

Lindsay Childs

# ALGEBRA

un'introduzione concreta

Traduzione di Carlo Traverso

ETS EDITRICE

# Indice

Parte I	
<b>INTERI</b>	<b>1</b>
Capitolo 1	
<b>I numeri</b>	<b>3</b>
Capitolo 2	
<b>Induzione; il Teorema Binomiale</b>	<b>7</b>
A. Induzione	7
B. Un'altra forma di induzione	11
C. Buoni ordinamenti	14
D. Il Teorema Binomiale	15
Capitolo 3	
<b>Fattorialità</b>	<b>20</b>
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	
<b>Primi</b>	<b>33</b>
A. Euclide	33
B. Alcuni risultati analitici	34
C. Il Teorema dei numeri primi	38
Capitolo 5	
<b>Basi</b>	<b>41</b>
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	
<b>Congruenze</b>	<b>52</b>
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	
<b>Classi di congruenza</b>	<b>62</b>
Capitolo 8	
<b>Anelli e campi</b>	<b>68</b>
A. Assiomi	68
B. $Z_m$	71
Capitolo 9	
<b>Matrici e vettori</b>	<b>74</b>
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	
<b>Crittografia, I</b>	<b>92</b>
Capitolo 11	
<b>Teorema di Fermat; gruppi abeliani</b>	<b>98</b>
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	
<b>Decimali periodici, I</b>	<b>110</b>

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  $C[x]$

148

B. Dimostrazione del Teorema Fondamentale

150

Capitolo 4

Polinomi irriducibili in  $R[x]$

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

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

Capitolo 15	
<b>Il discriminante. Teorema di Stickelberger</b>	<b>307</b>
A. Il discriminante	307
B. Radici dei polinomi irriducibili in $\mathbb{Z}_p[x]$	312
C. Teorema di Stickelberger	313
Capitolo 16	
<b>Residui quadratici</b>	<b>316</b>
A. Riduzione ai primi dispari	316
B. Il simbolo di Legendre	318
C. Dimostrazione della reciprocità quadratica	321
Capitolo 17	
<b>Tornei di bridge</b>	<b>326</b>
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	
<b>Campi di numeri algebrici</b>	<b>330</b>
Capitolo 19	
<b>Isomorfismi, II</b>	<b>341</b>
Capitolo 20	
<b>Somme di due quadrati</b>	<b>343</b>
Capitolo 21	
<b>Sulla fattorialità</b>	<b>348</b>
<b>Esercizi utilizzati in capitoli successivi</b>	<b>351</b>
<b>Commenti ai problemi asteriscati</b>	<b>352</b>
<b>Bibliografia</b>	<b>361</b>
<b>Indice analitico</b>	<b>366</b>