

Elementare Zahlentheorie

Jun.-Prof. Dr. Caroline Lassueur
RPTU Kaiserslautern-Landau

Kurzskript zur Vorlesung, SS 2017 / SS 2019 / SS 2023

Version: 15. Juli 2019 inkl. Updates vom SS 2023

Dieser Text ist ein Kurzsript für die Vorlesung **Elementare Zahlentheorie, Sommersemester 2017 / Sommersemester 2019 / Sommersemester 2023**. Der generelle Schreibstil dieses Skriptes ist bewusst knapp gehalten, da es schon viele Skripte für diese Vorlesung gibt, die zur Verfügung stehen, z.B. durch die Skriptensammlung der Fachschaft Mathematik:

<https://fachschaft.mathematik.uni-kl.de/misc/lecturenotes.php>

Genauer basiert dieses Skript auf früheren Fassungen der Vorlesung von C. Fieker [Fie15], G. Malle [Mal05], und T. Markwig [Mar10].

[Fie15] Claus Fieker, Elementare Zahlentheorie, Vorlesungsskript, SS 2015, TU Kaiserslautern.

[Mal05] Gunter Malle, Elementare Zahlentheorie, Vorlesungsskript, SS 2005, TU Kaiserslautern.

[Mar10] Thomas Markwig, Elementare Zahlentheorie, Vorlesungsskript, WS 2009/10, TU Kaiserslautern.

Ich danke Inga Schwabrow für das Lesen dieser Fassung des Skriptes und ausführliche Korrekturen. Ich danke auch den Studierenden, die verschiedene Arten von Druckfehler gemeldet haben. Weitere Kommentare und Korrekturen sind auch herzlich willkommen!

Generell

\mathbb{C}	Körper der komplexen Zahlen
i	$\sqrt{-1}$ in \mathbb{C} (feste Wahl)
\mathbb{N}	die natürlichen Zahlen ohne 0
\mathbb{N}_0	die natürlichen Zahlen mit 0
\mathbb{P}	Menge der Primzahlen in \mathbb{Z}
\mathbb{Q}	Körper der rationalen Zahlen
\mathbb{R}	Körper der reellen Zahlen
\mathbb{Z}	Ring der ganzen Zahlen
$\mathbb{Z}[i]$	Ring der ganzen Gaußschen Zahlen
$\mathbb{Z}_{\geq a}, \mathbb{Z}_{> a}, \mathbb{Z}_{\leq a}, \mathbb{Z}_{< a}$	$\{m \in \mathbb{Z} \mid m \geq a \text{ (bzw. } m > a, m \geq a, m < a)\}$
$\mathbb{Z}/m\mathbb{Z}$	Ring der ganzen Zahlen modulo m
$ X $	Mächtigkeit der Menge X
$\lfloor x \rfloor$	$\max\{n \in \mathbb{Z} \mid n \leq x\}$, das größte Ganze
\cup	Vereinigung
\bigsqcup	disjunkte Vereinigung
\prod, \times	kartesisches Produkt
\cap	Schnitt
\emptyset	leere Menge
$n!$	n Fakultät
M_n	n -te Mersenne-Zahl

Ringe

ggT	Menge der größten gemeinsamen Teiler
ggT	der größte gemeinsame Teiler
kgV	Menge der kleinsten gemeinsamen Vielfachen
$I \trianglelefteq R$	I ist ein Ideal von R
$R[X]$	Polynomring über R in einer Unbestimmten X
$R[X_1, \dots, X_n]$	Polynomring über R in n Unbestimmten X_1, \dots, X_n
R^\times	Einheitsgruppe des Ringes R
$(a)_R$	Hauptideal erzeugt von $a \in R$
$(a_1, \dots, a_n)_R$	Ideal erzeugt von $a_1, \dots, a_n \in R$
$a \mid b$	a teilt b
$[a], [a]_n, a + n\mathbb{Z}$	Restklasse von a in $\mathbb{Z}/n\mathbb{Z}$.
Φ_p	Reduktion modulo p von Polynomen in $\mathbb{Z}[X]$

Arithmetische Funktionen

*	Faltung
$\mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$	Ring der arithmetischen Funktionen
$\mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C})$	Menge der multiplikativen Funktionen
0	Nullfunktion
e	konstante Funktion
i	identische Abbildung
ε	neutrale Funktion bezüglich der Faltung
φ	eulersche φ -Funktion
μ	Möbius Funktion
σ	Teilersummenfunktion

Quadratische Reste

$\left(\frac{a}{p}\right)$	Legendre-Symbol
$\left(\frac{a}{b}\right)$	Jacobi-Symbol
\mathcal{R}_p	Gruppe der quadratischen Reste modulo p

Griechische Buchstaben

Minuskeln	Majuskeln	Name
α	A	Alpha
β	B	Beta
γ	Γ	Gamma
δ	Δ	Delta
ε, ϵ	E	Epsilon
ζ	Z	Zeta
η	H	Eta
θ	Θ	Theta
ι	I	Iota
κ	K	Kappa
λ	Λ	Lambda
μ	M	Mu
ν	N	Nu
ξ	Ξ	Xi
o	O	Omicron
π, ω	Π	Pi
ρ, ϱ	P	Rho
σ, ς	Σ	Sigma
τ	T	Tau
υ	Υ	Ypsilon
ϕ, φ	Φ	Phi
χ	X	Chi
ψ	Ψ	Psi
ω	Ω	Omega

Vorwort	i
Symbolverzeichnis	ii
Kapitel 0: Begriffe und Ergebnisse aus der AGS	vi
Kapitel 1: Lineare diophantische Gleichungen	6
1 Der größte gemeinsame Teiler	6
2 Lösbarkeit linearer diophantischer Gleichungen	8
Kapitel 2: Multiplikative Funktionen	10
3 Multiplikative Funktionen	10
4 Die Dirichlet-Faltung	12
5 Die Möbiusfunktion	15
6 Die eulersche φ -Funktion	17
7 Die Teilersummenfunktion und vollkommene Zahlen	19
Kapitel 3: Die Sätze von Euler, Fermat und Wilson	22
8 Der Satz von Euler	22
9 Der kleine Satz von Fermat	23
10 Der Satz von Wilson	24
11 Die diophantische Gleichung $X^2 + Y^2 = p$	25
12 Die diophantische Gleichung $X^2 + Y^2 = n$	27
13 Existenz unendlich vieler Primzahlen p mit $p \equiv \pm 1 \pmod{4}$	29
Kapitel 4: Das RSA-Verfahren	31
14 Das Prinzip	31
15 Das RSA-Verfahren	31
16 Das RSA-Verfahren in der Praxis	32
17 Das RSA-Verfahren: Sicherheit und Sicherheitslücken	34
18 Das Rabin-Verfahren*	35

Kapitel 5: Die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ und Primitivwurzeln modulo n	39
16 Die Einheitengruppe $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$	40
17 Die Einheitengruppe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ für p ungerade	41
18 Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$	44
Kapitel 6: Das quadratische Reziprozitätsgesetz	45
20 Quadratische Reste	45
21 Eine Methode von Gauß	48
22 Das quadratische Reziprozitätsgesetz	50
23 Die diophantische Gleichung $X^2 - mY^2 = \pm p$	53
24 Das Jacobi-Symbol*	55

Kapitel 0: Begriffe und Ergebnisse aus den *ALGEBRAISCHEN STRUKTUREN*

Integritätsbereiche

- Ein kommutativer Ring R heißt **Integritätsbereich**, falls R nullteilerfrei ist (d.h. es gibt keine Nullteiler in R außer 0.)
- Sei R ein Integritätsbereich und seien $a, b \in R$.
 - (a) $g \in R$ heißt **größter gemeinsamer Teiler** von a und b , wenn gilt:
 - (i) $g \mid a$ und $g \mid b$; und
 - (ii) ist $c \in R$ mit $c \mid a$ und $c \mid b$, so gilt $c \mid g$.Wir bezeichnen mit $\text{ggT}(a, b)$ die Menge aller größten gemeinsamen Teiler von a und b .
 - (b) $k \in R$ heißt **kleinstes gemeinsames Vielfaches** von a und b , wenn gilt:
 - (i) $a \mid k$ und $b \mid k$; und
 - (ii) ist $h \in R$ mit $a \mid h$ und $b \mid h$, so gilt $k \mid h$.Wir bezeichnen mit $\text{kgV}(a, b)$ die Menge aller kleinsten gemeinsamen Vielfachen von a und b .
- **Satz:** Ist $g \in \text{ggT}(a, b)$, so ist $\text{ggT}(a, b) = R^\times g$.
- Sei R ein Integritätsbereich und sei $0 \neq p \in R \setminus R^\times$.
 - (a) p heißt **irreduzibel**, wenn $\forall a, b \in R$ mit $p = ab$ gilt, dass $a \in R^\times$ oder $b \in R^\times$ ist.
 - (b) p heißt **prim** (oder **Primelement**), wenn $\forall a, b \in R$ mit $p \mid ab$ gilt, dass $p \mid a$ oder $p \mid b$ ist.
- **Lemma:** In einem Integritätsbereich ist jedes Primelement irreduzibel.

ZPE-Ringe:

- Sei R ein Integritätsbereich und sei $a \in R \setminus \{0\}$. Eine Darstellung

$$a = e \cdot \prod_{i=1}^r p_i^{n_i}$$

mit $e \in R^\times$ und Primelementen p_1, \dots, p_r ($r \in \mathbb{N}$) heißt **Primzerlegung** von a .

- Ein Integritätsbereich R heißt **ZPE-Ring**, wenn jedes $a \in R \setminus \{0\}$ eine Primzerlegung besitzt.

Hauptidealringe:

- Sei R ein kommutativer Ring. Das Erzeugnis von $a_1, \dots, a_n \in R$ ($n \geq 1$) ist

$$a_1R + \dots + a_nR = \{a_1r_1 + \dots + a_nr_n \mid r_1, \dots, r_n \in R\} =: (a_1, \dots, a_n)_R$$

Dies ist ein Ideal von R . Wenn $n = 1$ ist, heißt $aR = \{ar \mid r \in R\} =: (a)_R$ ein **Hauptideal** (erzeugt von a).

- Ein Integritätsbereich R heißt **Hauptidealring** (HIR), wenn jedes Ideal von R ein Hauptideal ist.
- **Satz:** In einem Hauptidealring ist ein Element genau dann irreduzible, wenn es prim ist.
- **Satz:** Jeder Hauptidealring ist ein ZPE-Ring.

Euklidische Ringe:

- Ein Integritätsbereich R heißt ein **euklidischer Ring**, wenn es eine **euklidische Funktion** $v : R \setminus \{0\} \rightarrow \mathbb{N}_0$ mit folgender Eigenschaft gibt: Zu $a, b \in R$ mit $b \neq 0$ gibt es $q, r \in R$ mit $a = bq + r$, wobei entweder $r = 0$ oder $r \neq 0$ und $v(r) < v(b)$.

Diese Darstellung nennt man die **Division mit Rest** von a durch b .

- Wichtige Beispiele: \mathbb{Z} (siehe unten), Körper, $\mathbb{Z}[i]$, $K[X]$ (mit K ein Körper) sind euklidische Ringe.
- **Satz [Euklidischer Algorithmus]:**
Seien R ein euklidischer Ring und $a_0, a_1 \in R$. Man konstruiert rekursiv eine Folge $a_0, a_1, a_2, \dots, a_n \in R$ wie folgt: sind $a_0, \dots, a_{n-1} \in R$ für ein $n \geq 2$ bereits bestimmt und ist $a_{n-1} \neq 0$, so teilen wir a_{n-2} mit Rest durch a_{n-1} und erhalten so

$$a_{n-2} = q_n a_{n-1} + r_n$$

für gewisse Elemente $q_n, r_n \in R$. Setze dann $a_n := r_n$. Es gilt:

- (a) Das Verfahren bricht nach endlich vielen Schritten ab: $\exists N \in \mathbb{N}$ mit $a_N = 0$.
- (b) $a_{N-1} \in \text{ggT}(a_0, a_1)$.
- (c) $\forall 0 \leq n \leq N-1$ lässt sich a_{N-1} in der Form $a_{N-1} = d_n a_n + e_n a_{n+1}$ für gewisse $d_n, e_n \in R$ schreiben. Insbesondere ist $a_{N-1} \in \text{ggT}(a_0, a_1)$ eine Linearkombination von a_0 und a_1 .
- **Folgerung:** In einem euklidischen Ring existiert zu je zwei Elementen stets ein größter gemeinsamer Teiler. Dieser ist bis auf Multiplikation mit Einheiten eindeutig bestimmt und kann mit dem euklidischen Algorithmus berechnet werden.
- **Satz:** Jeder euklidische Ring ist ein Hauptidealring.

Zusammenfassend:

euklidischer Ring \implies Hauptidealring \implies ZPE-Ring \implies Integritätsbereich \implies kommutativer Ring
--

Der Ring der ganzen Zahlen:

- Der Ring $(\mathbb{Z}, +, \cdot)$ der ganzen Zahlen ist ein Integritätsbereich mit $\mathbb{Z}^\times = \{\pm 1\}$.
- Der Ring $(\mathbb{Z}, +, \cdot)$ ist ein euklidischer Ring mit dem Betrag $|\cdot| : \mathbb{Z} \rightarrow \mathbb{N}, z \mapsto |z|$ als euklidischer Funktion. Insbesondere gibt es für $a, b \in \mathbb{Z}$ mit $b \neq 0$ eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit

$$a = q \cdot b + r \text{ und } 0 \leq r < |b|.$$

Man nennt diese Darstellung die **Division mit Rest** von a durch b .

- Der Ring $(\mathbb{Z}, +, \cdot)$ ist damit auch ein HIR. Insbesondere sind die Ideale $I \trianglelefteq \mathbb{Z}$ genau die Ideale

$$I = (m)_{\mathbb{Z}} = m\mathbb{Z} = \{m \cdot z \mid z \in \mathbb{Z}\} \text{ mit } m \in \mathbb{Z} \text{ beliebig.}$$

- Sei $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Da \mathbb{Z} ein HIR ist, gilt:

$$p \text{ ist prim} \iff p \text{ ist irreduzibel}$$

- Um Vorzeichen zu vermeiden, ist es oft nötig zwischen *primen Elementen* und *Primzahlen* (im klassischen Sinn) in \mathbb{Z} zu unterscheiden. Deswegen werden wir die folgende Definition einer *Primzahl* nutzen:

Eine ganze Zahl $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ heißt **Primzahl**, falls $p \in \mathbb{Z}_{\geq 0}$ und p prim ist, und wir bezeichnen mit $\mathbb{P} := \{p \in \mathbb{Z} \mid p \text{ Primzahl}\}$ die Menge der Primzahlen.

- Da \mathbb{Z} ein ZPE-Ring ist, besitzt jedes Element $z \in \mathbb{Z}$ eine Primzerlegung. Zusammen mit dem Begriff der Primzahlen erhalten wir:

Fundamentalsatz der Zahlentheorie: Für jedes $z \in \mathbb{Z} \setminus \{0\}$ gibt es eindeutig bestimmte, paarweise verschiedene Primzahlen $p_1, \dots, p_r \in \mathbb{P}$ ($r \in \mathbb{N}_0$) und eindeutig bestimmte positive ganze Zahlen $n_1, \dots, n_r \in \mathbb{N}$, so dass

$$z = \text{sign}(z) \cdot p_1^{n_1} \cdot \dots \cdot p_r^{n_r},$$

wobei $\text{sign}(z) := z/|z| \in \{\pm 1\}$.

Anmerkung: Mit der Notation $n_p(z) := \max\{n \in \mathbb{N}_0 \mid p^n \text{ teilt } z\}$ gilt

$$z = \text{sign}(z) \cdot \prod_{p \in \mathbb{P}} p^{n_p(z)}.$$

Wir nennen diese Darstellung von $z \in \mathbb{Z} \setminus \{0\}$ die **Primfaktorzerlegung** von z .

- **Teilbarkeit und Ideale in \mathbb{Z} .** Seien $a, b \in \mathbb{Z}$. Dann gelten:

$$(a) \ a \mid b \iff (a)_{\mathbb{Z}} \supseteq (b)_{\mathbb{Z}} \iff n_p(a) \leq n_p(b) \ \forall p \in \mathbb{P}.$$

$$(b) \ (a \mid b \text{ und } b \mid a) \iff (a)_{\mathbb{Z}} = (b)_{\mathbb{Z}}.$$

$$(c) \ g \in \text{ggT}(a, b) \iff (a, b)_{\mathbb{Z}} = (g)_{\mathbb{Z}}.$$

$$(d) \ g \in \text{ggT}(a, b) \Rightarrow \text{ggT}(a, b) = \{-g, g\}.$$

(e) Wenn $(a, b) \neq (0, 0)$ ist, so ist

$$\text{ggT}(a, b) := \prod_{p \in \mathbb{P}} p^{\min\{n_p(a), n_p(b)\}} \in \text{ggT}(a, b)$$

der *positive* größte gemeinsame Teiler von a und b , und wir setzen $\text{ggT}(0, 0) : \ddot{a} = 0$.

Wichtige Sätze aus der Gruppentheorie/Ringtheorie:

- **Der Chinesische Restsatz:** Seien $n_1, \dots, n_k \in \mathbb{Z}_{>1}$ ($k \geq 1$) mit $\text{ggT}(n_i, n_j) = 1$ für alle $1 \leq i \neq j \leq k$. Setze $N := \prod_{i=1}^k n_i$. Dann ist

$$\begin{aligned} \Phi: \quad \mathbb{Z}/N\mathbb{Z} &\longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z} \\ a + N\mathbb{Z} &\mapsto (a + n_1\mathbb{Z}, \dots, a + n_k\mathbb{Z}) \end{aligned}$$

ein Ringisomorphismus.

- **Der Satz von Lagrange:** Sei G eine endliche Gruppe mit neutralem Element 1_G und $U \leq G$ eine Untergruppe. Dann gilt $|G| = |G : U| \cdot |U|$. Insbesondere teilt $|U|$ die Ordnung von $|G|$. Daraus folgt, dass für alle $g \in G$

$$|\langle g \rangle| \mid |G|$$

gilt und somit ist

$$g^{|G|} = 1_G.$$

1 Der größte gemeinsame Teiler

Zunächst betrachten wir eine Verallgemeinerung des Begriffs eines *größten gemeinsamen Teilers* von zwei Elementen, der in der Vorlesung *Algebraische Strukturen* untersucht wurde.

Definition 1.1 (*größter gemeinsamer Teiler*)

Seien $z_1, \dots, z_n \in \mathbb{Z}$ mit $n \in \mathbb{Z}_{\geq 2}$. Dann heißt $g \in \mathbb{Z}$ ein **größter gemeinsamer Teiler** (ggT) von z_1, \dots, z_n , falls gelten:

- (i) $g \mid z_i \forall 1 \leq i \leq n$ (d.h. g ist ein gemeinsamer Teiler von z_1, \dots, z_n), und
- (ii) für alle $h \in \mathbb{Z}$ mit $h \mid z_i \forall 1 \leq i \leq n$ gilt $h \mid g$.

Setze $\text{ggT}(z_1, \dots, z_n) := \{g \in \mathbb{Z} \mid g \text{ größter gemeinsamer Teiler von } z_1, \dots, z_n\}$. Die Elemente z_1, \dots, z_n heißen **teilerfremd**, falls $1 \in \text{ggT}(z_1, \dots, z_n)$.

Lemma 1.2

Seien $z_1, \dots, z_n \in \mathbb{Z}$ mit $n \in \mathbb{Z}_{\geq 2}$. Sei $g \in \mathbb{Z}$.

- (a) Ist $n \geq 3$, so ist $\text{ggT}(z_1, \dots, z_n) = \text{ggT}(a, z_n)$ für alle $a \in \text{ggT}(z_1, \dots, z_{n-1})$.
- (b) $g \in \text{ggT}(z_1, \dots, z_n) \iff (g)_{\mathbb{Z}} = (z_1, \dots, z_n)_{\mathbb{Z}}$.
- (c) $g \in \text{ggT}(z_1, \dots, z_n) \implies \text{ggT}(z_1, \dots, z_n) = \{-g, g\}$.
- (d) Sind nicht alle z_i ($1 \leq i \leq n$) gleichzeitig Null, so gilt

$$\begin{aligned} \text{ggt}(z_1, \dots, z_n) &:= \max_{g \in \mathbb{Z}} \{g \text{ teilt } z_i \forall 1 \leq i \leq n\} \\ &= \prod_{p \in \mathbb{P}} p^{\min\{n_p(z_i) \mid 1 \leq i \leq n\}} \in \text{ggT}(z_1, \dots, z_n). \end{aligned}$$

- (e) $\text{ggt}(z_1, \dots, z_n) = \text{ggt}(\text{ggt}(z_1, \dots, z_{n-1}), z_n)$; und z_1, \dots, z_n sind teilerfremd $\iff \text{ggt}(z_1, \dots, z_n) = 1$.

Beweis: Übung. [Aufgabe 1, Blatt 1]



Anmerkung 1.3

- (a) Dank Lemma 1.2(d) ist es jetzt gerechtfertigt, von *dem* größten gemeinsamen Teiler von z_1, \dots, z_n zu sprechen, d.h. $\text{ggT}(z_1, \dots, z_n)$.
- (b) Aus Lemma 1.2(b) folgt, dass es $b_1, \dots, b_n \in \mathbb{Z}$ gibt, so daß

$$\text{ggT}(z_1, \dots, z_n) = b_1 z_1 + \dots + b_n z_n.$$

Die Elemente b_1, \dots, b_n und auch $\text{ggT}(z_1, \dots, z_n)$ können z.B. induktiv mit dem euklidischen Algorithmus bestimmt werden.

Achtung! Diese Darstellung hängt von der Reihenfolge der Operationen ab!

Beispiel 1

- (a) Seien $z_1 = 24$, $z_2 = 18$, $z_3 = 10$. Mit dem euklidischen Algorithmus erhalten wir:

$$\text{ggT}(24, 18) = 6 = 1 \cdot 24 + (-1) \cdot 18, \text{ und } \text{ggT}(6, 10) = 2 = 2 \cdot 6 + (-1) \cdot 10$$

Also ist

$$\begin{aligned} \text{ggT}(24, 18, 10) &= \text{ggT}(\text{ggT}(24, 18), 10) = 2 \\ &= 2 \cdot 6 + (-1) \cdot 10 \\ &= 2 \cdot (1 \cdot 24 + (-1) \cdot 18) + (-1) \cdot 10 \\ &= 2 \cdot 24 + (-2) \cdot 18 + (-1) \cdot 10 \\ &= 2 \cdot z_1 + (-2) \cdot z_2 + (-1) \cdot z_3 \end{aligned}$$

d.h. $b_1 = 2$, $b_2 = -2$ und $b_3 = -1$.

Aber mit einer verschiedenen Ordnung der Operationen erhalten wir:

$$\text{ggT}(18, 10) = 2 = (-1) \cdot 18 + 2 \cdot 10, \text{ und } \text{ggT}(24, 2) = 2 = 0 \cdot 24 + 1 \cdot 2,$$

also ist

$$\begin{aligned} \text{ggT}(24, 18, 10) &= \text{ggT}(24, \text{ggT}(18, 10)) = 2 \\ &= 0 \cdot 24 + 1 \cdot 2 \\ &= 0 \cdot 24 + 1 \cdot ((-1) \cdot 18 + 2 \cdot 10) \\ &= 0 \cdot 24 + (-1) \cdot 18 + 2 \cdot 10 \\ &= 0 \cdot z_1 + (-1) \cdot z_2 + 2 \cdot z_3. \end{aligned}$$

d.h. in diesem Fall: $b_1 = 0$, $b_2 = -1$ und $b_3 = 2$.

- (b) Es kann sein, dass $\text{ggT}(z_1, \dots, z_n) = 1$ ist, aber die Elemente z_1, \dots, z_n nicht paarweise teilerfremd sind! Z.B. $\text{ggT}(10, 15, 21) = 1$ aber $\text{ggT}(10, 15) = 5$ und $\text{ggT}(15, 21) = 3$.

2 Lösbarkeit linearer diophantischer Gleichungen

Definition 1.4 (diophantische Gleichung, lineare diophantische Gleichung)

- (a) Eine **diophantische Gleichung** ist eine Gleichung der Form

$$F(X_1, \dots, X_n) = c,$$

wobei $c \in \mathbb{Z}$, $F \in \mathbb{Z}[X_1, \dots, X_n]$ ($n \in \mathbb{Z}_{\geq 1}$), und bei der nur **ganzzahlige Lösungen** gesucht werden, d.h. n -Tupel $(a_1, \dots, a_n) \in \mathbb{Z}^n$ mit $F(a_1, \dots, a_n) = c$.

- (b) Eine **lineare diophantische Gleichung** ist eine diophantische Gleichung, die in jedem Term nur eine der Variablen in der ersten Potenz enthält, d.h. eine Gleichung der Form

$$c_1 X_1 + \dots + c_n X_n = c,$$

wobei $c_1, \dots, c_n, c \in \mathbb{Z}$ sind, und nur ganzzahlige Lösungen gesucht werden.

Beispiel 2

- (a) $X_1^2 + 10X_2^6 + 6X_3^2 = -5$ ist eine diophantische Gleichung, wobei $F = X_1^2 + 10X_2^6 + 6X_3^2 \in \mathbb{Z}[X_1, X_2, X_3]$. Diese Gleichung hat keine ganzzahlige Lösung, weil $F(a_1, a_2, a_3) \geq 0$ für alle $(a_1, a_2, a_3) \in \mathbb{Z}^3$ gilt.
- (b) $2X_1 + 6X_2 = 8$ ist eine lineare diophantische Gleichung. Z.B. ist $(1, 1) \in \mathbb{Z}^2$ eine ganzzahlige Lösung, aber diese Lösung ist nicht eindeutig, da $(7, -1)$ auch eine Lösung ist.
- (c) $2X = 5$ ist auch eine lineare diophantische Gleichung, aber sie besitzt keine ganzzahlige Lösung, weil $2 \nmid 5$.

Satz 1.5

Seien $c_1, \dots, c_n, c \in \mathbb{Z}$ ($n \in \mathbb{Z}_{\geq 1}$), so daß c_1, \dots, c_n nicht alle gleich Null sind. Genau dann besitzt die lineare diophantische Gleichung

$$c_1 X_1 + \dots + c_n X_n = c$$

eine Lösung $(a_1, \dots, a_n) \in \mathbb{Z}^n$, wenn $\text{ggT}(c_1, \dots, c_n) \mid c$.

Beweis:

' \Rightarrow ' Sei $(a_1, \dots, a_n) \in \mathbb{Z}^n$ eine Lösung. Dann gilt $\sum_{i=1}^n c_i a_i = c$ und damit ist

$$c \in (c_1, \dots, c_n)_{\mathbb{Z}} \stackrel{\text{Lem.1.2(b)}}{=} (\text{ggT}(c_1, \dots, c_n))_{\mathbb{Z}}$$

$\Rightarrow \exists x \in \mathbb{Z}$ mit $c = x \cdot \text{ggT}(c_1, \dots, c_n)$, d.h. $\text{ggT}(c_1, \dots, c_n) \mid c$.

' \Leftarrow ' Umgekehrt, falls $\text{ggT}(c_1, \dots, c_n) \mid c$ gilt, so existiert $x \in \mathbb{Z}$ mit $c = x \cdot \text{ggT}(c_1, \dots, c_n)$. Nach Anmerkung 1.3(b) gibt es Koeffizienten $b_1, \dots, b_n \in \mathbb{Z}$ mit $\text{ggT}(c_1, \dots, c_n) = \sum_{i=1}^n b_i c_i$. Daraus folgt

$$c = x \cdot \text{ggT}(c_1, \dots, c_n) = x \cdot \sum_{i=1}^n b_i c_i = \sum_{i=1}^n c_i (x b_i),$$

und damit ist $(x b_1, \dots, x b_n) \in \mathbb{Z}^n$ eine Lösung.



Beispiel 3

Z.B. besitzt die lineare diophantische Gleichung

$$24X_1 + 18X_2 + 10X_3 = 20$$

eine Lösung $(a_1, a_2, a_3) \in \mathbb{Z}^3$, weil $2 = \text{ggT}(24, 18, 10) \mid 20$ gilt. Außerdem ist $20 = 10 \cdot 2$ und nach Beispiel 1(a) ist $2 = \text{ggT}(24, 18, 10) = 2 \cdot 24 + (-2) \cdot 18 + (-1) \cdot 10$. Damit ist

$$20 = 10 \cdot 2 = 10 \cdot \text{ggT}(24, 18, 10) = 10 \cdot (2 \cdot 24 + (-2) \cdot 18 + (-1) \cdot 10) = 24 \cdot 20 + 18 \cdot (-20) + 10 \cdot (-10)$$

und $(20, -20, -10) \in \mathbb{Z}^3$ löst die Gleichung.

Aber diese Lösung ist nicht eindeutig bestimmt! Und zwar wissen wir aus Beispiel 1(a), dass $\text{ggT}(24, 18, 10) = 0 \cdot 24 + (-1) \cdot 18 + 2 \cdot 10$, und somit ist $(0, -10, 20)$ eine weitere Lösung der Gleichung.

Zusammenfassung:

(a) Wir haben die drei folgenden Fragen beantwortet:

Frage 1. Wie kann man die Lösbarkeit einer linearen diophantischen Gleichung entscheiden?
[Siehe Satz 1.5.]

Frage 2. Falls eine Lösung existiert: Wie kann eine Lösung bestimmt werden?
[Siehe Beweis des Satzes 1.5.]

Frage 3. Falls eine Lösung existiert: Ist diese eindeutig bestimmt?
[Siehe Beispiel 3.]

(b) Weitere Fragen, die man beantworten möchte, sind:

Frage 4. Kann man die Menge aller Lösungen einer gegebenen linearen diophantischen Gleichung parametrisieren?

Frage 5. Kann man eine Lösung $(a_1, \dots, a_n) \in \mathbb{Z}^n$ finden, bei der jeder Betrag $|a_i|$ ($1 \leq i \leq n$) so klein wie möglich ist?

Frage 4. kann mit Hilfe der *linearen Algebra über \mathbb{Z}* (genauer gesagt die *Theorie der \mathbb{Z} -Moduln*) beantwortet werden. Wegen Ostermontag und Maifeiertag haben wir dieses Semester nicht genug Zeit diese Frage zu betrachten. Sie können darüber im Skript von C. Fieker [Fie15] lesen.

Frage 5. ist ein sehr schweres Problem. Es lässt sich formal zeigen, dass dies ein Problem ist, für das es keinen effektiven Algorithmus gibt (das Problem ist *NP-schwer*).

(c) Die hilbertschen Probleme sind eine Liste von 23 Problemen, die von dem deutschen Mathematiker David Hilbert im Jahr 1900 beim Internationalen Mathematiker-Kongress in Paris vorgestellt wurden.

Hilberts zehntes Problem.

Fragestellung: Man gebe ein Verfahren an, das für eine *beliebige* diophantische Gleichung entscheidet, ob sie lösbar ist.

Lösung: Es wurde gezeigt, dass es im Allgemeinen kein solches Verfahren gibt. (~ 1970.)

3 Multiplikative Funktionen

Definition 2.1 (*arithmetische Funktion, (vollständig) multiplikative Funktion*)

(a) Eine Funktion $\alpha : \mathbb{Z}_{>0} \rightarrow \mathbb{C}$ heißt **arithmetisch** (oder **zahlentheoretisch**). Wir bezeichnen mit $\mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$ die Menge aller arithmetischen Funktionen.

(b) Eine arithmetische Funktion $\alpha : \mathbb{Z}_{>0} \rightarrow \mathbb{C}$ heißt **multiplikativ**, wenn für alle $m, n \in \mathbb{Z}_{>0}$ mit $\text{ggT}(m, n) = 1$ gilt:

$$\alpha(m \cdot n) = \alpha(m) \cdot \alpha(n)$$

Wir bezeichnen mit $\mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C})$ die Menge aller multiplikativen arithmetischen Funktionen.

(c) Eine multiplikative Funktion α heißt **vollständig multiplikativ**, wenn $\alpha(m \cdot n) = \alpha(m) \cdot \alpha(n)$ für alle $m, n \in \mathbb{Z}_{>0}$ gilt.

Beispiel 4

(a) Die **Nullfunktion**

$$\begin{array}{lcl} \mathbf{0}: & \mathbb{Z}_{>0} & \longrightarrow \mathbb{C} \\ & z & \longmapsto 0 \end{array}$$

ist eine multiplikative Funktion.

(b) Die Funktion

$$\begin{array}{lcl} \varepsilon: & \mathbb{Z}_{>0} & \longrightarrow \mathbb{C} \\ & z & \longmapsto \begin{cases} 1 & \text{falls } z = 1, \\ 0 & \text{falls } z > 1 \end{cases} \end{array}$$

ist auch multiplikativ.

(c) Ebenso multiplikativ ist die **konstante Funktion**

$$\begin{array}{lcl} \mathbf{e}: & \mathbb{Z}_{>0} & \longrightarrow \mathbb{C} \\ & z & \longmapsto 1. \end{array}$$

(d) Die **identische Abbildung**

$$\begin{aligned} \mathbf{i}: \mathbb{Z}_{>0} &\longrightarrow \mathbb{C} \\ z &\mapsto z \end{aligned}$$

ist ebenso multiplikativ.

(f) Siehe auch §5 (die Möbiusfunktion), §6 (die eulersche φ -Funktion), §7 (die Teilersummenfunktion) und Blatt 2.

Lemma 2.2

Ist $\alpha \in \mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C}) \setminus \{0\}$, so ist $\alpha(1) = 1$.

Beweis: Weil α nicht die Nullfunktion ist, existiert $z_0 \in \mathbb{Z}_{>0}$ mit $\alpha(z_0) \neq 0$. Wegen $\text{ggT}(z_0, 1) = 1$ gilt $\alpha(z_0) = \alpha(z_0 \cdot 1) = \alpha(z_0) \cdot \alpha(1)$. Also können wir $\alpha(z_0)$ kürzen und somit ist $\alpha(1) = 1$. ■

Wir charakterisieren nun multiplikative Funktionen mit Hilfe des Fundamentalsatzes der Zahlentheorie.

Satz 2.3

(a) Sei $\alpha \in \mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$ eine arithmetische Funktion. Dann sind äquivalent:

(i) α ist multiplikativ; und

(ii) ist $z \in \mathbb{Z}_{>0}$ mit Primfaktorzerlegung $z = p_1^{n_1} \cdots p_r^{n_r}$ (d.h. $r \in \mathbb{Z}_{\geq 0}$, $n_1, \dots, n_r \in \mathbb{Z}_{>0}$ und $p_1, \dots, p_r \in \mathbb{P}$ sind paarweise verschieden), so gilt $\alpha(z) = \alpha(p_1^{n_1}) \cdots \alpha(p_r^{n_r})$.

(b) Zwei multiplikative Funktionen $\alpha_1, \alpha_2 \in \mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C})$ sind genau dann gleich, wenn

$$\alpha_1(p^n) = \alpha_2(p^n)$$

für alle $p \in \mathbb{P}$ und für alle $n \in \mathbb{Z}_{\geq 0}$ gilt.

Beweis:

(a) Ist $\alpha = 0$, so ist die Aussage klar. Also nehmen wir an, dass $\alpha \neq 0$ ist.

(i) \Rightarrow (ii): Nun ist $z = 1$, so ist nach Lemma 2.2 die Behauptung trivial. Also nehmen wir an, dass $z \geq 2$ ist. Eine Induktion nach r liefert:

- Falls $r = 1$, so ist $z = p_1^{n_1}$ die Primfaktorzerlegung von z , und damit ist $\alpha(z) = \alpha(p_1^{n_1})$.
- Falls $r > 1$, so ist $\alpha(z) = \alpha(p_1^{n_1}) \cdot \alpha(p_2^{n_2} \cdots p_r^{n_r})$, da α multiplikativ und $\text{ggT}(p_1^{n_1}, p_2^{n_2} \cdots p_r^{n_r}) = 1$ ist. Nun nach Induktion ist $\alpha(p_2^{n_2} \cdots p_r^{n_r}) = \alpha(p_2^{n_2}) \cdots \alpha(p_r^{n_r})$. Also insgesamt:

$$\alpha(z) = \alpha(p_1^{n_1}) \cdot \alpha(p_2^{n_2}) \cdots \alpha(p_r^{n_r})$$

(ii) \Rightarrow (i): Wir nehmen an, es gelte umgekehrt Aussage (ii) und es seien $a, b \in \mathbb{Z}_{>0}$ mit $\text{ggT}(a, b) = 1$ gegeben. Also wenn

$$a = p_1^{n_1} \cdots p_r^{n_r} \quad \text{und} \quad b = p_{r+1}^{n_{r+1}} \cdots p_{r+s}^{n_{r+s}}$$

Primfaktorzerlegungen von a und b sind, müssen $p_1, \dots, p_r, p_{r+1}, \dots, p_{r+s}$ paarweise verschieden sein, da $\text{ggT}(a, b) = 1$ ist. Das Produkt $a \cdot b$ hat dann die Primfaktorzerlegung

$$a \cdot b = p_1^{n_1} \cdots p_r^{n_r} \cdot p_{r+1}^{n_{r+1}} \cdots p_{r+s}^{n_{r+s}}.$$

Damit gilt nach (ii), dass

$$\alpha(a \cdot b) \stackrel{(ii)}{=} \alpha(p_1^{n_1}) \cdots \alpha(p_r^{n_r}) \cdot \alpha(p_{r+1}^{n_{r+1}}) \cdots \alpha(p_{r+s}^{n_{r+s}}) \stackrel{(ii)}{=} \alpha(p_1^{n_1} \cdots p_r^{n_r}) \cdot \alpha(p_{r+1}^{n_{r+1}} \cdots p_{r+s}^{n_{r+s}}) = \alpha(a) \cdot \alpha(b),$$

d.h. α ist multiplikativ.

(b) Ist $\alpha_1 = \alpha_2$, so ist sicher $\alpha_1(p^n) = \alpha_2(p^n) \forall p \in \mathbb{P}$ und $\forall n \in \mathbb{Z}_{\geq 0}$. Umgekehrt ist $\alpha_1(p^n) = \alpha_2(p^n) \forall p \in \mathbb{P}$ und $\forall n \in \mathbb{Z}_{\geq 0}$, so gilt für $z \in \mathbb{Z}_{>0}$ mit Primfaktorzerlegung $z = p_1^{n_1} \cdots p_r^{n_r}$

$$\alpha_1(z) \stackrel{(a)}{=} \alpha_1(p_1^{n_1}) \cdots \alpha_1(p_r^{n_r}) = \alpha_2(p_1^{n_1}) \cdots \alpha_2(p_r^{n_r}) \stackrel{(a)}{=} \alpha_2(z),$$

wie behauptet. ■

Aufgabe 5 (Siehe Aufgabe 7, Blatt 3)

Sei $\alpha \in \mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C}) \setminus \{0\}$ eine multiplikative Funktion, die nicht die Nullfunktion ist. Genau dann ist α vollständig multiplikativ, wenn $\alpha(p^n) = \alpha(p)^n$ für alle $p \in \mathbb{P}$ und für alle $n \in \mathbb{Z}_{\geq 0}$ gilt.

4 Die Dirichlet-Faltung

Definition 2.4 (Dirichlet-Faltung)

Seien $\alpha, \beta \in \mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$ zwei arithmetische Funktionen. Die **(Dirichlet-)Faltung** von α und β ist die arithmetische Funktion

$$\alpha * \beta: \begin{array}{ccc} \mathbb{Z}_{>0} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & (\alpha * \beta)(z) := \sum_{\substack{d|z \\ 1 \leq d \leq z}} \alpha(d) \cdot \beta\left(\frac{z}{d}\right). \end{array}$$

Anmerkung 2.5

Die Faltung kann auch folgendermaßen geschrieben werden:

$$(\alpha * \beta)(z) = \sum_{ab=z} \alpha(a) \cdot \beta(b)$$

für alle $z \in \mathbb{Z}_{>0}$, wobei die Summe über alle Paare $(a, b) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$ mit $ab = z$ läuft.

Lemma 2.6

Seien α, β und γ arithmetische Funktionen. Dann gilt:

- (a) $\alpha * \beta = \beta * \alpha$ (Kommutativität);
- (b) $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$ (Assoziativität);
- (c) $\alpha * \varepsilon = \alpha = \varepsilon * \alpha$ (Die Funktion ε ist ein neutrales Element für die Faltung *).

Anders gesagt, bildet $\mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$ eine kommutative *Halbgruppe* bezüglich der Faltung.

Beweis:

(a) Aufgrund der Anmerkung 2.5 ergibt sich sofort

$$(\alpha * \beta)(z) = \sum_{ab=z} \alpha(a) \cdot \beta(b) = \sum_{ba=z} \beta(b) \cdot \alpha(a) = (\beta * \alpha)(z)$$

für alle $z \in \mathbb{Z}_{>0}$.

(b) Sei $z \in \mathbb{Z}_{>0}$. Dann gilt:

$$\begin{aligned} ((\alpha * \beta) * \gamma)(z) &= \sum_{ab=z} (\alpha * \beta)(a) \cdot \gamma(b) \\ &= \sum_{ab=z} \left(\sum_{cd=a} \alpha(c) \cdot \beta(d) \right) \cdot \gamma(b) \\ &= \sum_{cdb=z} \alpha(c) \cdot \beta(d) \cdot \gamma(b) \end{aligned}$$

Analog ist

$$\begin{aligned} (\alpha * (\beta * \gamma))(z) &= \sum_{xy=z} \alpha(x) \cdot (\beta * \gamma)(y) \\ &= \sum_{xy=z} \alpha(x) \cdot \left(\sum_{uv=y} \beta(u) \cdot \gamma(v) \right) \\ &= \sum_{xuv=z} \alpha(x) \cdot \beta(u) \cdot \gamma(v). \end{aligned}$$

Bis auf Umbenennung der Variablen, d.h. $x := c, u := d, v := b$, haben wir zweimal die gleiche Summe erhalten, also ist $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$.

(c) Sei $z \in \mathbb{Z}_{>0}$. Dann gilt:

$$(\alpha * \varepsilon)(z) = \sum_{\substack{d|z \\ 1 \leq d \leq z}} \alpha(d) \cdot \varepsilon\left(\frac{z}{d}\right) = \alpha(z) \cdot \underbrace{\varepsilon(1)}_{=1} + \sum_{\substack{d|z \\ 1 \leq d < z}} \alpha(d) \cdot \underbrace{\varepsilon\left(\frac{z}{d}\right)}_{=0} = \alpha(z)$$

und damit ist $\alpha * \varepsilon = \alpha$. Wegen der Kommutativität der Faltung ist zudem $\varepsilon * \alpha = \alpha * \varepsilon = \alpha$. ■

Lemma 2.7

Sind $\alpha, \beta \in \mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C})$ zwei multiplikative Funktionen, so ist auch die Faltung $\alpha * \beta$ eine multiplikative Funktion.

Beweis: Seien $m, n \in \mathbb{Z}_{>0}$ mit $\text{ggT}(m, n) = 1$. Wegen des Fundamentalsatzes der Zahlentheorie gilt: für jede Faktorisierung $ab = mn$ lassen sich a und b eindeutig in ein Produkt $a = a_1 a_2$ mit $a_1 | m, a_2 | n$ und $b = b_1 b_2$ mit $b_1 | m, b_2 | n$ zerlegen, wobei insbesondere $\text{ggT}(a_1, a_2) = \text{ggT}(b_1, b_2) = 1$ ist. Aufgrund der Multiplikativität von α und β folgt

$$\begin{aligned} (\alpha * \beta)(mn) &= \sum_{ab=mn} \alpha(a) \cdot \beta(b) \\ &= \sum_{\substack{a_1 b_1 = m \\ a_2 b_2 = n}} \alpha(a_1 a_2) \cdot \beta(b_1 b_2) \\ &= \sum_{\substack{a_1 b_1 = m \\ a_2 b_2 = n}} \alpha(a_1) \cdot \alpha(a_2) \cdot \beta(b_1) \cdot \beta(b_2) \end{aligned}$$

$$\begin{aligned}
 &= \sum_{\substack{a_1 b_1 = m \\ a_2 b_2 = n}} \alpha(a_1) \cdot \beta(b_1) \cdot \alpha(a_2) \cdot \beta(b_2) \\
 &= \left(\sum_{a_1 b_1 = m} \alpha(a_1) \cdot \beta(b_1) \right) \cdot \left(\sum_{a_2 b_2 = n} \alpha(a_2) \cdot \beta(b_2) \right) \\
 &= (\alpha * \beta)(m) \cdot (\alpha * \beta)(n),
 \end{aligned}$$

und damit ist $\alpha * \beta \in \mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C})$. ■

Satz 2.8

Sei $\alpha \in \mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$ eine arithmetische Funktion mit $\alpha(1) \neq 0$. Dann existiert eine arithmetische Funktion $\beta \in \mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$ mit $\beta(1) \neq 0$ und $\alpha * \beta = \varepsilon = \beta * \alpha$.

Beweis: Nach Definition der Faltung existiert genau dann zu α eine arithmetische Funktion β mit $\alpha * \beta = \varepsilon$, wenn die Gleichungen

$$1 = \varepsilon(1) = (\alpha * \beta)(1) = \alpha(1)\beta(1)$$

und für $z \in \mathbb{Z}_{>1}$

$$0 = \varepsilon(z) = (\alpha * \beta)(z) = \alpha(1)\beta(z) + \sum_{\substack{ab=z \\ b < z}} \alpha(a)\beta(b)$$

erfüllt sind.

Also können wir die Funktion β induktiv definieren. Da $1 = \alpha(1)\beta(1)$ gelten soll, setzen wir $\beta(1) := \frac{1}{\alpha(1)}$. ($\alpha(1) \neq 0$ nach Voraussetzung!) Sei nun $z > 1$. Induktiv nehmen wir an, dass $\beta(d)$ schon für alle $d < z$ definiert ist, und wegen der zweiten Gleichung setzen wir:

$$\beta(z) := \frac{-1}{\alpha(1)} \sum_{\substack{ab=z \\ b < z}} \alpha(a)\beta(b)$$

Offensichtlich gilt nach Konstruktion $\alpha * \beta = \varepsilon$. Zudem gilt auch $\varepsilon = \beta * \alpha$ wegen der Kommutativität der Faltung. ■

Betrachten wir nun noch die übliche Addition $+$ von Funktionen, so erhalten wir die folgenden algebraischen Strukturen auf $\mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$ und $\mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C})$.

Folgerung 2.9

- (a) $(\mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C}), +, *)$ ist ein Integritätsbereich mit Nullelement die Nullfunktion $\mathbf{0}$ und mit Einselement ε .
- (b) $\mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})^\times = \{\alpha \in \mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C}) \mid \alpha(1) \neq 0\}$.
- (c) $(\mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C}) \setminus \{\mathbf{0}\}, *)$ ist eine abelsche Gruppe mit neutralem Element ε .

Beweis: Siehe [Aufgabe 6, Blatt 2]. ■

5 Die Möbiusfunktion

Definition 2.10 (Möbiusfunktion)

Die Möbiusfunktion μ ist die arithmetische Funktion

$$\mu: \mathbb{Z}_{>0} \longrightarrow \mathbb{C}$$

$$z \longmapsto \begin{cases} 0 & \text{falls } \exists p \in \mathbb{P} \text{ mit } p^2 \mid z, \\ (-1)^{\#\{p \in \mathbb{P} \mid p \text{ teilt } z\}} & \text{sonst.} \end{cases}$$

Anmerkung 2.11

(1) Nennen wir eine Zahl **quadratrofrei**, wenn sie von keiner Quadratzahl außer 1 geteilt wird, so gibt die Möbiusfunktion an, ob eine positive Zahl quadratrofrei ist oder nicht. Insbesondere nimmt sie den Wert -1 an, falls die gegebene Zahl z eine Primzahl ist.

(2) zum Beispiel hat die Möbiusfunktion für $1 \leq z \leq 12$ die folgenden Werte:

z	1	2	3	4	5	6	7	8	9	10	11	12
$\mu(z)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0

Lemma 2.12

(a) Die Möbiusfunktion μ ist multiplikativ.

(b) Die Möbiusfunktion μ ist das Inverse von der konstanten Funktion \mathbf{e} bezüglich der Faltung, d.h.

$$\mu * \mathbf{e} = \mathbf{e} * \mu = \varepsilon.$$

Beweis:

(a) Zunächst ist $\mu(1) = 1$ nach Definition. Sei also $z \in \mathbb{Z}_{>1}$ mit Primfaktorzerlegung $z = p_1^{n_1} \cdots p_r^{n_r}$ (d.h. $r \in \mathbb{Z}_{\geq 1}$, $n_1, \dots, n_r \in \mathbb{Z}_{>0}$ und $p_1, \dots, p_r \in \mathbb{P}$ sind paarweise verschieden). Einerseits gilt

$$\mu(z) = \mu(p_1^{n_1} \cdots p_r^{n_r}) = \begin{cases} 0 & \text{falls } \exists 1 \leq i \leq r \text{ mit } n_i \geq 2, \\ (-1)^r & \text{falls } n_1 = \dots = n_r = 1. \end{cases}$$

Andererseits ist für $1 \leq i \leq r$

$$\mu(p_i^{n_i}) = \begin{cases} 0 & \text{falls } n_i \geq 2, \\ -1 & \text{falls } n_i = 1, \end{cases}$$

also ist auch

$$\mu(p_1^{n_1}) \cdots \mu(p_r^{n_r}) = \begin{cases} 0 & \text{falls } \exists 1 \leq i \leq r \text{ mit } n_i \geq 2, \\ (-1)^r & \text{falls } n_1 = \dots = n_r = 1. \end{cases}$$

Daher ist μ multiplikativ nach Satz 2.3(a).

(b) Wegen der Kommutativität der Faltung reicht es zu zeigen, dass $\mu * \mathbf{e} = \varepsilon$. Da μ und \mathbf{e} multiplikativ sind, so ist auch $\mu * \mathbf{e}$ multiplikativ nach Lemma 2.7. Deshalb reicht es nach Satz 2.3(b) die Identität

für Primzahlpotenzen nachzuweisen. Sei $p \in \mathbb{P}$ und $n \in \mathbb{Z}_{>0}$. Es gilt:

$$(\mu * \mathbf{e})(p^n) = \sum_{i=0}^n \mu(p^i) \cdot \underbrace{\mathbf{e}(p^{n-i})}_{=1} = \sum_{i=0}^n \mu(p^i) = \mu(1) + \mu(p) = 1 + (-1) = 0 = \varepsilon(p^n)$$

nach Definitionen von μ und ε . Außerdem ist $(\mu * \mathbf{e})(p^0) = \varepsilon(p^0) = 1$ nach Lemma 2.2. ■

Definition 2.13 (Summatorfunktion)

Sei $\alpha \in \mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$ eine arithmetische Funktion. Dann wird die **Summatorfunktion** β_α von α durch $\beta_\alpha := \alpha * \mathbf{e}$ definiert, d.h. die Funktion

$$\beta_\alpha: \mathbb{Z}_{>0} \longrightarrow \mathbb{C} \\ z \longmapsto \sum_{\substack{d|z \\ 1 \leq d \leq z}} \alpha(d).$$

Beispiel 5

Offenbar ist ε die Summatorfunktion der Möbiusfunktion, da $\mu * \mathbf{e} = \varepsilon$ nach Lemma 2.12.

Satz 2.14 (Möbius-Umkehrsatz)

Ist $\alpha \in \mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$ eine arithmetische Funktion, dann gilt $\alpha = \beta_\alpha * \mu$, d.h.

$$\alpha(z) = \sum_{\substack{d|z \\ 1 \leq d \leq z}} \beta_\alpha(d) \cdot \mu\left(\frac{z}{d}\right)$$

für alle $z \in \mathbb{Z}_{>0}$.

Beweis: Nach Definition ist $\beta_\alpha = \alpha * \mathbf{e}$, und nach Lemma 2.12 ist $\mu * \mathbf{e} = \mathbf{e} * \mu = \varepsilon$. Daraus folgt

$$\alpha = \alpha * \varepsilon = \alpha * (\mathbf{e} * \mu) \stackrel{\text{Lem. 2.6(b)}}{=} (\alpha * \mathbf{e}) * \mu = \beta_\alpha * \mu,$$

da ε das Einselement von $\mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$ ist. ■

Folgerung 2.15

Sei $\alpha \in \mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$ eine arithmetische Funktion mit Summatorfunktion β_α . Dann ist $\alpha \in \mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C})$ genau dann, wenn $\beta_\alpha \in \mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C})$ ist.

Beweis:

' \Rightarrow ' Falls $\alpha \in \mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C})$, so ist auch $\beta_\alpha \in \mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C})$ nach Lemma 2.7, da β_α eine Faltung zweier multiplikativen Funktionen ist.

' \Leftarrow ' Umgekehrt ist die Funktion α nach dem Möbius-Umkehrsatz vollständig von ihrer Summatorfunktion definiert, und zwar ist $\alpha = \beta_\alpha * \mu$. Nun ist die Möbiusfunktion multiplikativ nach Lemma 2.12(a), also ist α multiplikativ als Faltung zweier multiplikativen Funktionen. ■

Aufgabe 7 (Aufgabe 8, Blatt 3)

Sei $\alpha \in \mathcal{A}(\mathbb{Z}_{>0}, \mathbb{C})$ eine arithmetische Funktion mit Summatorfunktion β_α . Zeigen Sie:

- (a) $\alpha(p^n) = \beta_\alpha(p^n) - \beta_\alpha(p^{n-1})$ für alle $p \in \mathbb{P}$ und für alle $n \in \mathbb{Z}_{>0}$.
- (b) Sei $\alpha \in \mathcal{M}(\mathbb{Z}_{>0}, \mathbb{C}) \setminus \{0\}$. Sei $z \in \mathbb{Z}_{>1}$ mit Primfaktorzerlegung $z = p_1^{n_1} \cdots p_r^{n_r}$, dann gilt:

$$\alpha(z) = \prod_{i=1}^r (\beta_\alpha(p_i^{n_i}) - \beta_\alpha(p_i^{n_i-1}))$$

6 Die eulersche φ -Funktion

Definition 2.16 (eulersche φ -Funktion)

Die arithmetische Funktion

$$\begin{aligned} \varphi: \mathbb{Z}_{>0} &\longrightarrow \mathbb{C} \\ m &\longmapsto \#\{d \in \mathbb{Z} \mid 1 \leq d \leq m \text{ und } \text{ggT}(d, m) = 1\} \end{aligned}$$

heißt **eulersche φ -Funktion**.

Beispiel 6

Zum Beispiel nimmt die eulersche φ -Funktion für $1 \leq m \leq 12$ die folgenden Werte an:

m	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4

Satz 2.17

- (a) Ist $m \in \mathbb{Z}_{>0}$, so ist $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$.
- (b) Die eulersche φ -Funktion ist multiplikativ.
- (c) Für $p \in \mathbb{P}$ und $n \in \mathbb{Z}_{>0}$ gilt $\varphi(p^n) = p^n - p^{n-1}$.
- (d) Für $m \in \mathbb{Z}_{>1}$ mit Primfaktorzerlegung $m = \prod_{p \in \mathbb{P}} p^{n_p(m)}$ gilt

$$\varphi(m) = \prod_{p \in \mathbb{P}} (p^{n_p(m)} - p^{n_p(m)-1}) = m \prod_{\substack{p \in \mathbb{P} \\ p|m}} (1 - \frac{1}{p}).$$

- (e) Die Summatorfunktion der eulerschen φ -Funktion ist die identische Abbildung i.
- (f) **(Rekursionsformel)**. Für $m \in \mathbb{Z}_{>1}$ gilt

$$\varphi(m) = m - \sum_{\substack{1 \leq d < m \\ d|m}} \varphi(d).$$

Beweis:

- (a) Dies ist ein Ergebnis aus der AGS. (Anmerkung: $\mathbb{Z}/1\mathbb{Z}$ ist der Nullring und $(\mathbb{Z}/1\mathbb{Z})^\times$ ist die triviale Gruppe, also ist diese einelementig.)
- (b) Seien $m, n \in \mathbb{Z}_{>0}$ mit $\text{ggT}(m, n) = 1$. Der chinesische Restsatz liefert einen Ring-Isomorphismus

$$\begin{aligned} \Phi: \mathbb{Z}/(mn)\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ a + mn\mathbb{Z} &\mapsto (a + m\mathbb{Z}, a + n\mathbb{Z}). \end{aligned}$$

Die Einschränkung von Φ auf die Einheiten $(\mathbb{Z}/(mn)\mathbb{Z})^\times$ liefert die Existenz eines Gruppen-Isomorphismus

$$(\mathbb{Z}/(mn)\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

Damit folgt aus (a), dass

$$\varphi(mn) = |(\mathbb{Z}/(mn)\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times| \cdot |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(m) \cdot \varphi(n).$$

- (c) Wir betrachten den Gruppen-Homomorphismus $f : (\mathbb{Z}/p^n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times : a + p^n\mathbb{Z} \mapsto a + p\mathbb{Z}$. Dieser ist offensichtlich surjektiv mit Kern $\ker(f) = \{(1 + px) + p^n\mathbb{Z} \mid 0 \leq x \leq p^{n-1}\}$. Nun folgt aus dem Homomorphiesatz, dass

$$\varphi(p^n) \stackrel{(a)}{=} |(\mathbb{Z}/p^n\mathbb{Z})^\times| = |\ker(f)| \cdot |\text{Im}(f)| = p^{n-1} \cdot (p-1) = p^n - p^{n-1}$$

ist.

- (d) Folgt aus (c) und der Tatsache, dass $p^n - p^{n-1} = p^n(1 - \frac{1}{p})$ für alle $n \in \mathbb{Z}_{>0}$ ist.
- (e) Seien $p \in \mathbb{P}$ und $n \in \mathbb{Z}_{>0}$. Nach Definitionen gilt

$$(\mu * \mathbf{i})(p^n) = \sum_{j=0}^n \mu(p^j) \cdot \mathbf{i}(p^{n-j}) = 1 \cdot p^n + (-1) \cdot p^{n-1} = p^n - p^{n-1}.$$

Aber μ und \mathbf{i} sind multiplikativ und nach (b) ist φ auch multiplikativ. Es folgt also aus Lemma 2.2, dass $\mu * \mathbf{i}(1) = 1 = \varphi(1)$. Also stimmen die Funktionen $\mu * \mathbf{i}$ und φ für Primzahlpotenzen überein. Damit folgt aus Satz 2.3(b), dass $\mu * \mathbf{i} = \varphi$ ist und wegen Lemmata 2.6(a),(c) und 2.12(b) erhalten wir

$$\mathbf{i} = \mathbf{i} * \varepsilon = \mathbf{e} * \mu * \mathbf{i} = \mathbf{e} * \varphi = \beta_\varphi,$$

wie behauptet.

- (f) Weil \mathbf{i} die Summatorfunktion von φ ist, gilt

$$m = \mathbf{i}(m) = \varphi * \mathbf{e}(m) = \sum_{\substack{1 \leq d \leq m \\ d|m}} \varphi(d) = \sum_{\substack{1 \leq d < m \\ d|m}} \varphi(d) + \varphi(m).$$



Beispiel 7

Eine Anwendung von Satz 2.17 liefert z. B.:

- (a) Für $n = 12 = 3 \cdot 4$ ist $\varphi(12) = \varphi(3)\varphi(4) = (3^1 - 3^0) \cdot (2^2 - 2^1) = 2 \cdot 2 = 4$.
- (b) Für $n = 30 = 2 \cdot 3 \cdot 5$ ist $\varphi(30) = \varphi(2)\varphi(3)\varphi(5) = (2^1 - 2^0) \cdot (3^1 - 3^0) \cdot (5^1 - 5^0) = 1 \cdot 2 \cdot 4 = 8$.
In der Tat sind genau folgende acht Zahlen zwischen 1 und 30 prim zu 30:

$$1, 7, 11, 13, 17, 19, 23, 29.$$

7 Die Teilersummenfunktion und vollkommene Zahlen

Definition 2.18 (Teilersummenfunktion)

Die Teilersummenfunktion ist die Summatorfunktion $\sigma := i * e$ der identische Abbildung, d.h. die Funktion

$$\sigma: \mathbb{Z}_{>0} \longrightarrow \mathbb{C}$$

$$z \longmapsto \sum_{\substack{d|z \\ 1 \leq d \leq z}} d.$$

Bemerkung 2.19

Die Teilersummenfunktion σ ist multiplikativ, und für $p \in \mathbb{P}$ und $n \in \mathbb{Z}_{>0}$ gilt

$$\sigma(p^n) = \frac{p^{n+1} - 1}{p - 1}.$$

Beweis: Nach Definition ist die Teilersummenfunktion eine Faltung zweier multiplikativen Funktionen, so dass σ nach Lemma 2.7 multiplikativ ist. Zudem ist

$$\sigma(p^n) = \sum_{0 \leq d \leq n} p^d = 1 + p + \dots + p^n = \frac{p^{n+1} - 1}{p - 1},$$

wobei die letzte Gleichheit aus der Summenformel der geometrischen Reihe folgt. ■

Damit erhalten wir die ersten Resultate über Zahlen.

Definition 2.20 (vollkommene Zahl)

Eine Zahl $z \in \mathbb{Z}_{>0}$ mit $z = \sum_{\substack{d|z \\ 1 \leq d < z}} d$ heißt eine **vollkommene Zahl**, d.h. z ist Summe ihrer echten positiven Teiler.

Anmerkung 2.21

Der Begriff einer vollkommenen Zahl sowie die ersten vier vollkommenen Zahlen waren schon in der Antike bekannt. Diese sind

$$6, 28, 496, 8128.$$

Die fünfte vollkommene Zahl ist $33 \cdot 550 \cdot 336$. Es ist unbekannt, ob es unendlich viele vollkommene Zahlen gibt. Ferner sind alle bekannten vollkommenen Zahlen gerade und es ist nicht bekannt, ob es ungerade vollkommene Zahlen gibt. Zum Studium von vollkommenen Zahlen eignet sich die Teilersummenfunktion, wie die Definitionen und die folgende Bemerkung zeigen.

Bemerkung 2.22

Sei $z \in \mathbb{Z}_{>0}$. Genau dann ist z eine vollkommene Zahl, wenn $\sigma(z) = 2z$.

Beweis: Nach Definition ist

$$\sigma(z) = \sum_{\substack{d|z \\ 1 \leq d \leq z}} d = \sum_{\substack{d|z \\ 1 \leq d < z}} d + z,$$

also ist z vollkommen genau dann, wenn $\sigma(z) = 2z$. ■

Beispiel 8

Für die fünfte vollkommene Zahl erhalten wir die Primfaktorzerlegung $33\cdot 550\cdot 336 = 2^{12} \cdot 8 \cdot 191$.
Damit gilt

$$\sigma(33\cdot 550\cdot 336) = \frac{8\cdot 191^2 - 1}{8\cdot 191 - 1} \cdot (2^{13} - 1) = 67\cdot 100\cdot 672 = 2 \cdot 33\cdot 550\cdot 336$$

Die Zahl ist also eigentlich vollkommen.

Wir möchten jetzt zeigen, dass die vollkommenen Zahlen durch die sogenannten Mersenne-Primzahlen charakterisiert werden können.

Definition 2.23 (Mersenne-Zahl, Mersenne-Primzahl)

Für $n \in \mathbb{Z}_{>0}$ heißt $M_n := 2^n - 1$ die n -te **Mersenne-Zahl**. Die Primzahlen, die auch Mersenne-Zahlen sind, heißen **Mersenne-Primzahlen**.

Beispiel 9

Es ist $M_1 = 1, M_2 = 3, M_3 = 7, M_4 = 15, M_5 = 31, \dots$

Lemma 2.24

Sei $n \in \mathbb{Z}_{>0}$. Ist die n -te Mersenne-Zahl M_n eine Primzahl, so ist auch n eine Primzahl.

Offensichtlich gilt die Umkehrung nicht, da $M_{11} = 23 \cdot 89$.

Beweis: Wir zeigen die Kontraposition: Sei $n \in \mathbb{Z}_{>0}$ reduzibel, etwa $n = ab$ mit $a, b \in \mathbb{Z}_{>1}$. Dann ist auch $2^a - 1 > 1$, und damit ist

$$M_n = M_{ab} = 2^{ab} - 1 = (2^a - 1) \sum_{i=0}^{b-1} (2^a)^i$$

reduzibel. (Wende die Formel $X^n - 1 = (X - 1)(\sum_{i=0}^{n-1} X^i)$ mit $X = 2^a$ an.) ■

Satz 2.25 (Euler/Euklid)

Eine gerade Zahl $z \in \mathbb{Z}_{>0}$ ist genau dann vollkommen, wenn sie die Form

$$z = 2^{p-1}(2^p - 1)$$

hat, wobei $p \in \mathbb{P}$ und $2^p - 1 \in \mathbb{P}$ sind.

Beweis:

' \Rightarrow ' (Euler) Zunächst nehmen wir an, dass z gerade und vollkommen ist. Dann hat z eine Darstellung $z = 2^r \cdot u$ mit $r \in \mathbb{Z}_{>0}$ und $u \in \mathbb{Z}_{>0}$ ungerade. Wegen der Multiplikativität von σ und Bemerkung 2.19 ist

$$\sigma(z) = \sigma(2^r) \cdot \sigma(u) = (2^{r+1} - 1) \cdot \sigma(u).$$

Nach Bemerkung 2.22 ist zudem $\sigma(z) = 2z$. Damit gilt

$$(2^{r+1} - 1) \cdot \sigma(u) = 2^{r+1} \cdot u,$$

so dass

$$\sigma(u) = \frac{2^{r+1}}{2^{r+1}-1} \cdot u = \frac{(2^{r+1}-1)+1}{2^{r+1}-1} \cdot u = u + \frac{u}{2^{r+1}-1}.$$

Daraus folgt, dass

$$v := \frac{u}{2^{r+1}-1} = \sigma(u) - u \in \mathbb{Z}$$

ist, da $\sigma(u), u \in \mathbb{Z}$. Also ist $v + u = \sigma(u) = \sum_{\substack{d|u \\ 1 \leq d \leq u}} d$, und damit müssen u und v die einzigen Teiler

von u sein. Da $v < u$ ist, erhalten wir: $v = 1, u = 2^{r+1} - 1 \in \mathbb{P}$. Setzen wir also $p := r + 1$. Schließlich ist $p \in \mathbb{P}$ nach Lemma 2.24.

' \Leftarrow ' (Euklid) Umgekehrt nehmen wir an, dass $z = 2^{p-1}(2^p - 1)$ mit $p, 2^p - 1 \in \mathbb{P}$ ist. Also ist $z = 2^{p-1}(2^p - 1)$ eine Primfaktorzerlegung von z . Wegen der Multiplikativitat von σ und Bemerkung 2.19 erhalten wir

$$\sigma(z) = \sigma(2^{p-1}) \cdot \sigma(2^p - 1) = \frac{2^{p-1+1} - 1}{2 - 1} \cdot \frac{(2^p - 1)^{1+1} - 1}{2^p - 1 - 1} = (2^p - 1) \cdot ((2^p - 1) + 1) = 2^p \cdot (2^p - 1) = 2z,$$

und damit ist z nach Bemerkung 2.22 vollkommen. ■

Statt der Teilersummenfunktion kann man auch die Teileranzahlfunktion oder die Teilerproduktfunktion betrachten:

Aufgabe 8 (Aufgabe 11, Blatt 3)

Fur eine positive ganze Zahl $z \in \mathbb{Z}_{>0}$ bezeichnen wir mit

$$\tau(z) := \#\{d \in \mathbb{Z}_{>0} \mid d \text{ ist ein Teiler von } z\} \quad \text{und} \quad P(z) := \prod_{\substack{d|z \\ 1 \leq d \leq z}} d$$

die Anzahl der positiven Teiler von z , bzw. das Produkt aller positiven Teiler von z . Zeigen Sie:

- (a) $\tau = \mathbf{e} * \mathbf{e}$ ist multiplikativ;
- (b) $\forall z \in \mathbb{Z}_{>0}$ gilt $\tau(z) = \prod_{p \in \mathbb{P}} (n_p(z) + 1)$.
- (c) $\forall z \in \mathbb{Z}_{>0}$ gilt $P(z) = z^{\frac{\tau(z)}{2}}$.

Ist P eine multiplikative Funktion?

Zusammenfassung:

In der folgenden Tabelle sind fur wichtige arithmetische Funktionen α , die wir in diesem Kapitel untersucht haben, ihre Summatorfunktionen gegeben:

α	ε	μ	φ	\mathbf{i}	\mathbf{e}
$\beta_\alpha = \alpha * \mathbf{e}$	\mathbf{e}	ε	\mathbf{i}	σ	τ

Kapitel 3: Die Sätze von Euler, Fermat und Wilson

In diesem Kapitel wollen wir nun die eulersche φ -Funktion verwenden, um einen berühmten Satz von Euler zu formulieren, aus dem wir dann mehrere interessante Folgerungen ziehen werden. Insbesondere werden wir einen ersten Primzahltest bekommen und Fermats Lösbarkeitsaussage zur diophantischen Gleichung $X^2 + Y^2 = n$ für positive ganze Zahlen n untersuchen.

Notation: In diesem Kapitel bezeichnen wir mit $[k]$ die Restklasse von k in $\mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{Z}_{>0}$).

8 Der Satz von Euler

Satz 3.1 (Satz von Euler)

Für alle $k, n \in \mathbb{Z}_{>0}$ mit $\text{ggT}(k, n) = 1$ gilt

$$k^{\varphi(n)} \equiv 1 \pmod{n}.$$

Der Beweis des Satzes von Euler ist eine Anwendung des Satzes von Lagrange, der in den algebraischen Strukturen bewiesen wurde. (Siehe Kapitel 0.)

Beweis: Wegen $\text{ggT}(k, n) = 1$ ist also $[k] \in (\mathbb{Z}/n\mathbb{Z})^\times$ (d.h. invertierbar). Nach Satz 2.17(a) ist $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ und aus dem Satz von Lagrange folgt

$$[1] = [k]^{|(\mathbb{Z}/n\mathbb{Z})^\times|} = [k]^{\varphi(n)} = [k^{\varphi(n)}] \in \mathbb{Z}/n\mathbb{Z},$$

d.h.

$$k^{\varphi(n)} \equiv 1 \pmod{n}. \quad \blacksquare$$

Beispiel 10

Wir überlegen uns nun, wie lineare Kongruenzen mit dem Satz von Euler gelöst werden können. Sei dazu $ax \equiv b \pmod{n}$ mit $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ und $\text{ggT}(a, n) = 1$ gegeben. Damit ist $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ und es gilt

$$[x] = [b] \cdot [a]^{-1} = [b] \cdot [1] \cdot [a]^{-1} = [b] \cdot [a]^{\varphi(n)} \cdot [a]^{-1} = [b] \cdot [a]^{\varphi(n)-1} \in \mathbb{Z}/n\mathbb{Z}$$

nach dem Satz von Euler, da $a^{\varphi(n)} \equiv 1 \pmod{n}$. Somit ist $x = ba^{\varphi(n)-1}$ eine Lösung der Kongruenz $ax \equiv b \pmod{n}$.

Z.B.: Löse $5x \equiv 4 \pmod{12}$. Hier ist $\varphi(12) = 4$ und damit ist

$$x = 4 \cdot 5^3 = 4 \cdot 125 = 500$$

eine Lösung. Wegen $500 = 41 \cdot 12 + 8 \equiv 8 \pmod{12}$ ist auch $x = 8$ eine Lösung:

$$5 \cdot 8 = 40 \equiv 4 \pmod{12}.$$

9 Der kleine Satz von Fermat

Der kleine Satz von Fermat ist ein Spezialfall des Satzes von Euler.

Folgerung 3.2 (kleiner Satz von Fermat)

Sei $k \in \mathbb{Z}_{>0}$ eine positive ganze Zahl.

(1) Ist $p \in \mathbb{P}$ und $p \nmid k$, so gilt $k^{p-1} \equiv 1 \pmod{p}$.

(2) Ist $p \in \mathbb{P}$ und $p \mid k$, so gilt $k^p \equiv 0 \equiv k \pmod{p}$.

Zusammengefasst: für alle $k \in \mathbb{Z}_{>0}$ und alle Primzahlen $p \in \mathbb{P}$ gilt:

$$k^p \equiv k \pmod{p}$$

Beweis:

(2) ist trivial.

(1) ist ein Spezialfall des Satzes von Euler, weil $\text{ggT}(k, p) = 1$. Es gilt also

$$k^{p-1} = k^{\varphi(p)} \equiv 1 \pmod{p}$$

und multiplizieren mit k liefert

$$k^p \equiv k \pmod{p}. \quad \blacksquare$$

Anmerkung 3.3

Das vorstehende Resultat liefert also eine notwendige Bedingung dafür, dass eine positive Zahl p prim ist. Dies führt zu folgendem einfachen **Primzahltest**:

Für $n \in \mathbb{Z}_{>0}$ teste, ob $k^{n-1} \equiv 1 \pmod{n}$ für alle $k < n$.

· Falls dies nicht der Fall ist, so ist n keine Primzahl.

· Falls doch, so ist n entweder eine Primzahl oder eine sogenannte Carmichael-Zahl:

Eine zusammengesetzte natürliche Zahl n heißt **Carmichael-Zahl**, falls für alle zu n teilerfremden Zahlen a gilt: $a^{n-1} \equiv 1 \pmod{n}$.

10 Der Satz von Wilson

Der Satz von Euler impliziert auch den folgenden Satz von Wilson.

Satz 3.4 (Wilson)

Sei $p \in \mathbb{P}$ eine Primzahl. Dann ist

$$(p-1)! \equiv -1 \pmod{p}.$$

Anmerkung 3.5

Wie man leicht sieht, gilt hiervon auch die Umkehrung. (Aufgabe 14(a), Blatt 4)

Beweis: Betrachte das Polynom $f := X^{p-1} - [1] \in (\mathbb{Z}/p\mathbb{Z})[X]$. Da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, besitzt f höchstens $p-1$ verschiedene Nullstellen in $\mathbb{Z}/p\mathbb{Z}$. Nun ist nach dem Satz von Euler (Satz 3.1)

$$k^{p-1} \equiv 1 \pmod{p} \quad \text{für alle } 1 \leq k \leq p-1.$$

Also sind $[1], \dots, [p-1]$ verschiedene Nullstellen von f . Daher gilt

$$(X - [1]) \cdots (X - [p-1]) \mid f.$$

Da beide Polynome denselben Grad und denselben höchsten Koeffizient haben, folgt

$$(X - [1]) \cdots (X - [p-1]) = f = X^{p-1} - [1].$$

Auswerten bei $X = [0]$ ergibt

$$[(-1) \cdots (-(p-1))] = [-1] \in \mathbb{Z}/p\mathbb{Z}$$

und somit ist

$$(-1)^{p-1} \cdot (p-1)! \equiv -1 \pmod{p}.$$

Ist p ungerade, so ist $(-1)^{p-1} = 1$.

Für $p = 2$ gilt $-(p-1)! \equiv (p-1)! \pmod{p}$. Insgesamt haben wir also

$$(p-1)! \equiv (-1)^{p-1} (p-1)! \equiv -1 \pmod{p}. \quad \blacksquare$$

Beispiel 11

Es gilt

$$6! = 720 = 7 \cdot 103 - 1 \equiv -1 \pmod{7}.$$

Folgerung 3.6

Sei p eine ungerade Primzahl. Dann gilt:

$X^2 + [1] \in (\mathbb{Z}/p\mathbb{Z})[X]$ hat genau dann eine Nullstelle in $\mathbb{Z}/p\mathbb{Z}$, wenn $p \equiv 1 \pmod{4}$ ist.

Beweis:

' \Rightarrow ' Sei $[\alpha] \in \mathbb{Z}/p\mathbb{Z}$ eine Nullstelle von $X^2 + [1]$, also $\alpha^2 + 1 \equiv 0 \pmod{p}$, beziehungsweise $\alpha^2 \equiv -1 \pmod{p}$. Wegen Folgerung 3.2 (kleiner Satz von Fermat) ist

$$1 \equiv \alpha^{p-1} \equiv (\alpha^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Also ist $\frac{p-1}{2}$ gerade, und daher $p - 1$ durch 4 teilbar. Also gilt $p \equiv 1 \pmod{4}$.

' \Leftarrow ' Sei $p \equiv 1 \pmod{4}$ und somit $\frac{p-1}{2}$ gerade. Mit dem Satz von Wilson gilt

$$1 \cdot 2 \cdots (p-1) \equiv -1 \pmod{p}.$$

Nun ist $p - r \equiv -r \pmod{p}$ für $1 \leq r \leq \frac{p-1}{2}$, also

$$\begin{aligned} -1 &\equiv 1 \cdots \frac{p-1}{2} \cdot \left(p - \frac{p-1}{2}\right) \cdots (p-1) \pmod{p} \\ &\equiv 1 \cdots \frac{p-1}{2} \cdot (-1) \cdots \left(-\frac{p-1}{2}\right) \pmod{p}. \end{aligned}$$

Damit gilt

$$(-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}.$$

Also ist $\left[\left(\frac{p-1}{2}\right)!\right]$ eine Nullstelle von $X^2 + [1]$ in $\mathbb{Z}/p\mathbb{Z}$, wie gesucht. ■

11 Die diophantische Gleichung $X^2 + Y^2 = p$

In diesem Abschnitt erhalten wir das erste Teilergebnis zu Quadratsummen, indem wir die Frage beantworten, welche Primzahlen sich als Summe zweier Quadrate schreiben lassen. Anders gesagt, suchen wir nach positiven ganzzahligen Lösungen der diophantischen Gleichung

$$X^2 + Y^2 = p$$

wobei p eine Primzahl ist.

Anmerkung 3.7

Zunächst ist es klar, dass wir uns dabei auf die Betrachtung **ungerader** Primzahlen p beschränken können, da

$$1^2 + 1^2 = 2$$

die einzige Lösung für $p = 2$ ist.

Lemma 3.8

Sind $x, y \in \mathbb{Z}$ mit $x^2 + y^2 = p$, so ist $\text{ggT}(x, p) = \text{ggT}(y, p) = 1$.

Beweis: Wir nehmen an, dass $\text{ggT}(x, p) \neq 1$, und somit $p \mid x$. Dann aus $p \mid x$ folgt $p \mid x^2$, damit $p \mid y^2 = x^2 - p$ und sogar $p \mid y$. Damit $p^2 \mid y^2$ und $p^2 \mid x^2$, so dass $p^2 \mid x^2 + y^2 = p$ im Widerspruch zu $p^2 \nmid p$. Also ist $\text{ggT}(x, p) = 1$.

Ähnlich: $\text{ggT}(y, p) = 1$. ■

Aus Folgerung 3.6 lässt sich somit folgende Tatsache ableiten:

Lemma 3.9

Ist $p \neq 2$ eine Primzahl mit einer Darstellung $p = x^2 + y^2$, mit $x, y \in \mathbb{Z}$, so ist $p \equiv 1 \pmod{4}$.

Beweis: Aus $x^2 + y^2 = p$ folgt $x^2 + y^2 \equiv 0 \pmod{p}$ und daher

$$[x]^2 + [y]^2 = [0] \text{ in } \mathbb{Z}/p\mathbb{Z}.$$

Nach Lemma 3.8 ist $\text{ggT}(y, p) = 1$, daher ist $[y] \in (\mathbb{Z}/p\mathbb{Z})^\times$, also dürfen wir mit $[y^2]^{-1}$ multiplizieren. Dies liefert

$$\underbrace{[x]^2 \cdot [y]^{-2}}_{[(xy^{-1})^2]} + [1] = [0] \text{ in } \mathbb{Z}/p\mathbb{Z}$$

und somit ist $[(xy^{-1})]$ eine Nullstelle des Polynoms $X^2 + [1] \in (\mathbb{Z}/p\mathbb{Z})[X]$. Aus Folgerung 3.6 folgt nun $p \equiv 1 \pmod{4}$. ■

Es gilt auch die Umkehrung von Lemma 3.9. Um dies zu zeigen, bedarf es wieder eines Existenzbeweises, für den wir noch einen Satz von Thue benötigen. Dieser beruht auf Dirichlets bekanntem Schubfachprinzip.

Lemma 3.10 (Schubfachprinzip)

Werden n (mathematische oder physikalische) Objekte auf weniger als n Schubfächer (Teilmengen) verteilt, so enthält mindestens ein Schubfach mindestens zwei Objekte.

Satz 3.11 (Thue)

Seien $a \in \mathbb{Z}$ und $n \in \mathbb{Z}_{>0}$ keine Quadratzahl. Dann hat die Kongruenzgleichung

$$ax - y \equiv 0 \pmod{n}$$

eine Lösung $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ mit $|x|, |y| < \sqrt{n}$.

Beweis: Betrachte die Menge $A := \{(x, y) \in \mathbb{Z}^2 \mid 0 \leq x, y < \sqrt{n}\}$. Bezeichnet $m \in \mathbb{Z}$ die kleinste ganze Zahl größer gleich \sqrt{n} , so haben wir für x, y je genau m Möglichkeiten, also insgesamt $|A| = m^2$. Da n keine Quadratzahl ist, ist $m^2 > n$. Aber $\mathbb{Z}/n\mathbb{Z}$ hat genau $n < m^2$ Elemente. Nach dem Schubfachprinzip (Lemma 3.10) gibt es daher $(x_1, y_1), (x_2, y_2) \in A$ mit

$$(x_1, y_1) \neq (x_2, y_2) \text{ und } ax_1 - y_1 \equiv ax_2 - y_2 \pmod{n}.$$

Also ist $a(x_1 - x_2) - (y_1 - y_2) \equiv 0 \pmod{n}$ mit $|x_1 - x_2| < \sqrt{n}, |y_1 - y_2| < \sqrt{n}$. Damit ist

$$(x, y) := (x_1 - x_2, y_1 - y_2) \neq (0, 0)$$

eine Lösung, wie gewünscht. ■

Satz 3.12 (Fermat)

Sei $p \in \mathbb{P}$ eine ungerade Primzahl. Dann sind äquivalent:

- (a) es gibt $(x, y) \in \mathbb{Z}^2$ mit $x^2 + y^2 = p$;
- (b) es gibt $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \pmod{p}$; und
- (c) es gilt $p \equiv 1 \pmod{4}$.

Beweis:

(a)⇒(c): Dies ist Lemma 3.9.

(b)⇔(c): Dies ist Folgerung 3.6.

(b)⇒(a): Nach (b) existiert ein $a \in \mathbb{Z}$ mit

$$a^2 + 1 \equiv 0 \pmod{p},$$

also $a^2 \equiv -1 \pmod{p}$. Nach dem Satz von Thue (Satz 3.11) existiert $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ mit

$$ax \equiv y \pmod{p} \quad \text{und} \quad |x|, |y| < \sqrt{p}.$$

Damit gilt

$$-x^2 \equiv a^2 x^2 \equiv y^2 \pmod{p}$$

und somit

$$x^2 + y^2 \equiv 0 \pmod{p}.$$

Dies zeigt, dass $x^2 + y^2 = kp$ für ein $k \in \mathbb{Z}_{>0}$ ist. Wegen $|x|, |y| < \sqrt{p}$ gilt aber auch

$$x^2 + y^2 < 2p.$$

Damit folgt $0 < k < 2$, also $k = 1$, und $x^2 + y^2 = p$ wie behauptet. ■

Anmerkung 3.13

Der Beweis liefert keine gute Konstruktion von x, y mit $x^2 + y^2 = p$, da er auf dem nicht konstruktiven Schubfachprinzip beruht.

12 Die diophantische Gleichung $X^2 + Y^2 = n$

Wir können jetzt Fermats Lösbarkeitsaussage zur diophantischen Gleichung

$$X^2 + Y^2 = n$$

für beliebige positive ganze Zahlen n beweisen.

Lemma 3.14

Sind $n_1, n_2 \in \mathbb{Z}_{>0}$ positive ganze Zahlen, die jeweils Summe zweier Quadrate sind, dann ist auch ihr Produkt $n_1 \cdot n_2$ Summe zweier Quadrate.

Beweis: Schreibe $n_1 = a_1^2 + b_1^2$ und $n_2 = a_2^2 + b_2^2$ mit $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Dann gilt:

$$n_1 \cdot n_2 = (a_1^2 + b_1^2) \cdot (a_2^2 + b_2^2) = (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + b_1 a_2)^2$$

Setze also $c := a_1 a_2 - b_1 b_2$ und $d := a_1 b_2 + b_1 a_2$ und es gilt $n_1 \cdot n_2 = c^2 + d^2$, wobei $c, d \in \mathbb{Z}$. ■

Satz 3.15 (Fermat)

Sei $n \in \mathbb{Z}_{>0}$ eine ganze Zahl. Die folgenden Aussagen sind äquivalent.

- (a) Es gibt $(x, y) \in \mathbb{Z}^2$ mit $x^2 + y^2 = n$, d.h., n ist Summe zweier Quadrate.
- (b) Für jede Primzahl p mit $p \mid n$ und $p \equiv 3 \pmod{4}$ ist $n_p(n)$ gerade.

Anders gesagt: Die diophantische Gleichung $X^2 + Y^2 = n$ hat genau dann eine Lösung, wenn n eine Primfaktorzerlegung der Form

$$n = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot q_1^{2\beta_1} \cdots q_r^{2\beta_r}$$

besitzt mit $\alpha \in \mathbb{Z}_{\geq 0}$, Primzahlen $p_i \equiv 1 \pmod{4}$ und $q_j \equiv 3 \pmod{4}$, und $\alpha_i, \beta_j \in \mathbb{Z}_{>0}$ für alle $1 \leq i \leq k$ ($k \in \mathbb{Z}_{\geq 0}$) und für alle $1 \leq j \leq r$ ($r \in \mathbb{Z}_{\geq 0}$). (Dies bedeutet, dass die Fälle $k = 0$, $r = 0$ und $k = r = 0$ sind dabei erlaubt!)

Beweis:

(a)⇒(b): Sei n Summe zweier Quadrate, etwa $n = x^2 + y^2$ mit $x, y \in \mathbb{Z}$ und wir nehmen an, dass es eine Primzahl $p \in \mathbb{P}$ gäbe mit $p \mid n$, $p \equiv 3 \pmod{4}$ und $n_p(n)$ ungerade. Zudem können wir annehmen, dass n minimal mit dieser Eigenschaft ist. Wir unterscheiden zwei Fälle.

- **1. Fall:** $p \mid x$. Wegen $p \mid n$ gilt auch $p \mid y$ und sogar $p^2 \mid x^2$, $p^2 \mid y^2$, und daher $p^2 \mid n$. Aber dann ist auch

$$\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$$

Summe zweier Quadrate mit $1 \leq n_p\left(\frac{n}{p^2}\right) = n_p(n) - 2$ ungerade, im Widerspruch zur Minimalität von n .

- **2. Fall:** $p \nmid x$. Wegen $\text{ggT}(p, x) = 1$ ist $[x] \in (\mathbb{Z}/p\mathbb{Z})^\times$ (eine Einheit). Also existiert $z \in \mathbb{Z}$ mit $x \cdot z \equiv 1 \pmod{p}$ und damit ist

$$1 + (yz)^2 \equiv (xz)^2 + (yz)^2 = z^2(x^2 + y^2) = z^2n \equiv 0 \pmod{p}.$$

Damit gilt

$$(yz)^2 \equiv (-1) \pmod{p}.$$

Es folgt dann aus dem Satz von Fermat 3.12, dass $p \equiv 1 \pmod{4}$. Widerspruch!

(b)⇒(a): Wir nehmen nun an, dass für jede Primzahl p mit $p \mid n$ und $p \equiv 3 \pmod{4}$ die Zahl $n_p(n)$ gerade ist. Dann hat n eine Primfaktorzerlegung der Form

$$n = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot q_1^{2\beta_1} \cdots q_r^{2\beta_r}$$

(wie oben). Nach dem Satz von Fermat 3.12 sind p_1, \dots, p_k jeweils Summe zweier Quadrate. Ebenso $2 = 1^2 + 1^2$. Zudem ist auch

$$q_1^{2\beta_1} \cdots q_r^{2\beta_r} = (q_1^{\beta_1} \cdots q_r^{\beta_r})^2 + 0^2$$

Summe zweier Quadrate. Somit ist n das Produkt von Zahlen, die jeweils Summe zweier Quadrate sind, und ist damit selbst Summe zweier Quadrate nach Lemma 3.14. ■

13 Existenz unendlich vieler Primzahlen p mit $p \equiv \pm 1 \pmod{4}$

Zum Abschluss dieses Kapitels wollen wir noch zeigen, dass es unendlich viele Primzahlen $p \in \mathbb{P}$ mit $p \equiv \pm 1 \pmod{4}$ gibt.

Anmerkung 3.16

Die Tatsache, dass es unendlich viele Primzahlen $p \in \mathbb{P}$ mit $p \equiv -1 \equiv 3 \pmod{4}$ gibt ist einfacher zu beweisen:

Beweis: Sei P die Menge der Primzahlen der Form $4k + 3$ ($k \in \mathbb{Z}$). Wegen $3 \in P$ ist $P \neq \emptyset$. Wir nehmen an, dass $Q = \{q_1, \dots, q_r\} \subseteq P$ eine endliche Teilmenge ist. Betrachte die Zahl

$$m := 4q_1 \cdots q_r - 1 = 4(q_1 \cdots q_r - 1) + 3 \equiv 3 \pmod{4}$$

Sei also $p_1 \cdots p_s$ eine Primfaktorzerlegung von m . Da m ungerade ist, müssen auch alle Primteiler von m ungerade sein. Daraus folgt, dass für $1 \leq i \leq s$ entweder $p_i \equiv 1 \pmod{4}$ oder $p_i \equiv 3 \pmod{4}$ ist. Wäre $p_i \equiv 1 \pmod{4}$ für alle $1 \leq i \leq s$, so gelte in $\mathbb{Z}/4\mathbb{Z}$:

$$[m] = [p_1 \cdots p_s] = [p_1] \cdots [p_s] = [1] \cdots [1] = [1],$$

da $[1]$ das Einselement von $\mathbb{Z}/4\mathbb{Z}$ ist. Damit wäre $m \equiv 1 \pmod{4}$: Widerspruch. Also existiert eine Primzahl q mit $q \mid m$ und $q = 4k + 3$. Aber $q_i \nmid m$ für $i = 1, \dots, r$, also $q \in P \setminus Q$. Daher ist Q eine echte Teilmenge von P , und P notwendig unendlich. ■

Als Nächstes betrachten wir die Primzahlen, die kongruent zu 1 modulo 4 sind.

Dazu brauchen wir die *Reduktion modulo p* von Polynomen in $\mathbb{Z}[X]$, d.h. den Ringhomomorphismus

$$\begin{aligned} \Phi_p: \quad \mathbb{Z}[X] &\longrightarrow (\mathbb{Z}/p\mathbb{Z})[X] \\ f = \sum_{k=0}^n a_k \cdot X^k &\mapsto \Phi_p(f) := \sum_{k=0}^n [a_k] \cdot X^k, \end{aligned}$$

und die folgende Tatsache.

Anmerkung 3.17

Für ein Polynom $f \in \mathbb{Z}[X]$ mit $\deg(f) \geq 1$ und $r \in \mathbb{Z}$ gilt:

$$\#\{z \in \mathbb{Z} \mid f(z) = r\} \leq \deg(f)$$

Dies gilt sicherlich in $\mathbb{Q}[X]$, da \mathbb{Q} ein Körper ist, also auch in \mathbb{Z} . (Siehe die AGS.)

Satz 3.18

Sei $f \in \mathbb{Z}[X]$ mit $\deg(f) \geq 1$. Dann existiert unendlich viele Primzahlen $p \in \mathbb{P}$, so dass $\Phi_p(f) \in (\mathbb{Z}/p\mathbb{Z})[X]$ eine Nullstelle in $(\mathbb{Z}/p\mathbb{Z})$ besitzt.

Beweis: Da $\deg(f) \geq 1$ ist, hat f die Form $f = \sum_{k=0}^n a_k \cdot X^k$ mit $n \geq 1$, $a_i \in \mathbb{Z}$ ($0 \leq i \leq n$) und $a_n \neq 0$.

1. **Fall:** f besitzt eine Nullstelle α in \mathbb{Z} . Dann ist offensichtlich die Restklasse $[\alpha] \in \mathbb{Z}/p\mathbb{Z}$ eine Nullstelle von $\Phi_p(f)$ für jede Primzahl $p \in \mathbb{P}$. Die Behauptung folgt also aus $|\mathbb{P}| = \infty$.
2. **Fall:** f besitzt keine Nullstelle in \mathbb{Z} . Insbesondere ist dann $a_0 = f(0) \neq 0$.
Wir zeigen nun per Induktion, dass es unendlich viele Primzahlen $p \in \mathbb{P}$ gibt, so dass $\Phi_p(f)$ eine Nullstelle in $\mathbb{Z}/p\mathbb{Z}$ besitzt. Da f ein Polynom ist, existiert $\alpha \in \mathbb{Z}$ genügend groß, so dass $|f(\alpha)| > 1$. Insbesondere ist dann $\Phi_p(f)([\alpha]) = [0] \in \mathbb{Z}/p\mathbb{Z}$ für alle Primteiler p von $f(\alpha)$. Wir dürfen also

annehmen, dass $p_1, \dots, p_r \in \mathbb{P}$ mit $r \in \mathbb{Z}_{>0}$ schon gefunden sind, so dass $\Phi_{p_i}(f)$ eine Nullstelle in $\mathbb{Z}/p_i\mathbb{Z} \forall 1 \leq i \leq r$ besitzt. Dann betrachten wir das Polynom

$$\tilde{f} := f \left(a_0 \cdot \left(\prod_{i=1}^r p_i \right) \cdot X \right) \in \mathbb{Z}[X].$$

Es gilt

$$\tilde{f} = a_0 \cdot g$$

mit

$$g = \sum_{k=0}^n b_k \cdot X^k \quad \text{wobei} \quad \prod_{i=1}^r p_i \mid b_k \quad \forall 1 \leq k \leq n \quad \text{und} \quad b_0 = 1.$$

Also ist \tilde{f} ein Polynom, bei dem jeder Koeffizient durch $a_0 \neq 0$ teilbar ist, so dass $g = \frac{1}{a_0} \tilde{f} \in \mathbb{Z}[X]$ mit konstantem Term 1 ist. Nach Anmerkung 3.17 gibt es nun ein $z \in \mathbb{Z}$, so dass $g(z) \notin \{-1, 0, 1\}$. Sei also q eine Primzahl mit $q \mid g(z)$, d.h.

$$\Phi_q(g)([z]) = [g(z)] = [0] \in \mathbb{Z}/q\mathbb{Z}.$$

Dann gilt

$$\Phi_q(f)([a_0 \cdot \prod_{i=1}^r p_i \cdot z]) = [a_0] \cdot \Phi_q(g)([z]) = [a_0] \cdot [0] \in \mathbb{Z}/q\mathbb{Z}.$$

Damit hat f modulo q dann ebenfalls eine Nullstelle. Da alle Koeffizienten von g (bis auf den konstanten Term) durch p_i für alle $1 \leq i \leq r$ teilbar sind, gilt $q \neq p_i$ für alle $1 \leq i \leq r$. ■

Folgerung 3.19

Es gibt unendlich viele Primzahlen $p \in \mathbb{P}$ mit $p \equiv 1 \pmod{4}$.

Beweis: Nach Satz 3.18 gibt es unendlich viele Primzahlen p , so dass $X^2 + [1] \in \mathbb{Z}/p\mathbb{Z}[X]$ eine Nullstelle in $\mathbb{Z}/p\mathbb{Z}$ hat. Aus dem Satz von Fermat (Satz 3.12) folgt dann, dass es unendlich viele Primzahlen p mit $p \equiv 1 \pmod{4}$ gibt. ■

Die Eulersche φ -Funktion bildet die Grundlage für eines der bekanntesten und meistbenutzten Kryptosysteme: das **RSA-Verfahren**. Es wurde 1977/78 von R. Rivest, A. Shamir und L. Adleman am MIT entwickelt.

14 Das Prinzip

Wir betrachten das folgende Problem:

Problem 4.1

Bob (der Sender) will Alice (der Empfänger) eine Nachricht schicken, ohne dass Betzi (ein Abfänger) diese lesen oder unbemerkt verändern kann, falls er die Nachricht abfängt.

Die Lösung ist, die Nachricht zu verschlüsseln. Genauer: im RSA-Verfahren besteht die Verschlüsselung aus zwei Schlüsseln:

- einem öffentlichen, und
- einem privaten Schlüssel.

Mit dem öffentlichen Schlüssel kann man Nachrichten verschlüsseln, aber nicht entschlüsseln. Deshalb wird dieser Schlüssel öffentlich zur Verfügung gestellt, z. B. im Internet. Hier kann den Schlüssel dann jeder benutzen, um Nachrichten zu verschlüsseln, die aber nur der Empfänger (= derjenige, der den öffentlichen Schlüssel anbietet) wieder entschlüsseln kann. Zum Entschlüsseln braucht man den privaten Schlüssel, und den kennt nur der Empfänger.

15 Das RSA-Verfahren

Das RSA-Verfahren basiert auf der folgenden mathematischen Aussage:

Satz 4.2

Seien $p, q \in \mathbb{P}$ zwei verschiedene Primzahlen und setze $N := p \cdot q$. Ferner seien $e, d \in \mathbb{Z}$ mit $0 < e, d < N$, $\text{ggT}(e, \varphi(N)) = 1$ und $d \cdot e \equiv 1 \pmod{\varphi(N)}$. Dann gilt für jedes $m \in \mathbb{Z}$ mit $0 < m < N$, dass

$$(m^e)^d \equiv m \pmod{N}$$

ist.

Beweis: Zunächst folgt aus $d \cdot e \equiv 1 \pmod{\varphi(N)}$, dass es $k \in \mathbb{Z}$ mit $1 = de + k\varphi(N)$ existiert. Somit ist

$$(m^e)^d = m^{1-k\varphi(N)} = m \cdot (m^{\varphi(N)})^{-k}.$$

Wegen $m < N = p \cdot q$ gilt $\text{ggT}(m, N) \in \{1, p, q\}$, sodass wir drei Fälle unterscheiden können.

1. Fall: $\text{ggT}(m, N) = 1$.

Wegen $\text{ggT}(m, N) = 1$ folgt aus dem Satz von Euler, dass

$$m^{\varphi(N)} \equiv 1 \pmod{N}.$$

Also ist

$$(m^e)^d = m \cdot (m^{\varphi(N)})^{-k} \equiv m \cdot 1^{-k} = m \cdot 1 = m \pmod{N}.$$

2. Fall: $\text{ggT}(m, N) = p$. Wir benutzen hier den Chinesischen Restsatz. Zunächst impliziert $m \equiv 0 \pmod{p}$, dass

$$m^{ed} \equiv 0 \equiv m \pmod{p}$$

ist. Wegen $\text{ggT}(m, N) = p$ gilt $q \nmid m$ und es folgt aus dem Satz von Euler, dass

$$m^{q-1} \equiv 1 \pmod{q}$$

ist. Aus $\varphi(N) = (p-1)(q-1)$ folgt dann

$$m^{ed} = m \cdot (m^{\varphi(N)})^{-k} = m \cdot (m^{(q-1)})^{-k(p-1)} \equiv m \cdot 1 = m \pmod{q}.$$

Mit dem Chinesischen Restsatz erhalten wir also $m^{ed} \equiv m \pmod{p \cdot q}$, d.h. modulo N , wie behauptet.

3. Fall: $\text{ggT}(m, N) = q$. Analog zum 2. Fall! ■

16 Das RSA-Verfahren in der Praxis

Das RSA-Verfahren.

1. Schritt: Erzeugung des öffentlichen Schlüssels. (Alice)

1a. Eine Schranke N ermitteln:

Wähle $p \neq q \in \mathbb{P}$ zwei (sehr große) Primzahlen;
Setze $N := p \cdot q$.

1b. Eine Zahl e ermitteln:

Berechne $\varphi(N) = (p-1) \cdot (q-1)$;
Wähle eine beliebige Zahl $1 < e < \varphi(N)$ mit $\text{ggT}(e, \varphi(N)) = 1$.

Der **öffentliche Schlüssel** ist dann das 2-Tupel (e, N) . Dieser wird (von Alice) veröffentlicht (z.B. im Internet). (\triangle Die Primzahlen p und q müssen geheim bleiben.)

2. Schritt: Erzeugung des privaten Schlüssels (Alice)

2a. Berechne mit Hilfe des euklidischen Algorithmus eine Zahl d mit

$$e \cdot d \equiv 1 \pmod{\varphi(N)}.$$

Der **private Schlüssel** ist dann das 2-Tupel (d, N) . Dieser muss geheim bleiben.

3. Schritt: Nachricht verschlüsseln. (Bob mit dem öffentlichen Schlüssel (e, N))

3a. Die Nachricht $1 < m < N$ wird mit ihrer Restklasse $[m] \in \mathbb{Z}/N\mathbb{Z}$ identifiziert.

3b. Die Nachricht wird durch

$$s := m^e \pmod{N}$$

verschlüsselt.

Dieses s schickt Bob dann an Alice.

4. Schritt: Nachricht entschlüsseln. (Alice mit dem privaten Schlüssel (d, N))

4a. Die Nachricht wird nach Konstruktion von d durch

$$m := s^d \pmod{N}$$

entschlüsselt.

Beispiel 12

Sei $p = 47$ und $q = 71$. Somit ist $N = p \cdot q = 3337$ und $\varphi(N) = (p - 1)(q - 1) = 46 \cdot 70 = 3220$. Abhängig von $\varphi(N)$ wird eine zufällige Zahl e mit $\varphi(N) > e > 1$ gewählt, wobei $\text{ggT}(e, \varphi(N)) = 1$ sein muss. Wir wählen zum Beispiel

$$e = 79.$$

Aus e und $\varphi(N)$ können wir nun d mit dem euklidischen Algorithmus ausrechnen:

$$de \equiv 1 \pmod{\varphi(N)} \iff [d]_{3220} = [e]_{3220} = [79]_{3220} \iff d \equiv 1019 \pmod{3220}.$$

Somit haben wir die beiden Schlüssel:

Der öffentliche Schlüssel = $(e, N) = (79, 3337)$; und

der private Schlüssel = $(d, N) = (1019, 3337)$.

Bob kann nun seine Nachricht

$$m = 688$$

verschlüsseln und Alice schicken:

$$s = m^e = 688^{79} \equiv 1570 \pmod{3337}.$$

Alice kann dann dieses Chifftrat entschlüsseln. Dafür verwendet sie den privaten Schlüssel und sie bekommt:

$$m \equiv s^d \pmod{N} \equiv 1570^{1019} \pmod{3337} \equiv 688 \pmod{3337}$$

Anmerkung 4.3

(a) Das RSA-Verfahren verschlüsselt und entschlüsselt nur Zahlen in Zahlen, daher muss erst der Klartext mit einem öffentlich bekannten Alphabet in eine Zahlenfolge (numerical Encoding) übersetzt werden.

(b) **Beispiele von Anwendungsgebiete:**

- Internet- und Telefonie-Infrastruktur: X.509-Zertifikate
- E-Mail-Verschlüsselung: OpenPGP, S/MIME
- Authentifizierung SIM-Karten
- Kartenzahlung: EMV
- RFID Chip auf dem deutschen Reisepass
- Electronic Banking: HBCI
- Übertragungs-Protokolle: IPsec, TLS, SSH, WASTE

17 Das RSA-Verfahren: Sicherheit und Sicherheitslücken

Die Sicherheit des RSA-Verfahrens beruht auf dem Problem, Zahlen der Form $N = pq$ mit $p, q \in \mathbb{P}$ zu faktorisieren. Bisher hat es noch keiner geschafft, diese Zahlen effektiv und schnell zu zerlegen. Deswegen ist es wichtig *große* Primzahlen $p, q \in \mathbb{P}$ zu wählen. Selbst mit einem Computer braucht man in der Praxis bis zu einem Jahr, falls $pq \lesssim 10^{150}$ gilt. Für $pq \simeq 10^{300}$ würde ein Abfänger viele tausend Jahre und viele tausend Computer benötigen, um die Faktorisierung zu erreichen.

Problem/Nachteil: Es ist aber auch nicht bewiesen, dass es sich bei der Primfaktorzerlegung von $N = pq$ um ein prinzipiell schwieriges Problem handelt!

Satz 4.4 (*Sicherheit des RSA-Verfahrens*)

Seien $p, q \in \mathbb{P}$ zwei verschiedene Primzahlen und setze $N := p \cdot q$. Dann sind die folgenden Aussagen äquivalent:

- (i) N und $\varphi(N)$ sind bekannt; und
- (ii) p und q sind bekannt.

Beweis:

(i) \Rightarrow (ii): Es gilt

$$\varphi(N) = (p-1) \cdot (q-1) = p \cdot q - (p+q) + 1 = (N+1) - (p+q).$$

Somit ist $(p+q) = N+1-\varphi(N)$ bekannt, da N und $\varphi(N)$ bekannt sind. Daher ist auch das Polynom $X^2 - (p+q)X + N \in \mathbb{Z}[X]$ bekannt. Aber p und q sind die Nullstellen von diesem Polynom, da

$$X^2 - (p+q)X + N = (X-p) \cdot (X-q)$$

ist. Diese lassen sich leicht berechnen! D.h. mit den üblichen Formeln.

(ii) \Rightarrow (i): Wenn p und q bekannt sind, so sind offensichtlich auch $N = p \cdot q$ und $\varphi(N) = (p-1) \cdot (q-1)$. ■

Anmerkung 4.5

Der folgende Algorithmus zeigt, dass es extrem wichtig ist, dass die Zahl d geheim bleibt. Wenn ein Abfänger die Zahl d besitzt, so kann er N faktorisieren und Nachrichten entschlüsseln bzw. verändern. (Siehe Aufgabe 1 auf Blatt 7.)

Algorithmus 1 Faktorisierung des Modulus N unter Benutzung von e und d

- 1: **Input:** Modulus N , privater Schlüssel (d, N) , öffentlicher Schlüssel (e, N) .
 - 2: **Output:** Primzahlen p und q mit $N = pq$.
 - 3: Berechne $k := ed - 1$.
 - 4: Entferne gerade Faktoren: $k = 2^s \cdot t$ mit t ungerade.
 - 5: Setze $a := 2$.
 - 6: **while true do**
 - 7: $b = a^t \pmod N$
 - 8: **for** ℓ in $0 : s$ **do**
 - 9: Berechne $p = \text{ggT}(b^{2^\ell}, N)$
 - 10: **if** $1 < p$ und p ist prim **then**
 - 11: **return** p und $q = N/p$
 - 12: **else**
 - 13: Wähle neues $a \in \mathbb{Z}/N\mathbb{Z}$ zufällig.
 - 14: **end if**
 - 15: **end for**
 - 16: **end while**
-

18 Das Rabin-Verfahren*

Das Rabin-Kryptosystem ist ein weiteres Verfahren der Public-Key-Kryptographie, das Ähnlichkeiten mit dem RSA-Verfahren hat. Die Vorteile und Nachteile sind die folgenden.

VORTEILE:

Es lässt sich beweisen, dass das Brechen des Verfahrens äquivalent zur Faktorisierung ist großer Zahlen $N = p \cdot q$ ist.

NACHTEILE: Die Entschlüsselung ist nicht eindeutig!! (Bis 4 Möglichkeiten!) Es gibt kaum Anwendungen in der Praxis.

1. Schritt: Erzeugung der Schlüssel. (Alice)

- 1a. Alice wählt $p \neq q \in \mathbb{P}$ zwei (sehr große) Primzahlen mit $p \equiv q \equiv 1 \pmod 4$ und setzt $N := p \cdot q$.

- 1b. Der öffentliche Schlüssel ist die Zahl N .
- 1c. Der private Schlüssel ist das Paar $N := (p, q)$. Dieser muss geheim bleiben.

2. Schritt: Nachricht verschlüsseln. (Bob mit dem öffentlichen Schlüssel N)

- 2a. Bob verschlüsselt seine Nachricht $[m]_N \in \mathbb{Z}/N\mathbb{Z}$ (mit $[m]_N \neq [0]_N$) durch Verwendung der Abbildung

$$e : \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}, [m]_N \mapsto e([m]_N) := [m]_N^2$$

$[m] \in \mathbb{Z}/N\mathbb{Z}$ identifiziert.

- 2b. Bob schickt $e([m]_N)$ an Alice.

3. Schritt: Nachricht entschlüsseln. (Alice mit dem privaten Schlüssel (p, q))

- 3a. Alice empfängt die Nachricht $e([m]_N) \in \mathbb{Z}/N\mathbb{Z}$. Sie setzt $[y]_N := e([m]_N)$ mit $1 \leq y \leq N$. Die Nachricht wird durch

$$\left([y]_p^{\frac{p+1}{4}}, [y]_q^{\frac{p+1}{4}} \right) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/N\mathbb{Z}$$

entschlüsselt. Dies ist eine der **höchstens vier Quadratwurzeln** von der empfangenen Nachricht $[y]_N$.

Wir müssen also die Quadratwurzeln der Elemente aus $\mathbb{Z}/N\mathbb{Z}$ verstehen.

Anmerkung 4.6

- (a) Schreibe

$$\begin{aligned} \Psi : \mathbb{Z}/N\mathbb{Z} &\longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ [a]_N &\mapsto ([a]_p, [a]_q) \end{aligned}$$

für den Ring-Isomorphismus aus dem chinesischen Restsatz.

Da p, q ungerade Primzahlen sind, so sind $\mathbb{Z}/p\mathbb{Z}$ und $\mathbb{Z}/q\mathbb{Z}$ Körper und es gibt genau zwei Quadratwurzeln von $[1]_p$ bzw. $[1]_q$ in $\mathbb{Z}/p\mathbb{Z}$ bzw. $\mathbb{Z}/q\mathbb{Z}$, d.h. $[\pm 1]_p$ bzw. $[\pm 1]_q$. (Es sind die Nullstellen vom Polynom $X^2 - [1]_p$ bzw. $X^2 - [1]_q$.)

Somit hat $1_{\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}} = ([1]_p, [1]_q)$ genau **vier** Quadratwurzeln in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$:

$$([1]_p, [1]_q), ([-1]_p, [1]_q), ([1]_p, [-1]_q), \text{ und } ([-1]_p, [-1]_q).$$

In $\mathbb{Z}/N\mathbb{Z}$ gibt es also auch genau **vier** Quadratwurzeln von $[1]_N$, nämlich die Urbilder der oben angegebenen Elemente:

$$\begin{aligned} \Psi^{-1}([1]_p, [1]_q) &= [1]_N \\ \Psi^{-1}([-1]_p, [-1]_q) &= [-1]_N \\ \Psi^{-1}([-1]_p, [1]_q) &=: [\omega]_N \\ \Psi^{-1}([1]_p, [-1]_q) &= [-\omega]_N \end{aligned}$$

(b) Sei nun $[y]_N \in \mathbb{Z}/N\mathbb{Z}$ beliebig.

(c) Die Quadratwurzeln von $[y]_N$ in $\mathbb{Z}/N\mathbb{Z}$ entsprechen die Quadratwurzeln von

$$\Psi([y]_N) = ([y]_p, [y]_q) \text{ in } \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z},$$

d.h. die Paare $([m]_p, [m]_q) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ mit $[m]_p^2 = [y]_p$ und $[m]_q^2 = [y]_q$. Nun hat das Polynom $X^2 - [y]_p$ bzw. $X^2 - [y]_q$ höchstens zwei Nullstellen in $\mathbb{Z}/p\mathbb{Z}$ bzw. $\mathbb{Z}/q\mathbb{Z}$, so dass es höchstens vier Quadratwurzeln von $[y]_N$ in $\mathbb{Z}/N\mathbb{Z}$ existieren kann.

Nun, ist $[m]_N$ eine Quadratwurzel von $[y]_N$ in $\mathbb{Z}/N\mathbb{Z}$, so sind die anderen Quadratwurzeln von $[y]_N$ gegeben durch

$$-[m]_N, [\omega]_N \cdot [m]_N, \text{ und } -[\omega]_N \cdot [m]_N,$$

da $(-[m]_N)^2 = ([\omega]_N \cdot [m]_N)^2 = (-[\omega]_N \cdot [m]_N)^2 = [m]_N^2 = [y]_N$.

⚠ Wiederholungen in dieser Liste sind möglich!

(d) **Folgerung:** Die Verschlüsselungsfunktion $e : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}, [m]_N \mapsto [m]_N^2$ ist nicht injektiv! Daher ist die Entschlüsselung von Nachrichten nicht eindeutig! Es kann in der Tat bis vier Elemente aus $\mathbb{Z}/N\mathbb{Z}$ geben, die auf $[m]_N^2$ abgebildet werden. Siehe Aufgabe 1 auf Blatt 7 für ein Beispiel mit $N = 15$.

Lemma 4.7 (Korrektheit des Rabin-Verfahrens)

Sei $[y]_N := e([m]_N) = [m]_N^2$ mit $0 < y < N$ die empfangene Nachricht. Dann gilt

$$\left([y]_p^{\frac{p+1}{4}}, [y]_q^{\frac{q+1}{4}} \right)^2 = ([y]_p, [y]_q) \text{ in } \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/N\mathbb{Z}.$$

Beweis: Der kleine Satz von Fermat liefert $[m]_p^p = [m]_p$ in $\mathbb{Z}/p\mathbb{Z}$ und $[m]_q^q = [m]_q$ in $\mathbb{Z}/q\mathbb{Z}$. Somit gilt

$$\begin{aligned} \left([y]_p^{\frac{p+1}{4}}, [y]_q^{\frac{q+1}{4}} \right)^2 &= \left(([y]_p^{\frac{p+1}{4}})^2, ([y]_q^{\frac{q+1}{4}})^2 \right) \\ &= \left([y]_p^{\frac{p+1}{2}}, [y]_q^{\frac{q+1}{2}} \right) \\ &= \left(([m]_p^2)^{\frac{p+1}{2}}, ([m]_q^2)^{\frac{q+1}{2}} \right) \\ &= ([m]_p^{p+1}, [m]_q^{q+1}) \\ &= ([m]_p^p \cdot [m]_p, [m]_q^q \cdot [m]_q) \\ &= ([m]_p \cdot [m]_p, [m]_q \cdot [m]_q) \\ &= ([m]_p^2, [m]_q^2) \\ &= ([y]_p, [y]_q). \end{aligned}$$



Anmerkung 4.8 (Sicherheit des Rabin-Verfahrens)

(a) Zunächst ist es klar, dass ein Einbrecher das Rabin-Verfahren brechen kann, wenn er die Faktorisierung $N = p \cdot q$ kennt.

(b) Anders als beim RSA-Verfahren, gilt auch die Umkehrung! Angenommen, ein Angreifer das Verfahren brechen kann, d.h. er kann zu jedem Quadrat in $\mathbb{Z}/N\mathbb{Z}$ eine Quadratwurzel berechnen (und als Folgerung alle andere Quadratwurzeln auch), so kann er N als $N = p \cdot q$ mit $p, q \in \mathbb{P}$ faktorisieren.

(1.) Er wählt zufällig eine natürliche Zahl x mit $1 < x < N$.

Falls $\text{ggT}(N, x) \neq 1$, so hat er ein echter Primteiler gefunden. O.B.d.A. $x = p$ und $q = N/x$.

(2.) Er kann also annehmen, dass $\text{ggT}(N, x) = 1$. Er berechnet dann $x^2 \pmod{N}$ und eine Quadratwurzel $[m]_N$ von $[x^2]_N$.

Wir haben gesehen, dass es höchstens vier Quadratwurzeln gibt und diese sind die Lösungen von den folgenden Gleichungssystemen:

- (i) $m \equiv x \pmod{p}$ und $m \equiv x \pmod{1}$;
- (ii) $m \equiv x \pmod{p}$ und $m \equiv -x \pmod{1}$;
- (iii) $m \equiv -x \pmod{p}$ und $m \equiv x \pmod{1}$; und
- (iv) $m \equiv -x \pmod{p}$ und $m \equiv -x \pmod{1}$.

(3.) Er beobachtet:

- (i) liefert $\text{ggT}(N, m - x) = p \cdot q$;
- (ii) liefert $\text{ggT}(N, m - x) = p$;
- (iii) liefert $\text{ggT}(N, m - x) = q$; und
- (iv) liefert $\text{ggT}(N, m - x) = 1$;

Somit hat der Angreifer gewonnen, wenn er im Fall (ii) oder (iii) ist, da er ein Primteiler von N gefunden hat.

Sonst führt er die gleiche Prozedur mit einem anderen x zwischen 1 und N , zufällig gewählt! Da x zufällig gewählt wird, treten die Fälle (i) bis (iv) mit gleicher Wahrscheinlichkeit auf, d.h. $1/4$. Somit faktorisiert jeder Durchlauf vom Algorithmus N mit Wahrscheinlichkeit $1/2$ und nach k Durchläufen ist N mit Wahrscheinlichkeit $1 - \frac{1}{2^k}$ faktorisiert. Für $k \rightarrow \infty$ konvergiert diese Zahl nach 1. D.h. nach genügend vielen Durchläufen muss einer der Fälle (ii) oder (iii) auftreten und N ist faktorisiert.

Kapitel 5: Die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ und Primitivwurzeln modulo n

In diesem Kapitel haben wir zwei Ziele:

Ziel 1

Multiplikative Struktur der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ von $\mathbb{Z}/n\mathbb{Z}$ für eine beliebige positive Zahl $n \in \mathbb{Z}_{>0}$.

Ziel 2

Existenz von Primitivwurzeln modulo n entweder beweisen oder widerlegen.

Definition 5.1 (Primitivwurzel modulo n)

Eine natürliche Zahl $a \in \mathbb{N}$ heißt **Primitivwurzel modulo** $n \in \mathbb{N}$, wenn

$$(\mathbb{Z}/n\mathbb{Z})^\times = \langle [a]_n \rangle = \{[a]_n, \dots, [a]_n^{\varphi(n)}\},$$

d.h. die Ordnung von $[a]_n$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ ist $\varphi(n)$.

Beispiel 13

Durch Probieren erhalten wir modulo 7:

Für $[2]_7$ gilt: $[2]_7^2 = [4]_7$, $[2]_7^3 = [1]_7$, also ist 2 keine Primitivwurzel modulo 7, da $\varphi(7) = 6$ ist. Aber 3 ist eine Primitivwurzel modulo 7, denn

$$\{[3]_7^1, \dots, [3]_7^6\} = \{[3]_7^6, [3]_7^2, [3]_7^4, [3]_7^1, [3]_7^5, [3]_7^3\} = \{[3]_7, [2]_7, [6]_7, [4]_7, [5]_7, [1]_7\} = (\mathbb{Z}/7\mathbb{Z})^\times.$$

Anmerkung 5.2

Wir haben schon beobachtet, dass für $m_1, m_2 \in \mathbb{Z}_{>0}$ mit $\text{ggT}(m_1, m_2) = 1$ der Chinesische Restsatz einen Ring-Isomorphismus

$$\begin{aligned} \Phi: \mathbb{Z}/(m_1 m_2)\mathbb{Z} &\longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \\ [a]_{m_1 m_2} &\longmapsto ([a]_{m_1}, [a]_{m_2}) \end{aligned}$$

liefert, so dass die Einschränkung von Φ auf die Einheiten $(\mathbb{Z}/(m_1 m_2)\mathbb{Z})^\times$ die Existenz eines Gruppenisomorphismus

$$\begin{aligned} \Phi: (\mathbb{Z}/(m_1 m_2)\mathbb{Z})^\times &\longrightarrow (\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times \\ [a]_{m_1 m_2} &\longmapsto ([a]_{m_1}, [a]_{m_2}) \end{aligned}$$

liefert.

Ist nun $n = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die Primfaktorzerlegung von $n \in \mathbb{Z}_{>0}$ (mit ungeraden paarweise verschiedenen Primzahlen p_1, \dots, p_r , $\alpha \in \mathbb{N}_0, \alpha_1, \dots, \alpha_r \in \mathbb{N}$). Dann liefert den Chinesischen Restsatz einen Gruppenisomorphismus

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \times (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times.$$

Ziel 2 werden wir als Konsequenz von Ziel 1 erreichen. Zu Ziel 1 benötigen wir zuerst die Struktur der Gruppe $(\mathbb{Z}/q^r\mathbb{Z})$ für eine beliebige Primzahl q und $r \in \mathbb{N}$.

16 Die Einheitengruppe $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$

Als ersten Schritt untersuchen wir die Einheitengruppe $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ für 2-Potenzen 2^α . In diesem Abschnitt ist stets $\alpha \in \mathbb{N}$. Für kleine α beobachten wir Folgendes:

Beispiel 14

- Für $\alpha = 1$ ist $(\mathbb{Z}/2\mathbb{Z})^\times = \{[1]_2\} = \langle [1]_2 \rangle$ zyklisch der Ordnung 1.
- Für $\alpha = 2$ ist $(\mathbb{Z}/4\mathbb{Z})^\times = \{[1]_2, [3]_2\} = \langle [3]_2 \rangle$ zyklisch der Ordnung 2.
- Für $\alpha = 3$ gilt

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$$

wobei $[3]_8^2 = [1]_8$, $[5]_8^2 = [1]_8$, $[7]_8^2 = [1]_8$. Also haben $[3]_8, [5]_8, [7]_8$ Ordnung 2, und $(\mathbb{Z}/8\mathbb{Z})^\times$ ist nicht zyklisch. Es ist die kleinsche Viergruppe.

Bemerkung 5.3

Sind $a \in \mathbb{N}$ ungerade und $\alpha \in \mathbb{N}_{\geq 3}$, so gilt

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}.$$

Beweis: Per Induktion nach α .

Für $\alpha = 3$ behaupten wir, dass $a^2 \equiv 1 \pmod{8}$ für alle ungeraden a ist. Dies gilt nach obigem Beispiel. Sei die Behauptung nun für $\alpha - 1$ bewiesen. Dann ist demnach

$$a^{2^{\alpha-3}} \equiv 1 \pmod{2^{\alpha-1}},$$

d.h., es existiert ein $t \in \mathbb{N}$ mit

$$a^{2^{\alpha-3}} = 1 + 2^{\alpha-1}t.$$

Quadrieren liefert

$$a^{2^{\alpha-2}} = (1 + 2^{\alpha-1}t)^2 = 1 + 2^\alpha t + 2^{2\alpha-2}t^2 \equiv 1 \pmod{2^\alpha}. \quad \blacksquare$$

Anmerkung 5.4

Da gerade $a \in \mathbb{N}$ nicht invertierbar modulo 2^α sind, besagt Bemerkung 5.3, dass alle Elemente

$[a]_{2^\alpha} \in (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ für $\alpha \geq 3$ höchstens Ordnung $2^{\alpha-2}$ haben. Aber

$$|(\mathbb{Z}/2^\alpha\mathbb{Z})^\times| = \varphi(2^\alpha) = 2^{\alpha-1},$$

also ist $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ nicht zyklisch für $\alpha \geq 3$. Es gibt also **keine** Primitivwurzel modulo 2^α für $\alpha \geq 3$.

Satz 5.5

Ist $\alpha \in \mathbb{N}_{\geq 3}$, so gilt $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times = \langle [-1]_{2^\alpha} \rangle \times \langle [5]_{2^\alpha} \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

Beweis:

- (1) Nach Voraussetzung, ist $[-1]_{2^\alpha} \neq [1]_{2^\alpha}$ da $\alpha \geq 3$. Zudem gilt $[-1]_{2^\alpha}^2 = [1]_{2^\alpha}$, sodass die Ordnung von $[-1]_{2^\alpha}$ in $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ gleich 2 ist. Somit ist $\langle [-1]_{2^\alpha} \rangle$ eine zyklische Gruppe der Ordnung 2, d.h.

$$\langle [-1]_{2^\alpha} \rangle \cong \mathbb{Z}/2\mathbb{Z}.$$

- (2) Übung auf Blatt 8: Zeigen Sie, dass $\langle [5]_{2^\alpha} \rangle \cong \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

- (3) Wegen $5^x \equiv 1 \pmod{4}$ für alle $x \in \mathbb{N}$ ist $[-1]_{2^\alpha} \notin \langle [5]_{2^\alpha} \rangle$. Aus $\langle [-1]_{2^\alpha} \rangle = \{[1]_{2^\alpha}, [-1]_{2^\alpha}\}$ folgt $\langle [-1]_{2^\alpha} \rangle \cap \langle [5]_{2^\alpha} \rangle = \{[1]_{2^\alpha}\}$. Somit haben wir ein direktes Produkt $\langle [-1]_{2^\alpha} \rangle \times \langle [5]_{2^\alpha} \rangle$, das eine Untergruppe von $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ ist.

- (4) Nach (1) und (2) hat direktes Produkt $\langle [-1]_{2^\alpha} \rangle \times \langle [5]_{2^\alpha} \rangle$ die Ordnung $2 \cdot 2^{\alpha-2}$. Es muss also die ganze Gruppe sein, d.h.

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times = \langle [-1]_{2^\alpha} \rangle \times \langle [5]_{2^\alpha} \rangle$$

und die Behauptung folgt. ■

17 Die Einheitengruppe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ für p ungerade

Wir wollen zunächst den Primzahlfall behandeln. Dazu benötigen wir das folgende Ergebnis aus der elementaren Gruppentheorie (Algebra I):

Bemerkung 5.6

Sei G eine endliche Gruppe der Ordnung $n \in \mathbb{Z}_{>0}$.

- (a) Hat G für jeden positiven Teiler $d \mid n$ höchstens $\varphi(d)$ Elemente der Ordnung d , so ist G zyklisch.
- (b) Ist umgekehrt G zyklisch, so existieren für alle positiven Teiler $d \mid n$ genau $\varphi(d)$ Elemente der Ordnung d in G .

Beweis: Setze $\psi(d) :=$ Anzahl der Elemente der Ordnung d in G .

- (a) Nach Definition ist eine Gruppe (G, \cdot) genau dann zyklisch, wenn ein $g \in G$ existiert mit

$$G = \{g^k \mid k \in \mathbb{Z}_{>0}\}.$$

Nach Voraussetzung gilt $\psi(d) \leq \varphi(d)$ für alle $d \mid n$. Nach Lagrange ist die Ordnung jedes $g \in G$ ein Teiler von n . Daher gilt

$$n = |G| = \sum_{d \mid n} \psi(d) \leq \sum_{d \mid n} \varphi(d) = n$$

nach Satz 2.17(f), also ist $\sum_{d|n} \psi(d) = \sum_{d|n} \varphi(d)$. Da $\psi(d) \leq \varphi(d)$ für jedes d gilt, folgt sogar $\psi(d) = \varphi(d)$ für alle d . Also ist $\psi(n) = \varphi(n) > 0$ und somit enthält G ein Element g der Ordnung n . Daher folgt, dass $G = \{g, \dots, g^n\}$ zyklisch ist.

(b) Sei $G = \{g^k \mid k \in \mathbb{Z}_{>0}\}$ für ein $g \in G$. Dann ist die Ordnung von g^k gleich n genau dann, wenn $\text{ggT}(k, n) = 1$. Nach Definition der φ -Funktion gilt $\psi(n) = \varphi(n)$. Für jedes $d \mid n$ ist $g^{kd} = (g^d)^k$ ein Element der Ordnung $\frac{n}{d}$. Also erzeugt g^{kd} eine zyklische Gruppe der Ordnung $\frac{n}{d}$. Somit ist

$$\psi\left(\frac{n}{d}\right) \geq \varphi\left(\frac{n}{d}\right)$$

für alle $d \mid n$ und

$$n = |G| = \sum_{d|n} \psi(d) \geq \sum_{d|n} \varphi(d) = n.$$

Daraus folgt, dass $\psi(d) = \varphi(d)$ für alle $d \mid n$ gilt. ■

Bemerkung 5.7

Eine endliche Untergruppe (G, \cdot) der multiplikativen Gruppe (K^\times, \cdot) eines Körpers $(K, +, \cdot)$ ist zyklisch.

Beweis: Setze $|G| =: n \in \mathbb{Z}_{>0}$. Ist $g \in G$ ein Element der Ordnung d , so gilt $g^d = 1$, und somit ist g eine Nullstelle des Polynoms $X^d - 1 \in K[X]$. Da K ein Körper ist, hat $X^d - 1$ höchstens d Nullstellen. Also gibt es höchstens d Elemente der Ordnung d in G , nämlich g, \dots, g^d .

Dabei gilt: g^k hat genau dann Ordnung d , wenn $\text{ggT}(d, k) = 1$. Also gibt es genau $\varphi(d)$ Elemente der Ordnung d . Aus Bemerkung 5.6 folgt nun, dass G zyklisch ist. ■

Satz 5.8

Sei $p \in \mathbb{P}$ eine Primzahl. Dann ist $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch der Ordnung $\varphi(p) = p - 1$.

Beweis: Der Ring $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper. Aus Bemerkung 5.7 folgt, dass $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch ist. ■

Satz 5.8 besagt demnach: Es existieren Primitivwurzeln modulo p , falls p eine Primzahl ist. Aber wie findet man solche Zahlen?

Unser nächstes Ziel ist nun zu zeigen, dass $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ für ungerade Primzahlen p zyklisch ist. Wir nehmen also nun an, dass p stets eine ungerade Primzahl ist, und $\alpha \in \mathbb{N}$.

Lemma 5.9

Sei $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl und sei $a \in \mathbb{N}$ eine Primitivwurzel modulo p^α . Dann entweder

(i) a ist Primitivwurzel modulo $p^{\alpha+1}$, oder

(ii) $a^{\varphi(p^\alpha)} \equiv 1 \pmod{p^{\alpha+1}}$.

Beweis: Sei m die Ordnung von $[a]$ in $(\mathbb{Z}/p^{\alpha+1}\mathbb{Z})^\times$. Es gilt

$$m \mid |(\mathbb{Z}/p^{\alpha+1}\mathbb{Z})^\times| = \varphi(p^{\alpha+1}).$$

Andererseits ist $a^m \equiv 1 \pmod{p^{\alpha+1}}$, also ist $a^m \equiv 1 \pmod{p^\alpha}$ und somit $\varphi(p^\alpha) \mid m$, also

$$(p-1)p^{\alpha-1} = \varphi(p^\alpha) \mid m \mid \varphi(p^{\alpha+1}) = (p-1)p^\alpha.$$

Demnach gibt es nur zwei Möglichkeiten:

- (i) $m = \varphi(p^{\alpha+1})$, dann ist a Primitivwurzel in $(\mathbb{Z}/p^{\alpha+1}\mathbb{Z})^\times$, also modulo $p^{\alpha+1}$.
- (ii) $m = \varphi(p^\alpha)$, dann ist $a^{\varphi(p^\alpha)} \equiv 1 \pmod{p^{\alpha+1}}$. ■

Satz 5.10

Sei $a \in \mathbb{Z}_{>0}$ eine Primitivwurzel modulo p mit $a^{p-1} = 1 + mp$ für ein $m \in \mathbb{Z}$ mit $p \nmid m$. Dann ist a eine Primitivwurzel modulo p^α für alle $\alpha \geq 1$.

Beweis: Wir zeigen, dass $a^{\varphi(p^\alpha)} = 1 + m_\alpha p^\alpha$ für $p \nmid m_\alpha$ für alle $\alpha \in \mathbb{Z}_{>0}$ ist. Dann gilt $a^{\varphi(p^\alpha)} \not\equiv 1 \pmod{p^{\alpha+1}}$ und die Aussage folgt aus Lemma 5.9.

Per Induktion nach α . Für $\alpha = 1$ ist $a^{\varphi(p)} = a^{p-1} = 1 + m_1 p$ mit $m_1 := m$ nach Voraussetzung. Sei die Behauptung jetzt für α gezeigt. Potenzieren mit p liefert nach Induktionsvoraussetzung

$$\begin{aligned} a^{\varphi(p^{\alpha+1})} &= a^{p\varphi(p^\alpha)} = (1 + m_\alpha p^\alpha)^p = 1 + \binom{p}{1} m_\alpha p^\alpha + \binom{p}{2} m_\alpha^2 p^{2\alpha} + \dots \\ &\equiv 1 + m_\alpha p^{\alpha+1} \pmod{p^{\alpha+2}}. \end{aligned}$$

Daher existiert $k \in \mathbb{Z}$ mit

$$a^{\varphi(p^{\alpha+1})} = 1 + m_\alpha p^{\alpha+1} + kp^{\alpha+2} = 1 + \underbrace{(m_\alpha + kp)}_{=: m_{\alpha+1}} p^{\alpha+1}. \quad \blacksquare$$

Anmerkung 5.11

Um eine Primitivwurzeln modulo p^α zu finden, reicht es also eine Primitivwurzel modulo p zu bestimmen, welche die Voraussetzung aus Satz 5.10 erfüllt.

Beispiel 15

$p = 3$: $a = 2$ ist eine Primitivwurzel modulo 3 und $2^{3-1} = 2^2 = 4 = 1 + 1 \cdot 3$. Somit folgt aus Satz 5.10, dass 2 eine Primitivwurzel modulo aller 3^α ist.

$p = 5$: $a = 2$ ist eine Primitivwurzel modulo 5 und $2^{5-1} = 16 = 1 + 3 \cdot 5$. Nach Satz 5.10 ist 2 eine Primitivwurzel modulo aller 5^α .

$p = 5$: $a = 7$ ist eine Primitivwurzel modulo 5, aber $7^4 = 49^2 \equiv (-1)^2 \equiv 1 \pmod{25}$. Daher tritt Fall (ii) von Lemma 5.9 ein und die Voraussetzung von Satz 5.10 ist nicht erfüllt. Tatsächlich hat 7 nur Ordnung $4 < \varphi(25) = 20$ modulo 25 und ist damit keine Primitivwurzel modulo 25.

Lemma 5.12

Sei $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl. Dann existiert eine Primitivwurzel a modulo p mit

$$a^{p-1} = 1 + mp \text{ für ein } m \in \mathbb{Z} \text{ mit } p \nmid m.$$

Beweis: Sei a eine Primitivwurzel modulo p (Satz 5.8). Gilt $a^{p-1} = 1 + mp$ mit $p \nmid m$, so sind wir fertig. Sonst gilt $a^{p-1} = 1 + mp$ mit $p \mid m$. Mit a ist auch $a' := a + p \equiv a \pmod{p}$ eine Primitivwurzel modulo p . Aber alle Terme der binomischen Entwicklung von $(a')^{p-1} = (a + p)^{p-1}$ ab dem dritten Grad sind durch p^2 teilbar, existiert also ein $t \in \mathbb{Z}$ mit

$$\begin{aligned} (a')^{p-1} &= (a + p)^{p-1} = a^{p-1} + \binom{p-1}{1} a^{p-2} p + tp^2 \\ &= 1 + mp + (p-1)pa^{p-2} + tp^2 = 1 + m'p, \end{aligned}$$

wobei

$$m' = m + (p-1)a^{p-2} + tp.$$

Aber a ist Primitivwurzel modulo p , also $p \nmid a$ und somit $p \nmid a^{p-2}$ und daher $p \nmid m'$, d.h. a' hat die geforderte Eigenschaft. ■

Satz 5.13

Sei $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl. Dann sind die Einheitengruppen $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ und $(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times$ zyklisch für alle $\alpha \geq 1$.

Beweis: Nach Satz 5.10 zusammen mit Lemma 5.12 existiert eine Primitivwurzel a modulo p^α . Somit ist $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ nach Definition 5.1 zyklisch. Da $(\mathbb{Z}/2\mathbb{Z})^\times$ die triviale Gruppe ist, erhalten wir

$$(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$$

nach dem Chinesischen Restsatz. ■

18 Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$

Bevor wir die Frage beantworten können, wann $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch ist, benötigen wir folgendes einfaches gruppentheoretisches Lemma:

Lemma 5.14

Sind G, H endliche zyklische Gruppen, so gilt:

$$G \times H \text{ ist genau dann zyklisch, wenn } \text{ggT}(|G|, |H|) = 1.$$

Folgerung 5.15

Sei $n \in \mathbb{Z}_{\geq 2}$. Die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ ist genau dann zyklisch, wenn

$$n \in \{2, 4, p^\alpha, 2p^\alpha\},$$

wobei $p \in \mathbb{P} \setminus \{2\}$ und $\alpha \in \mathbb{Z}_{\geq 1}$.

Beweis: Verwende Lemma 5.14 induktiv zusammen mit Anmerkung 5.2, Satz 5.8, Satz 5.5 und Satz 5.13. ■

Zum Abschluss wollen wir eine weitere schon lange offene Frage erwähnen:

Anmerkung 5.16 (Die Vermutung von Artin)

Ist 2 Primitivwurzel modulo unendlich vieler Primzahlen?

Kapitel 6: Das quadratische Reziprozitätsgesetz

Ziel dieses Kapitels: Untersuchung der Lösbarkeit der Kongruenzgleichung

$$X^2 \equiv a \pmod{p},$$

also die Frage, ob die ganze Zahl $a \in \mathbb{Z}$ eine Quadratwurzel modulo $p \in \mathbb{P}$ besitzt.

In Kapitel 6 hatten wir bereits ein erstes Kriterium für die Lösbarkeit bewiesen:

Ist $p \in \mathbb{P}$ ungerade, $g \in \mathbb{Z}_{>0}$ Primitivwurzel modulo p und $a \equiv g^d \pmod{p}$, so ist $X^2 \equiv a \pmod{p}$ genau dann lösbar, wenn d gerade ist.

Wie finden wir aber g und d ? In der Praxis benötigen wir ein besseres Kriterium. Dies wird uns das **quadratische Reziprozitätsgesetz** liefern.

20 Quadratische Reste

Definition 6.1 (quadratischer Rest, quadratischer Nichtrest)

Sei $n \in \mathbb{N}$. Eine ganze Zahl $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$ heißt ein **quadratischer Rest modulo n** , falls die Kongruenz $x^2 \equiv a \pmod{n}$ eine Lösung hat, sonst heißt a **quadratischer Nichtrest modulo n** .

Bemerkung 6.2

Sei $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl. Eine ganze Zahl $a \in \mathbb{Z}_{>0}$ ist genau dann ein quadratischer Rest modulo p , wenn $\frac{p-1}{\text{ord}([a]_p)}$ gerade ist (wobei $[a]_p$ die Restklasse von a in $(\mathbb{Z}/p\mathbb{Z})^\times$ ist).

Beweis:

' \Rightarrow ' Ist a ein quadratischer Rest modulo p , dann existiert ein $b \in \mathbb{Z}_{>0}$ mit $b^2 \equiv a \pmod{p}$. Also gilt

$$[a]_p^{\frac{\varphi(p)}{2}} = [b]_p^{\frac{2\varphi(p)}{2}} = [1] \in \mathbb{Z}/p\mathbb{Z}$$

nach dem kleinen Satz von Fermat (Folgerung 3.2), somit

$$\text{ord}([a]_p) \mid \frac{\varphi(p)}{2} = \frac{p-1}{2}.$$

Dies bedeutet, dass $\frac{p-1}{\text{ord}([a]_p)}$ gerade sein muss.

' \Leftarrow ' Wir nehmen nun an, dass $\frac{p-1}{\text{ord}([a]_p)}$ gerade ist. Sei $g \in \mathbb{Z}_{>0}$ eine Primitivwurzel modulo p , d.h.

$$\langle [g]_p \rangle = (\mathbb{Z}/p\mathbb{Z})^\times \quad \text{und} \quad \text{ord}([g]_p) = p - 1 = |(\mathbb{Z}/p\mathbb{Z})^\times|$$

und es gibt $m \in \mathbb{Z}_{>0}$, so dass $[a]_p = [g]_p^m$ ist. Dann ist

$$[1] = [a]_p^{\text{ord}([a]_p)} = [g]_p^{m \cdot \text{ord}([a]_p)}.$$

Also ist $p - 1$ ein Teiler von $m \cdot \text{ord}([a]_p)$ und es gilt

$$\frac{p-1}{\text{ord}([a]_p)} \mid m.$$

Damit ist m als Vielfaches von $\frac{p-1}{\text{ord}([a]_p)}$ gerade. Setze also $b := g^{\frac{m}{2}}$, so dass $[b]_p^2 = [g]_p^m = [a]_p$ ist, und deshalb ist a ein quadratischer Rest modulo p . ■

Satz 6.3

Sei $p \in \mathbb{P} \setminus \{2\}$ ungerade. Die Menge

$$\begin{aligned} \mathcal{R}_p &:= \{[a]_p \in \mathbb{Z}/p\mathbb{Z} \mid a \in \mathbb{Z} \text{ quadratischer Rest modulo } p\} \\ &= \{[a]_p \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \exists [x]_p \in \mathbb{Z}/p\mathbb{Z} \text{ mit } [a]_p = [x]_p^2\} \end{aligned}$$

ist eine Untergruppe von $(\mathbb{Z}/p\mathbb{Z})^\times$ der Ordnung

$$\frac{\varphi(p)}{2} = \frac{p-1}{2}.$$

Beweis: Zunächst ist es klar nach Definition, dass $\mathcal{R}_p \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$. Nun sind $[a]_p, [b]_p \in \mathcal{R}_p$, so existieren $[x]_p, [y]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$ mit

$$[x]_p^2 = [a]_p, \quad \text{und} \quad [y]_p^2 = [b]_p.$$

Damit ist

$$[a]_p \cdot [b]_p^{-1} = [x]_p^2 \cdot [y]_p^{-2} = ([x]_p \cdot [y]_p^{-1})^2$$

ebenfalls ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ und \mathcal{R}_p ist eine Untergruppe von $(\mathbb{Z}/p\mathbb{Z})^\times$.

Weiter gilt $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$, und die Elemente $x, -x \in \mathbb{Z}$ haben jeweils dasselbe Quadrat, also gibt es $\frac{p-1}{2}$ Quadrate und somit gilt $|\mathcal{R}_p| = \frac{p-1}{2}$. ■

Definition 6.4 (Legendre Symbol)

Seien $p \in \mathbb{P} \setminus \{2\}$ ungerade und $a \in \mathbb{Z}$. Das **Legendre-Symbol** ist definiert als

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } \text{ggT}(a, p) = 1, \ a \text{ quadratischer Rest modulo } p, \\ -1 & \text{falls } \text{ggT}(a, p) = 1, \ a \text{ quadratischer Nichtrest modulo } p, \\ 0 & \text{falls } p \mid a. \end{cases}$$

Man spricht dies „ a über p “ aus.

Anmerkung 6.5

Anders gesagt gibt $\left(\frac{a}{p}\right)$ Antwort auf die Frage: Ist a ein quadratischer Rest modulo p ?

Beispiel 16

Sei $p = 7$. Nach Satz 6.3 gibt es

$$\frac{p-1}{2} = \frac{7-1}{2} = 3$$

quadratische Reste modulo 7. Es gilt

$$1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 2 \pmod{7}.$$

Damit ist

$$\mathcal{R}_7 = \{[1]_7, [2]_7, [4]_7\},$$

also

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1, \quad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1, \quad \left(\frac{0}{7}\right) = 0.$$

Bemerkung 6.6 (Rechenregeln)

Seien $p \in \mathbb{P} \setminus \{2\}$, $a, b \in \mathbb{Z}$. Dann gelten:

- (a) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, falls $a \equiv b \pmod{p}$;
- (b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$; und
- (c) $\left(\frac{a^2}{p}\right) = 1$, falls $p \nmid a$.

Beweis:

- (a) Nach Definition hängt das Legendre-Symbol $\left(\frac{a}{p}\right)$ nur von der Restklasse von a modulo p ab.
- (b) 1. Fall: Gilt $p \mid ab$, dann $p \mid a$ oder $p \mid b$. Damit ist $\left(\frac{ab}{p}\right) = 0$ genau dann, wenn $\left(\frac{a}{p}\right) = 0$ oder $\left(\frac{b}{p}\right) = 0$ ist.
2. Fall: Sei jetzt $\text{ggT}(a, p) = \text{ggT}(b, p) = 1$ und $\left(\frac{a}{p}\right) = 1$. Dann ist $[a]_p \in \mathcal{R}_p$ und daher $[b]_p \in \mathcal{R}_p$ genau dann, wenn $[a]_p[b]_p \in \mathcal{R}_p$ (nach Satz 6.3) und ebenso falls $\left(\frac{b}{p}\right) = 1$.
3. Fall: $\text{ggT}(a, p) = \text{ggT}(b, p) = 1$ und $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$. Somit sind $[a]_p, [b]_p \notin \mathcal{R}_p$. In diesem Fall müssen wir also zeigen, dass $[a]_p[b]_p \in \mathcal{R}_p$ ist, und somit ist $\left(\frac{ab}{p}\right) = 1$. Da $[a]_p$ invertierbar ist, ist die Multiplikation mit $[a]_p$

$$\begin{aligned} (\mathbb{Z}/p\mathbb{Z})^\times &\longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \\ [c]_p &\longmapsto [a]_p \cdot [c]_p, \end{aligned}$$

ist eine bijektive Abbildung. Falls $[c]_p \in \mathcal{R}_p$, dann ist $[a]_p[c]_p \in (\mathbb{Z}/p\mathbb{Z})^\times \setminus \mathcal{R}_p$, also wird \mathcal{R}_p nach $(\mathbb{Z}/p\mathbb{Z})^\times \setminus \mathcal{R}_p$ abgebildet: $[a]_p \mathcal{R}_p = (\mathbb{Z}/p\mathbb{Z})^\times \setminus \mathcal{R}_p$. Daher gilt

$$[a]_p((\mathbb{Z}/p\mathbb{Z})^\times \setminus \mathcal{R}_p) = [a]_p^2 \mathcal{R}_p = \mathcal{R}_p$$

und damit $[a]_p[b]_p \in \mathcal{R}_p$.

- (c) Dies ist der Spezialfall $b = a$ von Teil (b). ■

Aber wie berechnen wir $\left(\frac{a}{p}\right)$? Eine erste, jedoch recht aufwendige Methode, wird gegeben durch:

Satz 6.7 (Euler)

Für alle ungeraden $p \in \mathbb{P} \setminus \{2\}$ und $a \in \mathbb{Z}$ gilt: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

Beweis: Für $p \mid a$ sind beide Seiten Null. Sei nun $\text{ggT}(a, p) = 1$. Nach dem Satz von Fermat (Folgerung 3.2) gilt

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

d.h., $[a]_p^{\frac{p-1}{2}}$ ist eine Nullstelle von $X^2 - [1]_p$, also

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

Ist $a \equiv b^2 \pmod{p}$ einer der $\frac{p-1}{2}$ quadratischen Reste modulo p (Satz 6.3), so ist

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p},$$

und damit ist $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ wie behauptet. Insbesondere sind die Restklassen modulo p der $\frac{p-1}{2}$ quadratischen Reste modulo p Nullstellen von $X^{\frac{p-1}{2}} - [1]_p$. Dies sind sämtliche Nullstellen von $X^{\frac{p-1}{2}} - [1]_p$ in $\mathbb{Z}/p\mathbb{Z}$ (da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist und Polynome über Körpern höchstens so viele Nullstellen haben wie ihr Grad angibt). Die Restklassen der quadratischen Nichtreste modulo p sind also *keine* Nullstellen von $X^{\frac{p-1}{2}} - [1]_p$, also $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ für $[a]_p \in (\mathbb{Z}/p\mathbb{Z})^\times \setminus \mathcal{R}_p$. Somit ist für diese Zahl a wie verlangt

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



Beispiel 17

Wann ist -1 ein quadratischer Rest modulo p ? Dazu müssen wir $\left(\frac{-1}{p}\right)$ berechnen.

Nach Satz 6.7 gilt $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Aber $(-1)^{\frac{p-1}{2}} \in \{-1, 1\}$ und

$$\begin{cases} (-1)^{\frac{p-1}{2}} = 1 & \Leftrightarrow & (-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \\ (-1)^{\frac{p-1}{2}} = -1 & \Leftrightarrow & (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \end{cases}$$

Somit gilt

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod{4}, \\ -1 & p \equiv -1 \pmod{4}. \end{cases}$$

21 Eine Methode von Gauß

Das Hauptresultat dieses Kapitels ist eine überraschende und wichtige Beziehung zwischen den Legendre-Symbolen $\left(\frac{p}{q}\right)$ und $\left(\frac{q}{p}\right)$. Um diese im nächsten Abschnitt herleiten zu können, benötigen wir einige technische Vorbereitungen.

Lemma 6.8 (Gauß)

Seien $p \in \mathbb{P} \setminus \{2\}$ und $a \in \mathbb{Z}$ mit $\text{ggT}(a, p) = 1$. Für $1 \leq j \leq \frac{p-1}{2}$ sei a_j der betragsmäßig kleinste Rest von $a \cdot j$ modulo p , also

$$a \cdot j \equiv a_j \pmod{p} \quad \text{und} \quad -\frac{p-1}{2} \leq a_j \leq \frac{p-1}{2}.$$

Setze $\nu := |\{j \in \mathbb{Z}_{>0} \mid 1 \leq j \leq \frac{p-1}{2}, a_j < 0\}|$.

Dann gelten:

(a) die Beträge $|a_j|$ sind paarweise verschieden für alle $1 \leq j \leq \frac{p-1}{2}$, und daher ist

$$\{|a_j| \mid 1 \leq j \leq \frac{p-1}{2}\} = \{1, 2, \dots, \frac{p-1}{2}\};$$

(b) $(-1)^\nu \cdot \left(\frac{p-1}{2}\right)! = a_1 \cdots a_{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}$.

Insbesondere ist

$$\left(\frac{a}{p}\right) = (-1)^\nu.$$

Beispiel 18

Für $p = 7$ und $a = 3$ gelten

$$a \cdot 1 = 3 \cdot 1 = 3, \quad a \cdot 2 = 3 \cdot 2 = 6, \quad a \cdot 3 = 3 \cdot 3 = 9$$

und somit sind $a_1 = 3, a_2 = -1$, und $a_3 = 2$. Deshalb ist $\nu = 1$ und somit $\left(\frac{3}{7}\right) = -1$ (vergleiche mit dem vorigen Beispiel).

Für $a = 4$ ist

$$a \cdot 1 = 4 \cdot 1 = 4, \quad a \cdot 2 = 4 \cdot 2 = 8, \quad a \cdot 3 = 4 \cdot 3 = 12$$

und somit $a_1 = -3, a_2 = 1, a_3 = -2$. Hier gilt also $\nu = 2$ und somit $\left(\frac{4}{7}\right) = (-1)^2 = 1$.

Beweis:

(a) Angenommen $|a_i| = |a_j|$, also $ia \equiv a_i \equiv \pm a_j \equiv \pm ja \pmod{p}$, dann folgt $(i \pm j)a \equiv 0 \pmod{p}$, also $p \mid a(i \pm j)$, also $p \mid (i \pm j)$ wegen $\text{ggT}(a, p) = 1$. Aber $1 \leq i, j \leq \frac{p-1}{2}$ und daher $|i \pm j| \leq p-1$, damit muss $i \pm j = 0$ sein, also $i = j$. Die $|a_i|$ sind daher sämtlich verschieden und es gilt

$$\{|a_j| \mid 1 \leq j \leq \frac{p-1}{2}\} = \{1, 2, \dots, \frac{p-1}{2}\}.$$

(b) Nach Teil (a) gilt

$$a_1 \cdots a_{\frac{p-1}{2}} = (-1)^\nu \cdot 1 \cdot 2 \cdots \frac{p-1}{2} = (-1)^\nu \cdot \left(\frac{p-1}{2}\right)!.$$

Aber nach Definition ist auch

$$a_1 \cdots a_{\frac{p-1}{2}} \equiv (1 \cdot a) \cdots \left(\frac{p-1}{2} \cdot a\right) \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Wegen $p \nmid \left(\frac{p-1}{2}\right)!$ ist $\left(\frac{p-1}{2}\right)!$ invertierbar modulo p . Deshalb gilt

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

nach Satz 6.7. Da sowohl $(-1)^v$ als auch $\left(\frac{a}{p}\right)$ nur Werte in $\{\pm 1\}$ annehmen und p ungerade ist, folgt sogar

$$(-1)^v = \left(\frac{a}{p}\right).$$

■

Als Übung kann man mit diesem Lemma von Gauß zeigen:

Folgerung 6.9 (Aufgabe 2, Blatt 11)

Ist $p \in \mathbb{P} \setminus \{2\}$, so gilt

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{wenn } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{wenn } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Notation: Für $x \in \mathbb{R}$ ist $\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}$ das größte Ganze.

Wir brauchen noch das folgende technische Lemma:

Lemma 6.10

Seien $0 < j \leq k$ und $a \in \mathbb{Z}_{>0}$. Dann ist $\lfloor \frac{k}{a} \rfloor - \lfloor \frac{j}{a} \rfloor$ die Anzahl der positiven ganzzahligen Vielfachen m von a mit $j < m \leq k$.

Beweis: Division mit Rest von k durch a liefert $k = qa + r$, mit $0 \leq r < a$. Damit sind $a, 2a, \dots, qa \leq k$, also ist $q = \lfloor \frac{k}{a} \rfloor$ die Anzahl der i mit $ia \leq k$. Genauso ist $\lfloor \frac{j}{a} \rfloor$ die Anzahl der i mit $ia \leq j$, somit ist $\lfloor \frac{k}{a} \rfloor - \lfloor \frac{j}{a} \rfloor$ die gesuchte Zahl. ■

22 Das quadratische Reziprozitätsgesetz

Damit können wir das Hauptresultat dieses Kapitels beweisen.

Satz 6.11 (Gaußsches Quadratisches Reziprozitätsgesetz)

Seien $p \neq q \in \mathbb{P} \setminus \{2\}$ zwei ungerade Primzahlen. Dann gelten:

(a)

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} = \begin{cases} -1 & \text{falls } p \equiv q \equiv 3 \pmod{4}, \\ 1 & \text{sonst;} \end{cases}$$

(b)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{wenn } p \equiv 1 \pmod{4}, \\ -1 & \text{wenn } p \equiv -1 \pmod{4}; \end{cases}$$

(c)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{wenn } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{wenn } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Beweis: Die Teile (b) und (c) sind Satz 6.7 bzw. Folgerung 6.9, daher bleibt nur (a) zu beweisen.

(a) **1. Schritt:** Ist $p \equiv q \pmod{4}$, dann existiert $a \in \mathbb{Z}$ mit $p - q = 4a$ und $\text{ggT}(a, pq) = 1$. Ist $p \not\equiv q \pmod{4}$, also $p \equiv -q \pmod{4}$, dann existiert $a \in \mathbb{Z}$ mit $p + q = 4a$ mit $\text{ggT}(a, pq) = 1$. Also gilt für obiges a immer $p \equiv \pm q \pmod{4a}$ und $\text{ggT}(a, pq) = 1$.

2. Schritt: Nach Lemma 6.8 ist $\left(\frac{a}{p}\right) = (-1)^\nu$, wobei ν die Anzahl der $1 \leq j \leq \frac{p-1}{2}$ mit

$$j \cdot a \in \left(\frac{p}{2}, 2\frac{p}{2}\right] \sqcup \left(3\frac{p}{2}, 4\frac{p}{2}\right] \sqcup \dots = \bigsqcup_{\substack{i=2 \\ \text{gerade}}}^a \left((i-1)\frac{p}{2}, i\frac{p}{2}\right]$$

bezeichnet. Aus Lemma 6.10 folgt nun

$$\nu = \sum_{\substack{i=2 \\ \text{gerade}}}^a \left(\left\lfloor i\frac{p}{2a} \right\rfloor - \left\lfloor (i-1)\frac{p}{2a} \right\rfloor \right).$$

Ebenso ist $\left(\frac{a}{q}\right) = (-1)^\mu$ mit

$$\mu = \sum_{\substack{i=2 \\ \text{gerade}}}^a \left(\left\lfloor i\frac{q}{2a} \right\rfloor - \left\lfloor (i-1)\frac{q}{2a} \right\rfloor \right).$$

Wegen $p = \pm q + 4a$ gilt

$$\begin{aligned} \nu &= \sum_{\substack{i=2 \\ \text{gerade}}}^a \left(\left\lfloor i\frac{\pm q + 4a}{2a} \right\rfloor - \left\lfloor (i-1)\frac{\pm q + 4a}{2a} \right\rfloor \right) \\ &= \sum_{\substack{i=2 \\ \text{gerade}}}^a \left(\left\lfloor \frac{\pm iq}{2a} + 2i \right\rfloor - \left\lfloor \frac{\pm(i-1)q}{2a} + 2(i-1) \right\rfloor \right) \\ &= \sum_{\substack{i=2 \\ \text{gerade}}}^a \left(\left\lfloor \frac{\pm iq}{2a} \right\rfloor - \left\lfloor \frac{\pm(i-1)q}{2a} \right\rfloor + \underbrace{2i - 2(i-1)}_{\text{gerade}} \right) \\ &\equiv \sum_{\substack{i=2 \\ \text{gerade}}}^a \left(\left\lfloor \frac{\pm iq}{2a} \right\rfloor - \left\lfloor \frac{\pm(i-1)q}{2a} \right\rfloor \right) \pmod{2}. \end{aligned}$$

Im Fall $p = q + 4a$ zeigt dies bereits $\nu \equiv \mu \pmod{2}$. Sei jetzt $p = -q + 4a$. Hier verwenden wir

$$\lfloor -x \rfloor = -\lceil x \rceil - 1 \quad \text{für alle } x \in \mathbb{R} \setminus \mathbb{Z}.$$

Angenommen $\frac{iq}{2a}$ wäre ganz, also $\frac{iq}{2a} = s \in \mathbb{Z}$. Dann ist $s \leq \frac{q}{2}$ und $iq = 2as$, aber q teilt weder 2 noch a noch s , Widerspruch!

Also sind $\frac{iq}{2a}, \frac{(i-1)q}{2a}$ nie ganz und es gilt

$$\begin{aligned} \left\lfloor \frac{-iq}{2a} \right\rfloor - \left\lfloor \frac{-(i-1)q}{2a} \right\rfloor &= -\left\lceil \frac{iq}{2a} \right\rceil - 1 + \left\lceil \frac{(i-1)q}{2a} \right\rceil + 1 \\ &= -\left(\left\lfloor \frac{iq}{2a} \right\rfloor - \left\lfloor \frac{(i-1)q}{2a} \right\rfloor \right). \end{aligned}$$

Damit ist auch in diesem Fall $\nu \equiv \mu \pmod{2}$, was bedeutet

$$\left(\frac{a}{p}\right) = (-1)^\nu = (-1)^\mu = \left(\frac{a}{q}\right).$$

3. Schritt: Nach Bemerkung 6.6(a),(b) und (c) gilt:

$$\left(\frac{p}{q}\right) = \left(\frac{\pm q + 4a}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{2^2}{q}\right) \left(\frac{a}{q}\right) = 1 \cdot \left(\frac{a}{q}\right)$$

Aber nach Schritt 2 ist

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

un nun rechnen wir andersherum mit Bemerkung 6.6(a),(b) und (c):

$$\left(\frac{a}{p}\right) = \left(\frac{2^2}{p}\right) \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{-p + 4a}{p}\right) = \left(\frac{\mp q}{p}\right) = \left(\frac{\mp 1}{p}\right) \left(\frac{q}{p}\right)$$

und somit ist

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{-1}{p}\right) & p \equiv q \pmod{4} \\ 1 & p \not\equiv q \pmod{4} \end{cases} \stackrel{\text{Satz 6.7}}{=} \begin{cases} -1 & p \equiv 3 \equiv q \pmod{4} \\ 1 & p \equiv 1 \equiv q \pmod{4} \\ 1 & p \not\equiv q \pmod{4} \end{cases}$$

Anmerkung 6.12

Es folgt aus dem Beweis, dass Teil (a) auch so formuliert werden kann: Sind $p, q \in \mathbb{P} \setminus \{2\}$ ungerade Primzahlen, dann gilt

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{falls } p \equiv q \equiv 3 \pmod{4}, \\ \left(\frac{q}{p}\right) & \text{sonst.} \end{cases}$$

Damit erhalten wir eine sehr effiziente Methode zur Berechnung des Legendre-Symbols!!

Beispiel 19

(a) Ist 3 quadratischer Rest modulo 41?

$$\left(\frac{3}{41}\right) \stackrel{\text{Satz 6.11(a)}}{=} \left(\frac{41}{3}\right) \stackrel{\text{Bem.6.6(a)}}{=} \left(\frac{2}{3}\right) \stackrel{\text{Satz 6.11(c)}}{=} -1$$

Also ist 3 kein quadratischer Rest modulo 41.

(b)

$$\begin{aligned} \left(\frac{503}{773}\right) &= \left(\frac{773}{503}\right) = \left(\frac{270}{503}\right) = \left(\frac{3^3 \cdot 2 \cdot 5}{503}\right) \\ &= \left(\frac{3^2}{503}\right) \left(\frac{3}{503}\right) \left(\frac{2}{503}\right) \left(\frac{5}{503}\right) \\ &= -\left(\frac{503}{3}\right) \cdot 1 \cdot \left(\frac{503}{5}\right) = -\left(\frac{2}{3}\right) \cdot \left(\frac{3}{5}\right) \\ &= -(-1) \cdot \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1 \end{aligned}$$

(c)

$$\begin{aligned} \left(\frac{501}{773}\right) &= \left(\frac{3 \cdot 167}{773}\right) = \left(\frac{773}{3}\right) \left(\frac{773}{167}\right) \\ &= \left(\frac{2}{3}\right) \left(\frac{105}{167}\right) = -1 \cdot \left(\frac{3 \cdot 5 \cdot 7}{167}\right) = -\left(\frac{3}{167}\right) \left(\frac{5}{167}\right) \left(\frac{7}{167}\right) \\ &= -\left(-\left(\frac{167}{3}\right)\right) \left(\frac{167}{5}\right) \left(-\left(\frac{167}{7}\right)\right) \\ &= -\left(\frac{2}{3}\right) \left(\frac{2}{5}\right) \left(\frac{6}{7}\right) = 1 \end{aligned}$$

Also hat die Kongruenzgleichung $X^2 \equiv 501 \pmod{773}$ eine Lösung.

Folgerung 6.13

Es gibt unendlich viele Primzahlen $p \in \mathbb{P}$ mit $p \equiv \pm 1 \pmod{8}$.

Beweis: Nach Satz 3.18 gibt es unendlich viele Primzahlen p , modulo derer das Polynom

$$\Phi_p(X^2 - 2) = X^2 - [2] \in (\mathbb{Z}/p\mathbb{Z})[X]$$

eine Nullstelle besitzt. Für jede solche Primzahl p existiert demnach ein $\alpha \in \mathbb{Z}$ mit $\alpha^2 \equiv 2 \pmod{p}$. Für diese p ist also 2 ein quadratischer Rest, d.h. $p \equiv \pm 1 \pmod{8}$ nach Folgerung 6.9. ■

23 Die diophantische Gleichung $X^2 - mY^2 = \pm p$

Das quadratische Reziprozitätsgesetz erlaubt uns die Untersuchung der diophantischen Gleichung

$$X^2 - mY^2 = \pm p, \quad (m \in \mathbb{Z}, p \in \mathbb{P})$$

für kleine Werte von m .

Satz 6.14

Sei $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl. Seien $m, k \in \mathbb{Z}$ mit $\text{ggT}(p, mk) = 1$. Hat $X^2 - mY^2 = kp$ eine ganzzahlige Lösung, so ist $\left(\frac{m}{p}\right) = 1$.

Beweis: Sei $(x, y) \in \mathbb{Z}^2$ eine ganzzahlige Lösung der Gleichung: also $x^2 - my^2 = kp$. Wenn $p \mid y$, dann $p \mid x$ und $p^2 \mid (x^2 - my^2)$, damit folgt $p^2 \mid kp$. Aber $p \nmid k$. Widerspruch! Daher ist $\text{ggT}(y, p) = 1$ und y ist invertierbar modulo p .

Betrachten wir nun die Gleichung modulo p :

$$x^2 \equiv my^2 \pmod{p},$$

also

$$(xy^{-1})^2 \equiv m \pmod{p}.$$

Es folgt $\left(\frac{m}{p}\right) = 1$. ■

Anmerkung 6.15

Hat insbesondere $X^2 - mY^2 = \pm p$, $p \nmid m$ eine Lösung, so ist $\left(\frac{m}{p}\right) = 1$. Aber, Warnung: Im Allgemeinen gilt die Umkehrung *nicht*.

Beispiel 20

(a) Betrachte $X^2 + 5Y^2 = 7$, also $m = -5$, $p = 7$ und $k = 1$. Hier ist nach Satz 6.11(c)

$$\left(\frac{m}{p}\right) = \left(\frac{-5}{7}\right) = \left(\frac{2}{7}\right) = 1,$$

aber $X^2 = 7 - 5Y^2$ ist nicht lösbar, denn $X^2 \geq 0$ und die rechte Seite ist nur für $Y = 0, \pm 1$ positiv, aber kein Quadrat.

(b) Für $m = -1$ gilt nach Satz 3.12: $X^2 + Y^2 = p$ ist genau dann lösbar, wenn

$$\left(\frac{-1}{p}\right) = 1.$$

Lemma 6.16

Ist $\left(\frac{m}{p}\right) = 1$, so existieren ganze Zahlen x, y, k mit $(x, y) \neq (0, 0)$ und $|k| \leq |m|$, so dass

$$x^2 - my^2 = kp.$$

Beweis: Wegen $\left(\frac{m}{p}\right) = 1$ existiert $a \in \mathbb{Z}$ mit $a^2 \equiv m \pmod{p}$. Nach dem Satz von Thue (Satz 3.11) existieren $(x, y) \neq (0, 0)$, $|x|, |y| < \sqrt{p}$, mit $ay \equiv x \pmod{p}$. Quadrieren liefert

$$my^2 \equiv a^2y^2 \equiv x^2 \pmod{p},$$

also

$$x^2 - my^2 = kp$$

für ein $k \in \mathbb{Z}$. Schließlich ist

$$|k|p = |kp| = |x^2 - my^2| \leq |x^2| + |my^2| = x^2 + |m|y^2 < p + p|m| = (|m| + 1)p,$$

also ist $|k| < |m| + 1$ und wegen $k, m \in \mathbb{Z}$ sogar $|k| \leq |m|$. ■

Wir wollen noch zwei Fälle untersuchen, in denen sogar $k = \pm 1$ in Lemma 6.16 gewählt werden kann.

Satz 6.17

Die diophantische Gleichung $X^2 + 2Y^2 = p$ hat genau dann eine Lösung für $p \in \mathbb{P} \setminus \{2\}$, wenn $\left(\frac{-2}{p}\right) = 1$ ist.

Beweis:

' \Rightarrow ' Dies ist Satz 6.14 mit $m = -2$.

' \Leftarrow ' Sei $\left(\frac{-2}{p}\right) = 1$. Nach Lemma 6.16 existieren $x, y, k \in \mathbb{Z}$, $(x, y) \neq (0, 0)$ und $|k| \leq |m| = 2$ mit $x^2 + 2y^2 = kp$. Somit muss $k \in \{-2, -1, 0, 1, 2\}$ gelten; da aber die linke Seite nicht negativ ist und $(x, y) \neq (0, 0)$, gilt sogar $k \in \{1, 2\}$. Wäre $k = 2$, also $x^2 + 2y^2 = 2p$, dann folgt $2|x|$, etwa $x = 2u$ und aus $x^2 + 2y^2 = 2p$ wird $4u^2 + 2y^2 = 2p$, also $y^2 + 2u^2 = p$. Das Paar (y, u) ist die gesuchte Lösung. ■

Satz 6.18

Die diophantische Gleichung $X^2 - 2Y^2 = p$ hat genau dann eine Lösung für $p \in \mathbb{P} \setminus \{2\}$, wenn $\left(\frac{2}{p}\right) = 1$ ist.

Beweis:

' \Rightarrow ' Dies ist Satz 6.14 mit $m = 2$.

' \Leftarrow ' Sei $\left(\frac{2}{p}\right) = 1$. Nach Lemma 6.16 existieren $x, y, k \in \mathbb{Z}$, $(x, y) \neq (0, 0)$, $|k| \leq |m| = 2$, mit $x^2 - 2y^2 = kp$, also

$$k \in \{-2, -1, 0, 1, 2\}.$$

Die 0 fällt weg, da $\left(\frac{x}{y}\right)^2 = 2$ nicht möglich ist (sonst wäre $\sqrt{2} \in \mathbb{Q}$) und $k = 1$ ist die behauptete Aussage.

Nehmen wir $k = \pm 2$ an, dann ist $x^2 - 2y^2 = \pm 2p$. Dann folgt $2|x$, etwa $x = 2u$, $u \in \mathbb{Z}$, und $4u^2 - 2y^2 = \pm 2p$, also $y^2 - 2u^2 = \pm p$, und wir erhalten auch eine Lösung mit $k = \pm 1$.

Sei schließlich $k = -1$, dann ist $x^2 - 2y^2 = -p$. Mit $u = x + 2y$, $v = x + y$, gilt $(u, v) \neq (0, 0)$ (da $(x, y) \neq (0, 0)$), und somit

$$\begin{aligned} u^2 - 2v^2 &= (x + 2y)^2 - 2(x + y)^2 \\ &= x^2 + 4xy + 4y^2 - 2x^2 - 4xy - 2y^2 \\ &= -x^2 + 2y^2 = p. \end{aligned}$$



24 Das Jacobi-Symbol*

Das Jacobi-Symbol (benannt nach Carl Gustav Jacob Jacobi) ist eine Verallgemeinerung des Legendre-Symbols.

Definition 6.19 (Jacobi-Symbol)

Sei $a \in \mathbb{Z}$ und sei $b \in \mathbb{N}$ eine ungerade natürliche Zahl. Schreibe $b = p_1 \cdots p_m = \prod_{i=1}^m p_i$ ($m \in \mathbb{N}_0$) als Produkt von Primzahlen (nicht notwendig verschieden). Das **Jacobi-Symbol** ist

$$\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_m}\right) = \prod_{i=1}^m \left(\frac{a}{p_i}\right).$$

wobei für $i = 1, \dots, m$ das Symbol $\left(\frac{a}{p_i}\right)$ das Legendre-Symbol ist. Dabei werden $b = 1$ und somit auch $\left(\frac{a}{1}\right) = 1$ als leere Produkte verstanden (d.h. mit $m = 0$).

Man spricht dies auch „ a über b “ aus.

Anmerkung 6.20

(1) Ist b eine ungerade Primzahl, so ist das Jacobi-Symbol gleich dem Legendre-Symbol.

(2) Es folgt aus der Definition, dass $\left(\frac{a}{b}\right) \in \{-1, 0, 1\}$, weil dies schon für das Legendre-Symbol gilt. Außerdem gilt:

$$\left(\frac{a}{b}\right) = 0 \Leftrightarrow \text{ggT}(a, b) \neq 1.$$

(3) Ist a ein quadratischer Rest modulo b , so gilt $\left(\frac{a}{b}\right) = 1$.

Beweis:

a QR mod $b \implies \exists x \in \mathbb{Z}$ mit $a - x^2 = c \cdot b = c \cdot p_1 \cdots p_m \implies a$ ist QR mod $p_i \forall 1 \leq i \leq m$
 $\implies \left(\frac{a}{p_i}\right) = 1 \forall 1 \leq i \leq m \implies \left(\frac{a}{b}\right) = \prod_{i=1}^m \left(\frac{a}{p_i}\right) = \prod_{i=1}^m 1 = 1$.

(4) \triangle Die Umkehrung gilt nicht: i.A. $\left(\frac{a}{b}\right) = 1 \not\Rightarrow a$ ist quadratischer Rest modulo b .

Gegenbeispiel: Nehme $b = 3^2$ und $a = 2$. Es gilt $\left(\frac{2}{b}\right) = \left(\frac{2}{3^2}\right) = \left(\frac{2}{3}\right)^2 = 1$ aber 2 ist kein quadratischer Rest modulo 9, weil die Quadrate modulo 9 kongruent zu 0,1,4 oder 7 sind.

(5) Sind $a, a' \in \mathbb{Z}$ mit $a \equiv a' \pmod{b}$, so gilt $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$.

Beweis:

$a \equiv a' \pmod{b} \implies \exists c \in \mathbb{Z}$ mit $a - a' = c \cdot b = c \cdot p_1 \cdots p_m \implies a \equiv a' \pmod{p_i}$
 $\forall 1 \leq i \leq m \implies \left(\frac{a}{p_i}\right) = \left(\frac{a'}{p_i}\right) \forall 1 \leq i \leq m$ nach Bemerkung 6.6(a) und somit gilt

$$\left(\frac{a}{b}\right) = \prod_{i=1}^m \left(\frac{a}{p_i}\right) = \prod_{i=1}^m \left(\frac{a'}{p_i}\right) = \left(\frac{a'}{b}\right).$$

(6) Mit ähnlichen Argumenten zeigt man, dass das Jacobi-Symbol multiplikativ im Zähler und im Nenner ist, d.h.

$$\left(\frac{a_1 \cdot a_2}{b}\right) = \left(\frac{a_1}{b}\right) \cdot \left(\frac{a_2}{b}\right) \quad \text{für alle } a_1, a_2 \in \mathbb{Z}$$

und

$$\left(\frac{a}{b_1 \cdot b_2}\right) = \left(\frac{a}{b_1}\right) \cdot \left(\frac{a}{b_2}\right) \quad \text{für alle } b_1, b_2 \in \mathbb{Z} \text{ ungerade.}$$

Zur expliziten Berechnung des Jacobi-Symbols benutzen wir die folgende Verallgemeinerung des quadratischen Reziprozitätsgesetzes:

Satz 6.21

Seien $a, b \in \mathbb{N}$ zwei ungerade natürliche Zahlen. Dann gelten:

(a)

$$\left(\frac{a}{b}\right) = (-1)^{\frac{b-1}{2} \cdot \frac{a-1}{2}} \left(\frac{b}{a}\right) = \begin{cases} (-1) \cdot \left(\frac{b}{a}\right) & \text{falls } a \equiv b \equiv 3 \pmod{4}, \\ \left(\frac{b}{a}\right) & \text{sonst;} \end{cases}$$

(b)

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} = \begin{cases} 1 & \text{wenn } b \equiv 1 \pmod{4}, \\ -1 & \text{wenn } b \equiv -1 \pmod{4}; \end{cases}$$

(c)

$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} = \begin{cases} 1 & \text{wenn } b \equiv \pm 1 \pmod{8}, \\ -1 & \text{wenn } b \equiv \pm 3 \pmod{8}. \end{cases}$$

Beweis: Beobachtung 1. Für $r_1, \dots, r_m \in \mathbb{Z}$ ungerade ganze Zahlen gilt

$$\frac{r_1 \cdots r_m - 1}{2} \equiv \sum_{i=1}^m \frac{r_i - 1}{2} \pmod{2}.$$

Beobachtung 2. Für $r_1, \dots, r_m \in \mathbb{Z}$ ungerade ganze Zahlen gilt

$$\frac{r_1^2 \cdots r_m^2 - 1}{8} \equiv \sum_{i=1}^m \frac{r_i^2 - 1}{8} \pmod{2}.$$

Beobachtung 3. Bei allen 3 Aussagen reicht es die erste Gleichheit zu beweisen. Die zweite Gleichheit ist klar (Begründungen dafür haben wir schon beim Legendre-Symbol gegeben).

Nun, schreibe $b = \prod_{i=1}^m p_i$ ($m \in \mathbb{N}_0$) und $a = \prod_{j=1}^{\ell} q_j$ ($\ell \in \mathbb{N}_0$) als Produkte von Primzahlen.

- (a) Falls $\text{ggT}(a, b) \neq 1$, so existieren $i \in \{1, \dots, m\}$ und $j \in \{1, \dots, \ell\}$ mit $\text{ggT}(a, p_i) \neq 1 \neq \text{ggT}(b, q_j)$.
Somit gelten $\left(\frac{a}{p_i}\right) = 0 = \left(\frac{b}{q_j}\right)$ und daher gilt

$$\left(\frac{a}{b}\right) = 0 = \left(\frac{b}{a}\right),$$

so dass die erste Gleichheit in diesem Fall erfüllt ist.

Wir können also annehmen, dass $\text{ggT}(a, b) = 1$. Somit gilt $p_i \neq q_j$ für alle $i \in \{1, \dots, m\}$ und für alle $j \in \{1, \dots, \ell\}$. Die Definition, Satz 6.11(a) und die Beobachtung liefern

$$\begin{aligned} \left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) &= \prod_{i=1}^m \prod_{j=1}^{\ell} \left(\frac{q_j}{p_i}\right) \cdot \left(\frac{p_i}{q_j}\right) \\ &= \prod_{i=1}^m \prod_{j=1}^{\ell} (-1)^{\frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} \\ &= (-1)^{\sum_{i=1}^m \sum_{j=1}^{\ell} \frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} \\ &= (-1)^{(\sum_{i=1}^m \frac{p_i-1}{2}) \cdot (\sum_{j=1}^{\ell} \frac{q_j-1}{2})} \\ &= (-1)^{\frac{\prod_{i=1}^m p_i - 1}{2} \cdot \frac{\prod_{j=1}^{\ell} q_j - 1}{2}} \\ &= (-1)^{\frac{b-1}{2} \cdot \frac{a-1}{2}}. \end{aligned}$$

Nun ist $\left(\frac{b}{a}\right)^{-1} = \left(\frac{b}{a}\right)$, da $\left(\frac{b}{a}\right)^{-1} \in \{\pm 1\}$. Somit liefert die Multiplikation mit $\left(\frac{b}{a}\right)$ die gewünschte Formel:

$$\left(\frac{a}{b}\right) = (-1)^{\frac{b-1}{2} \cdot \frac{a-1}{2}} \left(\frac{b}{a}\right).$$

- (b) Nach Definition, Satz 6.11(b) und Beobachtung 1 gelten

$$\left(\frac{-1}{b}\right) = \prod_{i=1}^m \left(\frac{-1}{p_i}\right) = \prod_{i=1}^m (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^m \frac{p_i-1}{2}} = (-1)^{\frac{\prod_{i=1}^m p_i - 1}{2}} = (-1)^{\frac{b-1}{2}}.$$

- (c) Nach Definition, Satz 6.11(c) und Beobachtung 2 gelten

$$\left(\frac{2}{b}\right) = \prod_{i=1}^m \left(\frac{2}{p_i}\right) = \prod_{i=1}^m (-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum_{i=1}^m \frac{p_i^2-1}{8}} = (-1)^{\frac{\prod_{i=1}^m p_i^2 - 1}{8}} = (-1)^{\frac{b^2-1}{8}}. \quad \blacksquare$$

Mit diesen Rechenregeln können wir nun das Jacobi-Symbol sehr effizient berechnen, wie das folgende Beispiel zeigt:

Beispiel 21

Wir betrachten das Jacobi-Symbol $\left(\frac{131311}{151515}\right)$. Wir beobachten, dass $131311 \equiv 151515 \equiv 3 \pmod{4}$.

Mit den Rechenregeln aus Anmerkung 6.20 und Satz 6.21 erhalten wir

$$\begin{aligned} \left(\frac{131311}{151515}\right) &= \left(\frac{131311 - 151515}{151515}\right) = \left(\frac{(-1) \cdot (151515 - 131311)}{151515}\right) \\ &= \left(\frac{(-1)}{151515}\right) \cdot \left(\frac{151515 - 131311}{151515}\right) = (-1) \cdot \left(\frac{20204}{151515}\right) \\ &= (-1) \cdot \left(\frac{2^2 \cdot 5051}{151515}\right) = (-1) \cdot \left(\frac{2^2}{151515}\right) \cdot \left(\frac{5051}{151515}\right) \\ &= (-1) \cdot (-1) \cdot \left(\frac{151515}{5051}\right) = 1 \cdot \left(\frac{30 \cdot 5051 - 15}{5051}\right) \\ &= \left(\frac{-15}{5051}\right) = \left(\frac{-1}{5051}\right) \cdot \left(\frac{15}{5051}\right) = (-1) \cdot (-1) \cdot \left(\frac{5051}{15}\right) \\ &= \left(\frac{337 \cdot 15 - 4}{15}\right) = \left(\frac{-1}{15}\right) \cdot \left(\frac{2^2}{15}\right) = (-1) \cdot 1 = -1 \end{aligned}$$

Nach Anmerkung 6.20(3) kann also 131311 kein quadratischer Rest modulo 151515 sein. Daher muss 131311 quadratischer Nichtrest modulo 151515 sein.

- (Dirichlet-)Faltung, 12
- diophantische Gleichung
 - lineare , 8
- Division mit Rest, viii
- Euklidischer Algorithmus, vii
- Funktion
 - eulersche φ -Funktion, 17
 - arithmetische, 10
 - euklidische, vii
 - konstante, 10
 - Möbiusfunktion, 15
 - multiplikative, 10
 - Nullfunktion, 10
 - Summatorfunktion, 16
 - Teilersummenfunktion, 19
 - vollständig multiplikative, 10
 - zahlentheoretische, 10
- ganzzahlige Lösung, 8
- ggT, 6
- ggT, 6
- größter gemeinsamer Teiler, vi, 6
- identische Abbildung, 11
- Integritätsbereich, vi
- irreduzibel, vi
- Jacobi-Symbol, 55
- kleinstes gemeinsames Vielfaches, vi
- Legendre-Symbol, 46
- prim, vi
- Primelement, vi
- Primfaktorzerlegung, viii
- Primitivwurzel, 39
- Primzahltest, 23
- Primzerlegung, vi
- quadratfrei, 15
- quadratischer Nichtrest, 45
- quadratischer Rest, 45
- quadratisches Reziprozitätsgesetz, 51, 56
- Reduktion modulo p , 29
- Ring
 - euklidischer, vii
 - Hauptidealring, vii
 - ZPE-Ring, vi
- RSA-Verfahren, 31
- Satz
 - Chinesischer Restsatz, ix
 - kleiner Satz von Fermat, 23
 - Möbius-Umkehrsatz, 16
 - Satz von Wilson, 24
 - von Euler, 22
 - von Fermat, 26, 28
 - von Lagrange, ix
 - von Thue, 26
- Schubfachprinzip, 26
- teilerfremd, 6
- Zahl
 - Carmichael-Zahl, 23
 - Mersenne-Zahl, 20
 - Primzahl, viii
 - vollkommene Zahl, 19