

Harald Scheid / Andreas Frommer

Zahlentheorie

4. Auflage



Spektrum
AKADEMISCHER VERLAG

Inhaltsverzeichnis

Einleitung 1

I Teilbarkeit ganzer Zahlen

- I.1 Die Teiler einer ganzen Zahl 5
- I.2 Primzahlen 7
- I.3 Primfaktorzerlegung 12
- I.4 Eine Formel von Legendre und die Sätze von Tschebyscheff 19
- I.5 Irrationalitätsbeweise 25
- I.6 Der größte gemeinsame Teiler 27
- I.7 Das kleinste gemeinsame Vielfache 32
- I.8 Kettenbrüche 36
- I.9 Periodische Kettenbrüche 46
- I.10 Farey-Folgen 52
- I.11 Die Folge der Fibonacci-Zahlen 57
- I.12 Aufgaben 65
- I.13 Lösungen der Aufgaben 73

II Integritätsbereiche

- II.1 Teilbarkeit in Integritätsbereichen 83
- II.2 Euklidische Ringe 89
- II.3 Die ganzen gaußschen Zahlen 94
- II.4 Ganzalgebraische Zahlen zweiten Grades 100
- II.5 Die pellsche Gleichung 104
- II.6 Aufgaben 110
- II.7 Lösungen der Aufgaben 113

III Restklassen

- III.1 Kongruenzen und Restklassen 119
- III.2 Teilbarkeitskriterien 121
- III.3 Der Satz von Fermat 125
- III.4 Primitive Restklassen 132
- III.5 Dezimalbrüche 138
- III.6 Ewiger Kalender 143
- III.7 Magische Quadrate 145
- III.8 Primzahlkriterien und Pseudoprimzahlen 151
- III.9 Mersennesche und fermatsche Primzahlen (1) 155
- III.10 Aufgaben 158
- III.11 Lösungen der Aufgaben 162

VI

IV Zahlentheoretische Algorithmen in der Kryptographie

- IV.1 Algorithmen und Komplexität 169
- IV.2 Langzahl- und Restklassenarithmetik 174
- IV.3 Schnelle Multiplikation 184
- IV.4 Kommunikation, Kodierung, Kryptographie 188
- IV.5 Diskreter Logarithmus, Diffie-Hellmann-Protokoll, ElGamal-Chiffre 193
- IV.6 Faktorisierung, RSA- und Rabin-Chiffre 206
- IV.7 Aufgaben 219
- IV.8 Lösungen der Aufgaben 223

V Kongruenzen und diophantische Gleichungen

- V.1 Lineare diophantische Gleichungen und Kongruenzen 229
- V.2 Quadratische diophantische Gleichungen und Kongruenzen 236
- V.3 Quadratische Reste 238
- V.4 Mersennesche und fermatsche Primzahlen (2) 247
- V.5 Darstellung von Zahlen als Quadratsummen 251
- V.6 Pythagoräische Zahlentripel; die fermatsche Vermutung 260
- V.7 Rationale Punkte auf algebraischen Kurven 269
- V.8 Binäre quadratische Formen 273
- V.9 Ternäre quadratische Formen; der Drei-Quadrate-Satz 283
- V.10 Figurierte Zahlen 288
- V.11 Der Gitterpunktsatz von Minkowski 291
- V.12 Aufgaben 296
- V.13 Lösungen der Aufgaben 304

VI Zahlentheoretische Funktionen

- VI.1 Das Dirichlet-Produkt 315
- VI.2 Multiplikative Funktionen 320
- VI.3 Dirichlet-Reihen 323
- VI.4 Mittelwerte zahlentheoretischer Funktionen 329
- VI.5 Weitere Produkte zahlentheoretischer Funktionen 336
- VI.6 Die Teilersummenfunktion 342
- VI.7 Aufgaben 352
- VI.8 Lösungen der Aufgaben 357

VII Der Primzahlsatz

- VII.1 Der Primzahlsatz und der dirichletsche Primzahlsatz 365
- VII.2 Die selbergsche Formel 367
- VII.3 Der Beweis des Primzahlsatzes 372
- VII.4 Anmerkungen, Folgerungen 378
- VII.5 Primzahlen in arithmetischen Progressionen (1) 382
- VII.6 Zufallsprimzahlen 394
- VII.7 Aufgaben 399
- VII.8 Lösungen der Aufgaben 401

VIII Elemente der Additiven Zahlentheorie

VIII.1 Problemstellungen der Additiven Zahlentheorie	405
VIII.2 Partitionen	406
VIII.3 Ein spezielles Partitionsproblem	418
VIII.4 Anzahl der Darstellungen als Quadratsummen	426
VIII.5 Die Dichte einer Menge natürlicher Zahlen	433
VIII.6 Der Satz von Goldbach-Schnirelmann	443
VIII.7 Der Satz von Waring-Hilbert	446
VIII.8 Wesentliche Komponenten	454
VIII.9 Das Münzenproblem und das Briefmarkenproblem	458
VIII.10 Aufgaben	468
VIII.11 Lösungen der Aufgaben	470

IX Siebmethoden

IX.1 Allgemeine Bemerkungen über Siebverfahren	473
IX.2 Die Siebmethode von Selberg	476
IX.3 Primzahlen in arithmetischen Progressionen (2)	481
IX.4 Primzahlzwillinge	484
IX.5 Zur goldbachschen Vermutung	486
IX.6 Quadratsummen	489
IX.7 Stammbruchsummen	491
IX.8 Aufgaben	496
IX.9 Lösungen der Aufgaben	497

Literatur 499

Symbolverzeichnis 503

Namensverzeichnis 505

Sachverzeichnis 506