

W.M. Baldoni, C. Ciliberto
G.M. Piacentini Cattaneo

Aritmetica, crittografia e codici

 Springer

Indice

1	Qualche richiamo sui numeri	1
1.1	Principio di induzione completa	1
1.2	Il concetto di ricorsività	5
1.2.1	I numeri di Fibonacci	6
1.2.2	Altri esempi di dinamica di popolazioni	11
1.2.3	La torre di Hanok: un caso lineare non omogeneo	13
1.3	L'algoritmo di Euclide	14
1.3.1	La divisione	14
1.3.2	Il massimo comun divisore	16
1.3.3	L'identità di Bézout	17
1.3.4	Equazioni lineari diofantee	20
1.3.5	Anelli euclidei	21
1.3.6	Polinomi	23
1.4	Contare in basi diverse	30
1.4.1	La rappresentazione posizionale dei numeri	30
1.4.2	La base 2	32
1.4.3	Le quattro operazioni in base 2	33
1.4.4	Numeri interi in base qualunque	39
1.4.5	Rappresentazione dei numeri reali in base qualunque	40
1.5	Frazioni continue	43
1.5.1	Frazioni continue semplici finite e numeri razionali	45
1.5.2	Frazioni continue semplici infinite e numeri irrazionali	48
1.5.3	Frazioni continue periodiche	56
1.5.4	Modello geometrico delle frazioni continue	57
1.5.5	L'approssimazione di irrazionali mediante i convergenti	58
1.5.6	Frazioni continue ed equazioni diofantee	61
	Appendice al Capitolo 1	62
A1	Esercizi di carattere teorico	62
B1	Esercizi di carattere computazionale	73
C1	Esercizi di programmazione	83

2	Complessità computazionale	85
2.1	Il concetto di complessità computazionale	85
2.2	Il simbolo \mathcal{O}	87
2.3	Tempo polinomiale, tempo esponenziale	90
2.4	Complessità delle operazioni elementari	93
2.5	Algoritmi e complessità	95
2.5.1	Complessità dell'algoritmo di Euclide	95
2.5.2	Dalla scrittura binaria a quella decimale: complessità	99
2.5.3	Complessità delle operazioni tra polinomi	99
2.5.4	Un algoritmo più efficiente per la moltiplicazione	101
2.5.5	Metodo di Ruffini-Horner	102
	Appendice al Capitolo 2	104
A2	Esercizi di carattere teorico	104
B2	Esercizi di carattere computazionale	106
C2	Esercizi di programmazione	110
3	Dall'infinito al finito	111
3.1	Congruenze: prime proprietà	111
3.2	Prime applicazioni delle congruenze	116
3.2.1	La prova del nove	116
3.2.2	Criteri di divisibilità	117
3.3	Congruenze lineari	118
3.3.1	Potenze modulo n	122
3.4	Il Teorema cinese dei resti	125
3.5	Esempi	129
3.5.1	Il calendario perpetuo	129
3.5.2	Girene all'italiana	132
	Appendice al Capitolo 3	133
A3	Esercizi di carattere teorico	133
B3	Esercizi di carattere computazionale	136
C3	Esercizi di programmazione	143
4	Finito non basta: fattorizzazione di interi	145
4.1	Numeri primi	145
4.1.1	Il Teorema Fondamentale dell'Arithmetica	146
4.1.2	Distribuzione dei numeri primi	148
4.1.3	Il crivello di Eratostene	153
4.2	Numeri primi e congruenze	156
4.2.1	Il calcolo della funzione di Eulero	156
4.2.2	Il Piccolo Teorema di Fermat	158
4.2.3	Il teorema di Wilson	161
4.3	Rappresentazione in base qualunque dei numeri razionali	162
4.4	Primi di Fermat, primi di Mersenne e numeri perfetti	164
4.4.1	Fattorizzazione di interi della forma $b^n \pm 1$	164
4.4.2	Numeri primi di Fermat	166

4.4.3	Numeri primi di Mersenne	168
4.4.4	Numeri perfetti	169
4.5	Fattorizzazione in un dominio di integrità	169
4.5.1	Elementi primi e irriducibili in un anello	170
4.5.2	Domini fattoriali	171
4.5.3	Anelli noetheriani	172
4.5.4	Fattorizzazione di polinomi su un campo	175
4.5.5	Fattorizzazione di polinomi su un anello fattoriale	177
4.5.6	Polinomi a coefficienti razionali o interi	183
4.6	L'interpolazione di Lagrange e applicazioni	186
4.7	Il metodo di fattorizzazione di Kronecker	191
	Appendice al Capitolo 4	194
A4	Esercizi di carattere teorico	194
B4	Esercizi di carattere computazionale	200
C4	Esercizi di programmazione	207
5	Campi finiti e congruenze polinomiali	209
5.1	Un po' di teoria dei campi	209
5.1.1	Estensioni di campi	209
5.1.2	Estensioni algebriche	210
5.1.3	Campo di riducibilità completa di un polinomio	213
5.1.4	Radici dell'unità	214
5.1.5	Chiusura algebrica	215
5.1.6	Campi finiti e loro sottocampi	216
5.1.7	Automorfismi dei campi finiti	218
5.1.8	Polinomi irriducibili su \mathbb{Z}_p	218
5.1.9	Campo \mathbb{F}_4 di ordine quattro	219
5.1.10	Campo \mathbb{F}_8 di ordine otto	221
5.1.11	Campo \mathbb{F}_{16} di ordine sedici	221
5.1.12	Campo \mathbb{F}_9 di ordine nove	222
5.1.13	Sui generatori di un campo finito	223
5.1.14	Complessità del calcolo in un campo finito	223
5.2	Congruenze polinomiali non lineari	224
5.2.1	Equazioni di secondo grado	230
5.2.2	Residui quadratici	231
5.2.3	Il simbolo di Legendre e sue proprietà	233
5.2.4	La legge di reciprocità quadratica	238
5.2.5	Il simbolo di Jacobi	241
5.2.6	Un algoritmo per il calcolo delle radici quadrate	244
	Appendice al Capitolo 5	246
A5	Esercizi di carattere teorico	246
B5	Esercizi di carattere computazionale	250
C5	Esercizi di programmazione	255

6	Test di primalità e di fattorizzazione	257
6.1	Numeri pseudoprimi e test probabilistici	257
6.1.1	Numeri pseudoprimi	257
6.1.2	Test probabilistici e test deterministici	258
6.1.3	Un primo test di primalità probabilistico	259
6.1.4	Numeri di Carmichael	260
6.1.5	Pseudoprimi di Eulero	261
6.1.6	Il test probabilistico di primalità di Solovay-Strassen	264
6.1.7	Pseudoprimi forti	264
6.1.8	Test probabilistico di primalità di Miller-Rabin	268
6.2	Radici primitive	269
6.2.1	Radici primitive e indice	274
6.2.2	Ancora sul test di Miller-Rabin	275
6.3	Un test di primalità deterministico polinomiale	277
6.4	Metodi di fattorizzazione	286
6.4.1	Il metodo di fattorizzazione di Fermat	287
6.4.2	Generalizzazione del metodo fattorizzazione di Fermat	289
6.4.3	Il metodo delle basi di fattorizzazione	290
6.4.4	Fattorizzazione e frazioni continue	295
6.4.5	L'algoritmo del crivello quadratico	296
6.4.6	Il metodo p	305
6.4.7	Variazione del metodo p	306
	Appendice al Capitolo 6	308
A6	Esercizi di carattere teorico	308
B6	Esercizi di carattere computazionale	310
C6	Esercizi di programmazione	312
7	Segreti... e bugie	315
7.1	I cifrari classici	315
7.1.1	Le prime scritture segrete nella storia	315
7.2	L'analisi del testo cifrato	321
7.2.1	Macchinari per cifrare	325
7.3	Impostazione matematica di un crittosistema	327
7.4	Alcuni cifrari classici basati sull'aritmetica modulare	331
7.4.1	Cifrari affini	332
7.4.2	Cifrari con matrici o di Hill	336
7.5	L'idea di base della crittografia a chiave pubblica	338
7.5.1	Un algoritmo per il calcolo dei logaritmi discreti	341
7.6	Problema dello zaino e applicazioni alla crittografia	342
7.6.1	Cifrario a chiave pubblica basato sul problema dello zaino o di Merkle-Hellman	345
7.7	Il sistema <i>RSA</i>	346
7.7.1	Accesso al sistema <i>RSA</i>	348
7.7.2	Invio di un messaggio cifrato con il sistema <i>RSA</i>	349
7.7.3	Decifrazione di un messaggio cifrato con il sistema <i>RSA</i>	351

7.7.4	Perché ha funzionato?	353
7.7.5	Autenticazione delle firme con il sistema <i>RSA</i>	357
7.7.6	Un commento sulla sicurezza del sistema <i>RSA</i>	359
7.8	Varianti del sistema <i>RSA</i> e oltre	360
7.8.1	Scambio di chiavi private	360
7.8.2	Il crittosistema di ElGamal	361
7.8.3	Zero-knowledge proof: convincere che si conosce un risultato senza svelarne il contenuto o la dimostrazione	362
7.8.4	Nota storica	363
7.9	Crittografia e curve ellittiche	363
7.9.1	Crittografia in un gruppo	364
7.9.2	Curve algebriche in un piano affine numerico	365
7.9.3	Rette e curve razionali	366
7.9.4	Curve iperellittiche	367
7.9.5	Curve ellittiche	369
7.9.6	Legge di gruppo sulle curve ellittiche	371
7.9.7	Curve ellittiche su \mathbb{R} , \mathbb{C} e \mathbb{Q}	377
7.9.8	Curve ellittiche su campi finiti	378
7.9.9	Curve ellittiche e crittografia	381
7.9.10	Il metodo di fattorizzazione $p - 1$ di Pollard	382
	Appendice al Capitolo 7	384
A7	Esercizi di carattere teorico	384
B7	Esercizi di carattere computazionale	388
C7	Esercizi di programmazione	399
8	Trasmettere senza... paura di sbagliare	401
8.1	Auguri di buon compleanno!	402
8.2	Fotografando nello spazio o lanciando monete, arriviamo ai codici	403
8.3	Codici che correggono gli errori	406
8.4	Limitazioni sugli invarianti	410
8.5	Codici lineari	416
8.6	Codici ciclici	421
8.7	Codici di Goppa	426
	Appendice al Capitolo 8	433
A8	Esercizi di carattere teorico	433
B8	Esercizi di carattere computazionale	437
C8	Esercizi di programmazione	440
9	Il futuro è già presente: la crittografia quantistica	441
9.1	Una prima incursione nel mondo quantistico: l'esperimento di Young	442
9.2	Il computer quantistico	446
9.3	Il cifrario di Vernam	448
9.4	Un breve glossario di meccanica quantistica	451

9.5 Crittografia quantistica	457
Appendice al Capitolo 9	464
A9 Esercizi di carattere teorico	464
B9 Esercizi di carattere computazionale	465
C9 Esercizi di programmazione	466
10 Soluzione di alcuni esercizi	467
10.1 Esercizi del Capitolo 1	467
10.2 Esercizi del Capitolo 2	478
10.3 Esercizi del Capitolo 3	479
10.4 Esercizi del Capitolo 4	483
10.5 Esercizi del Capitolo 5	487
10.6 Esercizi del Capitolo 6	492
10.7 Esercizi del Capitolo 7	494
10.8 Esercizi del Capitolo 8	497
10.9 Esercizi del Capitolo 9	500
Riferimenti bibliografici	503
Indice analitico	507