Wolfgang K. Seiler

Zahlentheorie

Vorlesung an der Universität Mannheim
im Frühjahrssemester 2007

Dieses Skriptum entsteht parallel zur Vorlesung und soll mit möglichst geringer Verzögerung erscheinen. Es ist daher in seiner Qualität auf keinen Fall mit einem Lehrbuch zu vergleichen; insbesondere sind Fehler bei dieser Entstehensweise nicht nur möglich, sondern **sicher**. Dabei handelt es sich wohl leider nicht immer nur um harmlose Tippfehler, sondern auch um Fehler bei den mathematischen Aussagen. Da mehrere Teile aus anderen Skripten für Hörerkreise der verschiedensten Niveaus übernommen sind, ist die Präsentation auch teilweise ziemlich inhomogen.

Das Skriptum sollte daher mit Sorgfalt und einem gewissen Mißtrauen gegen seinen Inhalt gelesen werden. Falls Sie Fehler finden, teilen Sie mir dies bitte persönlich oder per e-mail (seiler@math.uni-mannheim.de) mit. Auch wenn Sie Teile des Skriptums unverständlich finden, bin ich für entsprechende Hinweise dankbar.

Falls genügend viele Hinweise eingehen, werde ich von Zeit zu Zeit Listen mit Berichtigungen und Verbesserungen zusammenstellen. In der online Version werden natürlich alle bekannten Fehler korrigiert.

Biographische Angaben von Mathematikern beruhen größtenteils auf den entsprechenden Artikeln im *MacTutor History of Mathematics archive* (`www-history.mcs.st-andrews.ac.uk/history/`), von wo auch die meisten abgedruckten Bilder stammen. Bei noch lebenden Mathematikern bezog ich mich, soweit möglich, auf deren eigenen Internetauftritt.

Inhalt

KAPITEL I: GANZE ZAHLEN UND IHRE PRIMZERLEGUNG 1
§1: Der Euklidische Algorithmus 1
§2: Der erweiterte EUKLIDische Algorithmus 4
§3: Der Aufwand des EUKLIDischen Algorithmus 9
§4: Die multiplikative Struktur der ganzen Zahlen 14
§5: Kongruenzenrechnung 15
§6: Der chinesische Restesatz 18
§7: Prime Restklassen 24

KAPITEL II: ANWENDUNGEN IN DER KRYPTOGRAPHIE 30
§1: New directions in cryptography 30
§2: Das RSA-Verfahren 33
§3: Weitere Anwendungen des RSA-Verfahrens 38
a) Identitätsnachweis 38
b) Elektronische Unterschriften 40
c) Blinde Unterschriften und elektronisches Bargeld 41
d) Bankkarten mit Chip 44
§4: Wie groß sollten die Primzahlen sein? 46
§5: Verfahren mit diskreten Logarithmen 49
§6: DSA 53
§7: Anwendungen bei SSL/TLS 55
§8: Ausblick 56

KAPITEL III: KETTENBRÜCHE 58
§1: Der Kettenbruchalgorithmus 58
§2: Geometrische Formulierung 61
§3: Optimale Approximation 65
§4: Eine kryptographische Anwendung 71

KAPITEL IV: QUADRATISCHE ZAHLKÖRPER 73
§1: Grundbegriffe der Ringtheorie 73
§2: Die Elemente quadratischer Zahlkörper 77
§3: Die Hauptordnung eines Zahlkörpers 78
§4: Normen und Spuren in quadratischen Zahlkörpern 82
§5: EUKLIDische Ringe 83
§6: Einheiten in quadratischen Zahlkörpern 92
§7: Quaternionen 95

KAPITEL V: QUADRATISCHE FORMEN 98
§1: Summen zweier Quadrate 98
§2: Anwendung auf die Berechnung von π 104
§3: Der Satz von LAGRANGE 110
§4: Quadratische Formen und Matrizen 113
§5: Kettenbruchentwicklung quadratischer Irrationalitäten 116
§6: Die PELLsche Gleichung 121

KAPITEL VI: QUADRATISCHE RESTE 127
§1: Das LEGENDRE-Symbol 127
§2: Das quadratische Reziprozitätsgesetz 129
§3: Das JACOBI-Symbol 133
§4: Berechnung der modularen Quadratwurzel 137
§5: Anwendungen quadratischer Reste 144
a) Münzwurf per Telephon 144
b) Akustik von Konzerthallen 145

KAPITEL VII: PRIMZAHLEN 152
§1: Das Sieb des ERATOSTHENES 152
§2: Der FERMAT-Test 154
§3: Der Test von MILLER und RABIN 159
§4: Der Test von Agrawal, Kayal und Saxena 161
§5: Die Verteilung der Primzahlen 172

KAPITEL VIII: FAKTORISIERUNGSVERFAHREN 184
§1: Die ersten Schritte 186
a) Test auf Primzahl 186
b) Abdividieren kleiner Primteiler 186
§2: Die Verfahren von POLLARD und ihre Varianten 187
a) Die Monte-Carlo-Methode 187
b) Die ($p-1$)-Methode 190
c) Varianten 192
§3: Das Verfahren von Fermat und seine Varianten 194