

Lindsay Childs

ALGEBRA

un'introduzione concreta

Traduzione di Carlo Traverso

ETS EDITRICE

Indice

Parte I	
INTERI	1
Capitolo 1	
I numeri	3
Capitolo 2	
Induzione; il Teorema Binomiale	7
A. Induzione	7
B. Un'altra forma di induzione	11
C. Buoni ordinamenti	14
D. Il Teorema Binomiale	15
Capitolo 3	
Fattorialità	20
A. L'algoritmo di Euclide	20
B. Il massimo comun divisore	24
C. Fattorizzazione unica	27
D. Notazione esponenziale; minimo comune multiplo	30
Capitolo 4	
Primi	33
A. Euclide	33
B. Alcuni risultati analitici	34
C. Il Teorema dei numeri primi	38
Capitolo 5	
Basi	41
A. Numeri in base a	41
B. Operazioni in base a	42
C. Divisione lunga in multipla precisione	44
D. Espansioni decimali	48

Capitolo 6	
Congruenze	52
A. Definizione di congruenza	52
B. Proprietà base	53
C. Criteri di divisibilità	54
D. Altre proprietà delle congruenze	56
E. Problemi di congruenze	57
F. Tornei all'italiana	60
Capitolo 7	
Classi di congruenza	62
Capitolo 8	
Anelli e campi	68
A. Assiomi	68
B. \mathbb{Z}_m	71
Capitolo 9	
Matrici e vettori	74
A. Moltiplicazione di matrici	74
B. L'anello delle matrici $n \times n$	76
C. Equazioni lineari	78
D. Determinanti e inverse	81
E. Operazioni elementari	82
F. Sottospazi, basi, dimensione	87
Capitolo 10	
Crittografia, I	92
Capitolo 11	
Teorema di Fermat; gruppi abeliani	98
A. Il teorema di Fermat	98
B. Gruppi abeliani	99
C. Teorema di Eulero	102
D. Calcolo di potenze elevate mod m	103
E. L'ordine di un elemento	104
F. Campi finiti	105
G. Gruppi non abeliani	107
Capitolo 12	
Decimali periodici, I	110

Capitolo 13	
Codici autocorrettori	114
Capitolo 14	
Il Teorema Cinese del Resto	121
A. Il teorema	121
B. Una generalizzazione del teorema di Fermat	126
Capitolo 15	
Crittografia II	128
Parte II	
POLINOMI	133
Capitolo 1	
Polinomi	135
Capitolo 2	
Fattorialità	140
A. Teorema di divisione	140
B. Massimo comun divisore	143
C. Fattorizzazione	146
Capitolo 3	
Il Teorema Fondamentale dell'Algebra	148
A. Polinomi irriducibili in $\mathbb{C}[x]$	148
B. Dimostrazione del Teorema Fondamentale	150
Capitolo 4	
Polinomi irriducibili in $\mathbb{R}[x]$	154
Capitolo 5	
Frazioni parziali	156
A. Funzioni razionali	156
B. Frazioni parziali	157
C. Integrazione	161
D. Una formula sulle partizioni	164
Capitolo 6	
La derivata di un polinomio	170

Capitolo 7	
L'algoritmo di Sturm	173
Capitolo 8	
Fattorizzazione in $\mathbb{Q}[x]$, I	179
A. Lemma di Gauss	179
B. Ricerca delle radici razionali	181
C. Test di irriducibilità	182
Capitolo 9	
Congruenze modulo un polinomio	186
Capitolo 10	
Teorema di Fermat, II	188
A. La caratteristica di un campo	188
B. Applicazioni del Teorema Binomiale	189
Capitolo 11	
Fattorizzazione in $\mathbb{Q}[x]$, III: Interpolazione di Lagrange	193
A. Il Teorema Cinese del Resto	193
B. Il metodo dell'interpolazione di Lagrange	194
Capitolo 12	
Fattorizzazione in $\mathbb{Z}_p[x]$	198
Capitolo 13	
Fattorizzazione in $\mathbb{Q}[x]$, III: Sollevamento Henseliano	207
A. Limitazione dei coefficienti dei fattori di un polinomio	208
B. Fattorizzazione modulo potenze dei primi	212
Parte III	
CAMPI	221
Capitolo 1	
Elementi primitivi	223
Capitolo 2	
Decimali periodici	228
Capitolo 3	
Test di primalità	235
Appendice. Il test di primalità di Rabin	238

Capitolo 4	
Radici quarte di uno in \mathbb{Z}_p	243
A. Primi	243
B. Campi complessi finiti	243
Capitolo 5	
Cavi telefonici	247
Capitolo 6	
Fattorizzazione in $\mathbb{Q}[x]$, IV: esempi cattivi mod p	252
Capitolo 7	
Classi di congruenza mod $f(z)$: estensioni semplici	253
Capitolo 8	
Polinomi e radici	260
A. Inventare radici di polinomi	260
B. Polinomi con radici date	261
Capitolo 9	
Codici autocorrettori, II	265
Capitolo 10	
Isomorfismi, I	279
A. Definizioni	279
B. Esempi con \mathbb{Z}	281
C. Esempi con $K[x]$	283
D. Automorfismi	285
Capitolo 11	
I campi finiti sono semplici	288
Capitolo 12	
Quadrati latini	291
Capitolo 13	
Polinomi irriducibili in $\mathbb{Z}_p[x]$	298
A. Fattorizzazione di $x^{p^n} - x$	298
B. Contare i polinomi irriducibili	301
Capitolo 14	
Campi finiti	305

Capitolo 15	
Il discriminante. Teorema di Stickelberger	307
A. Il discriminante	307
B. Radici dei polinomi irriducibili in $\mathbb{Z}_p[x]$	312
C. Teorema di Stickelberger	313
Capitolo 16	
Residui quadratici	316
A. Riduzione ai primi dispari	316
B. Il simbolo di Legendre	318
C. Dimostrazione della reciprocità quadratica	321
Capitolo 17	
Tornei di bridge	326
A. Matrici di Hadamard	326
B. Tornei di bridge in duplicato	329
C. Bridge per 8	331
D. Bridge per $p+1$	333
Capitolo 18	
Campi di numeri algebrici	336
Capitolo 19	
Isomorfismi, II	341
Capitolo 20	
Somme di due quadrati	343
Capitolo 21	
Sulla fattorialità	348
Esercizi utilizzati in capitoli successivi	351
Commenti ai problemi asteriscati	352
Bibliografia	361
Indice analitico	366