Westfälische
Wilhelms-Universität
Münster

Fachbereich 10
Mathematik und
Informatik

# Elementare Zahlentheorie

## gelesen von Prof. Dr. Falko Lorenz

Mitschrift von Phil Steinhorst

Wintersemester 2014/2015

http://wwwmath.uni-muenster.de/u/karin.halupczok/elZTWiSe14/

Stand: 12. Oktober 2014

## Vorwort

Der vorliegende Text ist eine Zusammenfassung zur Vorlesung Elementare Zahlentheorie, gelesen von Prof. Dr. Falko Lorenz an der WWU Münster im Wintersemester 2014/2015. Der Inhalt entspricht weitestgehend dem Skript, welches auf der Vorlesungswebsite bereitsgestellt wird, jedoch wird auf Beweise weitestgehend verzichtet. Für die Korrektheit des Inhalts wird keinerlei Garantie übernommen. Bemerkungen, Korrekturen und Ergänzungen kann man folgenderweise loswerden:

- persönlich durch Überreichen von Notizen oder per E-Mail
- durch Abändern der entsprechenden TeX-Dateien und Versand per E-Mail an mich
- direktes Mitarbeiten via GitHub. Dieses Skript befindet sich im `latex-wwu`-Repository von JaMeZ-B:

`https://github.com/JaMeZ-B/latex-wwu`

### Themenübersicht

Im Sommersemester 2013 wurden folgende Themen behandelt:

- Ein paar algebraische Grundlagen (Gruppen- und Ringtheorie, Ideale)
- Fundamentalsatz der Arithmetik (Satz von der eindeutigen Primfaktorzerlegung)
- Euklidischer Algorithmus, Kettenbruchdarstellung
- Simultane Kongruenzen, Satz von Euler-Fermat, chinesischer Restsatz
- Restklassengruppen, Hauptsatz über endliche abelsche Gruppen
- Gaußscher Zahlenring $\mathbb{Z}[\mathrm{i}]$
- Quadratische Reste, Quadratisches Reziprozitätsgesetz
- Fermat- und Mersenne-Primzahlen
- Zahlentheoretische Funktionen $\varphi\colon \mathbb{N} \longrightarrow \mathbb{C}$
- Satz von Lagrange ("Vier-Quadrate-Satz")

### Literatur

- F. Ischebeck: Einladung zur Zahlentheorie
- R. Remmert, P. Ullrich: Elementare Zahlentheorie
- A. Scholz, B. Schöneberg: Einführung in die Zahlentheorie
- K. Halupczok: Skript zur Elementaren Zahlentheorie

### Vorlesungswebsite

`http://wwwmath.uni-muenster.de/u/karin.halupczok/elZTWiSe14/`

Phil Steinhorst
p.st@wwu.de

# Inhaltsverzeichnis

# 1 Fundamentalsatz der elementaren Arithmetik

### Terminologie

Sei $R$ ein kommutativer Ring mit $1 \neq 0$. $R$ heißt **Integritätsring** bzw. **nullteilerfrei**, wenn gilt:

$$a \cdot b = 0 \quad \Rightarrow \quad a = 0 \text{ oder } b = 0.$$

**Beispiel 1.1**

- $\mathbb{Z}$
- $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$
  $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$
  $\mathbb{Z}[\sqrt{-5}] := \dots$
- $K[X]$ für $K$ Körper
  $\mathbb{Z}[X]$
- $K$ Körper
- $\mathbb{C}\langle z \rangle := \left\{ \text{konvergente Potenzreihen } \sum\limits_{n=0}^{\infty} a_n z^n \right\}$
- Nicht nullteilerfrei ist z.B. $\mathcal{C}[0,1] := \{f : [0,1] \to \mathbb{R} \text{ stetig}\}$

**Definition 1.1 (Teilbarkeit)**

Seien $a, b \in R$. $a$ heißt ein **Teiler** von $b$, wenn ein $q \in R$ existiert mit $b = qa$, und schreiben:

$$a|b$$

Ist $R$ nullteilerfrei und $a \neq 0$, so ist $q$ eindeutig bestimmt.

**F1.1 (Triviale Teilbarkeitsregeln)**

(i) $a|0, 1|a, a|a$

(ii) $a|b, b|c \quad \Rightarrow \quad a|c$

(iii) $a|b, a|c \quad \Rightarrow \quad a|b+c, a|b-c$

(iv) $a_1|b_1, a_2|b_2 \quad \Rightarrow \quad a_1a_2|b_1b_2$

(v) $ac|bc \quad \Rightarrow \quad a|b$, falls $c \neq 0$ und $R$ nullteilerfrei.

## Index

## Liste der Sätze und Definitionen