

Wolfgang K. Seiler

# Zahlentheorie

Vorlesung an der Universität Mannheim  
im Frühjahrssemester 2009

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 Entstehungsweise 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](mailto: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/](http://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.

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

## 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