

# Indice generale

**Prefazione 13**

**Prefazione all'edizione italiana 17**

**Ringraziamenti 19**

**1 Introduzione 21**

1.1 Fibonacci, le frazioni continue e la sezione aurea 1.2 Fermat, i primi e la ciclotomia 1.3 Eulero, i tozzenti e la crittografia 1.4 Gauss, le congruenze e la diffrazione 1.5 Galois, i campi e i codici

**2 I numeri naturali 43**

2.1 Il teorema fondamentale 2.2 Il minimo comune multiplo 2.3 "Marce" planetarie 2.4 Il massimo comun divisore 2.5 La percezione dell'altezza dei suoni nell'uomo 2.6 Ottave, temperamento, kili e decibel 2.7 I coprimi 2.8 L'algoritmo di Euclide

**3 I primi 55**

3.1 Quanti sono i numeri primi? 3.2 Il crivello di Eratostene 3.3 Un teorema cinese in errore 3.4 Una formula per i primi 3.5 I primi di Mersenne 3.6 Unità ripetute 3.7 I numeri perfetti 3.8 I primi di Fermat 3.9 Gauss e l'ottagono impossibile

- stema numerico cinese 16.3 Applicazioni della rappresentazione cinese 16.4 La trasformata discreta di Fourier in cinese 16.5 Un trasformatore di Fourier cino-ottico 16.6 Rappresentazione cinese generalizzata 16.7 Trasformata rapida di Fourier di lunghezza prima
- 17 Trasformate rapide e prodotti di Kronecher 273**  
 17.1 Una trasformata rapida di Hadamard 17.2 Il principio fondamentale delle trasformate rapide di Fourier
- 18 Congruenze quadratiche 280**  
 18.1 Un'applicazione del teorema cinese dei resti
- 19 Pseudoprimi, poker e testa o croce a distanza 283**  
 19.1 Estrarre radici per scoprire numeri composti 19.2 Fattori da radici quadrate 19.3 Testa o croce per telefono 19.4 Pseudoprimi forti e assoluti 19.5 Pseudoprimi forti e di Fermat 19.6 Test deterministici di primalità
- 20 La funzione di Möbius e la trasformata di Möbius 297**  
 20.1 La trasformata di Möbius e la sua inversa 20.2 Dimostrazione della formula di inversione 20.3 Seconda formula di inversione 20.4 Terza formula di inversione 20.5 Quarta formula di inversione 20.6 Somme infinite speciali 20.7 Serie di Dirichlet e funzione di Möbius
- 21 Funzioni generatrici e partizioni 307**  
 21.1 Funzioni generatrici 21.2 Partizioni di interi 21.3 Funzioni generatrici di partizioni 21.4 Partizioni ristrette
- 22 Polinomi ciclotomici 319**  
 22.1 Come dividere un cerchio in parti uguali 22.2 La grande idea di Gauss 22.3 Fattorizzazioni in campi diversi 22.4 Ciclotomia nel piano complesso 22.5 Come dividere il cerchio con riga e compasso 22.6 Un'altra fattorizzazione razionale 22.7 Relazioni fra fattori razionali e radici complesse 22.8 Come calcolare con i polinomi ciclotomici
- 23 Sistemi lineari e polinomi 341**  
 23.1 Risposte d'impulso 23.2 Sistemi discreti nel tempo e trasformata  $z$

- 23.3 Convoluzione discreta 23.4 Polinomi ciclotomici e trasformata z
- 24 Teoria dei polinomi 346**  
 24.1 Alcuni aspetti basilari della vita polinomiale 24.2 Residui polinomiali 24.3 Resti cinesi per i polinomi 24.4 L'algoritmo di Euclide per i polinomi
- 25 Campi di Galois 354**  
 25.1 Il caso in cui l'ordine è primo 25.2 Il caso in cui l'ordine è potenza di un primo 25.3 Come generare  $GF(2^4)$  25.4 Quanti elementi primitivi vi sono? 25.5 Relazioni ricorsive 25.6 Come fare i calcoli in  $GF(p^m)$  25.7 Il logaritmo di Zech, il radar Doppler e le funzioni perfette di ambiguità 25.8 Un eccezionale reticolo di fase basato sul logaritmo di Zech 25.9 Comunicazioni ad ampio spettro e logaritmo di Zech
- 26 Proprietà spettrali delle successioni di Galois 373**  
 26.1 Correlazione circolare 26.2 Applicazioni ai codici a correzione d'errore 26.3 Applicazioni alle misure di precisione 26.4 Misure in sale da concerto 26.5 Il quarto effetto della relatività generale 26.6 Per una migliore acustica delle sale da concerto 26.7 Diffusori in dimensione più alta 26.8 Applicazioni a sistemi attivi
- 27 Generatori di numeri casuali 393**  
 27.1 Successioni di Galois pseudocasuali 27.2 Casualità delle congruenze 27.3 Distribuzioni "continue" 27.4 Quattro modi per generare una variabile gaussiana 27.5 Successioni pseudocasuali in crittografia
- 28 Forme d'onda e schemi di irradiazione 403**  
 28.1 Fasi speciali 28.2 I polinomi di Rudin-Shapiro 28.3 Somme di Gauss e fattori di picco 28.4 Successioni di Galois e fattori di picco minimi 28.5 Antenne e ridondanza minima
- 29 Teoria dei numeri, casualità e "Arte" 417**  
 29.1 Teoria dei numeri e design grafico 29.2 Primi di Gauss e di Eisenstein 29.3 Campi di Galois e collane impossibili

**30 Conclusione 428**

**Appendice 430**

A. Un programma per calcolatore per l'elevazione a potenza e la riduzione al residuo B. Un programma per calcolatore per calcolare i numeri di Fibonacci e di Lucas C. Un programma per calcolatore per scomporre un intero secondo il sistema numerico di Fibonacci

**Glossario dei simboli 441**

**Bibliografia 445**