

KAPITEL III: PRIMZAHLEN	67
§1: Die Verteilung der Primzahlen	67
§2: Das Sieb des ERATOSTHENES	82
§3: FERMAT-Test und FERMAT-Zahlen	85
§4: Der Test von MILLER und RABIN	93
§5: Der Test von AGRAWAL, KAYAL und SAXENA	95
KAPITEL IV: FAKTORISIERUNGSVERFAHREN	107
§1: Die ersten Schritte	109
a) Test auf Primzahl	109
b) Abdividieren kleiner Primteiler	110
§2: Die Verfahren von POLLARD und ihre Varianten	112
a) Die Monte-Carlo-Methode	113
b) Die $(p - 1)$ -Methode	118
c) Varianten	120
§3: Das Verfahren von FERMAT und seine Varianten	122
KAPITEL V: KETTENBRÜCHE	134
§1: Der Kettenbruchalgorithmus	134
§2: Geometrische Formulierung	136
§3: Optimale Approximation	140
§4: Kettenbrüche und Kalender	146
§5: Eine kryptographische Anwendung	158
KAPITEL VI: QUADRATISCHE ZAHLKÖRPER	161
§1: Grundbegriffe der Ringtheorie	161
§2: Die Elemente quadratischer Zahlkörper	164
§3: Die Hauptordnung eines Zahlkörpers	166
§4: Normen und Spuren in quadratischen Zahlkörpern	169
§5: EUKLIDISCHE RINGE	171
§6: Einheiten in quadratischen Zahlkörpern	180
§7: Quaternionen	182

Inhalt

KAPITEL I: GANZE ZAHLEN UND IHRE PRIMZERLEGUNG	1
§0: Rationale und irrationale Zahlen	1
§1: Der Euklidische Algorithmus	5
§2: Der erweiterte EUKLIDISCHE Algorithmus	8
§3: Der Aufwand des EUKLIDISCHEN Algorithmus	13
§4: Die multiplikative Struktur der ganzen Zahlen	18
§5: Kongruenzenrechnung	20
§6: Der chinesische Restesatz	24
§7: Prime Restklassen	29
KAPITEL II: ANWENDUNGEN IN DER KRYPTOGRAPHIE	36
§1: New directions in cryptography	36
§2: Das RSA-Verfahren	40
§3: Weitere Anwendungen des RSA-Verfahrens	46
a) Identitätsnachweis	46
b) Elektronische Unterschriften	47
c) Blinde Unterschriften und elektronisches Bargeld	49
d) Bankkarten mit Chip	52
§4: Wie groß sollten die Primzahlen sein?	54
§5: Verfahren mit diskreten Logarithmen	58
§6: DSA	61
§7: Anwendungen bei SSL/TLS	63
§8: Ausblick	64

KAPITEL VII: QUADRATISCHE FORMEN	185
§1: Summen zweier Quadrate	185
§2: Anwendung auf die Berechnung von π	191
§3: Der Satz von LAGRANGE	197
§4: Quadratische Formen und Matrizen	200
§5: Kettenbruchentwicklung quadratischer Irrationalitäten	205
§6: Die PELLsche Gleichung	210
KAPITEL VIII: QUADRATISCHE RESTE	215
§1: Das LEGENDRE-Symbol	215
§2: Das quadratische Reziprozitätsgesetz	217
§3: Das JACOBI-Symbol	221
§4: Berechnung der modularen Quadratwurzel	225
§5: Anwendungen quadratischer Reste	231
a) Münzwurf per Telephon	232
a) Quadratische Formen und quadratische Reste	232
b) Münzwurf per Telephon	233
c) Akustik von Konzerthallen	235
KAPITEL IX: DIE FERMAT-VERMUTUNG FÜR ZAHLEN UND FÜR POLYNOME	241
§1: Zahlen und Funktionen	241
§2: Pythagoräische Tripel	243
§3: Der Satz von MASON	246
§4: Die abc-Vermutung	249
§5: Die FREY-Kurve	253