Dato che  $a \neq 0$  e appartiene ad un campo,  $a$  è invertibile in  $\mathbb{K}$ , ossia esiste  $a^{-1} \in \mathbb{K}$  tale che  $a \cdot a^{-1} = a^{-1} \cdot a = 1$ . Allora dalla  $ab = 0$ , moltiplicando ambo i membri per  $a^{-1}$  si ha  $a^{-1}(ab) = (a^{-1}a)b = 1b = b = 0$  che è quanto volevamo.

Se  $f(x) = 0$  o  $\partial f(x) < \partial g(x)$  basta porre  $q(x) = 0$  e  $r(x) = f(x)$ . Supponiamo quindi senz'altro  $\partial g(x) \leq \partial f(x)$ . Procederemo per induzione su  $\partial f(x)$ . Se  $\partial f(x) = 0$  (e quindi anche  $\partial g(x) = 0$ ), significa che  $f(x) = a_0$ ,  $g(x) = b_0$ ,  $a_0, b_0 \in \mathbb{K}$  e diversi da zero, da cui  $f(x) = a_0 = \underbrace{(a_0 \cdot b_0^{-1})}_{q(x)} b_0 + \underbrace{0}_{r(x)}$ .

Si osservi l'importanza che i coefficienti si trovino in un campo!

Supponiamo vero il teorema per polinomi di grado  $< n$  e dimostriamolo quando  $\partial f = n$ . Allora  $\partial f = n \geq \partial g = m$ . Siano  $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ ,  $a_n \neq 0$  e  $g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$ ,  $b_m \neq 0$ . Il polinomio  $\tilde{f}(x) = f(x) - a_nb_m^{-1}x^{n-m} \cdot g(x)$  appartiene a  $\mathbb{K}[x]$  e ha grado minore di  $n$ . Per l'ipotesi induttiva esistono  $\tilde{q}(x)$  e  $\tilde{r}(x)$  tali che  $\tilde{f}(x) = g(x)\tilde{q}(x) + \tilde{r}(x)$ ,  $\partial\tilde{r}(x) < m$  oppure  $\tilde{r}(x) = 0$ .

Allora

$$\begin{aligned} f(x) &= \tilde{f}(x) + a_nb_m^{-1}x^{n-m}g(x) = g(x)\tilde{q}(x) + \tilde{r}(x) + a_nb_m^{-1}x^{n-m}g(x) \\ &= g(x) \underbrace{[\tilde{q}(x) + a_nb_m^{-1}x^{n-m}]}_{q(x)} + \underbrace{\tilde{r}(x)}_{r(x)}. \end{aligned}$$

Abbiamo così trovato i polinomi  $q(x)$  e  $r(x)$  richiesti. Per quanto concerne l'unicità, supponiamo che sia  $f(x) = g(x)q(x) + r(x) = g(x)q'(x) + r'(x)$ ,  $\partial r(x) < \partial g(x)$ ,  $\partial r'(x) < \partial g(x)$ .

Allora  $r(x) - r'(x) = g(x)(q'(x) - q(x))$ , dove il primo membro o è il polinomio nullo, oppure ha grado minore di  $\partial g(x)$ ; il secondo membro o è zero, oppure ha grado  $\geq \partial g(x)$ . Quindi l'uguaglianza si può avere solo se  $r(x) = r'(x)$  e  $q(x) = q'(x)$ .

Per induzione sul grado  $n$  di  $f(x)$ . Se  $n = 0$ ,  $f(x)$  è una costante non nulla, che è priva di radici, quindi il teorema è vero. Supponiamo vero il teorema per ogni polinomio di grado  $< n$ . Sia  $f(x)$  di grado  $n$ . Se  $f(x)$  ha una radice  $\alpha$  di molteplicità  $m \geq 1$ ,  $m \leq n$ , allora  $f(x) = (x - \alpha)^m q(x)$ ,  $\partial q(x) = n - m$ .

Sia  $\beta \neq \alpha$  un'altra radice di  $f(x)$ . Allora,  $0 = f(\beta) = (\beta - \alpha)^m q(\beta)$ . Dato che è  $\beta \neq \alpha$ , si deve avere  $q(\beta) = 0$ , perché  $\mathbb{K}$  è privo di divisori dello zero. Quindi le uniche radici di  $f(x)$  sono  $\alpha$  (con molteplicità  $m$ ) e le radici di  $q(x)$ . Ora, per l'ipotesi induttiva,  $q(x)$  ha al più  $n - m$  (= grado di  $q(x)$ ) radici. In definitiva,  $f(x)$  può avere al massimo  $m + (n - m) = n$  radici in  $\mathbb{K}$ .

Col metodo delle divisioni successive, si ottiene:

$$(*) \quad q(x) = (x - 1)p(x) + 2x^2 + 2,$$

e  $p(x) = (1/2x^2 + 1/2x + 1/2)(2x^2 + 2)$  con resto nullo, quindi un MCD è l'ultimo resto non nullo, cioè  $2x^2 + 2$  (o anche  $x^2 + 1$ , poiché il MCD è definito a meno di associati).

Da (\*) si ottiene subito  $2x^2 + 2 = p(x)(-x + 1) + q(x)$ , quindi una possibile scelta per  $r(x)$  ed  $s(x)$  è  $r(x) = -x + 1$  e  $s(x) = 1$ .

Col metodo delle divisioni successive, si ottiene:

$$(**) \quad q(x) = (1/2x - 1/2)p(x) + x^2 + 1,$$

e  $p(x) = (x^2 + x + 1)(x^2 + 1)$  con resto nullo, quindi un MCD è l'ultimo resto non nullo, cioè  $x^2 + 1$ .

Da (\*\*) si ottiene subito  $x^2 + 1 = p(x)(-1/2x + 1/2) + q(x)$ , quindi una possibile scelta per  $r(x)$  ed  $s(x)$  è:  $r(x) = -1/2x + 1/2$  e  $s(x) = 1$ .

Siano  $f(x) = a_0 + a_1x + \dots + a_nx^n$ ,  $g(x) = b_0 + b_1x + \dots + b_mx^m$ ,  $a_i, b_i \in \mathbb{Z}$  i due polinomi primitivi. Supponiamo per assurdo  $f(x)g(x)$  non primitivo. Allora esiste un numero primo  $p$  che divide tutti i coefficienti di  $f(x)g(x)$ . Tale primo  $p$  non potrà dividere tutti i coefficienti di  $f(x)$  e di  $g(x)$  per l'ipotesi di primitività. Siano  $a_h$  e  $b_k$  i coefficienti rispettivamente di  $f(x)$  e di  $g(x)$  con indici più bassi non divisi da  $p$ . Esaminiamo il coefficiente  $c_{h+k}$  d'indice  $h + k$  in  $f(x)g(x)$ . Risulta  $c_{h+k} = a_h b_k + (a_{h-1} b_{k+1} + \dots + a_0 b_{h+k}) + (a_{h+1} b_{k-1} + \dots + a_{h+k} b_0)$ . Ora,  $p$  divide  $c_{h+k}$ , divide anche entrambe le quantità dentro le parentesi, come è facile verificare, quindi divide anche  $a_h b_k$ . Ma allora divide uno dei due fattori, il che contraddice l'ipotesi.

Nel caso in cui  $f(x) \in \mathbb{Z}[x]$  non sia primitivo, sia ancora  $f(x) = g(x)h(x)$  una sua fattorizzazione su  $\mathbb{Q}$ . Allora, posto  $f(x) = df^*(x)$  (cioè posto  $f(x)$  come prodotto del suo contenuto per un polinomio primitivo), sarà  $df^*(x) = g(x)h(x)$ , da cui  $f^*(x) = d^{-1}g(x)h(x)$ . Ora,  $f^*(x)$  è primitivo, quindi, per quanto dimostrato nel teorema, avendo una fattorizzazione su  $\mathbb{Q}$ , ne avrà una anche su  $\mathbb{Z}$ , cioè  $f^*(x) = \bar{g}(x)\bar{h}(x)$ ,  $\bar{g}(x), \bar{h}(x) \in \mathbb{Z}[x]$ . Ma allora, tornando all'espressione originale di  $f(x)$ , la  $f(x) = df^*(x) = d\bar{g}(x)\bar{h}(x)$  è una fattorizzazione di  $f(x)$  su  $\mathbb{Z}$ .

È riducibile su  $\mathbb{C}$  perché ha grado  $> 1$ , e riducibile su  $\mathbb{R}$  perché ha grado  $> 2$ .

È irriducibile su  $\mathbb{Q}$  per il criterio di Eisenstein con  $p = 5$ . Su  $\mathbb{Z}_2$  il polinomio si riduce a  $x^7$ , ed è evidentemente riducibile.

È riducibile su  $\mathbb{C}$  perché ha grado  $> 1$ , e riducibile su  $\mathbb{R}$  perché ha grado  $> 2$ .

È irriducibile su  $\mathbb{Q}$  per il criterio di Eisenstein con  $p = 3$ . Su  $\mathbb{Z}_2$  il polinomio si riduce a  $x^7$ , ed è evidentemente riducibile.

La scomposizione  $x^6 - 1 = (x^3 + 1)(x^3 - 1) = (x + 1)(x^2 - x + 1)(x - 1)(x^2 + x + 1)$  è valida su qualunque campo. I fattori sono irriducibili su  $\mathbb{R}$  e su  $\mathbb{Q}$  poiché  $x^2 - x + 1$  e  $x^2 + x + 1$  non hanno radici in  $\mathbb{R}$  e in  $\mathbb{Q}$ , e gli altri fattori sono di primo grado.

Su  $\mathbb{Z}_3$  si verifica che  $-1$  è radice di  $x^3 - x + 1$ , e  $x^2 - x + 1 = (x + 1)^2$ , e che  $1$  è radice di  $x^2 + x + 1$ , e  $x^2 + x + 1 = (x - 1)^2$ . In  $\mathbb{Z}_3$  risulta pertanto  $x^6 - 1 = (x + 1)^3(x - 1)^3$ .

$(x - 2)(3 + 6x - 15x^2 + x^5)$ . Il secondo fattore è irriducibile per il criterio di Eisenstein (con  $p = 3$ ).

- Il polinomio è sicuramente riducibile sia su  $\mathbb{R}$  sia su  $\mathbb{C}$  trattandosi di un polinomio di sesto grado.
- $2x^6 + 2x^5 + 15x^4 + 15x^3 + 75x + 75 = (2x^5 + 15x^3 + 75)(x + 1)$  Il polinomio  $2x^5 + 15x^3 + 75$  è irriducibile su  $\mathbb{Q}$  per il criterio di irriducibilità di Eisenstein (con  $p = 3$ , non  $p = 5$ ). Quindi i due polinomi sono entrambi irriducibili su  $\mathbb{Q}$ .
- Su  $\mathbb{Z}_5$  il polinomio  $2x^5 + 15x^3 + 75$  diventa  $2x^5$ . La fattorizzazione in irriducibili su  $\mathbb{Z}_5$  è pertanto  $2x^5 \cdot (x + 1)$ .

Le scomposizioni in fattori irriducibili su  $\mathbb{Q}$  di  $f(x)$  e  $g(x)$  sono rispettivamente:  $f(x) = (x^2 + x + 1)(x^2 - x + 1)$ , e  $g(x) = (x^2 + x + 1)(x^2 + x - 1)$ , quindi un MCD è  $x^2 + x + 1$ .

- Su  $\mathbb{Q}$   $x^5 - x^4 - 4x + 4 = (x - 1)(x^4 - 4) = (x - 1)(x^2 + 2)(x^2 - 2)$ .
- Su  $\mathbb{R}$   $x^5 - x^4 - 4x + 4 = (x - 1)(x^2 + 2)(x + \sqrt{2})(x - \sqrt{2})$ .
- Su  $\mathbb{Z}_3$   $x^5 - x^4 - 4x + 4 = (x - 1)(x + 1)(x + 2)(x^2 - 2) = (x + 1)(x + 2)^2(x^2 + 1)$ .

È irriducibile su  $\mathbb{Q}$  poiché di terzo grado senza radici (le uniche possibili radici sono  $1, -1, 1/3, -1/3, 2/3, -2/3, 2, -2$ , ma nessuno di questi valori è radice).

È riducibile su  $\mathbb{R}$  poiché tutti i polinomi di grado  $\geq 3$  sono riducibili su  $\mathbb{R}$ .

È riducibile su  $\mathbb{Z}_5$  poiché 2 è una radice.

Su  $\mathbb{Q}$ :  $(x + 1)(x - 2)(x^2 - 5)$ .

Su  $\mathbb{R}$ :  $(x + 1)(x - 2)(x - \sqrt{5})(x + \sqrt{5})$ .

Su  $\mathbb{Z}_5$ :  $(x + 1)(x - 2)x^3$ .

$(x - 2)(3 + 6x - 15x^2 + x^5)$ . Il secondo fattore è irriducibile per il criterio di Eisenstein (con  $p = 3$ ).

- Su  $\mathbb{R}$ :  $x^3 - x^2 - 5x + 2 = (x + 2)(x - \frac{3+\sqrt{5}}{2})(x - \frac{3-\sqrt{5}}{2})$ .
- Su  $\mathbb{Q}$ :  $x^3 - x^2 - 5x + 2 = (x + 2)(x^2 - 3x + 1)$ . Quest'ultimo è irriducibile perché di secondo grado privo di radici razionali.
- Su  $\mathbb{Z}_5$ :  $x^3 - x^2 - 5x + 2 = (x + 2)(x + 1)(x + 1)$ .

- Su  $\mathbb{C}$  sicuramente riducibile, perché gli unici polinomi irriducibili su  $\mathbb{C}$  sono quelli di primo grado.
- Su  $\mathbb{R}$  riducibile, perché gli unici polinomi irriducibili su  $\mathbb{R}$  sono quelli di primo grado e quelli di secondo grado privi di radici reali.

c. Su  $\mathbb{Q}$ :  $\frac{1}{5}x^4 + 6x^3 + 15x^2 + 18x + 30 = \frac{1}{5}(x^4 + 30x^3 + 75x^2 + 90x + 150)$ . Quindi il polinomio  $\frac{1}{5}x^4 + 6x^3 + 15x^2 + 18x + 30$  è associato in  $\mathbb{Q}[x]$  al polinomio a coefficienti interi  $x^4 + 30x^3 + 75x^2 + 90x + 150$ . Possiamo quindi lavorare su questo e applicare il criterio di Eisenstein, che è verificato per  $p = 3$ . Quindi il polinomio originario è irriducibile su  $\mathbb{Q}$ .

Osserviamo innanzitutto che  $x^{p-1} + x^{p-2} + \dots + x^2 + x + 1 = \frac{x^p - 1}{x - 1}$ . Ora, facendo la sostituzione  $x \rightarrow x + 1$ , si ottiene  $(x + 1)^{p-1} + (x + 1)^{p-2} + \dots + (x + 1)^2 + (x + 1) + 1 = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{\sum_{k=0}^p \binom{p}{k} x^{p-k} - 1}{x} = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \dots + p$ .

A questo punto si può applicare il criterio di Eisenstein, con il primo  $p$ , ed è così provato che il polinomio originario è irriducibile.

Consideriamo il polinomio  $p(x) = x^6 + 2x^5 + 5x^4 + 8x^3 + 18x^2 + 28x + 14$  associato al polinomio dato (ottenuto dividendo per 2, elemento invertibile in ciascuno dei campi considerati). Siccome  $p(-1) = 0$ , allora  $p(x)$  è divisibile per  $x + 1$ :  $p(x) = (x + 1)(x^5 + x^4 + 4x^3 + 4x^2 + 14x + 14) = (x + 1)^2(x^4 + 4x^2 + 14)$ .

Questa è una fattorizzazione in fattori irriducibili su  $\mathbb{Q}$ , poiché  $x^4 + 4x^2 + 14$  è irriducibile su  $\mathbb{Q}$  per il criterio di Eisenstein ( $p = 2$ ).

Su  $\mathbb{Z}_5$  si ottiene  $p(x) = (x + 1)^2(x^4 + 4x^2 + 4) = (x + 1)^2(x^2 + 2)^2$ . Questa è una fattorizzazione in fattori irriducibili su  $\mathbb{Z}_5$  poiché  $x^2 + 2$  è irriducibile su  $\mathbb{Z}_5$ , essendo di secondo grado e non avendo radici.

Su  $\mathbb{Z}_7$  si ottiene  $p(x) = (x + 1)^2(x^4 + 4x^2) = x^2(x + 1)^2(x^2 + 4)$ . Questa è una fattorizzazione in fattori irriducibili su  $\mathbb{Z}_7$  poiché  $x^2 + 4$  è irriducibile su  $\mathbb{Z}_7$ , essendo di secondo grado e non avendo radici.

Su  $\mathbb{R}$  si ha  

$$x^4 + 4x^2 + 14 = x^4 + 2\sqrt{14}x^2 + 14 - 2\sqrt{14}x^2 + 4x^2 = (x^2 + \sqrt{14})^2 - x^2(2\sqrt{14} - 4) = (x^2 + \sqrt{14} + x\sqrt{2\sqrt{14} - 4})(x^2 + \sqrt{14} - x\sqrt{2\sqrt{14} - 4})$$

Quindi  $p(x) = (x + 1)^2(x^2 + x\sqrt{2\sqrt{14} - 4} + \sqrt{14})(x^2 - x\sqrt{2\sqrt{14} - 4} + \sqrt{14})$ . Si noti che  $2\sqrt{14} - 4 > 0$ , quindi  $\sqrt{2\sqrt{14} - 4} \in \mathbb{R}$ .

$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$  quindi la complessità è  $\mathcal{O}(n^2)$ .

## SOLUZIONI RELATIVE AL CAPITOLO 7

Gli elementi invertibili di  $\mathbb{R}[x]/(x^2 - 2x + 2)$  sono tutte le classi non nulle, dato che il polinomio  $x^2 - 2x - 2$  è irriducibile su  $\mathbb{R}$  e pertanto  $\mathbb{R}[x]/(x^2 - 2x + 2)$  è un campo.

- Il polinomio  $x^4 - 3x - 1$  è irriducibile su  $\mathbb{Q}$  in quanto il polinomio pensato su  $\mathbb{Z}_2$ , ossia il polinomio  $x^4 + x + 1$ , è irriducibile su  $\mathbb{Z}_2$ . Quindi il quoziente è un campo.
- La classe  $x^3 + 2$  è diversa dalla classe nulla, quindi è invertibile e la classe inversa è

$$\frac{125}{149} \left( -\frac{1}{5}x^8 + \frac{1}{25}x^2 - \frac{1}{125}x + 1 \right).$$

$x^4 + 3x + 1$  è irriducibile su  $\mathbb{Q}$  dato che, per esempio, lo è in  $\mathbb{Z}_2[x]$  (in  $\mathbb{Z}_2[x]$  non ha zeri e non è il quadrato dell'unico polinomio irriducibile di grado 2, ossia  $x^2 + x + 1$ ). Dunque il quoziente  $\mathbb{Q}[x]/(x^4 + 3x + 1)$  è un campo. La classe  $x^2 + x$ , non essendo la classe nulla, è invertibile e la sua inversa è

$$\frac{-2x^3 + x^2 - x - 5}{-2x^3 + x^2 - x - 5}.$$

Basta dividere  $x^5 - 5x^3 + 1$  per  $x^3 - 2x - 3$ : se il resto è zero, allora  $x^5 - 5x^3 + 1 \in (f(x))$ , altrimenti non appartiene all'ideale.

- a. Rispettivamente,  $5^3$  e  $5^2$  elementi.  
 b. Siccome  $x^3 + 1$  è riducibile su  $\mathbb{Z}_5$ ,  $\mathbb{Z}_5[x]/(x^3 + 1)$  non è né un dominio né un campo. Siccome  $x^2 + x + 1$  è irriducibile su  $\mathbb{Z}_5$  (poiché di secondo grado senza radici in  $\mathbb{Z}_5$ ),  $\mathbb{Z}_5[x]/(x^2 + x + 1)$  è un dominio e un campo.  
 c.  $(x+1)(2x+3) = 2x^2 + 5x + 3 = 2x^2 + 3$ , e questa espressione non può essere semplificata in  $\mathbb{Z}_5[x]/(x^3 + 1)$ .  
 In  $\mathbb{Z}_5[x]/(x^2 + x + 1)$ , invece, la classe  $\overline{x^2}$  è la classe  $\overline{-x-1}$ , quindi la classe  $\overline{2x^2+3}$  è la classe  $\overline{-2x+1}$ .
- a. Rispettivamente,  $7^3$  e  $7^2$  elementi.  
 b. Siccome  $x^3 + 2$  è irriducibile su  $\mathbb{Z}_7$  (poiché di terzo grado senza radici in  $\mathbb{Z}_7$ ),  $\mathbb{Z}_7[x]/(x^3 + 2)$  è un dominio e un campo. Siccome  $x^2 + x + 1$  è riducibile su  $\mathbb{Z}_7$  ( $x=2$  è una radice),  $\mathbb{Z}_7[x]/(x^2 + x + 1)$  non è né un dominio né un campo.  
 c.  $\frac{x+1 \cdot 2x+3}{2x^2+5x+3} = \overline{2x^2+5x+3}$ , e questa espressione non può essere semplificata in  $\mathbb{Z}_7[x]/(x^3 + 1)$ .  
 In  $\mathbb{Z}_7[x]/(x^2 + x + 1)$ , invece, la classe  $\overline{x^2}$  è la classe  $\overline{-x-1}$ , quindi la classe  $\overline{2x^2+5x+3}$  è la classe  $\overline{3x+1}$ .
- a.  $1683 = 9 \cdot 11 \cdot 17$ : non essendo un numero primo l'anello  $\mathbb{Z}_{1683}$  non è un campo.  
 b. Due classi che verificano questa proprietà sono ad esempio  $\bar{a} = \overline{99}$ ,  $\bar{b} = \overline{17}$ .  
 c. La classe  $\bar{4}$  è invertibile, perché il MCD tra 4 e 1683 è 1. Per trovare la classe inversa si deve risolvere la congruenza  $4x \equiv 1 \pmod{1683}$  che ha come soluzione la classe  $\overline{421}$ .
- a.  $2079 = 3^3 \cdot 7 \cdot 11$ : non essendo un numero primo, l'anello  $\mathbb{Z}_{2079}$  non è un campo.  
 b. Due classi che verificano questa proprietà sono ad esempio  $\bar{a} = \overline{27}$ ,  $\bar{b} = \overline{77}$ .  
 c. La classe  $\bar{4}$  è invertibile, perché il MCD tra 4 e 2079 è 1. Per trovare la classe inversa si deve risolvere la congruenza  $4x \equiv 1 \pmod{2079}$  che ha come soluzione la classe  $\overline{520}$ .
- a. Per  $k=1$ .  
 b. Per  $k=1$  il MCD è  $x^2+1$ , per  $k \neq 1$  il MCD è 1.
- a.  $x^3 + 4x^2 + 2x + 3 = (x^2 + 2)(x + 4)$  in  $\mathbb{Z}_5[x]$ . Essendo il polinomio riducibile,  $A$  non è un campo.  
 b.  $\overline{3x^3+x}$  è un divisore dello zero, perché  $3x^3 + x = 3x(x^2 + 2)$ , da cui  $\overline{(3x^3+x)} \cdot \overline{(x+4)} = \overline{3x} \cdot \overline{(x^2+2)} \cdot \overline{(x+4)} = \overline{0}$ .
- a.  $x^3 + 3x + 2$  è irriducibile su  $\mathbb{Z}_5$  perché di terzo grado e privo di radici in  $\mathbb{Z}_5$ . Quindi il quoziente è un campo (che ha 125 elementi).  
 b. La classe  $\overline{x^5 + 4x + 1}$  è uguale a  $\overline{3x^2 + 3x + 2}$  che è diversa dalla classe nulla. Quindi è invertibile e la sua inversa è  $\overline{3x+2}$ .
- Trattandosi di un polinomio di terzo grado sarà sicuramente riducibile sia su  $\mathbb{C}$  sia su  $\mathbb{R}$ . Su  $\mathbb{Q}$  il polinomio è irriducibile qualunque sia  $a$  perché si può applicare il criterio di Eisenstein con  $p=5$ .

a. Il quoziente  $\mathbb{Z}_5[x]/(x^2 - c)$  è un campo se e solo se  $x^2 - c$  è un polinomio irriducibile su  $\mathbb{Z}_5$ . Trattandosi di un polinomio di secondo grado, esso sarà irriducibile se e solo se è privo di radici in  $\mathbb{Z}_5$ . Gli unici elementi di  $\mathbb{Z}_5$  che sono quadrati perfetti sono  $\bar{0}$ ,  $\bar{1}$  e  $\bar{4}$ . Quindi i valori di  $c$  per cui  $x^2 - c$  è irriducibile sono  $c = 2$  e  $c = 3$ . Quindi  $\mathbb{Z}_5[x]/(x^2 - c)$  è un campo se e solo se  $c = 2$  e  $c = 3$ .

b. Gli elementi invertibili di  $\mathbb{Z}_8[x]/(x^2 - 2)$  sono tutte le classi non nulle, ossia i 24 elementi non nulli.  
 c.  $\mathbb{Z}_5[x]/(x^2 - 4)$  non è un campo. Essendo finito, non può essere nemmeno un dominio di integrità, quindi avrà dei divisori dello zero. Dato che  $x^2 - 4 = (x-2)(x+2)$ , sicuramente  $\overline{x+2}$  e  $\overline{x-2}$  sono divisori dello zero. Ce ne sono altri?

Si deve prendere un polinomio di secondo grado irriducibile su  $\mathbb{Z}_3$ , ad esempio  $x^2 + 1$  e considerare il quoziente

$$\mathbb{Z}_3[x]/(x^2 + 1) = \{a_0 + a_1x, | a_0, a_1 \in \mathbb{Z}_3, x^2 \equiv -1\}$$

Gli elementi di  $\mathbb{Z}_3[x]/(x^2 + 1)$  sono le nove classi

$$\{\bar{0}, \bar{1}, \bar{2}, \bar{x}, \bar{2x}, \bar{1+x}, \bar{1+2x}, \bar{2+x}, \bar{2+2x}\}$$

e si deve tener presente che  $\bar{x}^2 = \bar{-1} = \bar{2}$ .

Fate voi la tavola additiva e la tavola moltiplicativa e verificate che si tratta di un campo.

## SOLUZIONI RELATIVE AL CAPITOLO 8

$(N, -)$  non è un gruppoide, dato che la differenza di due elementi di  $N$  non sempre è un elemento di  $N$ . Quindi non ha senso chiedersi se sia un semigruppo o un monoide.

L'insieme  $S$  rispetto all'unione è un monoide, perché, oltre ad essere un gruppoide e un semigruppo, possiede l'insieme vuoto  $\emptyset$  come elemento neutro.

Supponiamo per assurdo che esista un altro elemento  $u \in G$ , neutro rispetto all'operazione di  $G$ . Allora risulta  $eg = ge = g \quad \forall g \in G$ ,  $ug = gu = g \quad \forall g \in G$ . In particolare sarà  $eu = ue = e$  (dato che  $u$  è elemento neutro) e  $eu = ue = u$  (dato che  $e$  è elemento neutro) da cui  $u = e$ .

Siano  $a'$  e  $a''$  due inversi dello stesso elemento  $a \in G$ . Allora  $a' = ea' = (a''a)a' = a''(aa') = a''e = a''$ .

$b^{-1}a^{-1}$  è un inverso di  $ab$ , quindi è l'inverso. Così, dalle  $aa^{-1} = a^{-1}a = e$  segue che  $a$  è un inverso di  $a^{-1}$ , quindi è l'inverso.

Basta moltiplicare entrambi i membri della prima relazione a sinistra per  $a^{-1}$  e entrambi i membri della seconda a destra per  $a^{-1}$ . Si osservi che è importante che l'elemento da cancellare sia sempre dalla stessa parte, perché il gruppo non è abeliano in genere.

La condizione è ovviamente necessaria. Mostriamo la sufficienza. Se  $S$  è ridotto al solo elemento neutro, è automaticamente un sottogruppo. Sia allora  $a \in S$ ,  $a \neq e$ ; allora l'elemento  $e = aa^{-1}$  sta in  $S$ . Prendendo allora i due elementi  $e \in S$  e  $a \in S$ , si ha  $ea^{-1} = a^{-1} \in S$ . Infine, presi gli elementi  $a$  e  $b^{-1}$  (appartenenti ad  $S$  se  $a$  e  $b$  stanno in  $S$  per quanto mostrato ora), si ha  $a(b^{-1})^{-1} = ab \in S$ .

Occorre mostrare che se  $H$  è un qualunque sottogruppo di  $G$  che contiene  $g$ , allora  $H$  contiene necessariamente  $\langle g \rangle$ .

Sia  $H \leq G = \langle g \rangle$ . Se  $H = \{e\}$ , allora  $H$  è certamente ciclico. Sia quindi  $g^t \in H$ ,  $g^t \neq e$ . Allora anche  $g^{-t} \in H$ , e quindi  $H$  conterrà un elemento del tipo  $g^h$ , con  $h \in \mathbb{N}$ . Tra gli elementi appartenenti ad  $H$ , sia  $m$  il minimo intero positivo tale che  $g^m \in H$ . Proviamo che  $H = \langle g^m \rangle$ . Certamente  $\langle g^m \rangle \subseteq H$ . Viceversa, sia  $g^k \in H$ . Dividendo  $k$  per  $m$  si ha  $k = mq + r$ ,  $0 \leq r < m$ , da cui  $g^k = g^{mq}g^r$ , cioè  $g^r = g^{-mq}g^k \in H$ . Deve allora essere  $r = 0$ , ossia  $k = mq$ , cioè  $g^k = (g^m)^q \in \langle g^m \rangle$ .

a. Sia  $H = \langle g^m \rangle$  un sottogruppo di  $G$ . Ricordando che ogni sottogruppo di un gruppo ciclico è ciclico, risulta  $(g^m)^n = (g^n)^m = e^m = e$ . Quindi il periodo  $t$  di  $g^m$  divide  $n$  (basta dividere  $n$  per  $t$  e ricordare la definizione di periodo di un elemento). Dato che l'ordine di  $H$  coincide con il periodo di  $g^m$ , si ha la tesi.

b. Sia ora  $k$  un divisore di  $n$ . Il sottogruppo  $\langle g^{n/k} \rangle$  ha ordine  $k$ . Faremo vedere che è l'unico sottogruppo di  $G$  di quest'ordine. Sia  $H$  un sottogruppo di  $G$  di ordine  $k$ . Esso sarà del tipo  $H = \langle g^m \rangle$ , con  $m$  il minimo intero positivo tale che  $g^m \in H$ . Inoltre,  $m \mid n$ , come si vede facendo la divisione di  $n$  per  $m$ . Allora  $|H| = k = |\langle g^m \rangle| = n/m$ . Ne segue che  $m = n/k$ , e quindi  $H = \langle g^{n/k} \rangle$ .

Supponiamo  $g$  di periodo infinito. Allora la relazione  $g^h = g^k$  (ossia  $g^{h-k} = e$ ) implica  $h = k$ , per definizione di periodo infinito. Sia ora  $g$  di periodo  $n$ . Osserviamo innanzitutto che tutti gli elementi  $e, g, g^2, \dots, g^{n-1}$  sono distinti (perché?). Per provare che  $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$  basta far vedere che ogni potenza  $g^k$ ,  $k \in \mathbb{Z}$  sta in  $\{e, g, g^2, \dots, g^{n-1}\}$ : infatti dividendo  $k$  per  $n$  si ha  $k = nq + r$ ,  $0 \leq r < n$ , da cui  $g^k = g^{nq+r} = (g^n)^q g^r = e^q g^r = g^r$ . Quindi  $g^k \in \{e, g, g^2, \dots, g^{n-1}\}$  per ogni  $k \in \mathbb{Z}$ .

Supponiamo ora  $g^h = g^k$ . Allora  $g^{h-k} = e$ . Dividendo  $h - k$  per  $n$  si ha  $h - k = nq + r$ ,  $0 \leq r < n$  da cui  $g^{h-k} = (g^n)^q g^r = g^r = e$ . Quest'ultima uguaglianza non contraddice il fatto che  $n$  è il periodo di  $g$  solo se  $r = 0$  per cui  $h \equiv k \pmod{n}$ . Viceversa, se  $h \equiv k \pmod{n}$ , allora  $g^{h-k} = g^{nq} = (g^n)^q = e$ , ossia  $g^h = g^k$ .

Non è un sottogruppo, perché, pur essendo chiuso rispetto alla moltiplicazione, pur avendo l'elemento neutro ( $=1$ ),  $S$  non contiene gli inversi dei suoi elementi (l'inverso di un elemento del tipo  $\frac{1}{n}$  è  $n$  che non appartiene a  $S$ ).

Non è un sottogruppo, perché, pur essendo chiuso rispetto alla moltiplicazione, pur avendo l'elemento neutro ( $=1$ ),  $S$  non contiene gli inversi dei suoi elementi (l'inverso di un elemento del tipo  $n$  è  $\frac{1}{n}$  che non appartiene a  $S$ ).

$X$  è un sottogruppo di  $\mathbb{Z}_8$ , mentre  $Y$  non lo è: infatti, per esempio,  $\bar{1} + \bar{3} = \bar{4} \notin Y$ .

Il risultato dell'operazione  $*$  è ancora un numero naturale, quindi  $*$  è chiusa,  $*$  è associativa perché tale è l'addizione modulo 10. L'elemento neutro è lo zero. L'opposto del numero  $n_1 n_2 \dots n_h$  è il numero  $n'_1 n'_2 \dots n'_h$ , dove  $n'_i$  è l'opposto modulo 10 di  $n_i$ . Quindi  $(\mathbb{N}, *)$  è un gruppo. Si può generalizzare a basi arbitrarie  $n$ :  $(\mathbb{N}, *_n)$  è ancora un gruppo.

Basta dividere  $n$  per  $m$  e verificare che il resto è nullo.

Sia  $a \neq 0$  e sia  $k$  il suo ordine. Per definizione di ordine,  $k$  è il più piccolo intero positivo tale che  $ka = 0$ . Allora deve essere  $ka$  un multiplo di  $n$  (e ovviamente  $ka$  è un multiplo di  $a$ ). Allora  $ka$  è multiplo comune di  $a$  e di  $n$ ; dovendo essere il minimo, esso è il  $\text{mcm}(a, n)$ . Quindi  $ka = an/(a, n)$ , ossia  $k = n/(a, n)$ .

Servendosi dell'esercizio precedente, si verifica facilmente che gli elementi di periodo 4 sono 2500 e 7500. Quelli di periodo 8 sono 1250, 3750, 6250 e 8750.

Indicati con  $\gamma_1, \gamma_2, \dots, \gamma_k$  i cicli disgiunti della  $\sigma$ , per provare che  $\sigma = \gamma_1 \gamma_2 \dots \gamma_k$  occorre provare che per ogni  $x \in X = \{1, 2, \dots, n\}$  si ha  $\sigma(x) = (\gamma_1 \gamma_2 \dots \gamma_k)(x)$ . Ora, ogni  $x \in X$  compare nella scrittura di uno solo dei cicli  $\gamma_1, \gamma_2, \dots, \gamma_k$ ; sia questo il ciclo  $\gamma_i = (x, \sigma(x), \dots, \sigma^{m-1}(x))$ . Inoltre, per ogni  $j \neq i$ , e ogni  $y = \sigma^j(x)$  (cioè per ogni  $y$  che compare nella scrittura di  $\gamma_i$ ) risulta  $\gamma_j(y) = y$ . Allora, per ogni  $x \in X$   $(\gamma_1 \gamma_2 \dots \gamma_k)(x) = (\gamma_1 \gamma_2 \dots \gamma_k)(x) = \gamma_1 \gamma_2 \dots \gamma_{i-1}(\sigma(x)) = \sigma(x)$ . Quindi  $\sigma = \gamma_1 \gamma_2 \dots \gamma_k$ .

Se  $\sigma = \gamma_1 \gamma_2 \dots \gamma_k$ , indicato con  $m_i$  l'ordine del ciclo  $i$ -esimo, e con  $M = \text{mcm}(m_1, m_2, \dots, m_k)$ , si tratta di provare che  $M$  uguaglia il periodo  $N$  di  $\sigma$ . Infatti

$$\sigma^M = (\gamma_1 \gamma_2 \dots \gamma_k)^M \stackrel{\text{cicli disgiunti}}{=} \gamma_1^M \gamma_2^M \dots \gamma_k^M = id$$

quindi  $N \mid M$ . Inoltre,  $id = \sigma^N = \gamma_1^N \gamma_2^N \dots \gamma_k^N = id \cdot id \cdot id \dots id$ . Ma allora  $m_i \mid N$  per ogni  $i = 1, \dots, k$ , da cui  $M \mid N$ . Quindi  $N = M$ .

a. Scrivendo  $\sigma$  e  $\tau$  come prodotto di cicli disgiunti si ha  $\sigma = (1, 3, 4, 2)$ ,  $\tau = (1, 2, 4)$ , da cui si ha subito che  $\sigma$  ha periodo 4, mentre  $\tau$  ha periodo 3.

b.

$$\sigma^{-1} = (1, 2, 4, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

$$\tau^{-1} = (1, 4, 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (3, 4).$$

c. No, perché non è chiuso rispetto al prodotto ( $\sigma \circ \tau \notin S$ ) e nemmeno rispetto all'inverso ( $\sigma^{-1} \notin S$ ,  $\tau^{-1} \notin S$ ).

a. Scrivendo  $\sigma$  e  $\tau$  come prodotto di cicli disgiunti si ha  $\sigma = (1, 2, 3, 4)$ ,  $\tau = (1, 3, 4)$ , da cui si ha subito che  $\sigma$  ha periodo 4, mentre  $\tau$  ha periodo 3.

b.

$$\sigma^{-1} = (1, 4, 3, 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\tau^{-1} = (1, 4, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1, 4, 2, 3).$$

c. No, perché non è chiuso rispetto al prodotto ( $\sigma \circ \tau \notin S$ ) e nemmeno rispetto all'inverso ( $\sigma^{-1} \notin S$ ,  $\tau^{-1} \notin S$ ).

## SOLUZIONI RELATIVE AL CAPITOLO 9

a.  $(x + y + z)0$ .

$$b. \overline{x_1 + x_2 + \dots + x_n}.$$

$$c. x + y + \overline{(x + y + z)} = x + y + xy\bar{z} = x + x\bar{y}\bar{z} + y = (\text{per la legge di assorbimento}) = x + y.$$

$$d. x(\bar{x} + y) = xy.$$

- Basta provare che le tavole di verità del primo e del secondo membro coincidono.

$x$	$y$	$z$	$x\bar{y}$	$y\bar{z}$	$\bar{x}z$	$x\bar{y} + y\bar{z} + \bar{x}z$	$\bar{x}y$	$\bar{y}z$	$x\bar{z}$	$\bar{x}y + \bar{y}z + x\bar{z}$
1	1	1	0	0	0	0	0	0	0	0
1	1	0	0	1	0	1	0	0	1	1
1	0	1	1	0	0	1	0	1	0	1
0	1	1	0	0	1	1	1	0	0	1
1	0	0	1	0	0	1	0	0	1	1
0	1	0	0	1	0	1	1	0	0	1
0	0	1	0	0	1	0	0	1	0	1
0	0	0	0	0	0	0	0	0	0	0

●  $2^n$ .

●  $\bar{x}_1x_2\bar{x}_3\bar{x}_4x_5x_6$ .

●  $f(x, y, z) = x\bar{y}z + xy\bar{z} + xyz$ .

● Occorre innanzitutto determinare la tabella dei valori assunti da  $f$ :

$x$	$y$	$z$	$f(x, y, z) = x(y + \bar{z})$
0	0	0	0
0	0	1	0
0	1	0	0
1	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1
1	1	1	1

La forma normale disgiuntiva è pertanto

$$f(x, y, z) = x\bar{y}\bar{z} + xy\bar{z} + xyz.$$

● La tabella da associare è la seguente:

	$y$	$\bar{y}$
$x$	1	
$\bar{x}$		1

I rettangoli massimali sono due, e corrispondono ad un solo quadrato, cioè hanno area 1 (se pensiamo al quadrato unitario avente area 1).

	$y$	$\bar{y}$
$x$	-1-	
$\bar{x}$		-1-

Ciò significa che l'espressione originaria era già in forma minimale.

● L'espressione booleana è già in forma disgiuntiva normale. Risolveremo il problema in due modi servendoci di due mappe di Karnaugh diverse.

- *Prima mappa* (divisione delle congiunzioni fondamentali come prodotto di  $k = 1$  e  $4 - 1 = 3$  fattori)

	$yzt$	$y\bar{z}\bar{t}$	$y\bar{z}t$	$y\bar{z}t$	$\bar{y}zt$	$\bar{y}\bar{z}\bar{t}$	$\bar{y}\bar{z}t$	$\bar{y}zt$
$x$	1	1						1
$\bar{x}$	1							1

I rettangoli massimali sono i seguenti tre:

	$yzt$	$y\bar{z}\bar{t}$	$y\bar{z}t$	$\bar{y}zt$	$\bar{y}\bar{z}\bar{t}$	$\bar{y}\bar{z}t$	$\bar{y}zt$
$x$	1	1					
$\bar{x}$	1						

L'espressione minimale è pertanto:

$$xyz + yzt + \bar{y}zt.$$

- *Seconda mappa* (divisione delle congiunzioni fondamentali come prodotto di  $k = 2$  e  $4 - 2 = 2$  fattori)

	$zt$	$z\bar{t}$	$\bar{z}\bar{t}$	$\bar{z}t$
$xy$	1	1		
$x\bar{y}$			1	
$\bar{x}y$			1	
$\bar{x}\bar{y}$	1			

I rettangoli massimali sono i seguenti tre:

	$zt$	$z\bar{t}$	$\bar{z}\bar{t}$	$\bar{z}t$
$xy$	-1	-1		
$x\bar{y}$			1	
$\bar{x}y$			1	
$\bar{x}\bar{y}$	-1			

L'espressione minimale è pertanto:

$$xyz + yzt + \bar{y}zt.$$

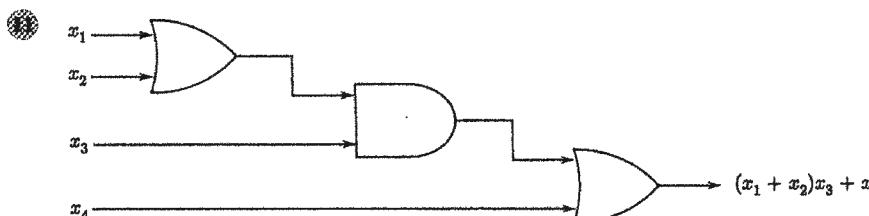


Figura 1.

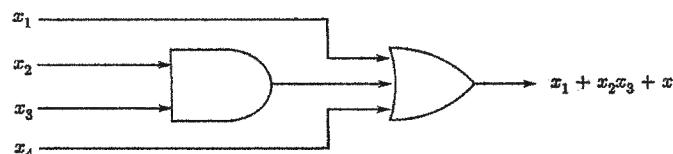


Figura 2.



Figura 3.



Figura 4.

La commutatività, la associatività e l'idempotenza di  $\wedge$  e  $\vee$  sono banali. Proviamo la legge di assorbimento:

$$x \wedge (x \vee y) = x \wedge \sup(x, y) = \inf(x, \sup(x, y)) = x$$

e analogamente l'altra.

Occorre provare che la  $x \preceq y$  è una relazione d'ordine.

- Riflessiva: dalla  $x \wedge y = x$  e  $x \vee x = x$  per ogni  $x$  segue  $x \preceq x$ .
- Antisimmetrica: per ogni  $x, y$  se  $x \preceq y$  e  $y \preceq x$  segue  $x \wedge y = x$  e  $y \wedge x = y$ ; per la commutatività di  $\wedge$  si ha  $x = y$ .
- Transitività: per ogni  $x, y, z$  se  $x \preceq y$  e  $y \preceq z$  segue  $y \wedge z = y$  e  $y \wedge z = y$ . Quindi  $x = x \wedge y = x \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge z$ , per cui  $x \preceq z$ .

Per ogni  $i = 1, 2, \dots, n$   $(x_1 + x_2 + \dots + x_n)x_i = 0 + 0 + \dots + 0 + x_i + 0 + \dots + 0 = x_i$ , da cui  $(x_1 + x_2 + \dots + x_n)x = x$  per ogni  $x \in \mathcal{B}$ . Ne segue che  $1 = x_1 + x_2 + \dots + x_n$ .

### SOLUZIONI RELATIVE AL CAPITOLO 10

8 grafi.

In  $2^n$  modi.

a. Nessuno.

b. Sono 10: 12345, 123945, 123987945, 1239765, 12398945, 12398765, 1239879345, 18765, 189765, 18945.

c. Il solo cammino 135.

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

N.B. Si tratta di una matrice simmetrica, dato che il grafo non è orientato.

Si tratta del grafo della figura 5.

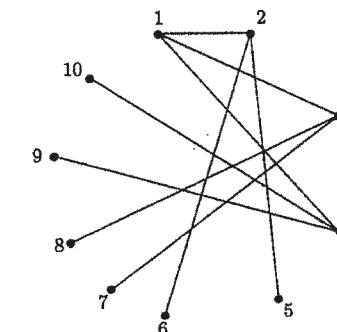


Figura 5.

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

La (i) è ovvia, perché quando si fa la somma di quantità non negative (corrispondenti agli elementi di  $A^k$ ) si ottiene un intero non negativo. Questa somma sarà positiva se almeno uno è positivo (strettamente).

La (ii) deriva dallo sviluppo

$$(I + A)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} A^k I^{n-1-k} = \sum_{k=0}^{n-1} \binom{n-1}{k} A^k$$

e dall'osservazione che ciascuno dei coefficienti binomiali è positivo.

a. Si tratta del grafo della figura 6

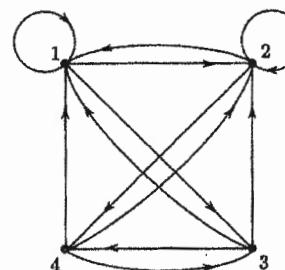


Figura 6.

$$\text{b. } A^2 = \begin{pmatrix} 3 & 3 & 1 & 2 \\ 3 & 3 & 1 & 2 \\ 3 & 3 & 1 & 2 \\ 3 & 3 & 0 & 3 \end{pmatrix}, \quad A^3 = \begin{pmatrix} 9 & 9 & 2 & 7 \\ 9 & 9 & 2 & 7 \\ 9 & 9 & 2 & 7 \\ 9 & 9 & 3 & 6 \end{pmatrix}$$

c. Facciamo qualche controllo. I percorsi di lunghezza 2 da  $v_1$  a  $v_1$  sono tre:  $v_1v_1v_1$ ,  $v_1v_2v_1$ ,  $v_1v_4v_1$ . I percorsi di lunghezza 2 da  $v_3$  a  $v_4$  sono due:  $v_3v_2v_4$  e  $v_3v_1v_4$ . I percorsi di lunghezza 2 da  $v_4$  a  $v_1$  sono tre:  $v_4v_1v_1$ ,  $v_4v_2v_1$  e  $v_4v_3v_1$ . I percorsi di lunghezza 3 da  $v_1$  a  $v_1$  sono nove:  $v_1v_1v_1v_1$ ,  $v_1v_1v_2v_1$ ,  $v_1v_1v_4v_1$ ,  $v_1v_2v_2v_1$ ,  $v_1v_2v_1v_1$ ,  $v_1v_2v_4v_1$ ,  $v_1v_4v_1v_1$ ,  $v_1v_4v_2v_1$  e  $v_1v_4v_3v_1$ . I percorsi di lunghezza 3 da  $v_4$  a  $v_1$  sono nove:  $v_4v_1v_1v_1$ ,  $v_4v_1v_4v_1$ ,  $v_4v_1v_2v_1$ ,  $v_4v_2v_2v_1$ ,  $v_4v_2v_1v_1$ ,  $v_4v_3v_2v_1$ ,  $v_4v_3v_4v_1$ ,  $v_4v_3v_1v_1$ ,  $v_4v_2v_4v_1$ . Proseguite voi i controlli.

È costituito da due soli elementi: l'applicazione identica e l'applicazione che scambia 1 con 4 e 2 con 3, e lascia fisso 5.

È costituito dai movimenti che lasciano fisso  $a$  (quindi sono in tutto 6).

No, perché contiene un sottografo contraibile per archi a  $K_{3,3}$ .

No, perché contiene un sottografo contraibile per archi a  $K_5$ .

## SOLUZIONI RELATIVE AL CAPITOLO 11

Ricordando che  $ab' = ba'$  e  $cd' = dc'$ , si vede immediatamente che tale relazione è verificata. Analoga dimostrazione per la moltiplicazione.

$f(x) = \sum_{k=0}^m \binom{n}{k} x^k$  = (in virtù della formula (2.2) dello sviluppo della potenza di un binomio)  $= (1+x)^n$ .

## SOLUZIONI RELATIVE ALL'APPENDICE

Dato che le fattorizzazioni in primi rispettivamente di 8, 15, 6 e 48 sono  $8 = 2^3$ ,  $15 = 3 \cdot 5$ ,  $6 = 2 \cdot 3$  e  $48 = 2^4 \cdot 3$ , utilizzando le proprietà delle potenze si ha:  $8^6 \cdot 15^3 \cdot 6^5 \cdot 48^8 = 2^{18} \cdot 3^3 \cdot 5^3 \cdot 2^6 \cdot 3^5 \cdot 2^{32} \cdot 3^8 = 2^{55} \cdot 3^{16} \cdot 5^3$ .

$3^{20}, 2^{89}, 1, -2^{12}$ .

$(5^{15})^2 = 5^{30}$ ,  $\frac{1}{2}4^{30} = \frac{1}{2}2^{60} = 2^{59}$ ,  $\frac{-2^8}{(-4)^8} = 2^8 \cdot 2^{-10} = 2^{-2} = \frac{1}{4}$ ,  $\frac{(-2)^5}{(-4)^{-4}} = -\frac{2^5}{2^{-8}} = -2^{13}$ .

$26^{15} = (2 \cdot 13)^{15}$ . Quindi  $\frac{1}{2}26^{15} = 2^{14} \cdot 13^{15}$ .

È il minimo comune multiplo tra 2, 3, 9, 11, quindi è  $2 \cdot 9 \cdot 11$ .

$-|-4| = -4$ ,  $| -2 | + | 2 | = 4 = |-4|$ ,  $| 2 | - | -2 | = 0 = -2 + | -2 |$  quindi

$-|-4| = -4 < | 2 | - | -2 | = 0 = -2 + | -2 | < | -2 | + | 2 | = |-4| = 4$ .

$-2^{3^2} = (-2)^{3^2} < -| 3.5 | = -3.5 < -\frac{8}{3} < | -3.5 | < 2^{3^2}$ .

$= (2^3)^3 \cdot 2^4 \cdot 5^4 \cdot 2^2 \cdot 3^2 \cdot (2^2)^4 \cdot 3^4 = 2^9 \cdot 2^4 \cdot 5^4 \cdot 2^2 \cdot 3^2 \cdot 2^8 \cdot 3^4 = 2^{23} \cdot 3^6 \cdot 5^4$ .

$\frac{1}{2} \cdot 2^{28} = \frac{1}{2} \cdot 2^{28} \cdot 7^{28} = 2^{27} \cdot 7^{28}$ .

$= 12^4 \cdot 6^2 \cdot 32^2 \cdot 14^3 = (2^2 \cdot 3)^4 \cdot (2 \cdot 3)^2 \cdot (2^5)^2 \cdot (2 \cdot 7)^3 = 2^8 \cdot 3^4 \cdot 2^2 \cdot 3^2 \cdot 2^{10} \cdot 2^3 \cdot 7^3 = 2^{8+2+10+3} \cdot 3^{4+2} \cdot 7^3 = 2^{23} \cdot 3^6 \cdot 7^3$ .

$(-3)^6 = 3^6$ .

9.

$\frac{1}{9}$ .

È il minimo comune multiplo tra 4, 25, 6, 15, ossia 300.

$(-2)^{8^2} = (-2)^9 = (-2)^4 \cdot (-2)^4 \cdot (-2) = 16 \cdot 16 \cdot (-2) = -512$

$(-2)^{2^3} = (-2)^8 = 256$

$((-2)^3)^2 = (-2)^{2 \cdot 3} = ((-2)^2)^3 = (-2)^6 = 64$

$(-2)^3 \cdot (-2)^2 = (-2)^{3+2} = (-2)^5 = -32$ .

Il terzo, il quarto e il quinto numero sono uguali, dato che

$$(a^b)^c = a^{bc} = a^{cb} = (a^c)^b$$

$-3^{2^5} < (-3)^{5^2} = -3^{5^2} < -(3^5)^2 < (3^5)^2 = ((-3)^5)^2 < 3^{5^2} < 3^{2^5} = (-3)^{2^5}$ .

$= (2 \cdot 3)^3 (2 \cdot 5)^4 (3^2)^3 (3 \cdot 5)^3 = 2^7 \cdot 3^{12} \cdot 5^7.$

$\frac{11}{100}.$

$-1.$

Dato che  $a^2 + b^2$  per  $a$  e  $b$  diversi da zero è diverso da zero, perché sia  $(a^2 + b^2)(a^2 - b^2) = 0$  deve essere  $a^2 - b^2 = 0$  ossia  $(a+b)(a-b) = 0$ . Ciò implica la relazione:  $a = b$  o  $a = -b$ .

Due interi che verificano la predetta relazione sono per esempio 5 e -5. Due interi che non la verificano sono 4 e 5.

Che  $a = b = 0$  e  $c \neq 0$ .

Che  $a = b$  oppure  $a = -b$ .

Il prodotto di due numeri interi è uguale a zero se e solo se almeno uno dei due è zero. Quindi o  $a + b = 0$  oppure  $a = -b$ . Quindi la relazione tra  $a$  e  $b$  è che sia  $a = -b$  oppure  $a = 2b$ . I due interi  $a = 5$  e  $b = -5$  verificano la condizione, e così anche i due interi  $a = 2$ ,  $b = 1$ .

Che almeno due tra loro devono essere coincidenti.

$-a < -b$  (moltiplicando i due membri di una diseguaglianza per un numero negativo (-1) la diseguaglianza si inverte).

$a - 3 > b - 3$  (aggiungendo o togliendo ad ambo i membri di una diseguaglianza uno stesso numero la diseguaglianza mantiene lo stesso verso)

$\frac{a}{3} > \frac{b}{3}$  (moltiplicando ambo i membri di una diseguaglianza per un numero positivo ( $\frac{1}{3}$ ) la diseguaglianza mantiene lo stesso verso).

$2x^5 - x^3 + 6x^2 - 3 = x^3(2x^2 - 1) + 3(2x^2 - 1) = (2x^2 - 1)(x^3 + 3).$

$(m+n)(m+n-1).$

$7x(x-5y) + 2(x-5y) = (x-5y)(7x+2).$

$a(x^2 + 1) - x(a^2 + 1) = ax^2 + a - xa^2 - x = ax^2 - xa^2 + a - x = ax(x-a) + a - x = (x-a)(ax-1).$

$x^3y^3 + 3x^3 - 3y^3 - 9 = x^3(y^3 + 3) - 3(y^3 + 3) = (x^3 - 3)(y^3 + 3).$

$-b^8$

Osservazione: non si dovevano sviluppare tutti i prodotti. Bastava osservare che si tratta di prodotti notevoli, quindi...

$2x^3$ . Anche qui si doveva osservare che  $(x+y)(x^2 - xy + y^2) = x^3 + y^3$  e che  $(x-y)(x^2 + xy + y^2) = x^3 - y^3$ .

0.

$\frac{2}{3}a + 5b.$

$-\frac{15}{64}.$

Attenzione: sostituire i valori numerici solo dopo avere semplificato l'espressione!

$-(a+b+c).$

Osservare che a numeratore c'è la differenza di due quadrati.

$-\frac{x(x+y)}{y}.$

Posto  $x = 3,0\overline{27}$  si ha  $10x = 30 + 0,\overline{27} = 30 + \frac{27}{99} = 30 + \frac{3}{11}$ , da cui  $x = 3 + \frac{3}{110} = \frac{333}{110}$ .

Posto  $x = 2,0\overline{36}$  si ha  $10x = 20 + 0,\overline{36} = 20 + \frac{36}{99} = 20 + \frac{4}{11}$ , da cui  $x = 2 + \frac{4}{110} = \frac{112}{55}$ .

$A = \mathbb{N} \setminus \{0\}, B = \{\pm 1, \pm 2, \pm 5, \pm 10\}, C = \{-3, -2, -1, 0, 1, 2, 3, 4\}.$

$B = \{0, 1, 2, 3\}$  (attenzione: si devono inserire solo i numeri *naturali* che soddisfano la disequazione  $n^2 - 16 < 0$ ).  $A \cap B = \{3\}, A \cup B = \{-5, -4, -3, 0, 1, 2, 3, 4, 5\}$ .

$A = \{0, \pm 1, \pm 2\}, B = \{0, 1, 2, 3\}, A \cap B = \{0, 1, 2\}, A \cup B = \{0, \pm 1, \pm 2, 3\}.$

$A = \{x \in \mathbb{Z} \mid (x-1)^2 \leq 0\} = \{1\}, B = \emptyset, C = \{x \in \mathbb{Z} \mid (x+1)^2 \geq 0\} = \mathbb{Z}$ . Quindi  $A \cap B = B \cap C = \emptyset, A \cap C = \{1\}, A \cup B = \{1\}, A \cup C = B \cup C = \mathbb{Z}$ .

Il prodotto cartesiano di due insiemi  $A$  e  $B$  è l'insieme  $A \times B := \{(a, b) \mid a \in A \text{ e } b \in B\}$ .

Attenzione quindi: il primo elemento della coppia deve stare in  $A$  e il secondo in  $B$ ; NON si possono mettere nel prodotto cartesiano nel primo elemento delle coppie elementi di  $B$  o viceversa.

Il prodotto cartesiano di due insiemi con rispettivamente  $n$  e  $m$  elementi ha  $n \cdot m$  elementi. Nel nostro caso avrà 8 elementi e si ha

$$A \times B = \{(1, 5), (2, 5), (3, 5), (4, 5), (1, 6), (2, 6), (3, 6), (4, 6)\}.$$

Per  $a \neq 0$   $\frac{x}{a} = \frac{b^2 - 5a^2}{6a}$ , per  $a = 0, b \neq 0$  nessuna soluzione, per  $a = 0, b = 0$  indeterminata (qualunque valore di  $x$  va bene).

$x = \pm \frac{\sqrt{6}}{2}.$

Le possibili radici sono da ricercarsi nell'insieme  $\{\pm 1, \pm 2, \pm \frac{1}{2}, \pm \frac{1}{4}\}$ . Sostituendo al posto della  $x$  questi numeri si vede che nessuno è radice del polinomio. Quindi il polinomio non ammette radici razionali.

$x^4 + 3x - a = (x^2 + 3)(x^2 - 3) + 3x + 9 - a$ . Quindi quoziente è  $x^2 - 3$  e resto  $3x + 9 - a$ . Ora, qualunque sia  $a$ , il polinomio  $3x + 9 - a$  non è mai il polinomio nullo, dato che il suo coefficiente direttivo è 3 che è indipendente da  $a$  e sempre diverso da zero. Quindi  $f(x)$  non è mai divisibile per  $g(x)$ .

Le possibili radici razionali sono i numeri razionali  $\frac{r}{s}$ , con  $\text{MCD}(r, s) = 1$  e  $r$  divisore di 1 (cioè  $\pm 1$ ) e  $s$  divisore di 3 (cioè  $\pm 1$  e  $\pm 3$ ). Quindi l'insieme delle possibili radici razionali è  $\{\pm 1, \pm \frac{1}{3}\}$ .

Si verifica (sostituendo tali valori al posto della  $x$ ) che nessuno di questi valori soddisfa l'equazione. Quindi l'equazione data non possiede radici razionali.

●  $x^4 + 3x^3 - 3 = (x^2 - 1)(x^2 + 3x + 1) + 3x - 2$ . Dato che il resto non è il polinomio nullo, il polinomio  $f(x)$  non è divisibile per  $g(x)$ .

●  $x = \frac{1}{2}, x = -5$ .

●  $x = 1, x = 3$ .

● Radici razionali:  $-\frac{3}{4}, 2, -7$ . Le ulteriori radici sono o complesse (le due radici di  $x^2 + 1 = 0$ , che è privo di radici reali) oppure reali e non razionali (le due radici di  $x^2 - 3 = 0$  che sono  $\pm\sqrt{3}$ ). Di queste sono intere 2 e -7. C'è un solo numero naturale soluzione del polinomio.

● Solamente per  $a = \pm 1$ . Infatti per  $a = \pm 1$  si ha  $0x = 1$ , che non è soddisfatta da nessun numero reale. Per  $a \neq \pm 1$  invece l'equazione ammette una e una sola soluzione che è  $\frac{1}{a^2-1}$ .

●  $x^4 - 16 = (x^2 - 4)(x^2 + 4) = (x - 2)(x + 2)(x^2 + 4)$ . Le uniche radici intere sono  $\pm 2$ . Il polinomio  $x^2 + 4$  è privo di radici reali (e quindi, a maggior ragione, di radici intere).

● Radici razionali:  $-\frac{2}{5}, -5, -10$ . Le ulteriori radici sono o complesse non reali (e quindi non razionali) (le due radici di  $x^2 + 6 = 0$ , che è privo di radici reali) oppure reali e non razionali (le due radici di  $x^2 - 5 = 0$  che sono  $\pm\sqrt{5}$ ). Di queste sono intere -5 e -10. Non ci sono soluzioni che sono interi naturali.

●  $(x-1)\left(1-\frac{3}{x-1}\right) = \frac{6-x^2}{1-x}$  è definita per ogni  $x \neq 1$ . Sviluppando si ha  $(x-1)\left(\frac{x-3}{x-1}\right) = \frac{6-x^2}{1-x}$  ossia  $x-4 = \frac{6-x^2}{1-x}$  da cui  $(1-x)(x-4) = 6-x^2$  e quindi  $x-4-x^2+4x=6-x^2$  da cui  $5x=10$  da cui  $x=2$  che è accettabile.

● Un tale polinomio è per esempio  $x^2 + 1$ , oppure un qualunque polinomio di secondo grado il cui discriminante sia minore di 0.

●  $x = \frac{2}{3}, x = -3$ .

● Tutte le radici di questa equazione sono le radici delle 4 equazioni:  $x^3 - 1 = 0$ ,  $(x^2 + 3) = 0$ ,  $x^2 - 8 = 0$  e  $x^2 - 16 = 0$ .  $x^3 - 1$  ha una sola radice razionale,  $x = 1$  che è anche un numero intero positivo. L'equazione  $x^2 + 3$  non ha radici razionali: non ha nemmeno radici reali. L'equazione  $x^2 - 8$  ha come radici  $\pm\sqrt{8}$  e  $\sqrt{8}$  non è un numero razionale.  $x^4 - 16 = (x^2 - 4)(x^2 + 4)$  e quindi le sue radici razionali sono  $\pm 2$ . In definitiva, le radici razionali dell'equazione data sono: 1, 2, -2. Si tratta di radici intere, delle quali 1 e 2 sono numeri naturali.

● Per nessun valore reale di  $k$ : infatti per ogni valore reale di  $k$   $k^2 + 1$  è sempre diverso da zero, e quindi per ogni  $k$  l'equazione data ha soluzione  $\bar{x} = \frac{8}{k^2+1}$ .

● L'equazione è equivalente alla  $(x+3)(x-1+x-2)=0$  ossia alla  $(x+3)(2x-3)=0$  le cui radici sono  $x = -3, x = \frac{3}{2}$ .

●  $(3x-1)[(x-5)-\frac{1}{3}(2x-3)] = (3x-1)(\frac{1}{3}x-4) = 0$  che ha come soluzioni  $x = \frac{1}{3}$  e  $x = 12$ .

● Definita per  $x \neq -1, -4$ . Per tali valori, essa è equivalente alla  $x+4-(x+1)(x+4)+x(x+1)=0$  che implica  $-3x=0$  ossia  $x=0$ . Quindi  $x=0$  è l'unica soluzione dell'equazione di partenza.

● Il discriminante dell'equazione quadratica è  $\Delta = a^2 + 4$  che è sempre  $> 0$ . Quindi l'equazione data ammette sempre radici reali qualunque sia  $a \in \mathbb{R}$ .

● Si tratta di risolvere la seguente disequazione:

$$4n - \frac{n}{3} < 5, \text{ ossia } 11n < 15.$$

C'è un unico numero naturale non nullo che soddisfa la diseguaglianza, ossia  $n = 1$ . Invece ci sono infiniti numeri interi che la soddisfano, ossia tutti gli interi minori o uguali ad 1.

●  $x = -\frac{7}{2}, x = \frac{11}{2}$ .

●  $x = -\frac{5}{2}, x = \frac{7}{2}$ . Spiegazione. Dobbiamo studiare il segno degli argomenti dei moduli, ossia di  $x+2$  e  $x-3$  per individuare i punti dell'asse reale in cui gli argomenti dei moduli cambiano segno.

Ora,  $x+2$  è maggiore o uguale a 0 per  $x \geq -2$  ( $e \leq 0$  per  $x \leq -2$ ), mentre  $x-3$  è minore o uguale a 0 per  $x \geq 3$  ( $e \leq 0$  per  $x \leq 3$ ). In corrispondenza agli intervalli dove l'argomento è negativo si deve cambiare il segno dell'argomento. Dobbiamo quindi prendere in considerazione i seguenti tre sistemi:

$$\begin{cases} x \leq -2 \\ -x-2+3-x=6 \end{cases} \quad \vee \quad \begin{cases} -2 \leq x \leq 3 \\ x+2+3-x=6 \end{cases} \quad \vee \quad \begin{cases} x \geq 3 \\ x+2+x-3=6 \end{cases}$$

ossia

$$\begin{cases} x \leq -2 \\ x=-\frac{5}{2} \end{cases} \quad \vee \quad \begin{cases} -2 \leq x \leq 3 \\ 5=6 \end{cases} \quad \vee \quad \begin{cases} x \geq 3 \\ x=\frac{7}{2} \end{cases}$$

Le soluzioni dell'equazione sono quindi date da  $x = -\frac{5}{2}, x = \frac{7}{2}$ .

● La funzione  $y = x^2 - x + 8$  rappresenta una parabola con la concavità rivolta verso l'alto (dato che il coefficiente direttivo è positivo). La parabola non interseca l'asse  $x$ , dato che per  $y=0$   $x^2 - x + 8 = 0$  non ammette radici reali: quindi  $x^2 - x + 8$  è sempre positivo per ogni valore di  $x$ .

● Dato che

$$|P(x)| = \begin{cases} P(x) & \text{se } P(x) \geq 0 \\ -P(x) & \text{se } P(x) < 0 \end{cases}$$

dobbiamo studiare il segno dell'argomento  $P(x)$  del modulo, ossia di  $x+1$  per individuare i punti dell'asse reale in cui l'argomento all'interno del modulo cambia segno.

Ora,  $x+1$  è maggiore o uguale a 0 per  $x \geq -1$  ( $e < 0$  per  $x < -1$ ). In corrispondenza all'intervallo dove l'argomento è negativo, per eliminare il modulo si deve cambiare il segno all'argomento, mentre nell'intervallo in cui l'argomento è maggiore o uguale a zero si può tranquillamente eliminare il modulo. Dobbiamo quindi prendere in considerazione i seguenti due sistemi:

$$\begin{cases} x \leq -1 \\ (x+1)^2 + 3x + 3 = 0 \end{cases} \quad \vee \quad \begin{cases} x > -1 \\ (x+1)^2 - 3x - 3 = 0 \end{cases}$$

Il primo sistema ammette come soluzioni -4 e -1, mentre il secondo ammette come soluzione  $x = 2$ . Quindi tutte e sole le soluzioni dell'equazione sono -4, -1, 2.

• Equivale alla

$$\frac{x+4}{x-9} - 1 < 0$$

ossia alla  $\frac{13}{x-9} < 0$ , che ha come soluzioni tutti i numeri reali compresi nell'intervallo  $(-\infty, 9)$ .

• Perché la frazione sia minore o uguale a zero, il numeratore e il denominatore devono essere discordi e il denominatore  $\neq 0$ . Dato però che il denominatore  $x^2$  è sempre  $\geq 0$ , ne segue che la frazione è  $\leq 0$  se e solo se il numeratore è minore o uguale a zero. Le radici del polinomio  $x^2 - 3x + 1$  sono  $\frac{3 \pm \sqrt{5}}{2}$ . Dato che le due radici sono entrambe positive, lo zero (dove non è definita la frazione) non si trova tra le due radici, quindi il numeratore sarà  $\leq 0$  per ogni  $x$  che sta nell'intervallo chiuso  $[\frac{3-\sqrt{5}}{2}, \frac{3+\sqrt{5}}{2}]$ .

•  $\log_2(x-2) + \log_2(2x-3) - 2\log_2 x = \log_2(x-2) + \log_2(2x-3) - \log_2 x^2$  da cui

$$\log \frac{(x-2)(2x-3)}{x^2} = 0$$

che implica che l'argomento deve essere 1, ossia  $\frac{(x-2)(2x-3)}{x^2} = 1$  da cui  $x^2 - (x-2)(2x-3) = 0$ , cioè  $x^2 - 7x + 6 = 0$  che ha come radici 6 e 1. Solo 6 è accettabile perché l'equazione originaria è definita solo per  $x > 2$ .

• È definita per ogni  $x > 0$ . Essa equivale alla  $\log_2 \frac{(x+3)}{x^2} = -2$  ossia alla  $\frac{x+3}{x^2} = \frac{1}{4}$  cioè  $x^2 - 4x - 12 = 0$  che ha come soluzioni 6 e -2: solo  $x = 6$  è però accettabile.

•  $(-\infty, -5] \cup (-4, \infty)$ .

• Definita per  $x > 1$ . Per tali valori è equivalente alla  $x^2 - 1 = 5$ . L'unica soluzione ammissibile è  $x = \sqrt{6}$ .

•  $(-\infty, -6) \cup [2, \infty)$ .

- a. Definito per ogni  $x \in \mathbb{R}$  tale che sia  $x^2 - 1 > 0$ , ossia per ogni  $x$  in  $(-\infty, -1) \cup (1, \infty)$ .  
 b. Si tratta di determinare gli  $x \in (-\infty, -1) \cup (1, \infty)$  tali che  $10^1 = x^2 - 1$ , ossia tali che  $x^2 = 11$ . Si tratta dei due numeri  $\pm\sqrt{11}$  (entrambi appartengono all'insieme di definizione).

## Indice analitico

### A

- Ackermann, funzione di, 63
- addizione tra polinomi, 150
- adiacenza
  - di vertici di un grafo, 242
  - matrice di, 251
  - relazione di, 242
- Adleman, 141
- al-Khowarizmi, 54
- albero, 258
- algebra
  - booleana, 215
  - di Boole, 216, 234
  - - isomorfe, 239
- algebrica, struttura, 185
- algebrico, reticolo, 232
- algoritmo, 54, 169
- complessità, 170
- euclideo per MCD
- - tra polinomi, 156
- - tra interi, 71
- ricorsivo, 54
- trattabili, 174
- alterno, sottogruppo, 261
- anagramma, 98
- AND, porta, 216
- anelli, 209
- somma diretta di, 210
- anello, 66
  - commutativo con unità, 66
  - degli interi di Gauss, 213
  - delle classi resto modulo  $n$ , 116
  - quoziente, 114, 212
- antisimmetria, 25
- antisimmetrica, proprietà, 25
- appartenenza di un elemento ad un insieme, 3
- Appel, 265
- applicazione, 19
  - di Karnaugh, 225
  - identica, 23
  - inversa, 22
- approssimazione di Stirling, 172
- arco, 242
  - di un grafo, 242

aritmetica, teorema fondamentale dell', 81

assiomi di Peano, 47

associati

- elementi, 68

- polinomi, 155

assoluto, valore, 69

assorbimento, leggi di, 219

atomo, 236

aureo, rapporto, 59

autenticazione di firme, 146

automorfismo di un grafo, 256

### B

Bachmann, 172

barbiere, paradosso del, 3

base, dell'induzione, 47

base

-  $b$ , 74

- 2, scrittura, 75

bene ordinato, insieme, 51

bijettiva, funzione, 22

big-o, notazione, 172

bilanciato, vertice, 249

binomiale, coefficiente, 101

bipartito, grafo, 258

bit, stringa, 8

biunivoca, funzione, 22

Boole, 216

- algebra di, 216, 234

booleana

- algebra, 215

- espressione, 220

- funzione, 218

- - variabile, 217

buon ordinamento, principio del, 51

Bézout, identità di, 76

- per polinomi, 156

### C

calcoli, in parallelo, 127

calcolo, combinatorio, 89, 94

cammino

- euleriano, 249

- in un grafo, 244

- lunghezza di, 245

campi, 176

- finiti, 176, 180  
 campo, 133  
 - dei quozienti, 162, 273  
 canonica, proiezione, 34  
 Cantor, procedimento diagonale di, 92  
 cappio, 244  
 caratteristica  
 - di Eulero, 264  
 - equazione, 57  
 - funzione, 23  
 - radice, 57  
 cardinalità  
 - di un insieme, 89  
 - inferiore, 93  
 - superiori al numerabile, 93  
 catena, 26  
 chiave, segreta, 143, 146  
 ciclico, gruppo, 194  
 ciclo  
 - di una permutazione, 199, 200  
 - in un grafo, 245  
 - lunghezza di, 199  
 cinese, teorema dei resti, 124, 125  
 circuito, 227  
 - dispari, 245  
 - euleriano, 245  
 - in un grafo, 245  
 - pari, 245  
 classe  
 - di equivalenza, 28  
 -  $NP$ , 174  
 classi resto modulo  $n$ , 114  
 codominio  
 - di una funzione, 19  
 - di una relazione, 17  
 coefficiente  
 - binomiale, 101  
 - direttivo, 152  
 combinatorio, calcolo, 89  
 combinazioni  
 - con ripetizione, 102, 103  
 - semplici, 99, 100  
 commesso viaggiatore, problema del, 265  
 compatibile, relazione, 115  
 complementare, insieme, 5  
 complementari, grafi, 263  
 complemento, 5  
 - relativo, 5  
 - reticolo con, 234  
 complessità  
 - di un algoritmo, 170  
 - esponenziale, 174  
 - fattoriale, 174  
 - lineare, 174  
 - logaritmica, 174  
 - polinomiale, 174  
 - spaziale, 170  
 - temporale, 170

completo, grafo, 244  
 componente连通的, 246  
 composizione di funzioni, 22  
 composta  
 - funzione, 22  
 - proposizione, 14  
 condizione  
 - necessaria, 12  
 - sufficiente, 12  
 - iniziale, 55  
 congettura, di Ulam, 256  
 congiunzione  
 - di proposizioni, 11  
 - fondamentale, 222  
 - operatore di, 11  
 congruenza, 113  
 - lineare, 122  
 - risoluzione di, 121  
 - relazione di, 113  
 connesso, grafo, 246  
 contenuto di un polinomio, 162  
 continuo  
 - ipotesi del, 94  
 - generalizzata, 94  
 - potenza del, 93  
 contraddizione, 3, 14  
 contrazione, di un grafo, 260  
 controimmagine, 21  
 coprimi  
 - interi, 70  
 - polinomi, 156  
 corollario, del piccolo teorema di Fermat, 119  
 crescita, di funzioni, 170  
 criterio  
 - di divisibilità, 119  
 - di irriducibilità di Eisenstein, 165  
 crittografia, 140  
 - a chiave pubblica, 141  
 crivello di Eratostene, 83

**D**

de la Vallée Poussin, 85  
 de Morgan, leggi di, 219  
 decidibile, problema, 169  
 definizione  
 - induuttiva, 53  
 - ricorsiva, 53  
 - di una successione, 53  
 diagramma, di Venn, 5  
 diamante, 233  
 diedrale, gruppo, 206  
 differenza insieme, 5  
 differenze finite, relazione alle, 55  
 Diffie, 141  
 digrafo, 242  
 dimostrazione, per induzione, 48  
 diofantea, equazione, 78  
 direttivo, coefficiente, 152  
 disunione, di proposizioni, 11

- operatore di, 11  
 disposizioni  
 - con ripetizione, 102  
 - semplici, 99  
 distanza, di due vertici di un grafo, 245  
 distributivo, reticolo, 233  
 distribuzione dei primi, 85  
 disuguaglianze distributive, 233  
 divina, proporzione, 59  
 divisibilità, 67  
 - criteri di, 119  
 - tra polinomi, 155  
 divisione  
 - tra interi, 69  
 - tra polinomi, 154  
 divisore, 67  
 - comune, 67  
 - dello zero, 66  
 - di un polinomio, 162  
 dominanza  
 - di una funzione, 172  
 - leggi di, 219  
 domini  
 - a fattorizzazione unica, 274  
 - che non sono a fattorizzazione unica, 274  
 dominio  
 - di integrità, 66  
 - di una funzione, 19  
 - di una relazione, 17  
 doppia sommatoria, 44  
 duale, legge, 219

**E**

Eisenstein, criterio di irriducibilità, 165  
 elementi, associati, 68  
 elemento, 2  
 - appartenenza di un  $\in$  a un insieme, 3  
 - di un insieme, 1  
 - invertibile, 68  
 - irriducibile, 68  
 - massimale, 230  
 - massimo, 230  
 - minimale, 230  
 - minimo, 230  
 - primo, 68  
 equazione  
 - caratteristica, 57  
 - diofantea, 78  
 equipotenza, 89  
 equivalenza  
 - classe di, 28  
 - relazione di, 28  
 Eratostene, crivello di, 83  
 esistenziale, quantificatore, 10  
 espressioni, booleane, 220  
 estremo  
 - inferiore, 231  
 - superiore, 231  
 etichettato, grafo, 251

**F**

fattoriale, 98  
 fattorizzazione  
 - con crivello di Eratostene, 136  
 - di interi, 136  
 - unica per polinomi, 157  
 Fermat  
 - metodo di fattorizzazione di, 137  
 - numero di, 86  
 - piccolo teorema di, 118  
 - primi di, 86  
 - ultimo teorema di, 84  
 fermata, problema della, 169  
 Fibonacci  
 - numeri di, 58  
 - successione di, 58  
 finito, insieme, 90  
 firme, autenticazione di, 146  
 foresta, 258  
 forma  
 - minimale di un'espressione booleana, 224  
 - normale disgiuntiva di una funzione booleana, 220  
 formula  
 - chiusa, 55  
 - di Eulero, 263  
 - di Stirling, 172  
 funzione, 19  
 -  $\zeta$ , 278  
 - a senso unico, 142  
 - biliettiva, 22  
 - biunivoca, 22  
 - booleana, 218  
 - forma normale disgiuntiva, 220  
 - caratteristica, 23  
 - codominio di, 19  
 - composta, 22  
 - crescita di, 170  
 - di Ackermann, 63  
 - di Eulero, 131  
 - proprietà della, 132  
 - di riferimento, 173  
 - dominanza di, 172  
 - dominio di, 19  
 - fattoriale, 98

- generatrice, 275
- grafico di una, 19
- iniettiva, 21
- ordine di grandezza di, 172
- relazione associata, 34
- suriettiva, 21
- funzioni
  - booleane uguali, 219
  - composizione di, 22

**G**

Gauss  
 - interi di, 213  
 - lemma di, 163  
 - teorema di, 163  
 geodetica, in un grafo, 245  
 gioco, della Torre di Hanoi, 56, 61  
 grado

- di un polinomio, 152
- di un vertice, 247
- grafi, 241
  - complementari, 263
  - isomorfi, 255
- grafico, di una funzione, 19
- grafo
  - arco di un, 242
  - bipartito, 258
  - completo, 244
  - connesso, 246
  - contraibile per archi, 260
  - etichettato, 251
  - euleriano, 246
  - grandezza di, 243
  - matrice di adiacenza di, 251
  - nodo di un, 242
  - non orientato, 243
  - nullo, 243
  - ordinato, 243
  - orientato, 242
  - planare, 259
  - semplice, 245
  - vertice di un, 242

grandezza  
 - di un grafo, 243  
 - ordine di - di una funzione, 172

gruppo, 97, 188  
 - abeliano, 189  
 - ciclico, 194  
 - diedrale, 206  
 - di Klein, 206  
 - simmetrico, 197  
 gruppoide, 186

**H**

Hadamard, 85  
 Haken, 265  
 Hanoi, gioco della torre, 61  
 Hellman, 141

**I**

ideale, 177, 211
 

- generato da, 177
- generato dal polinomio  $f(x)$ , 177

 idempotenza, 219
 identità di Bézout, 76
 

- per polinomi, 156

 immagine
 

- di un elemento, 19
- di un sottoinsieme, 21
- di una funzione, 19
- inversa, 21

 implicazione, 12
 inclusione-esclusione, principio di, 109
 indecidibile, problema, 169
 induttiva, definizione, 53
 induttivo, passo, 47
 induzione
 

- base dell'-, 47
- dimostrazione per, 48
- matematica, principio di, 47

 inferiore, cardinalità, 93
 infinito, insieme, 90
 infinità dei numeri primi, 84
 iniettiva, funzione, 21
 insieme, 1
 

- bene ordinato, 51
- cardinalità di, 89
- complementare, 5
- dei numeri
  - - interi, 2
  - - naturali, 2
  - - razionali, 2
  - delle parti, 6
  - differenza, 5
  - elemento di un, 1, 2
  - finito, 90
  - infinito, 90
  - partizione di un, 30
  - parzialmente ordinato, 26
  - potenza di, 90
  - quoziente, 29
  - totalmente ordinato, 26
  - universale, 3
  - vuoto, 2
- insiemni
  - intersezione di, 4
  - prodotto cartesiano di, 5
  - uguali, 3
  - unione di, 4

 integrità, dominio di, 66
 intera, parte, 19
 interi, 65
 

- come classi di equivalenza, 269
- coprimi, 70
- di Gauss, 213
- e polinomi a confronto, 154
- fattorizzazione di, 136

- insieme dei numeri, 2

- numeri, 268
- relativamente primi, 70
- intersezione, di insiemi, 4
- inversa
  - applicazione, 22
  - di una permutazione, 198
  - immagine, 21
  - relazione, 18
- invertibile
  - elemento, 68
  - polinomio, 155
- invertitore, 215
  - ipotesi del continuo, 94
  - generalizzata, 94
- irriducibile
  - elemento, 68
  - polinomio, 156
- irriducibili, polinomi
  - su  $\mathbb{C}$ , 160
  - su  $\mathbb{Q}$ , 162
  - su  $\mathbb{R}$ , 160
- irriducibilità, criterio di Eisenstein, 165
  - isometria, 206
- isomorfismo
  - di grafi, 255
  - di reticolati, 233
  - tra algebre di Boole, 239
  - tra anelli, 211

**K**

Karnaugh
 

- applicazione di, 225
- metodo di, 224

 Klein, gruppo di, 206
 Kuratowski, teorema di, 260
 Königsberg, ponti di, 241

**L**

Lamé, teorema di, 72
 legge, duale, 219
 leggi
 

- di assorbimento, 219
- di de Morgan, 219
- di dominanza, 219

 lemma, di Gauss, 163
 Lenstra, 144
 lettera, 222
 limitato, reticolo, 234
 lineare
 

- congruenza, 122
- relazione ricorsiva, 56

 logicamente equivalenti, proposizioni, 14
 Lucas, 61
 

- test di, 136
- per numeri di Mersenne, 87

 lunghezza
 

- di un cammino, 245
- di un ciclo di una permutazione, 199

- di una stringa, 38

**M**

maggioranti, 230
 massimale, 230
 massimo, 230
 - comun divisore, 70
 - - tra interi, 70
 - - tra polinomi, 156
 - elemento, 230
 matrice, 17
 - di adiacenza, 251
 - di una relazione, 18
 matrici
 

- prodotto di, 189
- somma di, 189

 MCD, 70
 - tra interi, 70
 - tra polinomi, 156
 mcm, 71
 - tra interi, 71
 Mersenne
 

- numeri di, 87
- primi di, 87

 metodo
 

- di fattorizzazione di Fermat, 137
- di Karnaugh, 224

 minimale, 230
 - forma - di un'espressione booleana, 224
 minimo, 230
 - comune multiplo, 71
 - - tra interi, 71
 - elemento, 230
 - principio del, 51
 minoranti, 230
 moltiplicazione tra polinomi, 150
 monico, polinomio, 152
 monoide, 187
 movimento rigido, 206
 multigrafo, 245

**N**

naturali
 

- insieme dei numeri, 2
- numeri, 46

 necessaria, condizione, 12
 negazione di una proposizione, 9
 nodo, di un grafo, 242
 NOT, porta, 216
 notazione, big-o, 172
 nove, prova del, 121
 nucleo, di un omomorfismo di anelli, 211
 nullo, grafo, 243
 numerabile, potenza del, 91
 numeri
 

- di Fibonacci, 58
- di Mersenne, 87
- insieme dei - interi, 2
- insieme dei - naturali, 2

- insieme dei - razionali, 2
- interi, 65, 268
- naturali, 46
- - prodotto di, 268
- somma di, 267
- primi, 82, 278
- distribuzione, 85
- teorema dei, 86
- razionali, 271
- numero
  - cardinale di in insieme, 90
  - di Fermat, 86

**O**

- omomorfismo
- di reticolati, 233
- tra anelli, 211
- operatore
  - di congiunzione, 11
  - di disgiunzione, 11
- operazione, 185
- operazioni
  - in  $\mathbb{N}$ , 267
  - tra classi resto, 114
  - tra polinomi, 150
- OR*, porta, 216
- orbita, 199
- ordine, 25
  - di grandezza di una funzione, 172
  - di un elemento di un gruppo, 193
  - di un grafo, 243
  - di un gruppo, 194
  - parziale, 25
- orientato, grafo, 242

**P**

- paradosso, del barbiere, 3
- parallelo, calcoli in, 127
- parte, intera, 19, 110
- parti, insieme delle, 6
- partizione, 30
  - di un intero, 203
- parzialmente ordinato
- insieme, 26
- Pascal triangolo di, 101
- passo, induttivo, 47
- Peano
  - assiomi di, 47
  - postulati di, 47
- pentagono, 233
  - grafo, 233
- Pépin, test di, 136
- percorso, in un grafo, 245
- periodo, di un elemento di un gruppo, 193
- permutazione, 96, 197
  - dispari, 201
  - identica, 198
  - inversa, 198
  - pari, 201

- piccolo teorema di Fermat, 118
- pitagorica, terna, 83
- planare, grafo, 259
- platonico, solido, 263
- polinomi, 149
  - addizione tra, 150
  - associati, 155
  - coprimi, 156
  - divisione, 154
  - identità di Bézout, 156
  - irriducibili
    - - su  $\mathbb{C}$ , 160
    - - su  $\mathbb{Q}$ , 162
    - - su  $\mathbb{R}$ , 160
  - massimo comun divisore, 156
  - MCD, 156
  - moltiplicazione tra, 150
  - operazioni tra, 150
  - relativamente primi, 156
  - uguali, 150
- polinomio, 149
  - contenuto di, 162
  - divisore di, 162
  - grado di, 152
  - invertibile, 155
  - irriducibile, 156
  - monico, 152
  - primitivo, 162
  - primo, 157
  - radice di, 158
  - riducibile, 156
  - zero di, 158
- ponti, di Königsberg, 241
- porta
  - AND, 216
  - NOT, 216
  - OR, 216
- portalettere, problema cinese del, 266
- porte, logiche, 215, 227
- postulati, di Peano, 47
- potenza
  - del continuo, 93
  - del numerabile, 91
  - di un elemento di un gruppo, 191
  - di un insieme, 90
  - modulo  $n$ , 139
- primalità, test di, 135
- primi
  - di Fermat, 86
  - di Mersenne, 87
  - numeri, 278
- primitiva, proposizione, 14
- primitivo, polinomio, 162
- primo
  - elemento, 68
  - polinomio, 157
- principio
  - del buon ordinamento, 51
  - del minimo, 51

- di inclusione-esclusione, 109
- di induzione matematica, 47
- problema
  - cinese del portalettere, 266
  - decidibile, 169
  - dei quattro colori, 265
  - del commesso viaggiatore, 265
  - della fermata, 169
  - indecidibile, 169
- procedimento, diagonale di Cantor, 92
- prodotto
  - cartesiano di insiemi, 5
  - di due numeri naturali, 268
  - di matrici, 189
  - regola del, 95
- progressione aritmetica, 55
- proiezione, canonica, 34
- proporzione, divina, 59
- proposizione, 9
  - composta, 14
  - negazione di, 9
  - primitiva, 14
- proposizioni
  - congiunzione di, 11
  - disgiunzione di, 11
  - logicamente equivalenti, 14
- proprietà
  - antisimmetrica, 25
  - dei numeri interi, 65
  - della funzione di Eulero, 132
  - delle sommatorie, 42
  - riflessiva, 25, 28
  - simmetrica, 28
  - transitiva, 25, 28
- prova del nove, 121

**Q**

- quantificatore, 10
  - esistenziale, 10
  - universale, 10
- quattro colori, problema dei, 265
- quoziente, 69
  - della divisione di polinomi, 154
  - insieme, 29
  - nella divisione tra interi, 69
- quozienti, campo dei, 273

**R**

- radice
  - caratteristica, 57
  - - di una relazione ricorsiva, 57
  - di un polinomio, 158
  - multipla, di un polinomio, 159
  - semplice, di un polinomio, 159
- radici razionali di polinomi su  $\mathbb{Z}$ , 165
- rapporto, aureo, 59
- rappresentazione
  - di un intero in base  $b$ , 74
  - teorema di, 239

- razionali
  - come classi di equivalenza, 272
  - insieme dei numeri, 2
  - numeri, 271

- regola
  - del prodotto, 95
  - della somma, 94
- relativamente primi
- interi, 70
- polinomi, 156
- relazione, 16
  - alle differenze finite, 55
  - associata a una funzione, 34
  - codominio di una, 17
  - compatibile, 115
  - d'ordine, 25
  - di congruenza modulo  $n$ , 113
  - di equivalenza, 28
  - dominio di una, 17
  - inversa, 18
  - matrice di una, 18
  - ricorsiva, 55
    - - lineare, 56
    - - lineare omogenea, 56
    - - soluzione di, 55
  - relazioni ricorsive lineari omogenee
  - risoluzione di, 60
- resto, 69
  - della divisione di polinomi, 154
  - nella divisione tra interi, 69
- reticoli
  - isomorfismi di, 233
  - omomorfismo di, 233
- reticolato, 229, 232
  - algebrico, 232
  - con complemento, 234
  - distributivo, 233
  - limitato, 234
  - non distributivo, 233
- ricorsiva
  - definizione, 53
  - relazione, 55
- ricorsività, 53
- ricorsivo, algoritmo, 54
- riducibile, polinomio, 156

- Riemann, 279
- riferimento, funzione di, 173
- riflessiva, proprietà, 25, 28
  - riflessività, 25, 28
- risoluzione
  - di congruenze lineari, 121
  - di relazioni ricorsive lineari omogenee, 60
- Rivest, 141

- RSA*, sistema, 142
- Ruffini, teorema di, 158
- Russell, 3

**S**

- scrittura, in base 2, 75

- semigruppo, 187
  - semplice, grafo, 245
  - senso unico, funzione a, 142
  - Shamir, 141
  - Shannon, 216
  - simmetria, 28
  - simmetrica, proprietà, 28
  - simmetrico, gruppo, 197
  - singleton, 3
  - sistema
    - RSA, 142
    - di congruenze lineari, 124
  - solido platonico, 263
  - soluzione, di una relazione ricorsiva, 55
  - somma
    - di due numeri naturali, 267
    - di matrici, 189
    - diretta di anelli, 210
    - regola della, 94
  - sommatoria, 38
    - doppia, 44
    - proprietà della, 42
  - sottoanello, 211
  - sottografo, 256
  - sottogruppo, 191
    - alterno, 201
    - generato da un sottoinsieme, 192
  - sottoinsieme, 2
    - immagine di, 21
  - sottoreticolò, 233
  - Stirling
    - approssimazione di, 172
    - formula di, 172
  - stringa, 38
    - bit, 8
    - lunghezza di, 38
  - struttura algebrica, 185
  - successione, 37
    - definita
    - - induttivamente, 53
    - - ricorsivamente, 53
    - termine di, 37
  - successione di Fibonacci, 58
  - successivo, 47
  - sufficiente, condizione, 12
  - suriettiva, funzione, 21
- T**
- Tartaglia, triangolo di, 101
  - tautologia, 14
  - tavola, di verità, 14
  - tavole, per le classi resto, 115
  - teorema
    - cinese dei resti, 124, 125
    - - conseguenze del, 127
    - dei numeri primi, 86
    - di Eulero, 133, 247
    - di fattorizzazione unica per polinomi, 157
    - di Gauss, 163

- di Kuratowski, 260
  - di Lamé, 72
  - di rappresentazione, 239
  - di Ruffini, 158
  - di Wilson, 135
  - fondamentale dell'algebra, 160
  - fondamentale dell'aritmetica, 81
  - piccolo, di Fermat, 118
  - ultimo, di Fermat, 84
  - termine, di una successione, 37
  - terna, pitagorica, 83
  - test
    - di Lucas, 136
    - - per numeri di Mersenne, 87
    - di Pépin, 136
    - di primalità, 135
  - torre di Hanoi, 56, 61
  - totalmente ordinato, insieme, 26
  - transitiva, proprietà, 25, 28
  - transitività, 25, 28
  - triangolo
    - di Pascal, 101
    - di Tartaglia, 101
  - Turing, 189
- U**
- uguaglianza
    - di funzioni booleane, 219
    - tra insiemi, 3
    - tra polinomi, 150
  - Ulam, congettura di, 256
  - ultimo teorema di Fermat, 84
  - unico, funzione a senso, 142
  - unione, di insiemi, 4
  - unità, 68
  - universale
    - insieme, 3
    - quantificatore, 10
  - universo, 8
- V**
- valore, assoluto, 69
  - variabile, booleana, 217
  - Venn, diagramma di, 5
  - verità, tavola di, 14
  - vertice
    - bilanciato, 249
    - di un grafo, 242
  - vuoto, insieme, 2
- W**
- Wilson, teorema di, 135
- Z**
- zero
    - di un polinomio, 158
    - divisore dello, 66
  - $\zeta$ , funzione, 278

## UNA SCOMMESA DI CIVILTÀ

La nuova legge italiana sulle fotocopie è chiara.

È possibile fotocopiare una parte di un libro (fino al 15%) pagando, tramite la SIAE, all'autore e all'editore un prezzo proporzionale alla parte riprodotta.

In questo modo, chi ha bisogno di leggere alcuni capitoli può evitare di acquistare l'opera intera.

Ma la fotocopia di tutto o di gran parte di un libro è illecita: induce al mancato acquisto, rendendo così vano il lavoro di chi il libro lo ha scritto, redatto, composto, impaginato e illustrato.

La legge si propone lo scopo di tenere vivo l'interesse a scrivere libri.

Se questo interesse venisse a mancare, ben pochi libri nuovi sarebbero pubblicati: saremmo tutti costretti a leggere fotocopie, ormai illeggibili, di libri vecchi e non aggiornati.

Fotocopiare tutto un libro è un po' come lasciare un'auto in seconda fila: i più non lo fanno, non solo per paura della multa, ma soprattutto perché si rendono conto che, se tutti si comportassero così, ne deriverebbe un danno generale.

Sta quindi ai lettori far sì che la legge funzioni e produca effetti positivi.

È una scommessa di civiltà: se la si vince, il premio non andrà solo ad autori ed editori, ma a tutto il sistema culturale e scientifico italiano.

• Nel sito [www.zanichelli.it/f\\_info\\_fotocopie.html](http://www.zanichelli.it/f_info_fotocopie.html) la normativa.

Nello stesso sito si darà comunicazione del giorno in cui la nuova normativa acquiserà piena efficacia.

La piena efficacia della nuova normativa infatti è subordinata alla stipulazione di accordi fra le categorie interessate.

•

L'editore mette a disposizione degli studenti non vedenti o con particolari problemi di apprendimento una copia dei file, solitamente in formato pdf, in cui sono memorizzate le pagine di questo libro. Il formato dei file permette l'ingrandimento dei caratteri del testo. I docenti o i responsabili educativi possono richiedere i file scrivendo a: Zanichelli - Direzione Generale - Via Irnerio 34 - 40126 Bologna

UNIVERSITÀ DI BARI  
BIBLIOTECA DIPARTIMENTO DI INFORMATICA

N. d'inventario \_\_\_\_\_

dib

INV. N°

531-2 9006556

