Westfälische
Wilhelms-Universität
Münster

Fachbereich 10
Mathematik und
Informatik

Elementare Zahlentheorie

gelesen von Prof. Dr. Falko Lorenz

Zusammenfassung von Phil Steinhorst

Wintersemester 2014/2015

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

Stand: 14. Dezember 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 Jannes Bantje:

  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

14.10. [1] 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

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

Definition 1.1 (Teilbarkeit)

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

$$a|b$$

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.

Definition 1.2 (Einheit, assoziiert)

(i) $e \in R$ heißt eine **Einheit** in R, falls $e|1$ gilt, d.h. falls ein $f \in R$ existiert mit $ef = 1$. f ist eindeutig bestimmt.
Wir setzen $e^{-1} := f$ und schreiben auch $\frac{1}{e}$ für e^{-1}.
Wir bezeichnen die **Einheitengruppe** von R mit $R^\times := \{x \in R : x \text{ ist Einheit in } R\}$.

(ii) $a \in R$ heißt **assoziiert** zu $b \in R$, falls $a|b$ und $b|a$ gilt. Schreibe: $a \mathrel{\hat{=}} b$.

Beispiel 1.2

1) Sei K ein Körper, dann ist $K^\times = K \setminus \{0\}$. $\quad \mathbb{Z}^\times = \{1, -1\}$, $\quad K[X]^\times = K^\times$,
$\mathcal{C}[0,1]^\times = \{f \in \mathcal{C}[0,1] : f(x) \neq 0$ für alle $x \in [0,1]\}$, $\quad \mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^k : k \in \mathbb{Z}\}$
$\mathbb{Z}[X]^\times = \{1, -1\}$ $\quad \mathbb{C}\langle z\rangle^\times = \{\sum a_n z^n \in \mathbb{C}\langle z\rangle : a_0 \neq 0\}$

2) $e \in R^\times \quad \Leftrightarrow \quad e|a$ für jedes $a \in R$.

F1.2

Sei R ein Integritätsring, $a, b \in R$ und $b \neq 0$. Dann gilt:

$$a \mathrel{\hat{=}} b \quad \Leftrightarrow \quad \exists e \in R^\times \text{ mit } b = ea$$

Beweis

"⇐": $a|b, e^{-1}b = a, b|a$

"⇒": Da $a|b$ und $b|a$, existieren $e, f \in R$, sodass $b = ea$ und $a = fb$. $\Rightarrow b = efb \Rightarrow ef = 1$, da $b \neq 0$ und R nullteilerfrei. □

Ab jetzt ist, wenn nichts anderes gesagt, R ein Integritätsring!

Definition 1.3 (unzerlegbar, irreduzibel, zusammengesetzt)

Sei $a \in R \setminus R^\times$. a heißt **unzerlegbar** oder **irreduzibel** in R, wenn gilt:

$$a = bc \text{ in } R \quad \Rightarrow \quad b \in R^\times \text{ oder } c \in R^\times.$$

Andernfalls heißt a **zerlegbar**, **zusammengesetzt** oder **reduzibel**.

Bemerkung

a unzerlegbar $\quad \Leftrightarrow \quad$ jeder Teiler von a ist Einheit oder assoziiert zu a
a zerlegbar $\quad \Leftrightarrow \quad a$ hat echten Teiler, d.h. einen Teiler, der weder eine Einheit ist noch assoziiert zu a

Definition 1.3 (Primzahl)

Ein $p \in \mathbb{Z}$ heißt **Primzahl**, wenn $p \in \mathbb{N}$ und p unzerlegbar in $\mathbb{Z}$. Wir bezeichnen mit $\mathbb{P}$ die Menge der Primzahlen von $\mathbb{Z}$. a unzerlegbar in $\mathbb{Z} \Leftrightarrow a = p$ oder $a = -p$ mit $p \in \mathbb{P}$.

Bemerkung

$a \in \mathbb{Z}$ sei zerlegbar, $a \neq 0$. Dann gibt es eine Primzahl p mit $p|a$ und $p \leq \sqrt{|a|}$.

Definition 1.4 (Zerlegung in unzerlegbare Faktoren)

Wir sagen, $a \in R$ besitzt in R eine **Zerlegung in unzerlegbare Faktoren**, wenn

$$a = ep_1p_2 \dots p_r \text{ mit } e \in R^\times \text{ und } p_1, \dots, p_r \text{ unzerlegbar} \tag{1.1}$$

(1.1) heißt eine Zerlegung von a in unzerlegbare Faktoren. Auch $r = 0$ ist erlaubt.

F1.3

In $\mathbb{Z}$ besitzt jedes $a \neq 0$ eine Zerlegung in unzerlegbare Faktoren.

F1.3
Jede natürliche Zahl $a > 1$ besitzt eine Zerlegung $a = p_1 p_2 \dots p_r$ mit Primzahlen $p_1, \dots, p_r$ und $r \geq 1$.

Bemerkung

1) Die Aussage F1.3 gilt auch für die Beispiele 1.1, mit Ausnahme von $\mathcal{C}[0,1]$.
2) Sei R ein Integritätsring, der die **Teilbarkeitsbedingung für Hauptideale** erfüllt, so besitzt jedes $a \neq 0$ aus R eine Zerlegung in unzerlegbare Faktoren.
3) Primzahlen sind die multiplikativen Bausteine (Atome) von $\mathbb{N}$.
4) Im Beispiel $\mathbb{C}\langle z \rangle$ von oben gibt es (bis auf Assoziiertheit) nur das einzige unzerlegbare Element z. Dieses ist ein **Primelement** (der Begriff folgt weiter unten).

Satz 1.1 (Existenz unendlich vieler Primzahlen)
Es gibt unendlich viele Primzahlen.

Bemerkungen
Es sei $p_1, p_2, \dots$ die aufsteigend sortierte Folge der Primzahlen.

1) $a_n := p_1 p_2 \dots p_n + 1$ ist Primzahl für $n \leq 5$, aber z.B. nicht für $n = 6$. Unklar ist, ob unendlich viele a_n Primzahlen oder keine Primzahlen sind.
2) Für $x \in \mathbb{R}_{>0}$ definieren wir:
$$\pi(x) := \#\{p \in \mathbb{P} : p \leq x\}$$

Primzahlsatz (Gauß, Legendre)

$$\pi(x) \sim \frac{x}{\log x}, \text{ d.h. } \lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1$$

$$\pi(x) \sim \int_2^x \frac{1}{\log t} dt =: \operatorname{li}(x)$$

$$\pi(x) > \frac{x}{\log x} \text{ für alle } x \geq 17$$

$$\pi(n) > \frac{n}{\log n} \text{ für alle } n \in \mathbb{N}, n \geq 11$$

Definition 1.5 (eindeutige Zerlegung)
Sei R ein kommutativer Ring mit $1 \neq 0$. Wir sagen, $a \in R \setminus \{0\}$ hat eine **eindeutige Zerlegung in unzerlegbare Faktoren**, wenn a eine Zerlegung

$$a = e p_1 p_2 \dots p_r$$

in unzerlegbare Faktoren besitzt und eine solche im folgendem Sinne eindeutig ist: Ist auch

$$a = e' p_1' p_2' \dots p_{r'}'$$

eine solche Zerlegung, so gilt $r = r'$ und nach Umnummerierung $p_i' \mathrel{\hat{=}} p_i$ für alle $1 \leq i \leq r$.

F1.4
In dem Integritätsring R besitze jedes Element $a \neq 0$ eine Zerlegung in unzerlegbare Faktoren. Dann sind äquivalent:

(i) Jedes $a \neq 0$ aus R hat eindeutige Zerlegung in unzerlegbare Faktoren.

(ii) Ist p unzerlegbar, so gilt: $p|ab \Rightarrow p|a$ oder $p|b$.

Definition 1.6 (Primelement)
Sei R ein kommutativer Ring mit $1 \neq 0$. Ein $p \in R \setminus R^\times$ heißt **Primelement** von R, wenn für alle $a, b \in R$ gilt:

$$p|ab \quad \Leftrightarrow \quad p|a \text{ oder } p|b \tag{1.2}$$

Bemerkung
1) 0 ist Primelement in $R \Leftrightarrow R$ ist Integritätsring

2) In einem Integritätsring R gilt: Jedes Primelement $p \neq 0$ ist unzerlegbar.

Lemma 1.1
Seien $a, b \in \mathbb{N}$. Sei $m = \mathrm{kgV}(a, b) \in \mathbb{N}$. Dann gilt:

$$a|c \text{ und } b|c \quad \Rightarrow \quad m|c$$

m ist also auch minimal bzgl. der Teilbarkeitsrelation $|$.

F1.5 (Satz von Euklid)
Jede Primzahl p ist ein Primelement von $\mathbb{Z}$, d.h. es gilt stets (1.2). (Das gleiche gilt für $-p$, also für jedes unzerlegbare Element von $\mathbb{Z}$.) 17.10. [2]

Fundamentalsatz der elementaren Arithmetik
In $\mathbb{Z}$ hat jedes $a \neq 0$ eine eindeutige Zerlegung in unzerlegbare Faktoren.

Bemerkung
Eindeutige Zerlegung in unzerlegbare Faktoren hat man zum Beispiel auch für die Ringe $\mathbb{Z}[\sqrt{2}], \mathbb{Z}[i], K[X]$ und K für K Körper, $\mathbb{Z}[X]$ und $\mathbb{C}\langle z\rangle$, nicht aber für $\mathbb{Z}[\sqrt{-5}]$:

$$3 \cdot 3 = 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

Dies sind zwei wesentlich verschiedene Zerlegungen in unzerlegbare Faktoren.

Definition 1.7 (Exponent)
Sei p eine Primzahl und $a \in \mathbb{Z} \setminus \{0\}$. Dann heißt

$$w_p(a) := \max\{k \in \mathbb{N}_0 : p^k | a\}$$

der **Exponent** von p in a. Wir setzen $w_p(0) := \infty$.

F1.6 (Eigenschaften der Exponentfunktion)
Die Funktion $w_p \colon \mathbb{Z} \to \mathbb{N}_0 \cup \{\infty\}$ hat folgende Eigenschaften:

(i) $w_p(a + b) \geq \min(w_p(a), w_p(b))$ und Gleichheit, falls $w_p(a) \neq w_p(b)$.

(ii) $w_p(ab) = w_p(a) + w_p(b)$

Satz 1.2 (Fundamentalsatz der elementaren Arithmetik)
Für jedes $a \in \mathbb{Z} \setminus \{0\}$ gilt $w_p(a) > 0$ nur für endlich viele p. Es ist

$$a = \operatorname{sgn}(a) \cdot \prod_p p^{w_p(a)} \tag{1.3}$$

Bemerkung

1) w_p lässt sich eindeutig zu einer Abbildung $w_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ fortsetzen, sodass (ii) für alle $a, b \in \mathbb{Q}$ gilt. Es gilt dann auch (i). Für $a \in \mathbb{Q} \setminus \{0\}$ ist $w_p(a) \neq 0$ nur für endlich viele p, und die Formel (1.3) gilt entsprechend. Ferner gilt: $a \in \mathbb{Z} \Leftrightarrow w_p(a) \geq 0$ für alle p.

2) Sei
$$\mathbb{N}_0^{(\mathbb{P})} := \{(e_p)_{p\in\mathbb{P}} : e_p \in \mathbb{N}_0, e_p = 0 \text{ für fast alle } p\}.$$
Nach Satz 1.2 sind $(\mathbb{N}, \cdot)$ und $(\mathbb{N}_0^{(\mathbb{P})}, +)$ zwei zueinander isomorphe Halbgruppen. Nach Bemerkung 1) sind $\mathbb{Q}^\times$ und $\{1, -1\} \times \mathbb{Z}^{(\mathbb{P})}$ sogar zwei zueinander isomorphe Gruppen.

Definition 1.8 (faktorieller Ring, Vertretersystem für Primelemente)
Ein Integritätsring R heißt **faktoriell**, wenn jedes $a \in R \setminus \{0\}$ eine eindeutige Zerlegung in unzerlegbare Faktoren hat. Man spricht dann auch von eindeutiger Primfaktorzerlegung in R.
P heißt **Vertretersystem für die Primelemente** $\neq 0$ von R, wenn:

(1) Zu jedem Primelement $q \neq 0$ von R gibt es ein $p \in P$ mit $q \mathrel{\hat{=}} p$.

(2) Für $p, p' \in P$ mit $p \mathrel{\hat{=}} p'$ gilt $p = p'$, d.h. p in (1) ist eindeutig bestimmt durch q.

Für $R = \mathbb{Z}$ nehme man stets $P = \mathbb{P}$. Für K Körper und $R = K[X]$ nimmt man $P = \{p \in K[X] : p \text{ irreduzibel und normiert}\}$.

F1.7
Sei R faktoriell und P ein Vertretersystem für Primelemente. Es gibt zu jedem $p \in P$ eine Funktion $w_p \colon R \to \mathbb{N}_0 \cup \{\infty\}$ mit den Eigenschaften (i) und (ii) aus F1.6, sodass gilt:

a) Für jedes $a \in R \setminus \{0\}$ ist $w_p(a) > 0$ nur für endlich viele $p \in P$.

b) Für jedes $a \in R \setminus \{0\}$ gilt
$$a = e \prod_{p\in P} p^{w_p(a)}$$
mit eindeutigem $e \in \mathbb{R}^\times$.

Definition 1.9 (ggT und kgV)
Sei R ein kommutativer Ring mit $1 \neq 0$. Gegeben $a_1, \ldots, a_n \in R$.

a) Ein $d \in R$ heißt ein **größter gemeinsamer Teiler** (ggT) von $a_1, \ldots, a_n$, falls:

1. $d | a_i$ für alle i 2. $t | a_i$ für alle $i \Rightarrow t | d$

b) Ein $m \in R$ heißt ein **kleinstes gemeinsames Vielfaches** (kgV) von $a_1, \ldots, a_n$, falls:

1. $a_i | m$ für alle i 2. $a_i | c$ für alle $i \Rightarrow m | c$

Bemerkung

1) d, d' ggT von $a_1, \ldots, a_n \Rightarrow d \mathrel{\hat{=}} d'$ und m, m' kgV von $a_1, \ldots, a_n \Rightarrow m \mathrel{\hat{=}} m'$

2) Im Allgemeinen ist die Existenz eines ggT und kgV nicht gesichert. In faktoriellen Ringen existieren sie aber immer, siehe dazu folgende Feststellung.

F1.8

Sei R faktoriell, P wie oben. Es gelten: 21.10. [3]

(i) $a|b \quad \Leftrightarrow \quad w_p(a) \leq w_p(b)$ für alle $p \in P$.

(ii) Für $a_1, \ldots, a_n \in R$ setze:

$$d := \prod_{p \in P} p^{\min(w_p(a_1), \ldots, w_p(a_n))} =: (a_1, \ldots, a_n)$$

$$m := \prod_{p \in P} p^{\max(w_p(a_1), \ldots, w_p(a_n))} =: [a_1, \ldots, a_n]$$

Hierbei setze $p^\infty = 0$. Dann ist d ein ggT von $a_1, \ldots, a_n$ und m ein kgV von $a_1, \ldots, a_n$.

(iii) $a, b \in R$. Dann ist $a, b \mathrel{\hat{=}} [a, b] \cdot (a, b)$ und $m \mathrel{\hat{=}} \frac{ab}{(a,b)}$, wenn a, b nicht beide 0.

(iv) $a_1, \ldots, a_n$ paarweise teilerfremd, d.h. $(a_i, a_j) = 1$ für $i \neq j \Leftrightarrow [a_1, \ldots, a_n] \simeq a_1 a_2 \ldots a_n$.

(v) $(a_i, b) = 1$ für $1 \leq i \leq n \Rightarrow (a_1 a_2 \ldots a_n, b) = 1$

(vi) $(a_1 f, \ldots, a_n f) \simeq (a_1, \ldots, a_n) f, [a_1 f, \ldots, a_n f] \simeq [a_1, \ldots, a_n] f$

(vii) $((a_1, \ldots, a_n), a_{n+1}) = (a_1, \ldots, a_n, a_{n+1}), [[a_1, \ldots, a_n], a_{n+1}] = [a_1, \ldots, a_n, a_{n+1}]$

Bemerkung (Verallgemeinerung von (iii)

Seien $a_1, \ldots, a_n \in R$ gegeben. Wähle $q_1, \ldots, q_n$ und c aus R mit

$$a_1 q_1 = a_2 q_2 = \ldots = a_n q_n = c$$

(z.B. $c = a_1 a_2 \ldots a_n, q_i = \prod_{j \neq i} a_j$). Dann gilt

$$c \mathrel{\hat{=}} (a_1, \ldots, a_n)[q_1, \ldots, q_n]$$

F1.9

Sei $n \in \mathbb{N}, a \in \mathbb{Z}$. Ist $X^n = a$ lösbar in $\mathbb{Q}$, so ist $X^n = a$ auch lösbar in $\mathbb{Z}$. Anders ausgedrückt: Ist $a \in \mathbb{Z}$ keine n-te Potenz in $\mathbb{Z}$, so ist a auch keine n-te Potenz in $\mathbb{Q}$.

Anwendung

$\sqrt{2}$ ist irrational, denn 2 ist kein Quadrat in $\mathbb{Z}$ aus Größengründen, also ist 2 nach F1.9 auch kein Quadrat in $\mathbb{Q}$, d.h. $\sqrt{2} \in \mathbb{Q}$.

Korollar
Sei $n \in \mathbb{N}, a \in \mathbb{N}$. Dann sind äquivalent:

(i) a ist n-te Potenz in $\mathbb{Z}$.

(ii) $n | w_p(a)$ für alle p.

(iii) a ist n-te Potenz in $\mathbb{Q}$.

F1.10 (Verallgemeinerung von F1.9)
Gegeben sei ein normiertes Polynom $f(X) \in \mathbb{Z}[X]$. Ist dann b eine Nullstelle von f mit $b \in \mathbb{Q}$, so ist notwendigerweise $b \in \mathbb{Z}$ und außerdem ist b ein Teiler des Absolutkoeffizienten a_0 von f.

2 Der euklidische Algorithmus

Sei R kommutativer Ring mit $1 \neq 0$. Für beliebiges $a \in R$ betrachte man die Menge der Vielfachen von $a \in R$, also

$$Ra := \{xa : x \in R\} = \{b \in R : a|b\}$$

Die Teilmenge $I = Ra$ hat folgende Eigenschaften:

(i) $0 \in I$

(ii) $b_1, b_2 \in I \Rightarrow b_1 + b_2 \in I$

(iii) $c \in R, b \in I \Rightarrow cb \in I$

Definition 2.1 (Ideal, Hauptideal)
Eine Teilmenge I von R heißt ein **Ideal** in R, falls die Eigenschaften (i), (ii), (iii) erfüllt sind. I heißt **Hauptideal**, wenn es ein $a \in R$ gibt mit $I = Ra$. Wir verwenden die Bezeichnung

$$(a) := Ra$$

und nennen (a) das von $a \in R$ erzeugte Hauptideal.

Bemerkung

(1) $(b) \subseteq (a) \Leftrightarrow a|b$

(2) $a \hat{=} b \Leftrightarrow (a) = (b)$

(3) c ist gemeinsames Vielfaches von $a_1, \ldots, a_n \Leftrightarrow (c) \subseteq (a_1) \cap \ldots \cap (a_n)$

(4) m ist ein kgV von $a_1, \ldots, a_n \Leftrightarrow (a_1) \cap \ldots \cap (a_n) = (m)$

(5) d ist ein gemeinsamer Teiler von $a_1, \ldots, a_n \Leftrightarrow (a_i) \subseteq (d)$ für $1 \leq i \leq n$

(6) d ist ein gemeinsamer Teiler von $a_1, \ldots, a_n \Leftrightarrow Ra_1 + Ra_2 + \ldots + Ra_n \subseteq (d)$

(7) d ist ein ggT von $a_1, \ldots, a_n \Leftrightarrow (d)$ ist das kleinste Hauptideal mit $Ra_1 + \ldots + Ra_n \subseteq (d)$.

Ein ggT lässt sich also idealtheoretisch nicht so einfach charakterisieren wie oben ein kgV durch (4). Am schönsten wäre es, wenn $Ra_1 + \ldots + Ra_n$ ein Hauptideal wäre, dann würde (7) übergehen in:

$$d \text{ ist ein ggT von } a_1, \ldots, a_n \Leftrightarrow Ra_1 + Ra_2 + \ldots + Ra_n = (d)$$

Definition 2.2 (Hauptidealring)
Ein Integritätsring R heißt ein **Hauptidealring**, wenn jedes Ideal I von R ein Hauptideal ist.

Bezeichnung
Für Elemente $a_1, \ldots, a_n$ in einem beliebigen kommutativen Ring R mit $1 \neq 0$ setze

$$(a_1, \ldots, a_n) := Ra_1 + \ldots + Ra_n$$

Man nennt $(a_1, \ldots, a_n)$ das von $a_1, \ldots, a_n$ erzeugte Ideal in R.

F2.1 (Satz vom größten gemeinsamen Teiler)

24.10. [4] Sei R ein Hauptidealring. Dann gilt: Zu jedem System $a_1, \ldots, a_n$ von Elementen aus R existiert ein ggT d von $a_1, \ldots, a_n$ und jedes solche d besitzt eine Darstellung der Gestalt

$$d = x_1 a_1 + \ldots + x_n a_n \quad \text{mit } x_i \in R \tag{2.1}$$

Wir sagen, in R gelte der **Satz vom größten gemeinsamen Teiler**.

Bemerkung

Sei R ein beliebiger Integritätsring. Ist d ein gemeinsamer Teiler von $a_1, \ldots, a_n$ aus R und gibt es eine Darstellung der Form (2.1), so ist d ein ggT von $a_1, \ldots, a_n$.

Satz 2.1

$\mathbb{Z}$ ist ein Hauptidealring.

Definition (Gaußklammer)

Für $x \in \mathbb{R}$ setze

$$[x] = \max\{g \in \mathbb{Z} : g \leq x\} \in \mathbb{Z}$$

$[x]$ ist charakterisiert durch folgende zwei Eigenschaften:

(1) $[x] \in \mathbb{Z}$

(2) $[x] \leq x < [x] + 1$

F2.2 (Division mit Rest in $\mathbb{Z}$)

Gegeben $a, b \in \mathbb{Z}$, $a \neq 0$. Dann gibt es eine Darstellung

$$b = qa + r \quad \text{mit } 0 \leq r < |a| \text{ und } q, r \in \mathbb{Z} \tag{2.2}$$

Bemerkung

1) Die Darstellung (2.2) ist eindeutig.

2) Es gibt eine Darstellung

$$b = qa + r \quad \text{mit } |r| < |a|; q, r \in \mathbb{Z},$$

doch diese ist nicht mehr eindeutig, z.B. $27 = 4 \cdot 6 + 3 = 5 \cdot 6 - 3$.

3) Es gibt eine Darstellung

$$b = qa + r \quad \text{mit } -\frac{|a|}{2} < r \leq \frac{|a|}{2}; q, r \in \mathbb{Z},$$

und diese ist eindeutig.

4) Es gibt eine Darstellung

$$b = qa + r \quad \text{mit } |r| \leq \frac{|a|}{2}; q, r \in \mathbb{Z},$$

doch diese ist nicht eindeutig, falls a gerade.

Definition 2.3 (euklidischer Ring)

Ein Integritätsring R heißt ein **euklidischer Ring**, falls eine Funktion $\nu \colon R \to \mathbb{N}_0$ mit $\nu(0) = 0$ existiert, sodass gilt: Zu $a, b \in R$ mit $a \neq 0$ existieren $q, r \in R$ mit

$$b = qa + r \text{ und } \nu(r) < \nu(a)$$

Beispiele

(1) $R = \mathbb{Z}$ mit $\nu(a) = |a|$.

(2) $R = K[X], K$ Körper, mit $\nu(g) = \deg(g) + 1$ für $g \neq 0$, $\nu(0) = 0$.

(3) $R = \mathbb{Z}[i]$ mit $\nu(z) = N(z) = z\overline{z} = |z|^2$.

F2.3

Jeder euklidische Ring ist ein Hauptidealring.

F2.4

Jeder Hauptidealring ist faktoriell.

Im Folgenden sei R ein euklidischer Ring mit euklidischer Normfunktion ν. Allgemein gilt folgende elementare Umformung:

$$(a_1, a_2, \ldots, a_n) = (a_1, a_2 - y_2 a_1, \ldots, a_n - y_n a_1) \text{ für bel. } y_i \in R \tag{2.3}$$

Euklidischer Algorithmus

Gegeben $a_1, \ldots, a_n \in R$. Wir wollen $d \in R$ bestimmen mit

$$(a_1, \ldots, a_n) = (d)$$

Sind alle $a_i = 0$, so ist $d = 0$ und wir sind fertig. Sei daher ohne Einschränkung

$$a_1 \neq 0 \text{ und } \nu(a_1) \leq \nu(a_i), \text{ falls } a_i \neq 0$$

Sei $a_i = q_i a_1 + r_i$ mit $\nu(r_i) < \nu(a_1)$ für $i \geq 2$. Dann ist

$$(a_1, \ldots, a_n) \overset{(2.3)}{=} (a_1, r_2, \ldots, r_n)$$

Fortsetzung des Verfahrens liefert

$$(d, 0, 0, \ldots, 0) = (d)$$

Beispiel

$$\begin{aligned} (27, 63, 114) \quad & 63 = 2 \cdot 27 + 9, 114 = 4 \cdot 27 + 6 \\ = (27, 9, 6) \quad & 27 = 4 \cdot 6 + 3, 9 = 1 \cdot 6 + 3 \\ = (3, 3, 6) \quad & 3 = 1 \cdot 3 + 0, 6 = 2 \cdot 3 + 0 \\ = (3, 0, 0) = (3) & \end{aligned}$$

Beispiel im Fall $n = 2$

Sei $a, b \in R \setminus \{0\}$.

28.10.
[5]

$$\begin{aligned} b &= q_0 a + r_1 && \nu(r_1) < \nu(a) && \text{Falls } r_1 = 0, \text{ dann Schluss. Sonst weiter:} \\ a &= q_1 r_1 + r_2 && \nu(r_2) < \nu(r_1) \\ r_1 &= q_2 r_2 + r_3 && \nu(r_3) < \nu(r_2) \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n && \nu(r_n) < \nu(r_{n-1}) \\ r_{n-1} &= q_n r_n + 0 \end{aligned}$$

Also:

$$(a, b) = (a, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n)$$

F2.5

r_n ist ein größter gemeinsamer Teiler von a und b. Es ist

$$r_n = xa + yb \text{ mit } x, y \in R,$$

wobei x und y aus obiger Rechnung rekursiv bestimmbar sind.

Bemerkung

1) Von neuem erhalten wir für jeden euklidischen Ring also den Satz vom größten gemeinsamen Teiler. (Satz 2.1)

2) Sei $R = \mathbb{Z}$. Verlangen wir $0 \leq r_i$ in obiger Rechnung, so sind $q_0, q_1, \ldots, q_n$ sowie die $r_1, \ldots, r_n$ eindeutig bestimmt.

Beispiel

Sei $a = 84, b = 133$.

$$\begin{aligned}
133 &= 1 \cdot 84 + 49 \\
84 &= 1 \cdot 49 + 35 \\
49 &= 1 \cdot 35 + 14 \\
35 &= 2 \cdot 14 + 7 \\
14 &= 2 \cdot 7 \qquad \Rightarrow n = 4, r_4 = 7
\end{aligned}$$

Also ist $(133, 84) = (7)$.

Wir können den euklidischen Algorithmus für a, b auch wie folgt aufschreiben:

$$\begin{array}{lll}
\frac{b}{a} = q_0 + \frac{r_1}{a} & q_0 = \left[\frac{b}{a}\right] & 0 < \frac{r_1}{a} < 1, \text{ falls } r_1 \neq 0 \\
\frac{a}{r_1} = q_1 + \frac{r_2}{r_1} & q_1 = \left[\frac{a}{r_1}\right] & \\
\frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2} & & \\
\quad\vdots & & \\
\frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}} & & \\
\frac{r_{n-1}}{r_n} = q_n & &
\end{array}$$

Zusammengefasst erhalten wir die **Kettenbruchentwicklung** von $\frac{b}{a}$:

$$\frac{b}{a} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}$$

Statt einer rationalen Zahl sei jetzt α allgemeiner eine beliebige reelle Zahl.

Es ist $\alpha = [\alpha] + \varepsilon$ mit $0 \leq \varepsilon < 1$. Falls $\alpha \notin \mathbb{Z}$, d.h. $\varepsilon > 0$, setze $q_0 := [\alpha]$ und $\rho_1 := \frac{1}{\varepsilon}$. Dann:

$$\begin{array}{lll}
\alpha = q_0 + \frac{1}{\rho_1} & \text{mit } \rho_1 > 1. & \text{Falls } \rho_1 \notin \mathbb{Z}, \text{ so setze } [\rho_1] =: q_1 \\
\rho_1 = q_1 + \frac{1}{\rho_2} & \text{mit } \rho_2 > 1. & \text{usw.} \\
\quad\vdots & & \\
\rho_k = q_k + \frac{1}{\rho_{k+1}} & \text{mit } \rho_{k+1} > 1. &
\end{array}$$

Abbrechen, wenn $\rho_{n+1} \in \mathbb{Z}$, sonst weiter. Jedenfalls:

$$\alpha = \frac{b}{a} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_k + \cfrac{1}{\rho_{k+1}}}}}$$

Definition 2.4 (Kettenbruch, k-ter Rest)

1) $q_0, q_1, \ldots, q_n$ seien reelle Zahlen mit $q_1, \ldots, q_n > 0$. Unter dem **endlichen Kettenbruch**

$$[q_0; q_1, \ldots, q_n] \tag{2.4}$$

mit den Teilquotienten q_i verstehen wir sowohl das $(n+1)$-Tupel $(q_0, q_1, \ldots, q_n)$, als auch seinen wie folgt definierten Wert:

$$[q_0; q_1, \ldots, q_n] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_n}}} \tag{2.5}$$

Für $0 \leq k \leq n$ nennen wir den Kettenbruch

$$\rho_k := [q_k; q_{k+1}, \ldots, q_n] \tag{2.6}$$

den k**-ten Rest** des Kettenbruchs (2.4). Für den Wert (2.4) des Kettenbruchs (2.4) gilt:

$$[q_0; q_1, \ldots, q_n] = [q_0; q_1, \ldots, q_{k-1}, \rho_k] \text{ für } 0 \leq k \leq n \tag{2.7}$$

Man kann den Wert (2.5) des Kettenbruchs (2.4) durch (2.7) mit (2.6) rekursiv definieren: Es ist $[q_0] = q_0, [q_0; q_1] = q_0 + \frac{1}{q_1}$, also:

$$[q_0; q_1, \ldots, q_n] = [q_0; \rho_1] = q_0 + \frac{1}{\rho_1} \text{ für } n \geq 1$$

2) Gegeben sei eine Folge $(q_k)_{k \geq 0}$ in $\mathbb{R}$ mit $q_k > 0$ für $k \geq 1$. Unter dem **unendlichen Kettenbruch**

$$[q_0; q_1, q_2, \ldots] \tag{2.8}$$

verstehen wir die Folge der

$$[q_0; q_1, \ldots, q_n] \qquad n = 0, 1, 2, \ldots$$

Falls diese Folge in $\mathbb{R}$ konvergiert, so bezeichnen wir auch deren Limes mit $[q_0; q_1, q_2, \ldots]$. Der unendliche Kettenbruch

$$\rho_k := [q_k; q_{k+1}, \ldots] \qquad k = 0, 1, 2, \ldots \tag{2.9}$$

heißt der k**-te Rest** von (2.8). Formal gilt:

$$[q_0; q_1, q_2, \ldots] = [q_0; q_1, \ldots, q_{k-1}, \rho_k] \tag{2.10}$$

Später werden wir sehen, dass (2.10) auch für die Werte der entsprechenden Kettenbrüche gilt, wenn (2.9) konvergiert.

Definition 2.5 (Näherungsbruch)
Jedem endlichen Kettenbruch $[q_0; q_1, \ldots, q_k]$ ordnen wir rekursiv ein Paar $\binom{c}{d} \in \mathbb{R} \times \mathbb{R}_{>0}$ reeller Zahlen zu mit

$$[q_0; q_1, \ldots, q_k] = \frac{c}{d} \tag{2.11}$$

$k = 0$: Für $[q_0]$ sei $\binom{c}{d} = \binom{q_0}{1}$. Es gilt dann in der Tat $[q_0] = q_0 = \frac{q_0}{1}$.
$k \geq 1$: Zuerst Motivation (Heuristik):

$$[q_0; q_1, \ldots, q_k] = [q_0; \rho_1] = q_0 + \frac{1}{\rho_1}$$

mit $\rho_1 = [q_1; q_2, \ldots, q_k]$. Gehöre $\binom{c'}{d'}$ zu ρ_1. Dann gilt

$$[q_0; q_1, \ldots, q_k] = q_0 + \frac{d'}{c'} = \frac{q_0 c' + d'}{c'}$$

Wir ordnen nun also $[q_0; q_1, \ldots, q_k]$ das Tupel

$$\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} q_0 c' + d' \\ c' \end{pmatrix} = \underbrace{\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}}_{=:M_1} \begin{pmatrix} c' \\ d' \end{pmatrix}$$

zu. Dann gilt (2.11). Sei jetzt

$$[q_0; q_1, \ldots] \tag{2.12}$$

ein endlicher oder unendlicher Kettenbruch. Das dem k-ten Abschnitt

$$[q_0; q_1, \ldots, q_k] \tag{2.13}$$

von (2.12) zugeordnete 2-Tupel

$$\begin{pmatrix} c_k \\ d_k \end{pmatrix}$$

heißt der k**-te Näherungsbruch** von (2.12). Auch $\frac{c_k}{d_k}$ heißt k-ter Näherungsbruch von (2.12). Ist (2.12) der endliche Kettenbruch $[q_0, q_1, \ldots, q_n]$, so ist der n-te Näherungsbruch $\frac{c_n}{d_n}$ gleich dem Wert dieses Kettenbruchs. Allgemein ist $\frac{c_k}{d_k}$ der Wert des Kettenbruchs (2.13). Aus formalen Gründen definieren wir noch

$$\begin{pmatrix} c_{-1} \\ d_{-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} c_{-2} \\ d_{-2} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

F2.6 (Rekursionsformeln für Näherungsbrüche)
Mit den Bezeichnungen wie oben gilt:

$$\begin{aligned} c_k &= q_k c_{k-1} + c_{k-1} \\ d_k &= q_k d_{k-1} + d_{k-2} \end{aligned} \tag{2.14}$$

Dies schreiben wir auch in Matrizenform:

$$\begin{pmatrix} c_k \\ d_k \end{pmatrix} = \underbrace{\begin{pmatrix} c_{k-1} & c_{k-2} \\ d_{k-1} & d_{k-2} \end{pmatrix}}_{=:M_k} \begin{pmatrix} q_k \\ 1 \end{pmatrix}$$

Bemerkung
$d_k > 0$ für $k \geq 0$ (vgl. Definition 2.5, oder auch (2.14)).

F2.7

Mit den obigen Bezeichnungen gilt: 31.10. [6]

(i) $M_{k+1} = M_k \cdot \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$, also:

(ii) $M_{k+1} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$

(iii) $d_k c_{k-1} - c_k d_{k-1} = (-1)^k$ für $k \geq -1$

(iv) $\frac{c_{k-1}}{d_{k-1}} - \frac{c_k}{d_k} = \frac{(-1)^k}{d_k d_{k-1}}$ für $k \geq 1$ $\qquad d_{-1} = 0$

(v) $d_k c_{k-2} - c_k d_{k-2} = (-1)^{k-1} q_k$ für $k \geq 0$

(vi) $\frac{c_{k-2}}{d_{k-2}} - \frac{c_k}{d_k} = \frac{(-1)^{k-1} q_k}{d_k d_{k-1}}$ für $k \geq 0$, aber $k \neq 1$

F2.8

(i) $\left(\frac{c_{2m}}{d_{2m}}\right)_{m \geq 0}$ ist streng monoton steigend

(ii) $\left(\frac{c_{2m+1}}{d_{2m+1}}\right)_{m \geq 0}$ ist streng monoton fallend

(iii) $\frac{c_{2m}}{d_{2m}} < \frac{c_{2n+1}}{d_{2n+1}}$ für alle $m \geq 0, n \geq 0$

F2.9

(i) $[q_0; q_1, \ldots, q_n] = \frac{\rho_k c_{k-1} + c_{k-2}}{\rho_k d_{k-1} + d_{k-2}}$ für $1 \leq k \leq n$.

(ii) $[q_k; q_{k-1}, \ldots, q_1] = \frac{d_k}{d_{k-1}}$ für $k \geq 1$

F2.10

Gegeben sei ein unendlicher Kettenbruch

$$\alpha = [q_0; q_1, \ldots]$$

Dann gelten:

(i) α konvergent $\Rightarrow$ jeder Rest $\rho_n = [q_n; q_{n+1}, \ldots]$ ist konvergent.

(ii) ρ_n konvergent für ein $n \Rightarrow \alpha$ ist konvergent

(iii) Ist α konvergent, so gilt für die Werte

$$\alpha = \frac{c_{n-1}\rho_n + c_{n-2}}{d_{n-1}\rho_n + d_{n-2}} \quad n \geq 1$$

d.h. $[q_0; q_1, \ldots] = [q_0; q_1, \ldots, q_{n-1}, \rho_0]$.

(iv) Ist α konvergent, so gilt $\frac{c_{2n}}{d_{2n}} < \alpha < \frac{c_{2m+1}}{d_{2m+1}}$ für alle $n, m \geq 0$.

F2.11

Der Wert α eines konvergenten unendlichen Kettenbruchs genügt den Ungleichungen

$$|\alpha - \frac{c_k}{d_k}| < \frac{1}{d_k d_{k+1}} \text{ für jedes } k \geq 0$$

Definition 2.6 (natürlicher Kettenbruch)
Ein Kettenbruch $[q_0; q_1, \ldots]$ – endlich oder unendlich – heißt **natürlicher Kettenbruch**, wenn $q_k \in \mathbb{Z}$ für alle $k \geq 0$. Nach wie vor setzen wir $q_k > 0$ für $k \geq 1$ voraus!

Im weiteren betrachten wir nur natürliche Kettenbrüche und sprechen dann schlechthin von Kettenbrüchen. Nach F2.6 ist dann

$$c_k, d_k \in \mathbb{Z} \text{ für alle } k \geq -2, \quad d_k \in \mathbb{N} \text{ für } k \geq 0, \quad d_k = q_k d_{k-1} + d_{k-2} \geq d_{k+1} + 1 > d_{k-1} \text{ für } k \geq 1$$

$$d_k > d_{k-1} \text{ für } k \geq 2, \quad d_k \geq k \text{ für } k \geq 1 \tag{2.15}$$

(2.15) gilt im Allgemeinen nicht für $k = 1$. Denn $d_0 = 1$, und es ist $d_1 = 1$ möglich.

Bemerkung
Induktiv folgt leicht $d_k > 2^{\frac{k-1}{2}}$ für $k \geq 2$.

F2.12
Jeder unendliche natürliche Kettenbruch ist konvergent.

F2.13
Die Näherungsbrüche eines natürlichen Kettenbruchs lassen sich nicht kürzen, d.h. c_k und d_k sind teilerfremd für jedes $k \geq -2$.
Wir können also wirklich $\binom{c_k}{d_k}$ mit $\frac{c_k}{d_k}$ identifizieren.

F2.14
Jede rationale Zahl ist durch einen endlichen natürlichen Kettenbruch darstellbar.

F2.15
04.11. [7] Jede irrationale Zahl α ist auf genau eine Weise als natürlicher Kettenbruch darstellbar, und dieser Kettenbruch ist notwendigermaßen unendlich.

Bemerkung
Ist $\alpha \in \mathbb{Q}$, so hat α eine Darstellung als endlicher Kettenbruch

$$\alpha = [q_0; q_1, \ldots, q_n],$$

der – falls $n \geq 1$ ist – mit einem $q_n \geq 2$ endet.

Definition 2.7 (normierter Kettenbruch)
Ein (natürlicher) Kettenbruch, der nicht mit 1 endet, falls er nicht von der Form $[q_0]$ ist, heißt ein **normierter Kettenbruch**. Unendliche Kettenbrüche sind alle normiert.

Bemerkung
Sind $[q_0; q_1, \ldots, q_n]$ und $[q'_0; q'_1, \ldots, q'_m]$ mit $n \geq m$ beide normiert vom selben Wert α, so folgt $m = n$ und $q_i = q'_i$ für alle i.

Satz 2.2

(i) Ordnet man jeder reellen Zahl ihre Kettenbruchentwicklung zu, so erhält man eine Bijektion zwischen $\mathbb{R}$ und der Menge aller normierten Kettenbrüche:

$$\mathbb{R} \ni \alpha \longleftrightarrow [q_0; q_1, \ldots]$$

Die Umkehrabbildung ordnet jedem normierten Kettenbruch dessen Wert zu:

$$\alpha = [q_0; q_1, \ldots]$$

(ii) α rational $\Leftrightarrow$ Kettenbruchentwicklung von α ist endlich.

(iii) Für die Näherungsbrüche $\frac{c_k}{d_k}$ des zu α gehörigen Kettenbruchs gilt[1]

$$\frac{1}{d_k(d_k + d_{k+1}} < \left|\alpha - \frac{c_k}{d_k}\right| \overset{(*)}{\leq} \frac{1}{d_k d_{k+1}} \qquad (k \geq 0),$$

anders geschrieben:

$$\frac{1}{d_k + d_{k+1}} < |d_k - \alpha - c_k| \overset{(*)}{\leq} \frac{1}{d_{k+1}} \qquad (k \geq 0)$$

Zusatz

Die Ungleichungen $(*)$ gelten mit $<$ bis auf den Fall $\alpha = [q_0; q_1, \ldots, q_n]$ und $k = n - 1$.

Bemerkung

Aus (iii) folgt:

$$\left|\alpha - \frac{c_{k-1}}{d_{k-1}}\right| < \alpha - \frac{c_k}{d_k}$$

F2.16

Für die Folge der Fibonacci-Zahlen $(u_n)_{n\in\mathbb{Z}}$ mit $u_0 = 0, u_1 = 1$ und $u_{n+1} = u_n + u_{n-1}$ gilt: 07.11. [8]

(i) $\frac{u_{n+2}}{u_{n+1}}$ ist der n-te Näherungsbruch von $\alpha = [1; 1, 1, \ldots]$, $n \geq 2$.

(ii) $\alpha = \frac{1}{2} + \frac{1}{2}\sqrt{5}$

(iii) $u_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$ mit $\beta = \frac{1}{2} - \frac{1}{2}\sqrt{5}$, $n \in \mathbb{Z}$.

(iv) $u_{m+n} = u_m u_{n+1} + u_{m-1} u_n$ mit $m, n \in \mathbb{Z}$, sowie für $m = n + 1$: $u_{2m-1} = u_m^2 + u_{m-1}^2$.

(v) $u_{n+1} u_{n-1} - u_n^2 = (-1)^n$, bzw. $u_n^2 = u_{n-1} u_{n+1} + (-1)^{n+1}$, etc.

Bemerkung

u_n ist die zu $\frac{\alpha^n}{\sqrt{5}}$ nächstgelegene ganze Zahl für $n \geq 0$.

F2.17

Für $a, b \in \mathbb{Z}$ gilt $(u_a, u_b) = u_{(a,b)}$, insbesondere $a|b \Rightarrow u_a|u_b$.

Bemerkung

u_n Primzahl $\xrightarrow{\text{F2.17}}$ n Primzahl ≥ 3, mit Ausnahme von $u_4 = 3$. Die Umkehrung gilt nicht.

[1] nur sinnvoll, falls es überhaupt noch ein d_{k+1} gibt.

3 Kongruenzrechnung

Zur Motivation:

Satz 3.1 (Fermats kleiner Satz)
Sei p Primzahl. Für jede ganze Zahl mit $p \nmid a$ gilt dann:

$$p|a^{p-1} - 1,$$

d.h. a^{p-1} lässt bei der Division durch p stets den Rest 1.

Definition 3.1 (Kongruenz in $\mathbb{Z}$)
11.11. [9]
Sei $m \in \mathbb{N}$ fest. Für $x \in \mathbb{Z}$ sei $r_m(x)$ der eindeutige nichtnegative Rest von x bei der Division von x durch m.

$$x = qm + r_m \quad 0 \leq r < m$$

Wir definieren eine Relation

Gleichheit bzgl. m

$$x \underset{m}{\sim} x' \qquad :\Leftrightarrow \qquad r_m(x) = r_m(x')$$

Statt $x \underset{m}{\sim} x'$ schreibt man nach Gauß:

$$x \equiv x' \bmod m$$

und sagt: x ist kongruent zu x' modulo m.

F3.1

$$x \equiv x' \bmod m \quad \Leftrightarrow \quad m|x - x'$$

Definition 3.1 (Kongruenz allgemeiner)
Sei R ein kommutativer Ring und $m \in R$. Definiere:

$$x \equiv y \bmod m :\Leftrightarrow m|x - y$$

$x \equiv y \bmod 0 \Rightarrow x = y$
$x \equiv y \bmod 1$ gilt für alle $x, y \in R$.
$x \equiv 0 \bmod m \Leftrightarrow m|x$

F3.2

(i) $x \equiv x \bmod m, \quad x \equiv y \bmod m \Rightarrow y \equiv x \bmod m, \quad x \equiv y \bmod m, y \equiv z \bmod m \Rightarrow x \equiv z \bmod m,$
d.h. $\cdot \equiv \cdot \bmod m$ ist eine Äquivalenzrelation auf R. Diese ist verträglich mit Addition und Multiplikation:

(ii) $x \equiv x' \bmod m, y \equiv y' \bmod m \quad \Rightarrow x + y \equiv x' + y' \bmod m, xy \equiv x'y' \bmod m$

(iii) $x \equiv y \bmod m, m'|m \quad \Rightarrow \quad x \equiv y \bmod m'$

(iv) Für $R = \mathbb{Z}$: $\quad x \equiv y \bmod m_i, 1 \leq i \leq r \quad \Leftrightarrow \quad x \equiv y \bmod \mathrm{kgV}(m_1, \ldots, m_r)$

(v) $x \equiv y \bmod m \quad \Rightarrow \quad cx \equiv cy \bmod xm \quad \Rightarrow \quad cx \equiv cy \bmod m$

(vi) Für einen Integritätsring R gilt: $x \equiv y \bmod m$ und $l|x, l|m, l \neq 0 \quad \Rightarrow \quad l|y$ und $\frac{x}{l} \equiv \frac{y}{l} \bmod \frac{m}{l}$

(vii) Für $R = \mathbb{Z}$: Ist $\mathrm{ggT}(c, m) = d$ mit $d \neq 0$, so gilt $ac \equiv bc \bmod m \quad \Rightarrow \quad a \equiv b \bmod \frac{m}{d}$

(viii) $m|ac - bc \quad \Rightarrow \quad m|c(a-b) \quad \Rightarrow \quad \frac{m}{d}|\frac{c}{d}(a-b) \quad \xrightarrow{\left(\frac{m}{d}, \frac{c}{d}\right)=1} \quad \frac{m}{d}|a-b$

Definition 3.2 (Restklasse)
Ein $m \in R$ teilt R in disjunkte Mengen ein, die den zugehörigen Äquivalenzklassen entsprechen. Diese heißen die **Restklassen** modulo m.

F3.3
Sei $n \in \mathbb{N}$ ungerade. Dann:

$$(n-1)! \equiv 1^2 \cdot 2^2 \dots \left(\frac{n-1}{2}\right)^2 \cdot (-1)^{\frac{n-1}{2}} \bmod n$$

F3.4
$a, b, c \in \mathbb{Z}$, $d := (a, b)$. Die Gleichung

$$aX + bY = c \tag{3.1}$$

ist genau dann lösbar über $\mathbb{Z}$, wenn $d|c$. Sei $d \neq 0$. Ist (x_0, y_0) eine Lösung von (3.1), so gehört zu jeder Lösung (x, y) von (3.1) genau ein $t \in \mathbb{Z}$ mit

$$x = x_0 + t\frac{b}{d} \qquad y = y_0 - t\frac{a}{d}, \tag{3.2}$$

und jedes (x, y) wie in (3.2) ist eine Lösung von (3.1).

F3.5
Die Kongruenz

$$aX \equiv c \bmod m \tag{3.3}$$

ist genau dann lösbar über $\mathbb{Z}$, wenn

$$(a, m)|c. \tag{3.4}$$

Sei $d := (a, m) \neq 0$, und es gelte (3.4). Die Lösungsmenge von (3.3) ist dann eine Restklasse modulo $\frac{m}{d}$. Die Kongruenz (3.3) besitzt genau $d = (a, m)$ viele Lösungen modulo m. Insbesondere gilt: Ist $(a, m) = 1$, so ist (3.3) für jedes c lösbar und die Lösungen sind modulo m eindeutig.

Definition 3.2 (Restklassen allgemein)
Sei R ein kommutativer Ring, $m \in R$. Die **Restklasse** modulo m, in der $a \in R$ liegt, hat die Gestalt

$$\{x \in R : x \equiv a \bmod m\} = a + mR = \{a + ym : y \in R\}.$$

Die Menge aller Restklassen modulo m bezeichnen wir mit R/mR, aber auch R/m. Der für uns wichtigste Fall ist $R = \mathbb{Z}$ und $m \in \mathbb{N}$.

Beispiel
Sei $m \in \mathbb{N}$. Betrachte

$$R = \mathbb{Z}_{(m)} := \left\{\frac{b}{a} : a, b \in \mathbb{Z}, (a, m) = 1\right\} \subseteq \mathbb{Q}$$

Die Inklusionsabbildung $\mathbb{Z} \to \mathbb{Z}_{(m)}$ vermittelt einen Ringisomorphismus

$$\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}_{(m)}/m\mathbb{Z}_{(m)}$$

Bemerkung
Sei $(a, m) = 1$. Wohlverstanden darf man also sagen:
Die Kongruenz $aX \equiv c \bmod m$ besitzt die Lösung $\frac{c}{a} \bmod m$. Es gibt ein $x \in \mathbb{Z}$ mit $x \equiv \frac{c}{a} \bmod m$, und für dieses ist $ax \equiv c \bmod m$.

Beispiel
Die Kongruenz $7X \equiv 1 \bmod 123$ ist "eindeutig" lösbar:

$$7x \equiv 1 \bmod 123 \quad \Rightarrow \quad x \equiv \frac{1}{7} = \frac{4}{28} \equiv \frac{-119}{28} = \frac{-17}{4} \equiv \frac{-140}{4} \equiv -35 \bmod 123$$

Das funktioniert nicht immer so gut, aber allgemein kann man folgendes sagen:

Bemerkung
Zur Lösung der Kongruenz

$$aX \equiv 1 \bmod m \quad \text{mit } (a,m) = 1 \text{ und } a \in \mathbb{N} \tag{3.5}$$

Betrachte $\alpha = \frac{m}{a} \in \mathbb{Q}$ und führe die Kettenbruchentwicklung durch. Diese endet mit $\frac{m}{a} = \frac{c_n}{d_n}$. Dann gilt (vgl. Beispiel nach Satz 2.2):

$$(-1)^n c_{n-1} a - (-1)^n d_{n-1} m = 1 \quad \Rightarrow \quad a(-1)^n c_{n-1} \equiv 1 \bmod m$$

Somit ist

$$x = (-1)^n c_{n-1}$$

eine Lösung von (3.5).

F3.6
14.11. [10]
Sei $m \in \mathbb{N}$.

(i) $\mathbb{Z}/m\mathbb{Z}$ ist auf natürliche Weise ein kommutativer Ring mit Eins ($\neq 0$, falls $m > 1$). Die Restklassenprojektion

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ a &\longmapsto \overline{a} = a + m\mathbb{Z} =: a \mod m \end{aligned}$$

ist ein Ringhomomorphismus. Für $m > 1$ ist $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}_{(m)}/m\mathbb{Z}_{(m)}$ ein Ringisomorphismus, sodass man $\mathbb{Z}_{(m)}/m\mathbb{Z}_{(m)}$ mit $\mathbb{Z}/m\mathbb{Z}$ identifizieren kann.

(ii) $\mathbb{Z}/m\mathbb{Z}$ hat genau m Elemente.

(iii) Für beliebige $c \in \mathbb{Z}$ ist $c, c+1, \ldots, c+(m-1)$ ein **Vertretersystem** modulo m.
$S \subseteq \mathbb{Z}$ heißt ein Vertretersystem modulo m bzw. von $\mathbb{Z}/m\mathbb{Z}$, wenn gilt: Zu jedem $x \in \mathbb{Z}$ existiert genau ein $a \in S$ mit $x \equiv a \bmod m$. Anders ausgedrückt: Die Einschränkung der Restklassenabbildung $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ auf S ist eine Bijektion. Äquivalent dazu ist, dass die Einschränkung injektiv oder surjektiv ist und $|S| = m$.

(iv) $\mathbb{Z}/m\mathbb{Z}$ Integritätsring $\Leftrightarrow$ $\mathbb{Z}/m\mathbb{Z}$ Körper $\Leftrightarrow$ m Primzahl.
Für eine Primzahl p heißt $\mathbb{Z}/p\mathbb{Z}$ der **Restklassenkörper** modulo p.

(v) $(a,m) = d, x \equiv a \bmod m \quad \Rightarrow \quad (x,m) = d$

(vi) $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times \quad \Leftrightarrow \quad (a,m) = 1$.
Die Elemente $\overline{a}$ von $(\mathbb{Z}/m\mathbb{Z})^\times$ heißen prime Restklassen modulo m.

Lemma 3.1
Sei R ein endlicher kommutativer Ring mit Eins. Dann ist

$$R^\times = \{a \in R : a \text{ ist kein Nullteiler von } R\}$$

F3.7 (Satz von Wilson)
Für $n \in \mathbb{N}$ gilt:

$$n \text{ Primzahl} \quad \Leftrightarrow \quad (n-1)! \equiv -1 \bmod n$$

F3.8
Sei $p \neq 2$ Primzahl. Dann ist die Kongruenz

$$X^2 \equiv -1 \bmod p$$

genau dann lösbar in $\mathbb{Z}$, wenn $p \equiv 1 \bmod 4$, d.h. $p = 1 + 4k$ für ein $k \in \mathbb{N}$.

Bemerkungen

1) 3.8 anders formuliert. Setze $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ Körper.

$$\sqrt{-1} \in \mathbb{F}_p \quad \Leftrightarrow \quad p \equiv 1 \bmod 4 \text{ oder } p = 2$$

2) Sei $p \neq 2$ Primzahl. Dann:

$$\left(\frac{p-1}{2}\right)!^2 \equiv \begin{cases} -1 \bmod p & \text{für } p \equiv 1 \bmod 4 \\ 1 \bmod p & \text{für } p \equiv 3 \bmod 4 \end{cases}$$

Für $p \equiv 3 \bmod 4$ gilt also $\left(\frac{p-1}{2}\right)!^2 \equiv \pm 1 \bmod p$. Mehr dazu in Abschnitt 6.

Definition 3.3 (Eulersche φ-Funktion)
Für jede natürliche Zahl m definiere

$$\varphi(m) := \#(\mathbb{Z}/m\mathbb{Z})^\times \qquad \varphi(1) = 1$$

Nach F3.6 gilt $\varphi(m) = \#\{a \in \{0, 1, 2, \ldots, m-1\} : a \text{ teilerfremd zu } m\}$. Für eine Primzahl p ist daher $\varphi(p) = p-1$. φ heißt **Eulersche φ-Funktion**.

Satz 3.1 (Satz von Euler-Fermat)
Aus $(a, m) = 1$ folgt $a^{\varphi(m)} \equiv 1 \bmod m$.

Lemma 3.2
Sei G eine abelsche Gruppe der Ordnung n. Dann gilt $x^n = 1$ für alle $x \in G$.

3.1 Simultane Kongruenzen

Satz 3.2 (Chinesischer Restsatz)
Ist $m = m_1 m_2 \cdot m_r$ mit paarweise teilerfremden natürlichen Zahlen $m_1, \ldots, m_r > 1$, so ist die Abbildung

$$\begin{aligned} \mathbb{Z}/m &\longrightarrow \mathbb{Z}/m_1 \times \mathbb{Z}/m_2 \times \cdots \times \mathbb{Z}/m_r \\ a \bmod m &\longmapsto (a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_r) \end{aligned} \tag{3.6}$$

ein Isomorphismus von Ringen. Ist insbesondere $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ die Primfaktorzerlegung einer natürlichen Zahl $m > 1$, so gilt

$$\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_r^{e_r}$$

mit kanonischer Isomorphie. Der Isomorphismus (3.6) vermittelt einen Isomorphismus

$$(\mathbb{Z}/m)^\times \simeq (\mathbb{Z}/m_1)^\times \times \ldots \times (\mathbb{Z}/m_r)^\times$$

der primen Restklassengruppen; insbesondere gilt

$$\varphi(m) = \varphi(m_1) \cdot \varphi(m_2) \cdots \varphi(m_r)$$

Satz 3.2 (Chinesischer Restsatz für simultane Kongruenzen)
Sei $m = m_1 m_2 \cdots m_r$ mit paarweise teilerfremden natürlichen Zahlen $m_1, \ldots, m_r > 1$. Sind dann $a_1, \ldots, a_r$ beliebige ganze Zahlen, so gibt es eine ganze Zahl x mit

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_r \bmod m_r \end{aligned} \tag{3.7}$$

Durch (3.7) ist x modulo m eindeutig bestimmt, ferner gilt:

$$x \text{ prim zu } m \quad \Leftrightarrow \quad a_i \text{ prim zu } m_i \text{ für alle } i$$

Bemerkung
Es genügt, sich x_i zu verschaffen mit

$q_i = \frac{m}{m_i}$

$$x_1 q_1 + x_2 q_2 + \ldots + x_r q_r \equiv 1 \mod m \tag{3.8}$$

Dann wird (3.7) erfüllt von

$$x = a_1(x_1 q_1) + \ldots + a_r(x_r q_r)$$

Für jedes $1 \leq i \leq r$ bestimme (notfalls mit Kettenbruchentwicklung) ein $x_i \in \mathbb{Z}$ mit

$(q_i, m_i) = 1$

$$q_i x_i \equiv 1 \bmod m_i$$

Dann ist

$$x_1 q_1 + \ldots + x_r q_r \equiv 1 \bmod m_i$$

für alle $1 \leq i \leq r$, und es folgt (3.8).

Korollar
18.11. [11] Sei $f \in \mathbb{Z}[X]$, $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$ mit paarweise teilerfremden $m_i > 1$. Dann:

$$f(X) \equiv 0 \bmod m \text{ lösbar in } \mathbb{Z} \quad \Leftrightarrow \quad f(X) \equiv 0 \bmod m_i \text{ lösbar in } \mathbb{Z} \text{ für jedes } 1 \leq i \leq r$$

Die natürliche Abbildung $\mathbb{Z}/m \to \prod_{i=1}^{r} \mathbb{Z}/m_i$ vermittelt eine Bijektion

$$\{\alpha \in \mathbb{Z}/m : f(\alpha) = 0\} \to \prod_{i=1}^{r} \{\alpha_i \in \mathbb{Z}/m_i : f(\alpha_i) = 0\}$$

Für die Lösungsanzahlen $N_f(n) := \#\{\alpha \in \mathbb{Z}/n : f(\alpha) = 0\}$ gilt also:

$$N_f(m_1 m_2 \ldots m_r) = N_f(m_1) N_f(m_2) \cdots N_f(m_r)$$

4 Die prime Restklassengruppe $\mathrm{mod}\, m$

Definition 4.1 (prime Restklassengruppe)
Sei $m \in \mathbb{N}$, $m > 1$. Dann heißt $(\mathbb{Z}/m\mathbb{Z})^\times$ die **prime Restklassengruppe** $\mathrm{mod}\, m$. Wir wissen:

(1) $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times \Leftrightarrow (a, m) = 1$

(2) $M := \{k \in \mathbb{Z} : 0 \leq k < m, (k, m) = 1\}$ ist ein Vertretersystem von $(\mathbb{Z}/m\mathbb{Z})^\times$.
$(\mathbb{Z}/m\mathbb{Z})^\times$ hat $\varphi(m) = \#M$ Elemente und ist eine abelsche Gruppe der Ordnung $\varphi(m)$.

(3) $\overline{a} = \alpha \in (\mathbb{Z}/m\mathbb{Z})^\times \Rightarrow \alpha^{\varphi(m)} = 1 \Leftrightarrow a^{\varphi(m)} \equiv 1 \,\mathrm{mod}\, m$ (Satz von Euler-Fermat)

Definition 4.2 (Primitivwurzel)
Ein $\omega \in (\mathbb{Z}/m\mathbb{Z})^\times$ heißt eine **Primitivwurzel** von $(\mathbb{Z}/m\mathbb{Z})^\times$, wenn sich jedes Element $\alpha \in (\mathbb{Z}/m\mathbb{Z})^\times$ in der Form

$$\alpha = \omega^i \text{ für ein } i \in \mathbb{N}_0$$

schreiben lässt; jedes $g \in \mathbb{Z}$ mit $\omega = \overline{g} = g \,\mathrm{mod}\, m$ heißt dann eine Primitivwurzel $\mathrm{mod}\, m$.

Satz 4.1 (Satz von Gauß)
Ist p eine Primzahl, so besitzt $(\mathbb{Z}/p\mathbb{Z})^\times$ eine Primitivwurzel. Es gibt also ein $\omega \in (\mathbb{Z}/p\mathbb{Z})^\times$, sodass sich jedes $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$ darstellen lässt in der Form

$$\alpha = \omega^i \text{ mit } 0 \leq i < p - 1 \tag{4.1}$$

Die Darstellung (4.1) ist unter der Bedingung $0 \leq i < p - 1$ eindeutig; $i = i(\alpha) = i_\omega(\alpha)$ heißt der **Index** von α bezüglich ω.

Wählt man ein $g \in \mathbb{Z}$ mit $\omega = g \,\mathrm{mod}\, m$, so gilt also: Zu jedem $a \in \mathbb{Z}$ mit $p \not| a$ gibt es genau ein $i \in \mathbb{Z}$ mit

$$a \equiv g \,\mathrm{mod}\, p, 0 \leq i < p - 1$$

$i = i(a) = i_g(a)$ heißt der Index von a bzgl. g.

Zusatz
Es gibt genau $\varphi(p - 1)$ verschiedene Primitivwurzeln von $(\mathbb{Z}/p\mathbb{Z})^\times$.

4.1 Gruppentheoretische Vorbereitungen

Definition 4.3 (Ordnung eines Gruppenelements)
Sei G eine (abelsche) Gruppe der Ordnung n, d.h. $\#G = n$. Sei $\alpha \in G$. Wir wissen: $\alpha^n = 1$. Unter allen $m \in \mathbb{N}$ mit $\alpha^m = 1$ sei nun k das kleinste. Setze dann

$$\mathrm{ord}(\alpha) := k,$$

die **Ordnung** von α. $\langle\alpha\rangle := \{\alpha^j : j \in \mathbb{Z}\}$ ist offenbar eine Untergruppe von G.

Lemma 4.1
In der Situation von Definition 4.3 gelten:

(1) $\langle\alpha\rangle = \{1, \alpha, \alpha^2, \ldots, \alpha^{k-1}\}$, insbesondere $\mathrm{ord}(\alpha) = \mathrm{ord}(\langle\alpha\rangle)$.

(2) $\alpha^m = 1$ für $m \in \mathbb{Z} \Rightarrow \mathrm{ord}(\alpha) | m$

(3) Sei $\mathrm{ord}(\alpha) = k$ wie oben, dann vermittelt der Gruppenhomomorphismus

$$\mathbb{Z} \longrightarrow \langle\alpha\rangle$$
$$j \longmapsto \alpha^j$$

einen Gruppenisomorphismus $\mathbb{Z}/k\mathbb{Z} \to \langle\alpha\rangle$, also $\langle\alpha\rangle \simeq \mathbb{Z}/k\mathbb{Z}$.

(4) G zyklisch $\Leftrightarrow \exists\alpha \in G$ mit $\mathrm{ord}(\alpha) = \mathrm{ord}(G)$.
Eine Gruppe G heißt **zyklisch**, wenn es ein $\alpha \in G$ gibt mit $G = \langle\alpha\rangle$. α heißt dann ein **Erzeuger** von G.

Bemerkung
Definitionsgemäß gilt:

$$(\mathbb{Z}/m\mathbb{Z})^\times \text{ besitzt Primitivwurzel} \quad \Leftrightarrow \quad (Z/m\mathbb{Z})^\times \text{ ist zyklisch,}$$

und nach dem zuvor Gesagten:

$$\omega \text{ ist Primitivwurzel von } (\mathbb{Z}/m\mathbb{Z})^\times \quad \Leftrightarrow \quad \mathrm{ord}(\omega) = \varphi(m)$$

Definition 4.4 (Gruppenexponent)
Sei G eine endliche Gruppe. Das kgV aller $\mathrm{ord}(\alpha), \alpha \in G$ heißt der **Exponent** $e = e(G)$ der Gruppe G.

Bemerkung
Ist $n = \mathrm{ord}(G), e = e(G)$, so gilt stets $e|n$, denn für jedes $\alpha \in G$ gilt $\alpha^n = 1 \Rightarrow \mathrm{ord}(\alpha)|n \Rightarrow e|n$.

F4.1
Sei G eine endliche abelsche Gruppe und sei e ihr Exponent. Dann gibt es ein Element $\omega \in G$ mit $\mathrm{ord}(\omega) = e$.

Satz 4.1
Sei K ein Körper und G eine endliche Untergruppe von $K^\times$. Dann ist G zyklisch.

4.2 Restklassengruppen

Definition 4.5 (Restklassen, Restklassenabbildung)
21.11. [12] Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Für $x, y \in G$ definiere eine Relation:

$$x \overset{H}{\sim} y :\Leftrightarrow yx^{-1} \in H (\Leftrightarrow y \in Hx),$$

oder für eine abelsche Gruppe mit $+$ statt $\cdot$ als Verknüpfungssymbol:

$$x \overset{H}{\sim} y :\Leftrightarrow y - x \in H (\Leftrightarrow y \in H + x),$$

$\overset{H}{\sim}$ ist eine Äquivalenzrelation. Mit G/H bezeichnen wir die Menge der zugehörigen Äquivalenzklassen (**Restklassen**).
Die Abbildung

$$G \longrightarrow G/H$$
$$x \longmapsto \overline{x} := Hx$$

heißt **Restklassenabbildung**.

Bemerkung
Die Relation $\overset{H}{\sim}$ ist verträglich mit der Multiplikation, falls G abelsch ist. In diesem Fall ist G/H eine Gruppe und die Restklassenabbildung ein Homomorphismus.
Ist G eine beliebige Gruppe, so gilt gleiches für G/H genau dann, wenn für jedes $x \in G$ gilt: $Hx = xH$.

F4.2
Sei G eine abelsche Gruppe der Ordnung n und $n = p_1^{\nu_1} p_2^{\nu_2} \dots p_r^{\nu_r}$ die Primfaktorzerlegung von n. Für $1 \leq i \leq r$ sei

$$G_{p_i} := \{\alpha \in G : \alpha^{p_i^{\nu_i}} = 1\} \leq G$$

Dann ist die Abbildung

$$f\colon \prod_{i=1}^{r} G_{p_i} \longrightarrow G$$
$$(\alpha_1, \dots, \alpha_r) \longmapsto \alpha_1 \alpha_2 \cdots \alpha_r$$

ein Isomorphismus von Gruppen. Ferner gilt $\#G_{p_i} = p_i^{\nu_i}$ für $1 \leq i \leq r$.

Bemerkung 1
G endliche Gruppe, $\alpha \in G$, $j \in \mathbb{Z}$. Dann gilt:

$$\mathrm{ord}(\alpha^j) = \frac{\mathrm{ord}(\alpha)}{(\mathrm{ord}(\alpha), j)}$$

Bemerkung 2
Eine zyklische Gruppe der Ordnung n hat genau $\varphi(n)$ Elemente der Ordnung n, also $\varphi(n)$ Erzeuger.

Wir werden jetzt die Struktur der primen Restklassengruppe modulo p^ν 25.11. [13]

$$G = G_\nu = (\mathbb{Z}/p^\nu\mathbb{Z})^\times, p \text{ Primzahl}, \nu \in \mathbb{N}, \nu > 1$$

untersuchen. Es ist

$$\mathrm{ord}(G) = \varphi(p^\nu) = \#\{0 \leq a < p^\nu : p \not| a\} = p^\nu - \#\{0 \leq a < p^\nu : p|a\} = p^\nu - p^{\nu-1} = (p-1)p^{\nu-1}$$

Damit gilt für jedes $n \in \mathbb{N}$:

$$\varphi(n) = \varphi\left(\prod_{p|n} p^{w_p(n)}\right) = \prod_{p|n} \varphi\left(p^{w_p(n)}\right) = \prod_{p|n}\left(p^{w_p(n)} - p^{w_p(n)-1}\right) = \prod_{p|n} p^{w_p(n)}\left(1 - \frac{1}{p}\right) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$$

F4.3
Für jedes $n \in \mathbb{N}$ gilt:

$$\varphi(n) = \prod_{p|n}\left(p^{w_p(n)} - p^{w_p(n)-1}\right) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$$

Definition 4.6 (1-Einheit und 1-Einheitengruppe)
Sei $G_\nu = (\mathbb{Z}/p^\nu\mathbb{Z})^\times$. Der Kern $G_\nu^{(1)}$ des Homomorphismus

$$(\mathbb{Z}/p^\nu\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$
$$a \bmod p^\nu \longmapsto a \bmod p$$

heißt die **Gruppe der 1-Einheiten** von $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$. Sie besteht aus den Elementen $a \bmod p^\nu$ von $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ mit $a \equiv 1 \bmod p$. Es ist $\mathrm{ord}(G_\nu^{(1)}) = p^{\nu-1}$.

Lemma 4.2
Sei p Primzahl, $j \in \mathbb{N}$, $a \in \mathbb{Z}$. Es gelte

$$a \equiv 1 \bmod p^j, \text{ aber } a \not\equiv 1 \bmod p^{j+1}$$

Dann folgt – außer für $p = 2$ und $j = 1$:

$$a^p \equiv 1 \bmod p^{j+1}, \text{ aber } a^p \not\equiv 1 \bmod p^{j+2}$$

F4.4
Sei $\nu > 1$.

(i) Im Fall $p \neq 2$ ist für jedes a der Gestalt $a = 1 + cp$ mit $p \nmid c$ die Restklasse $a \bmod p^\nu$ ein Element der Ordnung $p^{\nu-1}$ in der 1-Einheitengruppe von $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$. Insbesondere gilt dies für $a = 1 + p$.
Die 1-Einheitengruppe von $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ ist also für $p \neq 2$ zyklisch mit kanonischem Erzeuger $1 + p \bmod p^\nu$.

(ii) Im Falle $p = 2$ gilt: Für $\nu \geq 3$ ist $5 \bmod 2^\nu$ ein Element der Ordnung $2^{\nu-2}$ in $(\mathbb{Z}/2^\nu\mathbb{Z})^\times$.
Für $\nu = 2$: $(\mathbb{Z}/4\mathbb{Z})^\times$ ist zyklisch mit $-1 \bmod 4$ als Erzeuger.

Satz 4.2
Sei $p \neq 2$. Auch für $\nu \geq 2$ ist dann $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ zyklisch. Mit anderen Worten: $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ besitzt eine Primitivwurzel.
Es existiert also ein $g \in \mathbb{Z}$, sodass es zu jedem $a \in \mathbb{Z}$ mit $(a, p) = 1$ genau ein $i \in \mathbb{Z}$ gibt mit

$$a \equiv g^i \bmod p^\nu \quad \text{und} \quad 0 \leq i < \varphi(p^\nu)$$

Es gibt genau $\varphi(\varphi(p^\nu)) = \varphi((p-1)p^{\nu-1}) = \varphi(p-1)\varphi(p^{\nu-1})$ Primitivwurzeln von $(\mathbb{Z}/p^\nu)^\times$.

Zusatz
Ist schon eine Primitivwurzel $g_0 \bmod p$ bekannt, so findet man eine Primitivwurzel $\bmod p^\nu$ wie folgt: Ist $g_0^{p-1} \not\equiv 1 \bmod p^2$, so ist $g = g_0$ eine Primitivwurzel $\bmod p^\nu$. Ist $g_0^{p-1} \equiv 1 \bmod p^2$, so ist $g = g_0 + p$ eine Primitivwurzel $\bmod p^\nu$.

Bemerkung
Folgende Aussagen sind für $p \neq 2$ und $g \in \mathbb{Z}$ äquivalent:

(i) g ist Primitivwurzel $\bmod p$ und $g^{p-1} \not\equiv 1 \bmod p^2$.

(ii) g ist Primitivwurzel $\bmod p^n$ für alle $n \in \mathbb{N}$.

(iii) g ist Primitivwurzel $\bmod p^2$.

Satz 4.3
Sei $\nu \in \mathbb{N}, \nu \geq 3$. Zu jeder ungeraden Zahl $a \in \mathbb{Z}$ gibt es eindeutig bestimmte $k \in \{0, 1\}$ und $j \in \{0, 1, \ldots, 2^{\nu-2} - 1\}$ mit

$$a \equiv (-1)^k 5^j \bmod 2^\nu$$

Mit anderen Worten: Die Abbildung

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\nu-2}\mathbb{Z} \longrightarrow (\mathbb{Z}/2^\nu\mathbb{Z})^\times$$
$$(k \bmod 2, j \bmod 2^{\nu-2}) \longmapsto (-1 \bmod 2^\nu)^k \cdot (5 \bmod 2^\nu)^j$$

ist ein Isomorphismus von Gruppen. Es ist also

$$(\mathbb{Z}/2^\nu\mathbb{Z})^\times = \langle -1 \bmod 2^\nu \rangle \times \langle 5 \bmod 2^\nu \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\nu-2}\mathbb{Z}$$

Insbesondere ist $(\mathbb{Z}/2^\nu\mathbb{Z})^\times$ nicht zyklisch.

Satz 4.3
Sei p Primzahl mit $p \neq 2$, $\nu \in \mathbb{N}$, $\nu \geq 2$. Dann existiert eine Primitivwurzel $g \bmod p$, sodass die Abbildung

$$\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{\nu-1}\mathbb{Z} \longrightarrow (\mathbb{Z}/p^{\nu}\mathbb{Z})^{\times}$$
$$(i \bmod (p-1), j \bmod p^{\nu-1}) \longmapsto g^i(1+p)^j \bmod p^{\nu}$$

wohldefiniert und ein Isomorphismus von Gruppen ist. Insbesondere ist $(\mathbb{Z}/p^{\nu}\mathbb{Z})^{\times}$ zyklisch.

Bemerkung
Das direkte Produkt $G_1 \times G_2 \times \ldots \times G_r$ zyklischer Gruppen G_i mit paarweise teilerfremden Ordnungen m_i ist zyklisch von der Ordnung $m_1 m_2 \cdots m_r$. 28.11. [14]

F4.5
Seien $G_1, G_2, \ldots, G_r$ endliche abelsche Gruppen der Ordnungen $m_1, m_2, \ldots, m_r$. Wenn $G := G_1 \times \ldots \times G_r$ zyklisch ist, so sind die $m_1, \ldots, m_r$ paarweise teilerfremd und die G_i sind zyklisch.

F4.6
Sei G eine zyklische Gruppe der Ordnung n. Dann ist jede Untergruppe H von G zyklisch mit $\mathrm{ord}(H)|n$. Die Abbildung $H \mapsto \mathrm{ord}(H)$ ist eine Bijektion zwischen der Menge aller Untergruppen H von G und der Menge aller natürlichen Teiler d von n, und zwar ist $H_d := \{x \in G : x^d = 1\}$ die Untergruppe der Ordnung d von G. Es ist

$$H_{\frac{n}{d}} = \{x \in G : x^{\frac{n}{d}} = 1\} \stackrel{!}{=} \{y^d; y \in G\}$$

die Untergruppe der d-ten Potenzen in G.

Korollar
Für beliebige $n \in \mathbb{N}$ gilt:

$$\sum_{d|n} \varphi(d) = n$$

Bemerkung
Sei G eine beliebige endliche Gruppe der Ordnung n. Für jedes $d|n, d \in \mathbb{N}$ habe G höchstens d Elemente x mit $x^d = 1$. Dann ist G zyklisch.

Satz 4.4
Sei $m \in \mathbb{N}, m > 1$. Genau dann besitzt $(\mathbb{Z}/m\mathbb{Z})^{\times}$ eine Primitivwurzel, wenn m eine der Zahlen folgender Gestalt ist (mit einer Primzahl $p \neq 2$ und $\nu \geq 1$):

$$2, \qquad 4, \qquad p^{\nu}, \qquad 2p^{\nu}$$

5 Summen von zwei Quadraten in $\mathbb{Z}$ und der Gaußsche Zahlring $\mathbb{Z}[i]$

02.12. [15]

Ausgangspunkt ist F3.8:

$$p \equiv 1 \bmod 4 \quad \Rightarrow \quad \exists c \in \mathbb{Z} \text{ mit } c^2 \equiv -1 \bmod p,$$

d.h. $c^2 + 1 = kp$ mit einem $k \in \mathbb{Z}$.

Satz 5.1 (Fermat, Euler)
Sei p eine Primzahl. Ist $p \equiv 1 \bmod 4$, so gibt es $x, y \in \mathbb{Z}$ mit

$$p = x^2 + y^2 \tag{5.1}$$

Ist umgekehrt p in der Gestalt (5.1) darstellbar, so ist $p \equiv 1 \bmod 4$ oder $p = 2$.

Definition 5.1 (Gaußscher Zahlring)

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$$

heißt **Gaußscher Zahlring**. Es ist $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$ und $(a + bi)(a - bi) = a^2 + b^2$.

Satz 5.2 (Gaußscher Zahlring ist euklidisch)
$\mathbb{Z}[i]$ ist ein euklidischer Ring mit euklidischer Normfunktion ν definiert durch

$$\nu(z) = z \cdot \overline{z} =: N(z), z \in \mathbb{Z}[i]$$

F5.1
Sei π ein Primelement $\neq 0$ von $\mathbb{Z}[i]$. Dann gibt es genau eine Primzahl p mit $\pi | p$ in $\mathbb{Z}[i]$. Es gilt entweder $N(\pi) = p$ oder $N(\pi) = p^2$. Im ersten Fall nennen wir π vom Grad 1, im zweiten Fall vom Grad 2.

Um alle Primelemente π von $\mathbb{Z}[i]$ zu finden, haben wir also die Primfaktorzerlegung aller $p \in \mathbb{Z}[i]$ zu untersuchen. Die p heißen **rationale Primzahlen**, die π **Gaußsche Primzahlen**.

Satz 5.3
Sei p Primzahl sowie π ein Primfaktor von p in $\mathbb{Z}[i]$. Dann gibt es drei Fälle:

(i) $p \mathrel{\hat{=}} \pi^2$ (p ist **verzweigt** in $\mathbb{Z}[i]$)

(ii) $p \mathrel{\hat{=}} \pi$ (p ist **träge** in $\mathbb{Z}[i]$, d.h. p bleibt Primelement in $\mathbb{Z}[i]$)

(iii) $p = \pi\overline{\pi}$ mit $pi \neq \overline{\pi}$ (p **zerfällt** in $\mathbb{Z}[i]$)

Und zwar gilt:

$$\begin{array}{lcll} \text{(i)} & \Leftrightarrow & p = 2 & \\ \text{(ii)} & \Leftrightarrow & N(\pi) = p^2 & \Leftrightarrow \quad p \equiv 3 \bmod 4 \\ \text{(iii)} & \Leftrightarrow & N(\pi) = p & \Leftrightarrow \quad p \equiv 1 \bmod 4 \end{array}$$

Also ist z.B. 7 auch in $\mathbb{Z}[i]$ ein Primelement, aber $5 = (2 + i)(2 - i)$ nicht.

Korollar
Ist p eine Primzahl mit $p \equiv 1 \bmod 4$, so ist p in der Gestalt $p = a^2 + b^2$ mit $a, b \in \mathbb{N}$ darstellbar. Bis auf Vertauschung von a und b ist diese Darstellung eindeutig. Ferner ist notwendigerweise $(a, b) = 1$.

Satz 5.4
Sei $n \in \mathbb{N}$.

(i) Genau dann ist n eine Summe von zwei Quadraten in $\mathbb{Z}$, wenn für jede Primzahl $p \equiv 3 \bmod 4$ der Exponent $w_p(n)$ gerade ist.

(ii) Besitzt n eine primitive Darstellung als Summe von zwei Quadraten, d.h.

$$n = a^2 + b^2 \text{ mit teilerfremden } a, b \in \mathbb{Z},$$

so folgt:

$$n \text{ hat keine Primteiler } p \equiv 3 \bmod 4, \text{ und es ist } 4 \nmid n. \tag{5.2}$$

(iii) Umgekehrt: Gelte (5.2), und bezeichne s die Anzahl der ungeraden Primteiler von n. Für $n > 2$ hat dann n genau 2^{s-1} primitive Darstellungen als Summe von zwei Quadraten, wenn nur wesentlich verschiedene Darstellungen gezählt werden.
(Beachte: n kann außerdem noch nicht-primitive Darstellungen haben, z.B. $50 = 7^2 + 1^2 = 5^2 + 5^2$.)

Korollar
Es sei n eine ungerade natürliche Zahl, $n > 1$. Besitzt n im Wesentlichen nur eine einzige Darstellung als Summe von zwei Quadraten und ist diese Darstellung primitiv, so ist n eine Primzahl (Umkehrung des Korollars von Satz 5.3).

05.12.
[16]

Bemerkung
$45 = 6^2 + 3^2$ ist die einzige Darstellung von 45 als Summe von zwei Quadraten, doch diese ist nicht primitiv.
Im Übrigen ist die Voraussetzung, dass n ungerade ist, wesentlich: Für $n = 10$ ist $10 = 3^2 + 1^2$ die im Wesentlichen einzige Darstellung von 10 als Summe von zwei Quadraten und diese ist auch primitiv.

6 Quadratische Reste

Vorbemerkungen

Sei $m \in \mathbb{N}$, $m > 1$. Wir untersuchen Kongruenzen über $\mathbb{Z}$ der Gestalt

$$\begin{aligned} & aX^2 + bX + c \equiv 0 \bmod m, \quad a \neq 0 \\ \Leftrightarrow \quad & 4a^2X^2 + 4abX + 4ac \equiv 0 \bmod 4am \\ \Leftrightarrow \quad & (2aX + b)^2 \equiv b^2 - 4ac \bmod 4am \\ \Leftrightarrow \quad & \begin{cases} Y^2 \equiv D := b^2 - 4ac \bmod 4am \\ Y \equiv b \bmod 2a \end{cases} \end{aligned} \tag{6.1}$$

Bemerkung

1) Für $(a, m) = 1$: (6.1) ist äquivalent zu $X^2 + \frac{b}{a}X + \frac{c}{a} \equiv 0 \bmod m$.

2) Für m, a ungerade: (6.1) ist äquivalent zu $(aX + \frac{b}{2})^2 - \left(\left(\frac{b}{2}\right)^2 - ac\right) \equiv 0 \bmod am$.

F6.1

Die Kongruenz

$$X^2 \equiv D \bmod m \text{ mit } (D, m) = d = d_1^2 d_0 \text{ und } d_0 \text{ quadratfrei}$$

ist genau dann lösbar, wenn $\left(\frac{m}{d}, d_0\right) = 1$ und

$$X^2 \equiv d_0 \frac{D}{d} \bmod \frac{m}{d}$$

lösbar ist. Hier sind $d_0 \frac{D}{d}$ und $\frac{m}{d}$ teilerfremd! (Denn $\frac{m}{d}$ prim zu $\frac{D}{d}$ und wegen $\left(\frac{m}{d}, d_0\right) = 1$ auch zu d_0.)

Damit ist alles reduziert auf eine Kongruenz der Gestalt

$$X^2 \equiv a \bmod m \text{ mit } (a, m) = 1 \tag{6.2}$$

Definition 6.1 (Quadratischer Rest)

Ist (6.2) lösbar, d.h. existiert ein $b \in \mathbb{Z}$ mit $b^2 \equiv a \bmod m$, so heißt a ein **Quadratischer Rest** (QR) modulo m, andernfalls heißt a ein **quadratischer Nichtrest** modulo m.

Probleme

1) Sei m gegeben. Man verschaffe sich eine Übersicht über die sämtlichen quadratischen Reste modulo m.

2) Sei a gegeben. Für welche (zu a teilerfremden) natürlichen Zahlen $m > 1$ ist a quadratischer Rest modulo m?

Problem 2) ist schwieriger und tiefer. Eine Antwort liefert das **quadratische Reziprozitätsgesetz**.
Zuerst Problem 1):

F6.2

a ist quadratischer Rest modulo m genau dann, wenn gilt:

1) a ist quadratischer Rest modulo p für jeden ungeraden Primteiler p von m.

2) $\begin{cases} a \equiv 1 \bmod 4, & \text{falls } 4 \mid m, 8 \nmid m \\ a \equiv 1 \bmod 8, & \text{falls } 8 \mid m \end{cases}$

Ist a quadratischer Rest modulo m, so hat (6.2) genau 2^{s+t} Lösungen modulo m; dabei ist s die Anzahl der ungeraden Primteiler von m und

$$t = 2 \text{ für } w_2(m) \geq 3$$
$$t = 1 \text{ für } w_2(m) = 2$$
$$t = 0 \text{ für } w_2(m) \leq 1.$$

Damit ist alles reduziert auf den Fall $m = p$ mit $p \neq 2$ Primzahl. 09.12. [17]

$$X^2 \equiv a \bmod p, \quad (a, p) = 1 \tag{6.3}$$

Definition 6.2 (Legendresymbol)
Sei $p \neq 2$ eine Primzahl. Der Ausdruck

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{falls (6.3) lösbar} \\ -1, & \text{falls (6.3) nicht lösbar} \end{cases}$$

ist definiert für jedes $a \in \mathbb{Z}$ mit $(a, p) = 1$.

$S = \{1, 2, \ldots, p-1\}$ ist ein primes Restsystem modulo p (Vertretersystem von $(\mathbb{Z}/p)^\times$). $H := \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ heißt ein **unteres Halbsystem** und $H' := \left\{\frac{p+1}{2}, \ldots, p-2, p-1\right\}$ ein **oberes Halbsystem**. Ist a quadratischer Rest modulo p, so gibt es genau ein $b \in H$ mit $b^2 \equiv a \bmod p$. Also:

F6.3
Es gibt genau $\frac{p-1}{2}$ quadratische Reste modulo p und ebenso viele quadratische Reste modulo p.

F6.4 (Eulersches Kriterium)
Für jedes a teilerfremd zu $p \neq 2$ gilt

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$$

Bemerkung

1) 6.3 und 6.4 folgen auch sofort aus der Existenz einer Primitivwurzel modulo p. ($G = (\mathbb{Z}/p\mathbb{Z})^\times$ ist zyklisch von der Ordnung $p-1$.)
2) Aus $\left(\frac{a}{p}\right) \equiv \varepsilon \bmod p$ mit $\varepsilon \in \{1, -1\}$ folgt $\left(\frac{a}{p}\right) = \varepsilon$. Denn $1 \bmod -1 \bmod p$ ist unmöglich für $p \neq 2$.
3) 6.4 für $a = -1$: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$

$$\overset{2)}{\Rightarrow} \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{für } p \equiv 1 \bmod 4 \\ -1, & \text{für } p \equiv 3 \bmod 4 \end{cases}$$

Also folgt erneut 3.8. (**1. Ergänzungssatz**)

F6.5
(i) Das Legendresymbol $\left(\frac{a}{p}\right)$ hängt von a nur modulo p ab.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ für alle a, b prim zu p.

Bemerkung

1) Das Legendresymbol vermittelt eine Abbildung

$$\chi \colon (\mathbb{Z}/p)^\times \longrightarrow \{1, -1\}$$
$$a \bmod p \longmapsto \left(\frac{a}{p}\right)$$

Diese ist ein Homomorphismus von Gruppen. $\chi(a \bmod p)$ gibt quadratischen Charakter von $a \bmod p$ an. Allgemein: Jeder Homomorphismus einer endlichen abelschen Gruppe G in $\mathbb{C}^\times$ heißt ein **Charakter** von G.

2) $a = \pm q_1 q_2 \dots q_s$ mit $q_i \neq p$ Primzahlen.

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_s}{p}\right)$$

Zur Beantwortung von Problem 2 ist wegen 6.2 nur zu fragen: Für welche Primzahlen $p \neq 2$ ist die gegebene Zahl a quadratischer Rest modulo p? Wegen 6.5 genügt es dann weiter, für a folgende Fälle zu betrachten:

1. $a = -1$. Schon erlegt durch den 1. Ergänzungssatz.
2. $a = 2$. Wird erledigt durch den 2. Ergänzungssatz.
3. a ist eine ungerade Primzahl q. Lösung durch das quadratische Reziprozitätsgesetz.

F6.6 (Gaußsches Lemma)

$$\left(\frac{a}{p}\right) = \prod_{x \in H} \varepsilon(ax)$$

F6.7 (2. Ergänzungssatz)

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{für } p \equiv \pm 1 \bmod 8 \\ -1 & \text{für } p \equiv \pm 5 \bmod 8 \end{cases}$$

Satz 6.1 (Quadratisches Reziprozitätsgesetz)
Für ungerade Primzahlen $p \neq q$ gilt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Das bedeutet:

1) Ist eine der beiden Primzahlen p, q kongruent zu $1 \bmod 4$, so gilt

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right),$$

d.h. q ist quadratischer Rest modulo p genau dann, wenn p quadratischer Rest modulo q ist.

2) Sind beide Primzhlen p und q kongruent zu $3 \bmod 4$, so gilt

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right),$$

d.h. q ist quadratischer Rest modulo p genau dann, wenn p quadratischer Nichtrest modulo q ist.

Zusatz für $p \neq 2$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \text{ nach 1. Ergänzungssatz}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \text{ nach 2. Ergänzungssatz}$$

Das bedeutet:

$$-1 \text{ quadratischer Rest modulo } p \Leftrightarrow p \equiv 1 \bmod 4$$

$$2 \text{ quadratischer Rest modulo } p \Leftrightarrow p \equiv \pm 1 \bmod 8$$

Definition 6.3 (Jacobi-Symbol)

Seien $a, b \in \mathbb{Z} \setminus \{0\}$, b ungerade, $(a, b) = 1$. Definiere das **Jacobi-Symbol** durch

12.12.
[18]

$$\left(\frac{a}{b}\right)_J = \prod \left(\frac{a}{p}\right)^{w_p(b)}$$

Für $b = p$ prim ist also $\left(\frac{a}{p}\right)_J = \left(\frac{a}{p}\right)$. Daher verzichten wir auf das J im Index.

Eigenschaften

(1) $a \equiv a' \bmod b \Rightarrow \left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$

(2) $\left(\frac{a}{b}\right)\left(\frac{a'}{b}\right) = \left(\frac{aa'}{b}\right)$ und $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$

(3) $\left(\frac{x^2}{b}\right) = 1 = \left(\frac{a}{y^2}\right), \left(\frac{ax^2}{b}\right) = \left(\frac{a}{b}\right) = \left(\frac{a}{by^2}\right)$ für $(x, b) = (y, a) = 1$ und y ungerade

(4) a quadratischer Rest $\bmod b \Rightarrow \left(\frac{a}{b}\right) = 1$

Satz 6.1 (Reziprozitätsgesetz für das Jacobi-Symbol)

Sei $b \in \mathbb{Z}$ ungerade.

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2} + \frac{\operatorname{sgn}(b)-1}{2}}$$

$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} = \begin{cases} +1 & \text{für } b \equiv \pm 1 \bmod 8 \\ -1 & \text{für } b \equiv \pm 3 \bmod 8 \end{cases}$$

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2} + \frac{\operatorname{sgn}(a)-1}{2}\frac{\operatorname{sgn}(b)-1}{2}} \text{ für } a \text{ ungerade und } (a, b) = 1$$

Korollar

Sei $a \in \mathbb{N}$ gegeben. Für alle ungeraden $b \in \mathbb{Z}$ prim zu a hängt $\left(\frac{a}{b}\right)$ von b nur modulo $4a$ ab, im Falle $a \equiv 1 \bmod 4$ sogar nur modulo a.

Index

Liste der Sätze und Definitionen