Elementare Zahlentheorie

Thomas Markwig
Fachbereich Mathematik
Technische Universität Kaiserslautern

Vorlesungsskript

April 2008

Inhaltsverzeichnis

1 Einleitung

Die Vorlesung elementare Zahlentheorie setzt den Besuch der Vorlesung algebraische Strukturen voraus. Ich möchte diese Ausarbeitung deshalb damit beginnen, die Ergebnisse aus den algebraischen Strukturen zusammenzustellen, die im Folgenden als bekannt voraus gesetzt werden.

A) Begriffe und Ergebnisse aus den algebraischen Strukturen

Der erste Satz beschäftigt sich mit der algebraischen Struktur der ganzen Zahlen.

Satz 1.1 a. $(\mathbb{Z},+,\cdot)$ *ist ein* Integritätsbereich *mit* $\mathbb{Z}^* = \{1,-1\}$.

b. $(\mathbb{Z},+,\cdot)$ *ist ein* euklidischer Ring *mit dem Betrag als euklidischer Funktion. Insbesondere gibt es für* $a, b \in \mathbb{Z}$, $b \neq 0$, *eindeutig bestimmte ganze Zahlen* $q, r \in \mathbb{Z}$ *mit*

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

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

c. $(\mathbb{Z},+,\cdot)$ *ist ein* Hauptidealring, *d.h. für jedes Ideal* $I \trianglelefteq \mathbb{Z}$ *gibt es eine ganze Zahl* $a \in \mathbb{Z}$, *so daß*

$$I = \langle a \rangle_{\mathbb{Z}} = \{z \cdot a \mid z \in \mathbb{Z}\}.$$

Bemerkung 1.2
In einem Integritätsbereich haben wir den Begriff der Teilbarkeit eingeführt als $a \mid b$ falls $b = a \cdot c$ ein Vielfaches von a ist. Damit konnten wir dann für Elemente a, die weder Null noch eine Einheit sind, die Begriffe *prim* und *irreduzibel* definieren. Dabei ist a *prim*, wenn aus $a \mid b \cdot c$ schon $a \mid b$ oder $a \mid c$ folgt. Und a ist *irreduzibel*, wenn aus $a = b \cdot c$ folgt, daß b oder c eine Einheit ist. Da $\mathbb{Z}$ ein Hauptidealring ist, gilt in $\mathbb{Z}$ die folgende Beziehung:

$$p \in \mathbb{Z} \text{ ist prim} \quad \Longleftrightarrow \quad p \text{ ist irreduzibel.}$$

In diesem Sinne ist die Zahl 2 sowohl prim als auch irreduzibel, und das gleiche trifft auf die Zahl -2 zu. Wir wollen in dieser Vorlesung nun zwischen *primen Elementen* (in obigem Sinn) und *Primzahlen* (im klassischen Sinn) unterscheiden, um einige Zweideutigkeiten und umständliche Formulierungen zu vermeiden. Dazu dient die folgende Definition.

Definition 1.3
Eine ganze Zahl $p \in \mathbb{Z}$ heißt *Primzahl*, wenn p prim und *positiv* ist. Wir bezeichnen mit

$$\mathbb{P} = \{p \in \mathbb{Z} \mid p \text{ ist Primzahl}\} \subset \mathbb{N}$$

die Menge der Primzahlen.

Satz 1.4 (Euklid)
$|\mathbb{P}| = \infty$, *d.h. es gibt unendlich viele Primzahlen.*

Die Untersuchung der ganzen Zahlen, wie wir sie in dieser Vorlesung vornehmen wollen, basiert letztlich auf einer weiteren strukturellen Eigenschaft des Ringes $\mathbb{Z}$, die als Fundamentalsatz der elementaren Zahlentheorie bekannt ist, deren Beweis nichtsdestotrotz bereits Gegenstand der algebraischen Strukturen war. Der Satz sagt aus, daß $(\mathbb{Z}, +, \cdot)$ ein *faktorieller Ring* ist.

Theorem 1.5 (Fundamentalsatz der elementaren Zahlentheorie)
Für jedes $0 \neq z \in \mathbb{Z}$ *gibt es eindeutig bestimmte, paarweise verschiedene Primzahlen* $p_1, \ldots, p_k \in \mathbb{P}$ *und eindeutig bestimmte positive ganze Zahlen* $n_1, \ldots, n_k \in \mathbb{Z}_{>0}$*, so daß*

$$z = \operatorname{sign}(z) \cdot p_1^{n_1} \cdots p_k^{n_k},$$

wobei

$$\operatorname{sign}(z) := \begin{cases} 1, & z > 0, \\ -1, & z < 0. \end{cases}$$

Führen wir für eine Primzahl $p \in \mathbb{P}$ *die Notation*

$$n_p(z) = \max\left\{n \in \mathbb{N} \;\middle|\; p^n \mid z\right\}$$

ein, so gilt

$$n_p(z) = \begin{cases} n_i, & p = p_i, \\ 0, & \textit{sonst} \end{cases}$$

und

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

Wir nennen diese Darstellung die Primfaktorzerlegung *von* z*.*

Bemerkung 1.6
Eine unmittelbare Konsequenz des Fundamentalsatzes ist, daß eine positive ganze Zahl p genau dann eine Primzahl ist, wenn 1 und p ihre einzigen positiven Teiler sind.

Der Vollständigkeit halber setzen wir $n_p(0) := \infty$ für $p \in \mathbb{P}$. □

Den Begriff der Teilbarkeit haben wir zudem mit Hilfe von Idealen auszudrücken gelernt. Dabei bezeichnet $\operatorname{ggT}(a, b)$ für zwei ganze Zahlen $a, b \in \mathbb{Z}$ die Menge der *größten gemeinsamen Teiler* von a und b, und eine Zahl $g \in \mathbb{Z}$ heißt *größter gemeinsamer Teiler* von a und b, wenn sie sowohl a als auch b teilt und wenn sie von jeder anderen Zahl geteilt wird, die ihrerseits a und b teilt.

Bemerkung 1.7
Es seien $a, b \in \mathbb{Z}$.

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

b. $a \mid b \;\&\; b \mid a \;\Leftrightarrow\; \langle a \rangle_{\mathbb{Z}} = \langle b \rangle_{\mathbb{Z}} \;\Leftrightarrow\; n_p(a) = n_p(b) \;\; \forall\, p \in \mathbb{P} \;\Leftrightarrow\; a = \pm b$.

c. $g \in \operatorname{ggT}(a, b) \iff \langle a, b \rangle_{\mathbb{Z}} = \langle g \rangle_{\mathbb{Z}}$.

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

Wieder wurde der Begriff des größten gemeinsamen Teilers in dieser Form eingeführt für beliebige Integritätsbereiche und ist nicht eindeutig. Die Zahlen 4 und 6 haben zwei größte gemeinsame Teiler, nämlich 2 und −2. Wir wollen diese Doppeldeutigkeit vermeiden, und führen dazu folgende Definition ein.

Definition 1.8
Für $a, b \in \mathbb{Z}$, nicht beide Null, ist

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

der *positive* größte gemeinsame Teiler von a und b. Wir nennen dann a und b *teilerfremd*, wenn $\mathrm{ggt}(a, b) = 1$.

Aufgabe 1.9
Zeige, für $a, b, c \in \mathbb{Z}$ gilt

$$\mathrm{ggt}(a, b) = \mathrm{ggt}(a + c \cdot b, b).$$

Beweis: Es gilt offenbar

$$a = (a + c \cdot b) - c \cdot b \in \langle a + c \cdot b, b \rangle_{\mathbb{Z}}$$

und

$$a + c \cdot b \in \langle a, b \rangle_{\mathbb{Z}},$$

so daß

$$\langle \mathrm{ggt}(a, b) \rangle_{\mathbb{Z}} = \langle a, b \rangle_{\mathbb{Z}} = \langle a + c \cdot b, b \rangle_{\mathbb{Z}} = \langle \mathrm{ggt}(a + c \cdot b, b) \rangle_{\mathbb{Z}}.$$

Daraus folgt die Behauptung, da der Erzeuger eines Ideals in $\mathbb{Z}$ bis auf sein Vorzeichen eindeutig bestimmt ist. □

Man beachte auch, daß man $\mathrm{ggt}(a, b)$ mit Hilfe des *Euklidischen Algorithmus* berechnen kann.

Analog zu den größten gemeinsamen Teilern haben wir *kleinste gemeinsame Vielfache* von a und b eingeführt als Zahlen, die sowohl von a als auch von b geteilt werden und jede andere Zahl mit dieser Eigenschaft ihrerseits teilen. Mit $\mathrm{kgV}(a, b)$ bezeichnen wir die Menge aller kleinsten gemeinsamen Vielfachen von a und b. Der Begriff ist dual zum größten gemeinsamen Teiler und folgende einfachen Eigenschaften gelten.

Bemerkung 1.10
Es seien $a, b \in \mathbb{Z} \setminus \{0\}$.

a. $k \in \mathrm{kgV}(a, b) \iff \langle a \rangle \cap \langle b \rangle_{\mathbb{Z}} = \langle k \rangle_{\mathbb{Z}}$.

b. $k \in \mathrm{kgV}(a, b) \implies \mathrm{kgV}(a, b) = \{k, -k\}$.

c. $\mathrm{kgv}(a, b) := \prod_{p \in \mathbb{P}} p^{\max\{n_p(a), n_p(b)\}} \in \mathrm{kgV}(a, b)$.

d. $|a \cdot b| = \mathrm{ggt}(a, b) \cdot \mathrm{kgv}(a, b)$.

Aufgrund der letzten Gleichheit kann $\operatorname{kgv}(a, b)$ ebenfalls mit Hilfe des Euklidischen Algorithmus berechnet werden.

In den algebraischen Strukturen wurde eine Äquivalenzrelation auf den ganzen Zahlen eingeführt, die für die vorliegende Vorlesung von zentraler Bedeutung ist, die *Kongruenz* ganzer Zahlen.

Bemerkung 1.11
Seien $a, b, n \in \mathbb{Z}$, dann heißen a und b zueinander *kongruent modulo* n, falls $n \mid a-b$. Wir schreiben dann $a \equiv b \pmod n$ und nennen n den *Modulus* der Kongruenz modulo n. Dies bedeutet, daß a und b bei Division mit Rest durch n den gleichen Rest haben, und falls $0 \leq b < n$, so heißt es, daß b der Rest von a bei Division mit Rest durch n ist. Wir werden diese Gleichwertigkeit immer wieder in der Form verwenden, daß

$$a \equiv b \pmod n \iff a \text{ hat die Form } a = n \cdot k + b \text{ für ein } k \in \mathbb{Z}.$$

Die Kongruenz modulo n ist eine Äquivalenzrelation mit genau n paarweise verschiedenen Äquivalenzklassen $\overline{0}, \overline{1}, \ldots, \overline{n-1}$, wobei

$$\overline{a} = \{a + n \cdot z \mid z \in \mathbb{Z}\}.$$

Wenn wir verdeutlichen wollen, daß $\overline{a}$ eine Äquivalenzklasse in $\mathbb{Z}_n$ ist, so schreiben wir $\overline{a}_n$ statt $\overline{a}$. Wir bezeichnen die Menge der Äquivalenzklassen mit

$$\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}.$$

Für zwei Äquivalenzklassen $\overline{a}, \overline{b} \in \mathbb{Z}_n$ haben wir eine Addition

$$\overline{a} + \overline{b} := \overline{a+b}$$

und eine Multiplikation

$$\overline{a} \cdot \overline{b} := \overline{a \cdot b}$$

eingeführt und gezeigt, daß beide unabhängig von der Wahl der Repräsentanten sind.

Satz 1.12
$(\mathbb{Z}_n, +, \cdot)$ ist ein kommutativer Ring mit Eins und die Einheitengruppe von $\mathbb{Z}_n$ ist

$$\mathbb{Z}_n^* = \left\{\overline{a} \in \mathbb{Z}_n \;\middle|\; \operatorname{ggt}(a, n) = 1\right\}.$$

Insbesondere ist $\mathbb{Z}_n$ genau dann ein Körper, wenn n prim ist.

Abschließend wollen wir noch den chinesischen Restsatz in Erinnerung rufen.

Satz 1.13 (Chinesischer Restsatz)
Sind $n_1, \ldots, n_k \in \mathbb{Z}$ paarweise teilerfremd, so ist die Abbildung

$$\mathbb{Z}_{n_1 \cdots n_k} \longrightarrow \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k} : \overline{z} \mapsto \left(\overline{z}, \ldots, \overline{z}\right)$$

ein Isomorphismus von Ringen.

Die Surjektivität bedeutet, daß zu beliebigen $a_1, \dots, a_k \in \mathbb{Z}$ *eine Lösung des Kongruenzgleichungssystems*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

existiert, und die Injektivität bedeutet, daß sich je zwei Lösungen um ein Vielfaches von $n_1 \cdots n_k$ *unterscheiden.*

B) **Einige "elementare" Fragen zu den ganzen Zahlen**

Nachdem geklärt ist, welche Eigenschaften der ganzen Zahlen wir als bekannt voraussetzen, möchte ich einige Fragen formulieren, die einen Eindruck davon geben, womit sich die elementare Zahlentheorie beschäftigt. Dabei ist das *elementare* an den Fragen der Umstand, daß zu ihrem Verständnis nur der klassische Begriff der *Primzahl* bekannt sein muß. Der mathematische Schwierigkeitsgrad möglicher Antworten auf die Fragen ist sehr unterschiedlich und zum Teil alles andere als elementar. Wir wollen es dem Leser zunächst anheim stellen, sich an Antworten zu versuchen – sei es durch Beweis, Gegenbeispiel oder auch nur durch Argumente, die die aufgestellte These stützen.

Die erste Frage beschäftigt sich mit der Anzahl von Primzahlen, die bestimmten Bedingungen genügen, etwa einen vorgegebenen Rest bei Division mit Rest durch eine vorgegebene Zahl haben.

Frage A:

a. Wie viele Primzahlen p genügen der Bedingung mit $p \equiv 0 \pmod 4$?
b. Wie viele Primzahlen p genügen der Bedingung mit $p \equiv 1 \pmod 4$?
c. Wie viele Primzahlen p genügen der Bedingung mit $p \equiv 2 \pmod 4$?
d. Wie viele Primzahlen p genügen der Bedingung mit $p \equiv 3 \pmod 4$?

Eine andere Bedingung, die man an Primzahlen stellen kann, führt zum Begriff der *Primzahlzwillinge*. Ist für eine Primzahl p auch $p+2$ eine Primzahl, so nennt man $(p, p+2)$ ein Primzahlzwillingspaar. $(3, 5)$ und $(5, 7)$ sind solche Primzahlzwillingspaare.

Frage B: Gibt es unendlich viele Primzwillingspaare?

Primzahlen sind dadurch ausgezeichnet, daß sie nur zwei positive Teiler besitzen. Man kann sich auch andere Eigenschaften ganzer Zahlen aussuchen und versuchen, alle Zahlen mit diesen Eigenschaften zu finden, sofern es nur endlich viele sind.

Die Zahl 6 hat die ungewöhnliche Eigenschaft, daß sie die Summe ihrer *echten* Teiler ist, d.h.

$$6 = 1 + 2 + 3 = \sum_{\substack{1 \leq d < 6 \\ d \mid 6}} d.$$

Zahlen mit dieser Eigenschaft nennt man *vollkommene Zahlen.* Etwas formaler ausgedrückt heißt eine positive ganze Zahl $z \in \mathbb{Z}_{>0}$ *vollkommen*, wenn

$$z = \sum_{\substack{1 \leq d < z \\ d \mid z}} d.$$

Eine weitere Zahl, für die dies gilt ist $28 = 1 + 2 + 4 + 7 + 14$.

Frage C:

a. Wie viele gerade vollkommene Zahlen gibt es?
b. Gibt es auch ungerade vollkommene Zahlen?

Aufgrund des Fundamentalsatzes der elementaren Zahlentheorie ist die Anzahl $n_{\mathbb{P}}(z)$ an Primteilern einer Zahl z eine wohldefinierte Größe, nämlich

$$n_{\mathbb{P}}(z) = \sum_{p \in \mathbb{P}} n_p(z).$$

Schauen wir uns einige Werte von $n_{\mathbb{P}}(z)$ an.

z	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$n_{\mathbb{P}}(z)$	0	1	1	2	1	2	1	3	2	2	1	3	1	2

Ist $n_{\mathbb{P}}(z)$ öfter eine gerade Zahl oder öfter eine ungerade? In dieser Form ist die Frage sicher wenig sinnvoll, ist doch z.B. $n_{\mathbb{P}}(2^k)$ gerade sobald k gerade ist und ungerade sobald dies für k zutrifft, so daß beide Fälle unendlich oft eintreten. Beschränken wir uns aber auf diejenigen ganzen Zahlen, die zwischen 1 und einer fest vorgegebenen Zahl n liegen, so verschwindet das eben angedeutete Problem. Wir führen dazu folgende Notation ein:

$$g_n = \left|\{z \in \mathbb{Z} \mid 1 \leq z \leq n,\ n_{\mathbb{P}}(z) \equiv 0 \pmod 2\}\right| \in \mathbb{N}$$

und

$$u_n = \left|\{z \in \mathbb{Z} \mid 1 \leq z \leq n,\ n_{\mathbb{P}}(z) \equiv 1 \pmod 2\}\right| \in \mathbb{N}.$$

Für $n = 14$ erhalten wir

$$g_{14} = \left|\{1, 4, 6, 9, 10, 14\}\right| = 6$$

und

$$u_{14} = \left|\{2, 3, 5, 7, 8, 11, 12, 13\}\right| = 8.$$

Betrachtet man obige Tabelle, so stellt man fest, daß für alle $2 \leq n \leq 14$ gilt $u_n \geq g_n$. Dies scheint auch nicht zu verwundern, denn wann immer wir eine Zahl z haben, die sich als Produkt von einer geraden Anzahl an Primteilern schreiben läßt, so lassen sich aus den Primteilern der Zahl mindestens zwei kleinere Zahlen bilden, die eine ungerade Anzahl an Primteilern haben. Dies legt die folgende Frage nahe.

Frage D: Gilt $u_n \geq g_n$ für alle $n \geq 2$?

Der Fundamentalsatz der elementaren Zahlentheorie impliziert, daß die Primzahlen die Elementarbausteine der ganzen Zahlen sind. Als solche spielen sie eine wesentliche Rolle für die Theorie. Aber auch bei praktischen Anwendungen von zahlentheoretischen Ergebnissen, etwa in der Kryptographie, stehen sie im Zentrum des Interesses, wie wir später in der Vorlesung noch sehen werden. Von daher wäre es schön, eine algebraische oder analytische Funktion zu besitzen, die Primzahlen produziert, d.h., die ihren Bildbereich in $\mathbb{P}$ hat. Dahin zielt die nächste Frage.

Frage E:

a. Ist $n^2 + n + 41$ eine Primzahl für alle $n \geq 0$?

b. Ist $2^q - 1$ eine Primzahl für alle $q \in \mathbb{P}$?

c. Ist $2^{(2^n)} + 1$ eine Primzahl für alle $n \in \mathbb{N}$?

Ebenso wichtig wie die Frage, wie man Primzahlen konstruieren kann, sind Kriterien, die es erlauben, festzustellen, ob eine Zahl eine Primzahl ist. Wie steht es um die im folgenden formulierten Bedingungen?

Frage F:

a. p ungerade, $3 \not| p$, $5 \not| p \quad \Longrightarrow \quad p \in \mathbb{P}$?

b. $p \in \mathbb{P} \quad \Longleftrightarrow \quad p \mid 2^p - 2$?

c. $p \in \mathbb{P} \quad \Longleftrightarrow \quad p \mid \big((p-1)! + 1\big)$?

Der Fundamentalsatz der elementaren Zahlentheorie klärt im Prinzip auf welche Weise eine ganze Zahl multiplikativ zerlegt werden kann. Die vollkommenen Zahlen setzen diese multiplikative Zerlegung mit einer additiven Zerlegung in Beziehung. Man kann aber auch eine Vielzahl anderer additiver Zerlegungen einer ganzen Zahl betrachten, etwa indem man Primzahlen zuläßt, die nicht notwendigerweise Teiler der Zahl sind.

Frage G:

a. Ist jede gerade Zahl $z \geq 4$ Summe zweier Primzahlen?

b. Welche ungeraden Zahlen sind Summe zweier Primzahlen?

Man kann sich aber auch gänzlich von den Primzahlen lösen und andere Bedingungen an die Summanden stellen.

Frage H: Welche Zahlen $n \in \mathbb{N}$ lassen sich als Summe zweier Quadratzahlen darstellen, d.h. für welche $n \in \mathbb{N}$ hat die Gleichung

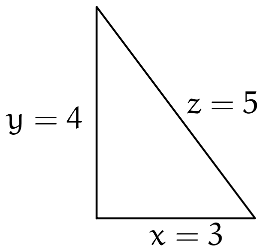
$$x^2 + y^2 = n$$

eine Lösung $(x, y) \in \mathbb{Z}^2$ über den ganzen Zahlen?

Beschränkt man sich hier auf Zahlen $n = z^2$, die selbst Quadratzahlen sind, so erhält man eine Gleichung

$$x^2 + y^2 = z^2,$$

die an den Satz von Pythagoras erinnert. Ein Zahlentripel (x, y, z), das dieser Gleichung genügt, repräsentiert die Seitenlängen eines rechtwinkligen Dreiecks, wobei z die Länge der Hypothenuse ist. Man nennt solche Zahlentripel deshalb auch *pythagoreische Zahlentripel*. $(3, 4, 5)$ ist sicher das bekannteste pythagoreische Zahlentripel.



Frage I: Kann man alle ganzzahligen pythagoreischen Zahlentripel angeben?

Die obige Gleichung läßt sich natürlich in vielfacher Weise verallgemeinern, und stets können wir die Frage nach ihrer Lösbarkeit stellen.

Frage J: Welche ganzzahligen Lösungen besitzt die Gleichung $x^n + y^n = z^n$ für ein festes $n \geq 3$?

Frage K: Ist die Gleichung $x^2 - 1141y^2 = 1$ lösbar über $\mathbb{Z}$? D.h. gibt es eine ganze Zahl $y \in \mathbb{Z}$, so daß $\sqrt{1141y^2 + 1}$ eine ganze Zahl ist?

Gleichungen wie sie in den Fragen H bis K betrachtet wurden, sind Spezialfälle von sogenannten *diophantischen Gleichungen*. Dabei handelt es sich um Gleichungen der Form

$$F = 0$$

wobei $F \in \mathbb{Z}[x_1, \ldots, x_n]$ ein Polynom mit ganzzahligen Koeffizienten in den Unbestimmten $x_1, \ldots, x_n$ ist. Man sagt, die diophantische Gleichung $F = 0$ ist lösbar, wenn es ganze Zahlen $z_1, \ldots, z_n \in \mathbb{Z}$ gibt, so daß $F(z_1, \ldots, z_n)$ Null ist. Ein Großteil der Vorlesung wird sich mit der Lösbarkeit diophantischer Gleichungen beschäftigen. Die betrachteten Gleichungen werden aber so speziell sein, daß wir an dieser Stelle nicht weiter auf die Bedeutung des *Polynomrings* $\mathbb{Z}[x_1, \ldots, x_n]$ eingehen müssen.

C) Einige “elementare” Antworten

Wir wollen im folgenden versuchen, die obigen Fragen zu beantworten, soweit das mit unseren *elementaren* Mitteln möglich ist. Etliche Male wird uns aber nur der Verweis auf den Verlauf der Vorlesung oder auf tiefergehende Literatur der Zahlentheorie bleiben, und zu einigen Fragen ist die Antwort bislang schlicht unbekannt. Ich hoffe, Ihr habt Euch eigene Antworten zu den Fragen überlegt, Beispiele gerechnet, eigene Vermutungen dazu aufgestellt, bevor Ihr den folgenden Abschnitt lest. Falls dies nicht der Fall ist, holt es nach. Die Antworten sind weit interessanter, wenn Ihr sie mit Eurer eigenen Intuition vergleichen könnt.

Zu Frage A: Bei der ersten Frage geht es um den Rest einer Primzahl bei Division durch vier. Ist der Rest Null, so ist die Zahl durch $4 = 2 \cdot 2$ teilbar und damit keine Primzahl. Die Antwort zu Teil a. lautet mithin, daß *keine* Primzahl Rest 0 modulo 4 haben kann. Ähnlich leicht ist Teil c. zu beantworten. Denn wenn der Rest 2 ist bei Division mit Rest durch 4, so ist die Zahl von der Form $4 \cdot k + 2 = 2 \cdot (2k + 1)$ und mithin gerade. Die einzige gerade Primzahl ist aber 2. Es gibt also genau eine Primzahl, die modulo 4 den Rest 2 hat.

Bei den Resten 1 und 3 handelt es sich um ungerade Zahlen, und in die erste Kategorie fallen z.B. 5, 13 und 17, in die zweite die Primzahlen 7, 11 und 19. Dies erweckt den ersten Eindruck, daß es *genauso viele* Primzahlen mit Rest 1 gibt wie mit Rest 3, was in Anbetracht der Tatsache, daß es unendlich viele Primzahlen gibt, zunächst nur heißen soll, daß es auch jeweils unendlich viele Primzahlen der Form

$$4 \cdot k + 1 \quad \text{bzw.} \quad 4 \cdot k + 3$$

gibt. Das ist in der Tat auch richtig, aber der Beweis ist unterschiedlich schwierig. Den letzteren Fall können wir gleich mit ähnlichen Argumenten beweisen wie den Satz des Euklid. Den ersteren Fall müssen wir auf später verschieben.

Proposition 1.14
Es gibt unendlich viele Primzahlen $p \in \mathbb{P}$ *mit* $p \equiv 3 \pmod 4$.

Beweis: Nehmen wir an, es gäbe nur endlich viele solcher Primzahlen

$$p_1 = 4 \cdot k_1 + 3, \ldots, p_n = 4 \cdot k_n + 3 \in \mathbb{P}$$

mit $k_1, \ldots, k_n \in \mathbb{Z}$. Dann betrachten wir die Zahl

$$z = 4 \cdot p_1 \cdots p_n - 1 = 4 \cdot (p_1 \cdots p_n - 1) + 3 \equiv 3 \pmod 4. \tag{1}$$

Nach dem Fundamentalsatz ist z das Produkt von Primzahlen $q_1, \ldots, q_m \in \mathbb{P}$. Wären diese alle von der Form $q_i = 4 \cdot l_i + 1$ mit $l_i \in \mathbb{Z}$, so hätte $z = q_1 \cdots q_m$ nach Aufgabe 1.15 Rest 1 modulo 4, im Widerspruch zu (1). Mithin stimmt eine der Primzahlen q_i mit einer der Primzahlen p_j überein. Dann gilt aber

$$p_j = q_i \mid q_1 \cdots q_m = z = 4 \cdot p_1 \cdots p_n - 1,$$

was nicht möglich ist. □

Aufgabe 1.15
Sind $z_1, \ldots, z_n \in \mathbb{Z}$ mit $z_i \equiv 1 \pmod 4$, so gilt $z_1 \cdots z_n \equiv 1 \pmod 4$.

Proposition 1.14 ist ein Spezialfall des *Primzahlsatzes für arithmetische Progressionen* von Dirichlet, den wir hier zwar formulieren, dessen Beweis aber die Mittel unserer Vorlesung weit übersteigt.

Bemerkung 1.16 (Primzahlsatz von Dirichlet für arithmetische Progressionen)
Sind $n, r \in \mathbb{Z}$ zwei teilerfremde Zahlen, so ist

$$\left|\{p \in \mathbb{P} \mid p \equiv r \pmod n\}\right| = \infty.$$

Zu Frage B: Es ist nicht bekannt, ob es unendlich viele Primzahlzwillingspaare gibt. Alle bisherigen Versuche, die Frage zu beantworten, sind gescheitert. Das größte bekannte Primzahlzwillingspaar ist

$$\left(2003663613 \cdot 2^{195000} - 1, 2003663613 \cdot 2^{195000} + 1\right).$$

Bezeichnen wir mit

$$\pi : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto \left|\{p \in \mathbb{P} \mid p \leq x\}\right|$$

die *Primzahlverteilungsfunktion* bezeichnen und betrachten wir einige Werte dieser Funktion (siehe [RU95, p. 74]),

x	$\pi(x)$
10	4
10^2	25
10^3	168
10^4	1229
10^5	9592
10^6	78498
10^7	664579
10^8	5761445
10^9	50847534
10^{10}	455052512

so sehen wir, daß der Quotient $\frac{\pi(x)}{x}$ für größere Werte von x immer kleiner wird. Etwas salopp ausgedrückt bedeutet das, mit zunehmender Größe werden Primzahlen immer seltener. Der *Große Primzahlsatz* sagt etwas exakter aus, wie sich obiger Quotient verhält, wenn x gegen unendlich strebt:

$$\lim_{x\to\infty} \frac{\pi(x) \cdot \ln(x)}{x} = 1,$$

d.h. $\frac{\pi(x)}{x} \approx \frac{1}{\ln(x)}$. Der Beweis dieses Satzes ist wieder jenseits unserer Möglichkeiten, aber seine Interpretation läßt es mit zunehmender Größe der Zahlen immer unwahrscheinlicher erscheinen, daß auf eine Primzahl *sehr bald* wieder eine Primzahl folgt.

Das legt nahe, daß es nur *endlich* viele Primzahlzwillinge gibt. Daß diese Schlußfolgerung unzulässig ist, wurde kürzlich in der Arbeit [GPY05] gezeigt. Es gibt immer wieder Primzahlen, die dicht beieinander liegen. Also gibt es wohl doch *unendlich* viele Primzahlzwillinge?

Eine verblüffend einfache Frage, auf die die Mathematik die Antwort bislang schuldig geblieben ist!

Aufgabe 1.17
Ist $(p, p+2)$ ein Primzahlzwillingspaar mit $p \geq 5$, so ist $p \equiv 5 \pmod 6$.

Zu Frage C: Wir haben eine positive ganze Zahl $z \in \mathbb{Z}_{>0}$ *vollkommen* genannt, wenn

$$z = \sum_{\substack{1 \leq d < z \\ d \mid z}} d$$

Summe ihrer *echten* positiven Teiler ist. Die *Teilersummenfunktion*

$$\sigma : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} : z \mapsto \sum_{\substack{1 \leq d \leq z \\ d \mid z}} d,$$

die einer positiven ganzen Zahl z *alle* positiven Teiler zuordnet, hat bessere Eigenschaften, und es gilt

$$z \text{ ist vollkommen} \quad \Longleftrightarrow \quad \sigma(z) = 2z.$$

Wir haben auch schon einige Beispiele für vollkommene Zahlen gesehen, und ich will die Liste hier noch etwas ergänzen:

$$\begin{array}{rcl}
z & & \text{Teilersummenzerlegung} \\
6 & = & 1 + 2 + 3 \\
28 & = & 1 + 2 + 4 + 7 + 14 \\
496 & = & 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 \\
8.128 & = & 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064
\end{array}$$

Diese vier vollkommenen Zahlen waren bereits Euklid bekannt. Die nächst größere nicht mehr, was nicht verwundert, wenn wir uns die folgende Liste der fünften bis zehnten vollkommenen Zahl anschauen:

$$\begin{array}{r}
33.550.336 \\
8.589.869.056 \\
137.438.691.328 \\
2.305.843.008.139.952.128 \\
2.658.455.991.569.831.744.654.692.615.953.842.176 \\
191.561.942.608.236.107.294.793.378.084.303.638.130.997.321.548.169.216
\end{array}$$

Wieviel Arbeit ist es eigentlich, zu zeigen, daß die hier angegebenen Zahlen wirklich genau die ersten zehn vollkommenen Zahlen sind? Wenn man naiv an diese Frage herangeht, und schlicht alle Zahlen bis zu der größten oben angegebenen testen möchte, indem man deren Teilersumme bestimmt, so wird man recht alt über dem

Problem. Wir werden unten sehen, daß es mit ein wenig theoretischer Vorarbeit gar nicht so viel rechnerischen Aufwands bedarf.

Es fällt unmittelbar auf, daß die angegebenen Zahlen alle gerade sind, und dies führt uns zur zweiten der Fragen, die wir im Zusammenhang mit vollkommenen Zahlen gestellt haben. Es ist bis heute unbekannt, ob es überhaupt ungerade vollkommene Zahlen gibt. Es ist kein Beispiel bekannt, aber es konnte auch noch niemand zeigen, daß es keine ungerade vollkommene Zahl geben kann. Dies ist ein weiteres Beispiel für eine sehr einfach zu formulierende Frage, auf die die Mathematiker nach wie vor eine Antwort schuldig bleiben.

Ich sollte gleich vorweg sagen, daß wir auch nicht wissen, ob es unendlich viele gerade vollkommene Zahlen gibt oder nur endlich viele! Dennoch sind wir bei dieser Frage ein ganzes Stück weiter. Die Struktur, d.h. die Primfaktorzerlegung, gerader vollkommener Zahlen ist bekannt, und sie ist mit einem Aspekt von Frage E eng verknüpft.

Im folgenden wollen wir diese Strukturaussage beweisen. Dazu ist es zunächst notwendig zu zeigen, daß die Teilersummenfunktion mit der Primfaktorzerlegung ganzer Zahlen verträglich ist.

Proposition 1.18
Für $p \in \mathbb{P}$ *und* $n \in \mathbb{N}$ *gilt*

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

und für eine positive ganze Zahl $z \in \mathbb{Z}$ *gilt*

$$\sigma(z) = \prod_{p \in \mathbb{P}} \sigma\big(p^{n_p(z)}\big).$$

Insbesondere gilt $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$ *für teilerfremde positive ganze Zahlen* a, b*.*

Beweis: Man beachte, daß die positiven Teiler von p^n genau die Zahlen $1, p, p^2, \ldots, p^n$ sind, so daß deren Summe

$$\sigma(p^n) = 1 + p + p^2 + \cdots + p^n = \frac{p^{n+1} - 1}{p - 1}$$

ist, wobei das letzte Gleichheitszeichen aus der Summenformel der geometrischen Reihe folgt. Insbesondere gilt also $\sigma(p^0) = \sigma(1) = 1$, und wir können uns für den Beweis der zweiten Aussage der Proposition auf die Primzahlen $p \in \mathbb{P}$ beschränken, die mit positiver Vielfachheit $n_p(z)$ in z vorkommen.

Für den allgemeinen Fall betrachte man die Primfaktorzerlegung

$$z = \prod_{p \in \mathbb{P}} p^{n_p(z)} = p_1^{n_1} \cdots p_k^{n_k}$$

mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_k \in \mathbb{P}$ und natürlichen Zahlen $n_1, \ldots, n_k \geq 1$. Die positiven Teiler von z sind dann genau die Zahlen

$$p_1^{m_1} \cdots p_k^{m_k}$$

mit
$$0 \le m_k \le n_k.$$
Mithin erhalten wir für die Teilersummenfunktion
$$\sigma(z) = \sum_{m_1=0}^{n_1} \cdots \sum_{m_k=0}^{n_k} p_1^{m_1} \cdots p_k^{m_k} = \left(\sum_{m_1=0}^{n_1} p_1^{m_1}\right) \cdots \left(\sum_{m_k=0}^{n_k} p_k^{m_k}\right) = \sigma\big(p_1^{n_1}\big) \cdots \sigma\big(p_k^{n_k}\big).$$
Die Aussage für teilerfremde a und b folgt unmittelbar, da sie keine gemeinsamen Primteiler besitzen. □

Das Ergebnis der Proposition erlaubt es uns, aus der Primfaktorzerlegung der Zahl mittels einer sehr kurzen Rechnung festzustellen, ob eine Zahl eine vollkommene Zahl ist.

Beispiel 1.19
Für die oben angegebene fünfte vollkommene Zahl erhalten wir die Primfaktorzerlegung
$$33.550.336 = 2^{12} \cdot 8191.$$
Damit gilt
$$\sigma(33.550.336) = \frac{8191^2 - 1}{8191 - 1} \cdot \frac{2^{13} - 1}{2 - 1} = 67.100.672 = 2 \cdot 33.550.336.$$
Die Zahl ist also vollkommen, auch wenn die Rechnung per Hand einige Zeit in Anspruch nimmt.

Auf die gleiche Weise können wir für Zahlen zeigen, daß sie nicht vollkommen sind. Dies leiten wir z.B. aus der Primfaktorzerlegung
$$52 = 2^2 \cdot 13$$
und dem daraus resultierendem Wert
$$\sigma(52) = \frac{13^2 - 1}{12} \cdot (2^3 - 1) = \frac{168}{12} \cdot 7 = 98 \neq 2 \cdot 52.$$
□

Nun sind wir in der Lage, die Charakterisierung gerader vollkommener Zahlen mittels ihrer Primfaktorzerlegung anzugeben. Man beachte dabei, daß jede gerade ganze Zahl z die Gestalt $z = 2^s \cdot a$, wobei $s \ge 1$ eine positive ganze Zahl und $a \in \mathbb{Z}$ ungerade ist. Aus technischen Gründen ist es dabei sinnvoll, den Exponenten s um eins zu verschieben, was wir dadurch erreichen, daß wir ihn durch $q - 1$ mit $q \ge 2$ ersetzen.

Satz 1.20 (Euklid)
Es sei $z = 2^{q-1} \cdot a \in \mathbb{Z}$ eine positive gerade ganze Zahl mit $a \in \mathbb{Z}$ ungerade und $q \ge 2$. Genau dann ist z vollkommen, wenn $a = 2^q - 1$ gilt und a eine Primzahl ist.

Beweis: Setzen wir zunächst voraus, daß $a = 2^q - 1$ eine Primzahl ist. Dann ist $z = 2^{q-1} \cdot a$ die Primfaktorzerlegung von z und aus Proposition 1.18 erhalten wir

$$\sigma(z) = \frac{2^q - 1}{2 - 1} \cdot \frac{a^2 - 1}{a - 1} = a \cdot (a + 1) = a \cdot 2^q = 2 \cdot z.$$

Also ist z eine vollkommene Zahl.

Sei nun umgekehrt z eine vollkommene Zahl, d.h. $\sigma(z) = 2 \cdot z = 2^q \cdot a$. Nach Voraussetzung sind 2^{q-1} und a teilerfremd, so daß wir mit Proposition 1.18

$$2^q \cdot a = \sigma(z) = \sigma(2^{q-1}) \cdot \sigma(a) = (2^q - 1) \cdot \sigma(a)$$

erhalten. Lösen wir die Gleichung nach $\sigma(a)$ auf so folgt

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

Insbesondere gilt dann aber

$$b := \frac{a}{2^q - 1} = \sigma(a) - a \in \mathbb{Z},$$

da sowohl $\sigma(a)$ als auch a ganze Zahlen sind. Damit sind sowohl a als auch b positive Teiler von a, $b < a$ und für die Teilersummenfunktion angewendet auf a gilt

$$a + b = \sigma(a) = \sum_{\substack{1 \le d \le a \\ d \mid a}} d.$$

Dies ist nur möglich, wenn a und b die einzigen Teiler von a sind, was notwendig $b = 1$ zur Folge hat, d.h.

$$a = 2^q - 1.$$

Zudem ist eine Zahl mit nur zwei positiven Teilern eine Primzahl. □

Mit diesem Satz haben wir die Suche nach vollkommenen Zahlen auf die Suche nach Primzahlen der Form $2^q - 1$ reduziert. Darauf kommen wir in Frage E zurück. Wir wollen an dieser Stelle nur noch einige Beispiele betrachten.

Beispiel 1.21
Setzen wir für q kleine Werte ein, so erhalten wir die Tabelle in Abbildung 1.

Wir sehen, wenn wir den obigen Satz anwenden, können wir mit vergleichsweise wenig Rechnungen alle geraden vollkommenen Zahlen bis zu einer vorgegebenen Größe bestimmen, zumindest theoretisch. Denn es bleibt das Problem, bei einer Zahl wie $618.970.019.642.690.137.449.562.111$ zu entscheiden, ob sie prim ist oder nicht!

Weiter oben haben wir angemerkt, daß es bislang weder gelungen ist, eine ungerade vollkommene Zahl zu finden, noch zu zeigen, daß es keine gibt. Es sind jedoch Teilergebnisse bekannt. So weiß man, daß eine ungerade vollkommene Zahl mindestens acht verschiedene Primfaktoren besitzt, und daß sie mindestens 300 Ziffern hat. Acht Primfaktoren ist sicherlich keine besonders große Einschränkung, wo es doch unendlich viele Primzahlen gibt. Aber wenn es unter den ersten 10^{300} ganzen

q	$a = 2^q - 1$	Primzahl?	$z = 2^{q-1} \cdot a.$
2	3	ja	$6 = 2 \cdot 3$
3	7	ja	$28 = 2^2 \cdot 7$
4	15	nein	—
5	31	ja	$496 = 2^4 \cdot 31$
6	63	nein	—
7	127	ja	$8.128 = 2^6 \cdot 127$
$\vdots$			
13	8.191	ja	33.509.376
17	131.071	ja	8.589.869.056
19	524.287	ja	137.438.691.328
31	2.147.483.647	ja	8. vollkommene Zahl
61	2.305.843.009.213.693.951	ja	9. vollkommene Zahl
89	618.970.019.642.690.137.449.562.111	ja	10. vollkommene Zahl

Abbildung 1. Vollkommene Zahlen

Zahlen keine ungerade vollkommene Zahl gibt, ist das nicht so gut wie ein Beweis, daß es keine geben kann? Dazu sollte man die Antwort auf die nächste Frage lesen.

Statt der Teilersummenfunktion kann man auch die *Teileranzahlfunktion* oder die *Teilerproduktfunktion* betrachten, was wir in der folgenden Aufgabe tun wollen.

Aufgabe 1.22
Für eine positive ganze Zahl $z \in \mathbb{Z}_{>0}$ bezeichnen wir mit

$$\tau(z) = \left|\left\{d \in \mathbb{Z}_{>0} \;\middle|\; d \mid z\right\}\right|$$

die Anzahl der positiven Teiler von z, und mit

$$P(z) = \prod_{\substack{1 \le d \le z \\ d \mid z}} d$$

das Produkt aller positiven Teiler. Zeige

$$\tau(z) = \prod_{p \in \mathbb{P}} \left(n_p(z) + 1\right)$$

und

$$P(z) = z^{\frac{\tau(z)}{2}}.$$

Zu Frage D: Die Vermutung, $u_n \geq g_n$ für $n \geq 2$, geht auf den ungarischen Mathematiker Georg Pólya zurück, der sie um 1919 aufstellte (siehe [Pol19]). Er hatte gute Gründe, anzunehmen, daß die Ungleichung gilt. Ein erstes Argument für die Korrektheit haben wir bereits oben gegeben. Zudem prüfte er seine Vermutung für alle natürlichen Zahlen bis 1500. Und schließlich hängt die Korrektheit dieser Vermutung mit einer anderen, weit bekannteren Vermutung zusammen, der *riemannschen Vermutung* zu den Nullstellen der riemannschen Zetafunktion. Der Beweis der *Vermutung von Pólya* würde zugleich einen Beweis für die riemannsche Vermutung liefern, die zu dem Zeitpunkt, als Pólya seine Vermutung aufstellte immerhin schon 60 Jahre einer befriedigenden Antwort harrte, und von deren Richtigkeit man allenthalben überzeugt war. Daß Pólya nicht mehr Beispiele rechnete, lag schlicht am Fehlen von Computern und vielleicht auch einer größeren Anzahl rechenwilliger Studenten.

Pólyas Frage stand ihrerseits etwa 40 Jahre im Raum, ehe eine Antwort gegeben werden konnte, zunächst noch ohne den Einsatz von Rechnern. Es gelang Colin Haselgrove 1958 zu zeigen, daß es in der Tat unendlich viele Zahlen n gibt, für die $u_n < g_n$ gilt, ohne auch nur eine einzige solche Zahl benennen zu können (siehe [Has58]). Das gelang erst zwei Jahre später, und der Grund dafür ist recht offensichtlich, wenn man sich die *kleinste* natürliche Zahl $n \geq 2$ betrachtet, für die $u_n < g_n$ gilt (siehe [Tan80]):

$$n = 906.150.257.$$

Für dieses n gilt $u_n = g_n - 1$. Die größte bekannte Differenz ist $g_n - u_n = 828$.

Pólyas Vermutung ist also falsch, und das Gegenbeispiel hat schon eine beachtliche Größe. Das sollte eine erste Warnung davor sein, einen Beweis durch das Testen *vieler* Zahlen ersetzen zu wollen!

Die riemannsche Vermutung harrt im Übrigen weiter ihrer Antwort, nun schon fast seit 150 Jahren, denn Pólyas Vermutung hätte die riemannsche Vermutung zwar impliziert, nicht aber umgekehrt.

Zu Frage E, Teil a.: Die Funktion $n \mapsto n^2 + n + 41$ ist eine sehr bemerkenswerte Funktion. Betrachten wir ihre Werte für $n = 0, \ldots, 39$:

n	0	1	2	3	4	5	6	7	8	9
n^2+n+41	41	43	47	53	61	71	83	97	113	131
n	10	11	12	13	14	15	16	17	18	19
n^2+n+41	151	173	197	223	251	281	313	347	383	421
n	20	21	22	23	24	25	26	27	28	29
n^2+n+41	461	503	547	593	641	691	743	797	853	911
n	30	31	32	33	34	35	36	37	38	39
n^2+n+41	971	1033	1097	1163	1231	1301	1373	1447	1523	1601

Der Wert von n^2+n+41 ist in jedem dieser Beispiele eine Primzahl. Die erste Zahl n für die das nicht mehr der Fall ist, ist $n = 40$. Dann ist $n^2+n+41 = 1681 = 41^2$. Ein Polynom so kleinen Grades, das eine so große Anzahl an Primzahlen produziert ist ein Kuriosum.

Im Übrigen kann kein Polynom wirklich eine Primzahl erzeugende Funktion sein.

Proposition 1.23
Es sei $f \in \mathbb{Z}[t]$ *ein Polynom mit* $\deg(f) \geq 1$*, so gibt es kein* $n_0 \in \mathbb{N}$ *mit* $f(n) \in \mathbb{P}$ *für alle* $n \geq n_0$*.*

Beweis: Sei $f \in \mathbb{Z}[t]$ ein Polynom, für das es ein $n_0 \in \mathbb{N}$ gibt mit $f(n) \in \mathbb{P}$ für alle $n \geq n_0$. Nach Voraussetzung ist

$$p := f(n_0) \in \mathbb{P}$$

eine Primzahl und für $j \in \mathbb{N}$ gilt $n_0 \equiv n_0 + j \cdot p \pmod{p}$. Nach Aufgabe 1.24 gilt deshalb

$$f(n_0 + j \cdot p) \equiv f(n_0) \equiv 0 \pmod{p},$$

d.h. p ist ein Teiler der ganzen Zahl $f(n_0+j\cdot p)$. Da $f(n_0+j\cdot p)$ nach Voraussetzung eine Primzahl ist, bedeutet das $f(n_0 + j \cdot p) = p$ für alle $j \in \mathbb{N}$. Aber dann hat das Polynom

$$g := f - p \in \mathbb{Z}[t] \subset \mathbb{Q}[t]$$

unendlich viele Nullstellen. Aus der Vorlesung algebraische Strukturen wissen wir, daß das nur geht, wenn $g = 0$ das Nullpolynom ist. Also ist $f = p$ ein Polynom vom Grad 0. $\square$

Aufgabe 1.24
Ist $f \in \mathbb{Z}[t]$ ein Polynom und sind $a, b, n \in \mathbb{Z}$ ganze Zahlen mit $a \equiv b \pmod{n}$, so ist $f(a) \equiv f(b) \pmod{n}$.

Zu Frage E, Teil b.: In Satz 1.20 haben wir gesehen, daß die Zahl $a = 2^{q-1}\cdot(2^q-1)$ genau dann vollkommen ist, wenn $2^q - 1$ eine Primzahl ist. Primzahlen der Form $M_q := 2^q - 1$ mit $q \geq 2$ nennen wir *Mersennesche Primzahlen.*

Zudem haben wir in Beispiel 1.21 gesehen, daß dies für $q \in \{2, 3, 5, 7, 13, 17, 19, 31, 61, 89\}$ der Fall ist. Dem geübten Auge fällt auf, daß diese Zahlen Primzahlen sind. Das ist kein Zufall, wie Proposition 1.25 zeigt. Ist M_q eine Primzahl, so trifft dies auf q notwendigerweise ebenfalls zu. Aber nicht jede Primzahl q führt auch zu einer Mersenneschen Primzahl:

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

Der französische Mathematiker Marin Mersenne gab 1644 eine Liste der Mersenneschen Primzahlen für $2 \leq q \leq 257$, die allerdings Fehler enthielt, was nicht so verwundert, wenn man bedenkt, wie rasch die Zahlen anwachsen. So erkannte er z.B. nicht, daß

$$M_{257}=231.584.178.474.632.390.847.141.970.017.375.815.706.539.969.331.281.128.078.915.168.015.826.259.279.871$$

keine Primzahl ist. Ein verzeihlicher Fehler, wie mir scheint, wenn man bedenkt, daß ihm keine elektronischen Hilfsmittel zur Faktorisierung zur Verfügung standen. Der Leser mag sich daran versuchen, die Primfaktorzerlegung von M_{257} zu finden.

Die größte zur Zeit bekannte Mersennesche Primzahl ist zugleich die größte zur Zeit überhaupt bekannte Primzahl:

$$M_{32.582.657} = 2^{32582657} - 1.$$

Die zugehörige vollkommene Zahl hat über 19 Millionen Stellen.

Bislang hat man nur 44 Mersennesche Primzahlen finden können, und es ist ein weiteres offenes Problem, ob es unendlich viele Mersennesche Primzahlen gibt! Wer sich an der Suche nach weiteren Mersenneschen Primzahlen beteiligen möchte, kann dies über das GIMPS-Projekt tun:

http://www.mersenne.org

Proposition 1.25 (Mersennesche Primzahlen)
Ist $M_q = 2^q - 1 \in \mathbb{P}$, $q \geq 2$, *eine Mersennesche Primzahl, so ist* $q \in \mathbb{P}$ *eine Primzahl.*

Beweis: Ist q keine Primzahl, so gibt es ganze Zahlen $m, n \geq 2$ mit $q = m \cdot n$. Dann ist

$$M_q = ((2^m)^n - 1) = (2^m - 1) \cdot \sum_{i=0}^{n-1} 2^{mi}$$

ein Produkt von zwei positiven Zahlen, die beide größer als 1 sind. Mithin ist q nicht irreduzibel, also keine Primzahl. □

Zu Frage E, Teil c.: Wir haben gesehen, daß keine polynomiale Funktion primzahlerzeugend sein kann und daß die exponentielle Funktion $\mathbb{P} \to \mathbb{Z} : q \mapsto 2^q - 1$ auch nicht funktioniert. Beides war Pierre de Fermat (1601-1665) bekannt, und er versuchte sich an einer doppelt exponentiellen Funktion. Er stellte die Vermutung auf, daß die *Fermatschen Zahlen*

$$F_n := 2^{(2^n)} + 1$$

für alle $n \in \mathbb{N}$ Primzahlen sind. Man nennt Primzahlen dieser Form *Fermatsche Primzahlen*. Er verifizierte seine Behauptung für $n = 0, \ldots, 4$:

n	F_n		
0	3	$=$	$2^1 + 1$
1	5	$=$	$2^2 + 1$
2	17	$=$	$2^4 + 1$
3	257	$=$	$2^8 + 1$
4	65537	$=$	$2^{16} + 1$

Leonard Euler zeigte 1732, daß aber schon die fünfte Fermatsche Zahl

$$F_5 = 2^{32} + 1 = 4.294.967.297 = 641 \cdot 6.700.417$$

keine Primzahl mehr ist. Aufgrund des schnellen Wachstums der Exponentialfunktion, ist es schwierig, die Fermatschen Zahlen für wachsendes n zu untersuchen.

Bislang ist es gelungen, für $F_5, \ldots, F_{12}$ die zugehörige Primfaktorzerlegung anzugeben, und keine von ihnen ist eine Primzahl.

Es wäre in der Tat interessant, weitere Fermatsche Primzahlen zu finden, denn Carl Friedrich Gauß (1777–1855) zeigte, daß das regelmäßige n-Eck für ungerades n genau dann mit Zirkel und Lineal zu konstruieren ist, wenn n ein Produkt verschiedener Fermatscher Primzahlen ist. Fragen dieser Art werden in der Vorlesung *Einführung in die Algebra* behandelt.

Bemerkung 1.26
Ist $p = 2^q + 1 \in \mathbb{P}$, so ist p notwendigerweise eine Fermatsche Primzahl, d.h. $q = 2^n$ für ein $n \in \mathbb{N}$.

Beweis: Ist p eine Primzahl und $q = 2^n \cdot k$ mit $k \in \mathbb{Z}_{>0}$ ungerade. Dann hat p die Zerlegung

$$p = 1 + 2^{2^n \cdot k} = 1 - \left(-2^{(2^n)}\right)^k = \left(1 + 2^{(2^n)}\right) \cdot \sum_{i=0}^{k-1} \left(-2^{(2^n)}\right)^i ,$$

wobei das zweite Gleichheitszeichen ausnutzt, daß k ungerade ist, und das dritte auf die Summenformel der geometrischen Reihe zurück geht. Da der erste der beiden Faktoren, $1 + 2^{2^n}$, größer als 1 ist und da p eine Primzahl ist, muß der zweite Faktor 1 sein. Das geht aber nur, wenn er nur einen Summanden hat, k also 1 ist. $\square$

Zu Frage F, Teil a.: Der Test "p ungerade, $3 \not| \; p$, $5 \not| \; p$ impliziert $p \in \mathbb{P}$" funktioniert für die positiven ganzen Zahlen bis 48 und liefert die Primzahlen $7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$. Bei der Zahl $49 = 7 \cdot 7$ versagt er jedoch. Es wäre schön, einen solch einfachen Test der Primzahleigenschaft zu haben, aber das zu erwarten, ist etwas viel verlangt.

Zu Frage F, Teil b.: Vor etwa 2500 Jahren verwendeten die Chinesen den Test

$$p \in \mathbb{P} \quad \Longleftrightarrow \quad p \mid (2^p - 2),$$

um für eine Zahl festzustellen, ob sie eine Primzahl ist. Schauen wir uns kleine Beispiele an:

p	$2^p - 2$	$p \mid (2^p - 2)$?	$p \in \mathbb{P}$?
2	2	ja	ja
3	6	ja	ja
4	14	nein	nein
5	30	ja	ja
6	62	nein	nein
7	126	ja	ja
8	254	nein	nein

Das sieht doch recht überzeugend aus. Die Aussage ist dennoch nicht korrekt. Obwohl $341 = 11 \cdot 31$ keine Primzahl ist, gilt

$$341 \mid 2^{341} - 2.$$

Es ist das kleinste Gegenbeispiel und die Zahl $2^{341} - 2$ hat bereits 106 Ziffern. Insofern verwundert es nicht, daß der Fehler vor 2500 Jahren nicht aufgefallen ist. Ich würde auch nicht unbedingt dazu raten, die Zahl $2^{341} - 2$ auszurechnen, um zu zeigen, daß 341 ein Teiler ist. Wir werden später sehen, daß dieses Resultat mit ein wenig Theorie leicht folgt. Zugleich werden wir zeigen, daß immerhin eine der beiden obigen Implikationen richtig ist:

$$p \in \mathbb{P} \quad \Longrightarrow \quad p \mid (2^p - 2). \tag{2}$$

Zwar sind Zahlen, die der Bedingung $p \mid (2^p - 2)$ genügen, nicht notwendigerweise Primzahlen, aber sie haben interessante Eigenschaften, aufgrund derer sie für manche Anwendungen *fast* so gut geeignet sind wie Primzahlen. Man nennt sie deshalb *Pseudoprimzahlen zur Basis* 2. Wir werden später sehen, daß alle Fermatschen Zahlen F_n, $n \in \mathbb{N}$, Pseudoprimzahlen zur Basis 2 sind.

Aufgabe 1.27
Verwende (2), um zu zeigen, daß jede Mersennesche Zahl $M_q = 2^q - 1$ mit $q \in \mathbb{P}$ eine Pseudoprimzahl zur Basis 2 ist.

Zu Frage F, Teil c.: Der Test

$$p \in \mathbb{P} \quad \Longleftrightarrow \quad p \mid \big((p-1)! + 1\big)$$

funktioniert! Dies ist im wesentlichen die Aussage des *Satzes von Wilson*, den wir im Laufe der Vorlesung beweisen werden. Einen praktischen Nutzen als Primzahltest hat die Bedingung allerdings nicht, da die Fakultät eine viel zu schnell wachsende Funktion auf $\mathbb{N}$ ist. Man kann das Ergebnis des Satzes jedoch verwenden, um weitere interessante Fragen zu lösen.

Die folgende Aufgabe beweist eine der beiden Folgerichtungen der obigen Aussage.

Aufgabe 1.28
Ist $n \in \mathbb{Z}$ mit $n > 4$ keine Primzahl, so gilt $n \mid (n-1)!$.

Zu Frage G: Die Antwort auf Teil b. ist leicht zu geben. Damit eine ungerade Zahl z Summe zweier Primzahlen ist, muß eine der beiden Primzahlen notwendigerweise 2 sein. Mithin ist

$$\{p + 2 \mid p \in \mathbb{P}\}$$

genau die Menge der ungeraden Zahlen, die Summe zweier Primzahlen sind, und diese Menge ist unendlich. Schränken wir die Frage darauf ein, wann eine Primzahl $q \in \mathbb{P}$ Summe zweier Primzahlen ist, so stellen wir fest, daß dies genau dann der Fall ist, wenn $(q-2, q)$ ein Primzahlzwilling ist. Ob es davon unendlich viele gibt, ist nicht bekannt, wie wir in Frage B gesehen haben.

Teil a. der Frage ist die sogenannte *Goldbachsche Vermutung*, die Christian Goldbach im Zusammenwirken mit Leonard Euler 1742 aufstellte.

z	4	6	8	10	12	14	16	18	20
$p+q$	$2+2$	$3+3$	$3+5$	$5+5$	$5+7$	$7+7$	$5+11$	$7+11$	$7+13$

Eine solche Zerlegung ist natürlich nicht notwendigerweise eindeutig bestimmt:

$$16 = 5 + 11 = 3 + 13.$$

Im Übrigen ist bis heute unbekannt, ob die Goldbachsche Vermutung zutrifft oder nicht. Sie ist ein weiteres *elementares* ungelöstes Problem.

Zu Frage H: Es geht um die Frage, welche natürlichen Zahlen n sich als Summe zweier Quadratzahlen darstellen lassen. Indem man systematisch alle natürlichen Zahlen quadriert und Summen bildet, kann man erste Beispiele konstruieren:

$$\begin{aligned}
0&=0^2+0^2\\
1&=0^2+1^2\\
2&=1^2+1^2\\
4&=0^2+2^2\\
5&=1^2+2^2\\
8&=2^2+2^2\\
9&=0^2+3^2
\end{aligned}$$

Wir wollen noch mehr Beispiele anführen, geben dabei aber nicht mehr die Zerlegung an. Zudem ordnen wir sie schematisch, so daß eine gewisse Struktur erkennbar wird:

0	1	2	·	4	5	·	·
8	9	10	·	·	13	·	·
16	17	18	·	20	·	·	·
·	25	26	·	·	29	·	·
32	·	34	·	36	37	·	·
40	41	·	·	·	45	·	·
·	49	50	·	52	53	·	·

Ein Punkt in der Tabelle deutet an, daß die Zahl nicht Summe zweier Quadrate ist. Es fällt auf, daß die vierte, die siebte und die achte Spalte leer bleiben. Eine Zahl in der vierten Spalte hat modulo 8 den Rest 3, analoges gilt für die Zahlen der Spalten sieben und acht. Um solche Zahlen scheint es also nicht gut bestellt zu sein, bei dieser Fragestellung. Es wird eines der Hauptanliegen dieser Vorlesung sein, die Zahlen n vollständig zu klassifizieren, die sich als Summe zweier Quadratzahlen schreiben lassen. Dabei soll klassifizieren bedeuten, daß wir die Primfaktorzerlegung der zulässigen Zahlen n angeben.

Zu Frage I: Wir wollen alle Tripel (x, y, z) positiver ganzer Zahlen bestimmen, die der Bedingung

$$x^2 + y^2 = z^2$$

genügen. Da diese als ganzzahlige Seitenlängen von rechtwinkligen Dreiecken auftreten, haben wir sie *pythagoreische Zahlentripel* genannt. Wir nennen ein pythagoreisches Zahlentripel *teilerfremd*, falls es keine Primzahl gibt, die alle drei Zahlen x, y und z teilt. Wir werden weiter unten im Zusammenhang mit *linearen diophantischen Gleichungen* den Begriff teilerfremd genauer untersuchen (siehe Definition 2.1).

Satz 1.29 (Pythagoreische Zahlentripel)
Es seien $x, y, z \in \mathbb{Z}_{>0}$ positive ganze Zahlen.

a. *Genau dann ist (x, y, z) ein pythagoreisches Zahlentripel, wenn für alle $a \in \mathbb{Z}_{>0}$ auch $(a \cdot x, a \cdot y, a \cdot z)$ ein pythagoreisches Zahlentripel ist.*

b. *Ist (x, y, z) ein teilerfremdes pythagoreisches Zahlentripel, so ist genau eine der beiden Zahlen x oder y eine gerade Zahl und z ist auf alle Fälle ungerade.*

c. *Genau dann ist (x, y, z) ein teilerfremdes pythagoreisches Zahlentripel mit geradem x, wenn es positive ganze Zahlen $u, v \in \mathbb{Z}_{>0}$ mit*

$$u < v, \quad \mathrm{ggt}(u, v) = 1 \quad \textit{und} \quad v - u \equiv 1 \pmod 2$$

gibt, so daß

$$x = 2 \cdot u \cdot v, \quad y = v^2 - u^2 \quad \textit{und} \quad z = v^2 + u^2.$$

Bemerkung 1.30
Bevor wir den Satz beweisen wollen wir anmerken, daß damit die pythagoreischen Zahlentripel vollständig klassifiziert sind. Teil a. sagt aus, daß es reicht, die teilerfremden pythagoreischen Zahlentripel zu bestimmen, um alle zu kennen. Da (x, y, z) genau dann ein pythagoreisches Zahlentripel ist, wenn dies auf (y, x, z) zutrifft, folgt aus Teil b., daß in Teil c. alle teilerfremden pythagoreischen Zahlentripel bis auf Vertauschung von x und y bestimmt werden.

Man beachte auch, daß die Bedingung in Teil c. konstruktiv ist:

Pythagoreische Zahlentripel

u	v	$x = 2 \cdot u \cdot v$	$y = v^2 - u^2$	$z = v^2 + u^2$	$x^2 + y^2 = z^2$
1	2	4	3	5	25
2	3	12	5	13	169
1	4	8	15	17	289

Beweis von Satz 1.29:

a. Für $a \in \mathbb{Z}_{>0}$ gilt

$$(a \cdot x)^2 + (a \cdot y)^2 - (a \cdot z)^2 = a^2 \cdot \left(x^2 + y^2 - z^2\right),$$

und da $\mathbb{Z}$ ein Integritätsbereich ist, ist dieser Ausdruck genau dann Null, wenn $x^2 + y^2 = z^2$ gilt. Dies beweist Teil a. der Aussage.

b. Betrachten wir die Gleichung

$$x^2 + y^2 = z^2$$

modulo 2, so sehen wir, daß nur die folgenden drei Fälle möglich sind:

- z ist gerade und
  - x und y sind beide auch gerade, oder
  - x und y sind beide ungerade.
- z ist ungerade und genau eine der Zahlen x und y ist ungerade.

Im ersten Fall hätten die Zahlen x, y und z den gemeinsamen Primteiler 2 im Widerspruch zur Voraussetzung. Wären $x = 2 \cdot k + 1$ und $y = 2 \cdot l + 1$ beide ungerade, so wäre

$$z^2 = x^2 + y^2 = 4 \cdot \left(k^2 + k + l^2 + l\right) + 2 \equiv 2 \pmod 4,$$

im Widerspruch dazu, daß z^2 als Quadrat einer geraden Zahl durch 4 teilbar sein muß. Mithin ist z ungerade und genau eine der Zahlen x und y ist gerade.

c. Sei zunächst (x, y, z) ein teilerfremdes pythagoreisches Zahlentripel mit geradem x. Dann sind y und z nach Teil b. ungerade und mithin gibt es ganze Zahlen $a, b, c \in \mathbb{Z}_{>0}$ so, daß

$$x = 2 \cdot a, \quad z - y = 2 \cdot b \quad \text{und} \quad z + y = 2 \cdot c.$$

Für einen Primteiler $p \in \mathbb{P}$ von b und c würde

$$\begin{aligned} &p \mid b + c = z, \\ &p \mid c - b = y, \\ &p \mid 2 \cdot b \cdot 2 \cdot c = (z - y) \cdot (z + y) = z^2 - y^2 = x^2 \end{aligned}$$

gelten. Da p eine Primzahl ist, würde p dann auch x teilen, im Widerspruch zur Annahme, daß die Zahlen x, y und z keinen gemeinsamen Primteiler haben. Mithin sind b und c teilerfremd. Betrachten wir die Primfaktorzerlegung von

$$x^2 = 4 \cdot b \cdot c,$$

so folgt aus der Teilerfremdheit von b und c, daß b und c Quadratzahlen sein müssen, d.h. es gibt Zahlen $u, v \in \mathbb{Z}_{>0}$ mit

$$b = u^2 \quad \text{und} \quad c = v^2.$$

Damit gilt

$$z = b + c = u^2 + v^2, \ y = c - b = v^2 - u^2 \text{ und } x = \sqrt{4 \cdot b \cdot c} = 2 \cdot u \cdot v.$$

Zudem sind mit b und c auch u und v teilerfremd, aus $y > 0$ folgt $v > u$, und da $y = (v + u) \cdot (v - u)$ ungerade ist, kann $v - u$ nicht gerade sein.

Seien nun umgekehrt teilerfremde Zahlen $u, v \in \mathbb{Z}_{>0}$, so daß $v - u$ eine ungerade positive Zahl ist. Setzen wir

$$x := 2 \cdot u \cdot v, \quad y := v^2 - u^2 \quad \text{und} \quad z := v^2 + u^2,$$

so gilt

$$x^2 + y^2 = 4 \cdot u^2 \cdot v^2 + v^4 - 2 \cdot u^2 \cdot v^2 + u^4 = v^4 + 2 \cdot u^2 \cdot v^2 + u^4 = z^2.$$

Also ist (x, y, z) ein pythagoreisches Zahlentripel und es bleibt nur zu zeigen, daß die Zahlen x, y und z keinen gemeinsamen Teiler haben. Dazu nehmen wir an, $p \in \mathbb{P}$ sei ein Teiler dieser drei Zahlen. Dann gilt

$$p \mid z + y = 2 \cdot v^2 \quad \text{und} \quad p \mid z - y = 2 \cdot u^2.$$

Da u und v teilerfremd sind, muß notwendigerweise $p = 2$ gelten. Aber nach Voraussetzung ist 2 kein Teiler von $v - u$ und mithin weder ein Teiler von $v + u = (v - u) + 2 \cdot u$ noch von $y = (v + u) \cdot (v - u)$. Also gibt es keine solche Primzahl p.

□

Zu Frage J: Diese Frage ist auch als *Fermats letzter Satz* bekannt. 1637 schrieb Pierre de Fermat eine Randnotiz in seine Ausgabe von Diophantus' Arithmetica, in der er behauptete, einen Beweis dafür erbracht zu haben, daß die Gleichung

$$x^n + y^n = z^n$$

für $n \geq 3$ keine ganzzahlige Lösung besitze, bei der nicht mindestens eine der Zahlen x, y oder z Null ist. Er schrieb dort auch, daß der Rand leider zu schmal sei, seinen Beweis zu fassen. Da dieser Beweis von Fermat auch in keinem anderen Schriftstück überliefert ist, kann nicht geklärt werden, ob er in der Tat über einen (korrekten) Beweis verfügte. *Falsche Beweis(versuch)e* gab es seither in reichlicher Anzahl, aber für Jahrhunderte zählte die Aussage Fermats als die *Fermatsche Vermutung* zu den vielen ungelösten elementaren Problemen der Zahlentheorie, bis 1993. In diesem Jahr bewies Andrew Wiles eine andere, weit tiefliegendere Vermutung von Taniyama und Shimura zur Modularität von elliptischen Kurven, die dank der Vorarbeit anderer Mathematiker Fermats Vermutung als richtig erwies.

Die Fermatsche Vermutung, oder nun zu recht Fermats letzter *Satz*, ist ein gutes Beispiel dafür, wie eine scheinbar simple Frage die Entwicklung von schwierigen mathematischen Theorien anstoßen und beflügeln kann. Angesichts der schweren Maschinerie, die aufgeboten wurde, um den Satz zu beweisen, mögen Zweifel an der Frage erlaubt sein, ob Fermat wirklich einen Beweis seiner Behauptung hatte, aber zumindest scheint es sehr glaubhaft, daß er nicht auf den Rand von Diophantus' Arithmetica paßte.

Für einige spezielle Werte von n waren Beweise der Aussage seit langem bekannt. Fermat selbst gab einen Beweis für $n = 4$; auf Leonhard Euler geht ein Beweis für $n = 3$ zurück (1753); 1825 bewiesen Peter Gustav Lejeune-Dirichlet und Adrien-Marie Legendre die Aussage für $n = 5$; der Fall $n = 7$ wurde 1839 von Gabriel Lamé gezeigt.

Fermats letzter Satz für den Fall $n = 4$ ist eine unmittelbare Folgerung aus der folgenden Aufgabe.

Aufgabe 1.31
Zeige, es gibt keine ganzen positiven Zahlen $x, y, z \in \mathbb{Z}_{>0}$, so daß $x^4 + y^4 = z^2$.

Hinweis, man betrachte ein solches Tripel mit *minimalem* z und wende zweimal Satz 1.29 zur Klassifikation der pythagoreischen Zahlentripel an.

Zu Frage K: Diese Frage ist noch besser geeignet als Frage D, um zu zeigen, daß es gefährlich ist, die ersten paar Millionen positiver ganzer Zahlen zu testen, um eine allgemeingültige Aussage über alle ganzen Zahlen zu treffen. Es gibt *unendlich viele* positive Zahlen $y \in \mathbb{Z}_{>0}$, so daß die reelle Zahl

$$\sqrt{1141 \cdot y^2 + 1} \in \mathbb{Z}$$

wieder eine ganze Zahl ist, aber die kleinste solche Zahl hat 26 Ziffern:

$$30.693.385.322.765.657.197.397.208.$$

Wir haben oben gesehen, daß diese Frage gleichwertig zur Suche einer ganzzahligen Lösung der Gleichung

$$x^2 - 1141 \cdot y^2 = 1$$

ist. Man nennt Gleichungen der Form

$$x^2 - d \cdot y^2 = \pm 1$$

Pellsche Gleichungen, wenn $d \in \mathbb{Z}_{>0}$ *keine Quadratzahl* ist. Wir kommen auf die Lösbarkeit solcher Gleichungen im Zusammenhang mit den quadratischen Zahlkörpern zurück.

Dies soll als erste Antwort auf die oben gestellten Fragen genügen. Einige der Probleme werden im Verlauf der Vorlesung wieder auftauchen, und wir werden sehen, wie die entwickelte Theorie dazu beiträgt, Licht ins Dunkel zu bringen.

2 Lineare diophantische Gleichungen

Wir haben schon am Ende von Kapitel 1, Abschnitt B) darauf hingewiesen, daß die Lösbarkeit von diophantischen Gleichungen ein zentrales Thema dieser Vorlesung ist. Wir wollen hier den einfachsten Fall, daß nämlich alle Exponenten der Variablen in der Gleichung 1 sind, vollständig lösen. Dazu verallgemeinern wir zunächst den Begriff des *größten gemeinsamen Teilers*, der aus den algebraischen Strukturen bekannt ist.

Definition 2.1
Es seien $z_1, \ldots, z_n \in \mathbb{Z}$ ganze Zahlen. Eine ganze Zahl $g \in \mathbb{Z}$ heißt *größter gemeinsamer Teiler* von $z_1, \ldots, z_n$, wenn sie folgenden beiden Eigenschaften genügt:

- $g \mid z_i$ für alle $i = 1, \ldots, n$, und
- $\forall\, h \in \mathbb{Z}$ mit $h \mid z_i$ für alle $i = 1, \ldots, n$ gilt $h \mid g$.

Wir bezeichnen mit $\mathrm{ggT}(z_1, \ldots, z_n)$ die Menge der größten gemeinsamen Teiler von $z_1, \ldots, z_n$, und wir nennen $z_1, \ldots, z_n$ *teilerfremd*, wenn $1 \in \mathrm{ggT}(z_1, \ldots, z_n)$.

Man beachte, daß die erste Bedingung bedeutet, daß g ein Teiler von $z_1, \ldots, z_n$ ist, und die zweite Bedingung faßt den Begriff *größer* als jeder andere Teiler zu sein.

Für den Fall $n = 2$ stimmt die Definition mit der Definition der Vorlesung algebraische Strukturen überein, und die Aussagen der folgenden Proposition wurden für diesen Fall in derselben Vorlesung bewiesen. Der Beweis der allgemeineren Aussage ist dem Leser als Übungsaufgabe überlassen. Allerdings möchte ich an dieser Stelle in Erinnerung rufen, daß das Erzeugnis von $z_1, \ldots, z_n \in \mathbb{Z}$,

$$\langle z_1, \ldots, z_n \rangle_{\mathbb{Z}} = \bigcap_{z_1,\ldots,z_n \in I \trianglelefteq \mathbb{Z}} I = \{a_1 \cdot z_1 + \ldots + a_n \cdot z_n \mid a_1, \ldots, a_n \in \mathbb{Z}\},$$

der Schnitt aller Ideale ist, die $z_1, \ldots, z_n$ enthalten, und zugleich die Menge der $\mathbb{Z}$-Linearkombinationen von $z_1, \ldots, z_n$ ist.

Proposition 2.2
Es seien $z_1, \ldots, z_n \in \mathbb{Z}$ ganze Zahlen.

a. $g \in \mathrm{ggT}(z_1, \ldots, z_n)$ *genau dann, wenn* $g \in \mathrm{ggT}\big(\mathrm{ggt}(z_1, z_2), z_3, \ldots, z_n\big)$.
b. $g \in \mathrm{ggT}(z_1, \ldots, z_n)$ *genau dann, wenn* $\langle g \rangle_{\mathbb{Z}} = \langle z_1, \ldots, z_n \rangle_{\mathbb{Z}}$.
c. *Ist* $g \in \mathrm{ggT}(z_1, \ldots, z_n)$, *so ist* $\mathrm{ggT}(z_1, \ldots, z_n) = \{g, -g\}$.
d. *Wenn nicht alle* z_i *Null sind, dann gilt*

$$\mathrm{ggt}(z_1, \ldots, z_n) := \prod_{p \in \mathbb{P}} p^{\min\{n_p(z_1), \ldots, n_p(z_n)\}} \in \mathrm{ggT}(z_1, \ldots, z_n).$$

Bemerkung 2.3
Man beachte, daß aus Teil c. und d. folgt, daß $\mathrm{ggt}(z_1, \ldots, z_n)$ *der* eindeutig bestimmte positive größte gemeinsame Teiler von $z_1, \ldots, z_n$ ist. Damit sind $z_1, \ldots, z_n$ genau dann teilerfremd, wenn $\mathrm{ggt}(z_1, \ldots, z_n) = 1$.

Aus Teil b. folgt, daß es ganze Zahlen $a_1, \ldots, a_n \in \mathbb{Z}$ gibt, so daß

$$\operatorname{ggt}(z_1, \ldots, z_n) = a_1 \cdot z_1 + \ldots + a_n \cdot z_n. \tag{3}$$

Im Fall $n = 2$ haben wir in der Vorlesung algebraische Strukturen gesehen, daß man mittels des Euklidischen Algorithmus den positiven größten gemeinsamen Teiler $\operatorname{ggt}(z_1, z_2)$ berechnen kann, und daß man darüber hinaus durch Rückeinsetzen auch Zahlen a_1 und a_2 bestimmen kann mit $\operatorname{ggt}(z_1, z_2) = a_1 \cdot z_1 + a_2 \cdot z_2$. Teil a. von Proposition 2.2 zeigt nun, daß man induktiv mittels des Euklidischen Algorithmus auch den positiven größten gemeinsamen Teiler $\operatorname{ggt}(z_1, \ldots, z_n)$ von $z_1, \ldots, z_n$ bestimmen kann. Zudem kann man durch sukzessives Rückeinsetzen auch die Zahlen $a_1, \ldots, a_n$ in (3) bestimmen.

Beispiel 2.4
Betrachten wir die Zahlen $z_1 = 70$, $z_2 = 84$ und $z_3 = 105$. Wir berechnen zunächst $\operatorname{ggt}(70, 84)$.

$$\begin{aligned} 84 =& 1 \cdot 70 + 14 \\ 70 =& 5 \cdot 14 + 0 \\ \Longrightarrow & \operatorname{ggt}(70, 84) = 14 \end{aligned}$$

Dann berechnen wir $\operatorname{ggt}\big(\operatorname{ggt}(70, 84), 105\big) = \operatorname{ggt}(14, 105)$:

$$\begin{aligned} 105 =& 7 \cdot 14 + 7 \\ 14 =& 2 \cdot 7 + 0 \\ \Longrightarrow & \operatorname{ggt}(14, 105) = 7 \end{aligned}$$

Nun können wir sukzessive rückeinsetzen. Aus der zweiten ggt-Berechnung erhalten wir

$$7 = 1 \cdot 105 - 7 \cdot 14,$$

und die erste liefert uns

$$14 = 1 \cdot 84 - 1 \cdot 70.$$

Setzen wir beide Gleichungen ineinander ein, so erhalten wir:

$$\operatorname{ggt}(70, 84, 105) = 7 = 1 \cdot 105 - 7 \cdot (1 \cdot 84 - 1 \cdot 70) = 7 \cdot 70 - 7 \cdot 84 + 1 \cdot 105.$$

Mit den Bezeichnungen aus Bemerkung 2.3 ist also $a_1 = 7$, $a_2 = -7$ und $a_3 = 1$.

Eine unmittelbare Folgerung aus Proposition 2.2 ist die Lösbarkeit linearer diophantischer Gleichungen.

Satz 2.5 (Lineare diophantische Gleichungen)
Seien $c_0, c_1, \ldots, c_n \in \mathbb{Z}$ ganze Zahlen, so daß $c_1, \ldots, c_n$ nicht alle Null sind. Genau dann besitzt die lineare diophantische Gleichung

$$c_0 = c_1 \cdot x_1 + \ldots + c_n \cdot x_n$$

eine Lösung in $\mathbb{Z}$, wenn $\operatorname{ggt}(c_1, \ldots, c_n)$ die Zahl c_0 teilt.

Beweis: Genau dann gibt es ganze Zahlen $z_1, \ldots, z_n \in \mathbb{Z}$ mit

$$c_0 = c_1 \cdot z_1 + \ldots + c_n \cdot z_n,$$

wenn

$$c_0 \in \{c_1 \cdot a_1 + \ldots + c_n \cdot a_n \mid a_1, \ldots, a_n \in \mathbb{Z}\} = \langle c_1, \ldots, c_n \rangle_{\mathbb{Z}}.$$

Aber nach Proposition 2.2 ist dieses Ideal von $\mathrm{ggt}(c_1, \ldots, c_n)$ erzeugt, so daß c_0 genau dann darin enthalten ist, wenn $\mathrm{ggt}(c_1, \ldots, c_n)$ ein Teiler von c_0 ist. □

Bemerkung 2.6
Der Satz gibt ein Kriterium, wie man feststellen kann, ob eine lineare diophantische Gleichung lösbar ist, und die Ausführungen in Bemerkung 2.3 zeigen, wie man eine Lösung bestimmen kann. Ist nämlich

$$g = \mathrm{ggt}(c_1, \ldots, c_n) = a_1 \cdot c_1 + \ldots + a_n \cdot c_n$$

und

$$c_0 = a_0 \cdot g,$$

so haben wir mit

$$c_0 = c_1 \cdot (a_1 \cdot a_0) + \ldots + c_n \cdot (a_n \cdot a_0)$$

eine Lösung gefunden.

Beispiel 2.7
Wir wollen eine Lösung der linearen diophantischen Gleichung

$$21 = 70 \cdot x_1 + 84 \cdot x_2 + 105 \cdot x_3 \tag{4}$$

bestimmen. Wir wissen aus Beispiel 2.4, daß $7 = \mathrm{ggt}(70, 84, 105)$ der positive größte gemeinsame Teiler von 70, 84 und 105 ist. Damit gilt

$$\mathrm{ggt}(70, 84, 105) = 7 \mid 3 \cdot 7 = 21,$$

so daß die Gleichung (4) lösbar ist in $\mathbb{Z}$. Zudem wissen wir aus Beispiel 2.4, daß

$$7 = 7 \cdot 70 - 7 \cdot 80 + 1 \cdot 105$$

ist. Damit lösen also $x_1 = 7 \cdot 3 = 21$, $x_2 = -7 \cdot 3 = -21$ und $x_3 = 1 \cdot 3 = 3$ Gleichung (4), d.h.

$$21 = 70 \cdot 21 + 84 \cdot (-21) + 105 \cdot 3.$$

Die Lösung einer linearen diophantischen Gleichung ist natürlich nicht eindeutig bestimmt, und in aller Regel ist es etwas aufwendig, alle Lösungen oder, woran man meist interessiert ist, alle positiven Lösungen anzugeben. Wenn man aber nur zwei Variablen hat, kann man die Menge aller Lösungen sogar noch in einer geschlossenen Form angeben.

Aufgabe 2.8
Es seien $c_0, c_1, c_2, a_1, a_2 \in \mathbb{Z}$ mit $\operatorname{ggt}(c_1, c_2) \mid c_0$ und $\operatorname{ggt}(c_1, c_2) = a_1 \cdot c_1 + a_2 \cdot c_2$. Zeige, genau dann ist $(z_1, z_2) \in \mathbb{Z}^2$ eine Lösung der diophantischen Gleichung

$$c_0 = c_1 \cdot x_1 + c_2 \cdot x_2,$$

wenn es ein $k \in \mathbb{Z}$ gibt, so daß

$$z_1 = \frac{c_0 \cdot a_1}{\operatorname{ggt}(c_1, c_2)} + \frac{c_2 \cdot k}{\operatorname{ggt}(c_1, c_2)} \quad \text{und} \quad z_2 = \frac{c_0 \cdot a_2}{\operatorname{ggt}(c_1, c_2)} - \frac{c_1 \cdot k}{\operatorname{ggt}(c_1, c_2)}.$$

Das folgende Beispiel zeigt, weshalb man in aller Regel an positiven Lösungen interessiert ist.

Aufgabe 2.9
Ein Straßenverkäufer verkauft Luftballons, kleine zu 56 Cent das Stück und große zu 84 Cent. Am Abend hat er $55,44$ Euro in der Tasche. Wieviele Ballons von welcher Größe hat er verkauft?

Bemerkung 2.10
Satz 2.5 liefert auch ein Kriterium dafür, wann eine *lineare Kongruenzgleichung* der Form

$$c_1 \cdot x_1 + \ldots + c_k \cdot x_k \equiv c_0 \pmod{n}$$

für gegebene ganze Zahlen $c_0, \ldots, c_k \in \mathbb{Z}$ und $n \in \mathbb{Z}_{>0}$ lösbar ist. Dies ist genau dann der Fall, wenn

$$\operatorname{ggt}(c_1, \ldots, c_k, n) \mid c_0.$$

Der Grund dafür ist, daß die Lösbarkeit der Kongruenzgleichung gleichwertig zur Lösbarkeit der linearen diophantischen Gleichung

$$c_1 \cdot x_1 + \ldots + c_k \cdot x_k + n \cdot x_{k+1} = c_0$$

ist.

Insbesondere erhalten wir für $a, b \in \mathbb{Z}$ und $n \in \mathbb{Z}_{>0}$ also, daß

$$a \cdot x \equiv b \pmod{n}$$

genau dann mit $x \in \mathbb{Z}$ lösbar ist, wenn

$$\operatorname{ggt}(a, n) \mid b.$$

Die Lösung x kann dann mit Hilfe des Euklidischen Algorithmus berechnet werden. Ist $d = \operatorname{ggt}(a, n)$ und gilt

$$a \cdot x' + n \cdot y' = d,$$

dann ist

$$x = x' \cdot \frac{b}{d} \in \mathbb{Z}$$

eine Lösung.

3 Multiplikative zahlentheoretische Funktionen

Wir haben auf Seite 11 die *Teilersummenfunktion* $\sigma : \mathbb{Z}_{>0} \longrightarrow \mathbb{Z}_{>0}$ kennen gelernt, die einer positiven ganzen Zahl die Summe ihrer positiven Teiler zuordnet. Diese Funktion hat uns bei der Untersuchung *vollkommener Zahlen* gute Dienste geleistet. Dabei kam uns zupasse, daß die Funktion für ein Produkt teilerfremder Zahlen mit der Multiplikation verträglich ist. Es gibt eine ganze Reihe solcher Funktionen auf den positiven ganzen Zahlen, die in verschiedenen Fragen der Zahlentheorie eine wichtige Rolle spielen. Es lohnt deshalb, die Klasse solcher *multiplikativer zahlentheoretischer Funktionen* genauer zu untersuchen.

Definition 3.1
Eine Funktion $\alpha : \mathbb{Z}_{>0} \longrightarrow \mathbb{R}$ heißt *zahlentheoretisch* oder *arithmetisch*. Eine zahlentheoretische Funktion α heißt *multiplikativ*, wenn

$$\alpha(a \cdot b) = \alpha(a) \cdot \alpha(b) \quad \text{für alle } a, b \in \mathbb{Z}_{>0} \text{ mit } \operatorname{ggt}(a, b) = 1.$$

Wir wollen mit

$$\mathcal{Z} = \{\alpha : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} \mid \alpha \text{ ist multiplikativ}\}$$

die Menge der multiplikativen zahlentheoretischen Funktionen bezeichnen.

Da wir in diesem Kapitel nur zahlentheoretische Funktionen betrachten wollen, werden wir den Zusatz *zahlentheoretisch* meist weglassen und nur von *multiplikativen Funktionen* sprechen.

Beispiel 3.2

a. Die Nullfunktion $0 : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} : z \mapsto 0$ ist eine multiplikative Funktion, die aber keinerlei wesentliche Information in sich birgt.

b. Auch die kleinstmögliche Störung der Nullfunktion, die eine multiplikative Funktion liefern könnte (siehe Lemma 3.3 a.), tut dies, nämlich die Funktion

$$o : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} : z \mapsto \begin{cases} 1, & \text{falls } z = 1, \\ 0, & \text{falls } z \neq 1. \end{cases}$$

   Erstaunlich ist allerdings, daß sich aus ihr bereits interessante Informationen gewinnen lassen, wie wir weiter unten sehen werden. Das gilt auch für das nächste Beispiel.

c. Die konstante Funktion

$$e : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} : z \mapsto 1$$

   ist multiplikativ.

d. Ebenso ist die identische Abbildung

$$i : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} : z \mapsto z$$

   eine multiplikative Funktion.

e. Während die bisher betrachteten Funktionen offensichtlich multiplikativ waren, bedurfte es für die *Teilersummenfunktion*

$$\sigma : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} : z \mapsto \sum_{\substack{1 \leq d \leq z \\ d \mid z}} d$$

eines Beweises, den wir in Proposition 1.18 geführt haben. σ ist multiplikativ.

f. Aus Aufgabe 1.22 folgt, daß auch die *Teileranzahlfunktion*

$$\tau : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} : z \mapsto \big|\{d \in \mathbb{Z}_{>0} \mid \quad d \mid z\}\big|$$

multiplikativ ist, da

$$\tau(z) = \prod_{p \in \mathbb{P}} \big(n_p(z) + 1\big).$$

Lemma 3.3

a. *Ist eine multiplikative Funktion α nicht die Nullfunktion, so ist $\alpha(1) = 1$.*

b. *Eine zahlentheoretische Funktion $\alpha : \mathbb{Z}_{>0} \longrightarrow \mathbb{R}$ ist genau dann* multiplikativ, *wenn*

$$\alpha(z) = \prod_{p \in \mathbb{P}} \alpha\big(p^{n_p(z)}\big) = \alpha\big(p_1^{n_1}\big) \cdots \alpha\big(p_k^{n_k}\big) \tag{5}$$

für alle $z \in \mathbb{Z}_{>0}$ mit Primfaktorzerlegung $z = p_1^{n_1} \cdots p_k^{n_k}$ gilt.

c. *Zwei multiplikative Funktionen $0 \neq \alpha, \beta \in \mathcal{Z}$ sind genau dann gleich, wenn für alle Primzahlen $p \in \mathbb{P}$ und für alle positiven ganzen Zahlen $n \in \mathbb{Z}_{>0}$*

$$\alpha\big(p^n\big) = \beta\big(p^n\big).$$

Beweis: a. Ist $z \in \mathbb{Z}_{>0}$ mit $\alpha(z) \neq 0$, so können wir in der Gleichung

$$1 \cdot \alpha(z) = \alpha(z) = \alpha(1 \cdot z) = \alpha(1) \cdot \alpha(z)$$

$\alpha(z)$ kürzen und erhalten $\alpha(1) = 1$.

b. Wir können ohne Einschränkung voraussetzen, daß α nicht die Nullfunktion ist.

Ist α multiplikativ und hat z die Primfaktorzerlegung $z = p_1^{n_1} \cdots p_k^{n_k}$, so folgt

$$\alpha(z) = \alpha\big(p_1^{n_1}\big) \cdots \alpha\big(p_k^{n_k}\big) = \prod_{p \in \mathbb{P}} \alpha\big(p^{n_p(z)}\big)$$

mittels Induktion nach der Anzahl k der Primteiler von z. Beachte dabei, daß $\alpha\big(p^{n_p(z)}\big) = 1$, wenn $p \notin \{p_1, \ldots, p_k\}$.

Nehmen wir nun umgekehrt an, daß (5) gilt und daß $a, b \in \mathbb{Z}_{>0}$ mit $\operatorname{ggt}(a, b) = 1$ und Primfaktorzerlegung

$$a = p_1^{n_1} \cdots p_l^{n_l} \quad \text{bzw.} \quad b = p_{l+1}^{n_{l+1}} \cdots p_k^{n_k}$$

gegeben sind. Dann sind $p_1, \ldots, p_k$ paarweise verschieden und $a \cdot b$ hat die Primfaktorzerlegung

$$a \cdot b = p_1^{n_1} \cdots p_k^{n_k}.$$

Mithin gilt

$$\alpha(a \cdot b) = \alpha\big(p_1^{n_1}\big) \cdots \alpha\big(p_l^{n_l}\big) \cdot \alpha\big(p_{l+1}^{n_{l+1}}\big) \cdots \alpha\big(p_k^{n_k}\big) = \alpha(a) \cdot \alpha(b)$$

und α ist multiplikativ.

c. Sind α und β gleich, so stimmen ihre Werte für p^n sicher überein. Stimmen umgekehrt die Werte von α und β für alle p^n mit $p \in \mathbb{P}$ und $n \in \mathbb{Z}_{>0}$ überein, so gilt nach Teil a. und b. für $z \in \mathbb{Z}_{>0}$

$$\alpha(z) = \prod_{p \in \mathbb{P}} \alpha\big(p^{n_p(z)}\big) = \prod_{p \in \mathbb{P}} \beta\big(p^{n_p(z)}\big) = \beta(z).$$

□

Wir wollen in diesem Kapitel einige Konstruktionsverfahren zum Erzeugen weiterer multiplikativer Funktionen kennenlernen und diese verwenden, um den Zusammenhang zwischen den oben aufgeführten Funktionen aufzuzeigen. Dabei werden wir sehen, daß die Menge $\mathcal{Z}$ der multiplikativen zahlentheoretischen Funktionen selbst eine interessante algebraische Struktur besitzt, und wir werden zwei weitere wichtige multiplikative Funktionen kennenlernen.

Definition 3.4
Für zwei Funktionen $\alpha, \beta \in \mathcal{Z}$ definieren wir die *Dirichlet-Faltung* von α und β als

$$\alpha * \beta : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} : z \mapsto \sum_{\substack{1 \leq d \leq z \\ d \mid z}} \alpha(d) \cdot \beta\left(\frac{z}{d}\right).$$

Satz 3.5
$(\mathcal{Z}, *)$ ist eine kommutative Halbgruppe mit neutralem Element o.
D.h. wenn α ,β und γ multiplikative Funktionen sind, so gilt

1) $\alpha * \beta$ *ist multiplikativ,*
2) $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$,
3) $\alpha * \beta = \beta * \alpha$, *und*
4) $\alpha * o = o * \alpha = \alpha$.

Beweis: 1) Hat $z \in \mathbb{Z}_{>0}$ die Primfaktorzerlegung

$$z = p_1^{n_1} \cdots p_k^{n_k},$$

so sehen wir wie im Beweis von Proposition 1.18

$$\big\{d \in \mathbb{Z}_{>0} \;\big|\; 1 \leq d \leq z, d \mid z\big\} = \big\{p_1^{m_1} \cdots p_k^{m_k} \;\big|\; 0 \leq m_i \leq n_i, i = 1, \ldots, k\big\}$$

und deshalb

$$
\begin{aligned}
(\alpha * \beta)(z) &= \sum_{m_1=0}^{n_1} \cdots \sum_{m_k=0}^{n_k} \alpha\big(p_1^{m_1} \cdots p_k^{m_k}\big) \cdot \beta\big(p_1^{n_1-m_1} \cdots p_k^{n_k-m_k}\big) \\
&= \sum_{m_1=0}^{n_1} \cdots \sum_{m_k=0}^{n_k} \alpha\big(p_1^{m_1}\big) \cdots \alpha\big(p_k^{m_k}\big) \cdot \beta\big(p_1^{n_1-m_1}\big) \cdots \beta\big(p_k^{n_k-m_k}\big) \\
&= \left(\sum_{m_1=0}^{n_1} \alpha\big(p_1^{m_1}\big) \cdot \beta\big(p_1^{n_1-m_1}\big)\right) \cdots \left(\sum_{m_k=0}^{n_k} \alpha\big(p_k^{m_k}\big) \cdot \beta\big(p_k^{n_k-m_k}\big)\right) \\
&= (\alpha * \beta)\big(p_1^{n_1}\big) \cdot \ldots \cdot (\alpha * \beta)\big(p_k^{n_k}\big).
\end{aligned}
$$

Mithin ist $\alpha * \beta$ multiplikativ nach Lemma 3.3.

3) Für $p \in \mathbb{P}$ und $n \in \mathbb{Z}_{>0}$ gilt nach Definition

$$
(\alpha * \beta)\big(p^n\big) = \sum_{\substack{0 \le k,l \le n \\ k+l=n}} \alpha\big(p^k\big) \cdot \beta\big(p^l\big) = \sum_{\substack{0 \le k,l \le n \\ k+l=n}} \beta\big(p^l\big) \cdot \alpha\big(p^k\big) = (\beta * \alpha)\big(p^n\big)
$$

und mit Lemma 3.3 stimmen $\alpha * \beta$ und $\beta * \alpha$ dann überein.

2) Für $p \in \mathbb{P}$ und $n \in \mathbb{Z}_{>0}$ gilt

$$
\begin{aligned}
\big((\alpha * \beta) * \gamma\big)\big(p^n\big) &= \sum_{\substack{0 \le k,l \le n \\ k+l=n}} (\alpha * \beta)\big(p^k\big) \cdot \gamma\big(p^l\big) \\
&= \sum_{\substack{0 \le k,l \le n \\ k+l=n}} \sum_{\substack{0 \le i,j \le n \\ i+j=k}} \alpha\big(p^i\big) \cdot \beta\big(p^j\big) \cdot \gamma\big(p^l\big) \\
&= \sum_{\substack{0 \le i,j,l \le n \\ i+j+l=n}} \alpha\big(p^i\big) \cdot \beta\big(p^j\big) \cdot \gamma\big(p^l\big) \\
&= \sum_{\substack{0 \le i,k \le n \\ i+k=n}} \sum_{\substack{0 \le j,l \le n \\ j+l=k}} \alpha\big(p^i\big) \cdot \beta\big(p^j\big) \cdot \gamma\big(p^l\big) \\
&= \sum_{\substack{0 \le i,k \le n \\ i+k=n}} \alpha\big(p^i\big) \cdot (\beta * \gamma)\big(p^k\big) \\
&= \big(\alpha * (\beta * \gamma)\big)\big(p^n\big)
\end{aligned}
$$

und nach Lemma 3.3 stimmen $(\alpha * \beta) * \gamma$ und $\alpha * (\beta * \gamma)$ deshalb überein.

4) Da $o(d) = 0$ für alle $d \neq 1$, gilt für $z \in \mathbb{Z}_{>0}$

$$
(o * \alpha)(z) = \sum_{\substack{1 \le d \le z \\ d \mid z}} o(d) \cdot \alpha\left(\frac{z}{d}\right) = o(1) \cdot \alpha(z) = \alpha(z).
$$

Aus der Kommutativität der Faltung folgt zudem $\alpha * o = \alpha$.

$\square$

Wir wollen als nächstes zeigen, daß die Funktion e eine Inverse besitzt, die *Möbiussche* μ*-Funktion.* Dazu erinnern wir uns, daß wir auf Seite 6 die Anzahl

$$n_{\mathbb{P}}(z) = \sum_{p \in \mathbb{P}} n_p(z)$$

der Primteiler einer ganzen Zahl z eingeführt haben.

Definition 3.6
Die zahlentheoretische Funktion

$$\mu : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} : z \mapsto \begin{cases} 0, & \text{falls es ein } p \in \mathbb{P} \text{ gibt mit } n_p(z) > 1, \\ (-1)^{n_{\mathbb{P}}(z)}, & \text{falls } n_p(z) \leq 1 \text{ für alle } p \in \mathbb{P} \end{cases}$$

heißt die *Möbiussche* μ*-Funktion.*

Wenn wir eine Zahl *quadratfrei* nennen, wenn sie von keiner Quadratzahl außer 1 geteilt wird, so gibt die Möbiussche μ-Funktion an, ob eine Zahl quadratfrei ist oder nicht.

Beispiel 3.7
Zur Verdeutlichung wollen wir einige Werte der Möbiusschen μ-Funktion angeben:

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

Proposition 3.8
Die Möbiussche μ*-Funktion ist multiplikativ, und es gilt*

$$\mu * e = e * \mu = o,$$

d.h. μ *ist in* $\mathcal{Z}$ *das Inverse zu* e*.*

Beweis: Sind $a, b \in \mathbb{Z}_{>0}$ mit $\mathrm{ggt}(a, b) = 1$, so teilt keine Primzahl sowohl a, als auch b. Mithin können $n_p(a)$ und $n_p(b)$ nicht beide ungleich Null sein, so daß

$$n_p(a \cdot b) = \max\{n_p(a), n_p(b)\} \tag{6}$$

und

$$n_{\mathbb{P}}(a \cdot b) = \sum_{p \in \mathbb{P}} n_p(a \cdot b) = \sum_{p \in \mathbb{P}} \big(n_p(a) + n_p(b)\big) = n_{\mathbb{P}}(a) + n_{\mathbb{P}}(b). \tag{7}$$

Aus (6) folgt

$$\mu(a \cdot b) = 0 \quad \Longleftrightarrow \quad \mu(a) = 0 \text{ oder } \mu(b) = 0,$$

so daß in diesem Fall $\mu(a \cdot b) = 0 = \mu(a) \cdot \mu(b)$. Sind $\mu(a)$ und $\mu(b)$ beide ungleich Null, so folgt aus (7)

$$\mu(a \cdot b) = (-1)^{n_{\mathbb{P}}(a \cdot b)} = (-1)^{n_{\mathbb{P}}(a)} \cdot (-1)^{n_{\mathbb{P}}(b)} = \mu(a) \cdot \mu(b).$$

Mithin ist $\mu \in \mathcal{Z}$.

Sei nun $p \in \mathbb{P}$ und $n \in \mathbb{Z}_{>0}$ dann gilt

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

Damit ist $\mu * e = o$ nach Lemma 3.3 und $e * \mu = o$ wegen der Kommutativität der Faltung. □

Die zentrale Bedeutung der Möbiusschen μ-Funktion liegt darin, daß sie eine zahlentheoretische Funktionen mit ihren Summatorfunktionen in Beziehung setzt.

Definition 3.9
Für $\alpha \in \mathcal{Z}$ definieren wir die *Summatorfunktion* von α als

$$\alpha * e : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} : z \mapsto \sum_{\substack{1 \leq d \leq z \\ d \mid z}} \alpha(d).$$

Satz 3.10 (Möbiusscher Umkehrsatz)
Ist $\alpha \in \mathcal{Z}$ eine multiplikative Funktion, dann ist die Summatorfunktion β von α multiplikativ und es gilt $\alpha = \beta * \mu$, d.h.

$$\alpha(z) = \sum_{\substack{1 \leq d \leq z \\ d \mid z}} \beta(d) \cdot \mu\left(\frac{z}{d}\right).$$

Beweis: Da α und e multiplikativ sind, trifft dies nach Satz 3.5 auch auf $\beta = \alpha * e$ zu. Zudem folgt aus Proposition 3.8

$$\alpha = \alpha * o = \alpha * (e * \mu) = (\alpha * e) * \mu = \beta * \mu.$$

□

Wir wollen nun die für unsere Vorlesung wichtigste multiplikative Funktion einführen, die *Eulersche φ-Funktion.* Dazu erinnern wir uns an die multiplikative Gruppe $\mathbb{Z}_n^*$ des Ringes $(\mathbb{Z}_n, +, \cdot)$ aus Satz 1.12, deren erste Eigenschaften in den algebraischen Strukturen untersucht wurden. Im folgenden Kapitel 5 werden wir uns die Struktur der Gruppe näher anschauen.

Definition 3.11
Wir definieren die *Eulersche φ-Funktion* durch

$$\varphi : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} : n \mapsto |\mathbb{Z}_n^*| = \big|\{a \in \mathbb{Z} \mid 1 \leq a \leq n, \operatorname{ggt}(a, n) = 1\}\big|,$$

wobei die letzte Gleichheit wegen Satz 1.12 gilt.

In der folgenden Proposition wollen wir die Restklasse einer ganzen Zahl z in einem Restklassenring $\mathbb{Z}_k$ mit $\overline{z}_k$ bezeichnen, da wir z modulo verschiedener Residuen betrachten müssen. Zudem sollte man beachten, daß das kartesische Produkt $\mathbb{Z}_m \times \mathbb{Z}_n$ bezüglich der komponentenweisen Addition und Multiplikation ein Ring ist und daß analog $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ bezüglich der komponentenweisen Multiplikation eine Gruppe ist.

Satz 3.12
Sind $m, n \in \mathbb{Z}_{>0}$ teilerfremd, so ist die Abbildung

$$\mathbb{Z}_{m \cdot n}^* \longrightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^* : \overline{z}_{mn} \mapsto \left(\overline{z}_m, \overline{z}_n\right)$$

ein Isomorphismus von Gruppen. Insbesondere gilt also

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n),$$

und $\varphi \in \mathcal{Z}$ *ist eine multiplikative Funktion.*

Beweis: Ist $z \in \mathbb{Z}$ mit $\overline{z}_{mn} \in \mathbb{Z}^*_{m\cdot n}$, so gilt sind z und $m \cdot n$ teilerfremd nach Satz 1.12. Aber dann sind auch z und m sowie z und n teilerfremd, so daß

$$\left(\overline{z}_m, \overline{z}_n\right) \in \mathbb{Z}^*_m \times \mathbb{Z}^*_n. \tag{8}$$

Wir wissen aus dem Chinesischen Restsatz 1.13, daß die Abbildung

$$\alpha : \mathbb{Z}_{m\cdot n} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n : \overline{z}_{mn} \mapsto \left(\overline{z}_m, \overline{z}_n\right)$$

ein Isomorphismus von Ringen ist, und mithin induziert α wegen (8) durch Einschränkung eine Abbildung

$$\alpha_| : \mathbb{Z}^*_{m\cdot n} \longrightarrow \mathbb{Z}^*_m \times \mathbb{Z}^*_n,$$

die ebenfalls injektiv und mit der Multiplikation verträglich ist. Es bleibt also nur zu zeigen, daß $\alpha_|$ surjektiv ist.

Sei dazu $\left(\overline{a}_m, \overline{b}_n\right) \in \mathbb{Z}^*_m \times \mathbb{Z}^*_n$, dann gibt es ein $z \in \mathbb{Z}$ mit

$$\left(\overline{a}_m, \overline{b}_n\right) = \alpha\left(\overline{z}_{mn}\right) = \left(\overline{z}_m, \overline{z}_n\right),$$

da α surjektiv ist. Aus dieser Gleichung folgt die Existenz ganzer Zahlen $p, q \in \mathbb{Z}$, so daß $z = a + p \cdot m = b + q \cdot n$. Aus Aufgabe 1.9 folgt dann

$$\mathrm{ggt}(z, m) = \mathrm{ggt}(a, m) = 1 = \mathrm{ggt}(b, n) = \mathrm{ggt}(z, n)$$

und folglich sind auch z und $m \cdot n$ teilerfremd, d.h. $\overline{z}_{mn} \in \mathbb{Z}^*_{m\cdot n}$. Die Abbildung $\alpha_|$ ist also surjektiv, und damit ein Isomorphismus von Gruppen.

Insbesondere gilt

$$\varphi(m \cdot n) = |\mathbb{Z}^*_{m\cdot n}| = |\mathbb{Z}^*_m \times \mathbb{Z}^*_n| = |\mathbb{Z}^*_m| \cdot |\mathbb{Z}^*_n| = \varphi(m) \cdot \varphi(n).$$

□

Korollar 3.13
Für $p \in \mathbb{P}$ *und* $n \in \mathbb{Z}_{>0}$ *gilt*

$$\varphi\left(p^n\right) = p^n - p^{n-1},$$

und für $z \in \mathbb{Z}_{>0}$ *gilt*

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

Beweis: Eine Zahl ist genau dann nicht zu p^n teilerfremd, wenn p ein Teiler dieser Zahl ist. Deshalb ist die Menge der zu p^n nicht teilerfremden Zahlen zwischen 1 und p^n gerade

$$\left\{z \in \mathbb{Z} \;\middle|\; 1 \le z \le p^n, \mathrm{ggt}(z,p) \ne 1\right\} = \left\{p \cdot k \;\middle|\; 1 \le k \le p^{n-1}\right\}.$$

Die Mächtigkeit dieser Menge ist p^{n-1} und ihr Komplement in

$$\left\{z \in \mathbb{Z} \;\middle|\; 1 \le z \le p^n\right\}$$

hat nach Definition die Mächtigkeit $\varphi\big(p^n\big)$, so daß

$$\varphi\big(p^n\big) = p^n - p^{n-1}$$

gilt. Der Rest folgt aus Lemma 3.3, da φ nach Satz 3.12 multiplikativ ist. □

Korollar 3.14 (Rekursionsformel der Eulerschen φ-Funktion)
Die Summatorfunktion der Eulerschen φ-Funktion ist i, d.h. für $z \in \mathbb{Z}_{>0}$ gilt

$$\sum_{\substack{1 \le d \le z \\ d \mid z}} \varphi(d) = z.$$

Durch Umstellen der Gleichung erhalten wir eine Rekursionsformel zur Berechnung der Werte der Eulerschen φ-Funktion:

$$\varphi(z) = z - \sum_{\substack{1 \le d < z \\ d \mid z}} \varphi(d).$$

Beweis: Da die Summatorfunktion $\varphi * e$ von φ und die Funktion i beide multiplikativ sind, reicht es nach Lemma 3.3 zu zeigen, daß sie für p^n mit $p \in \mathbb{P}$ und $n \in \mathbb{Z}_{>0}$ übereinstimmen. Dazu wenden wir das Ergebnis von Korollar 3.13 an und erhalten

$$(\varphi * e)\big(p^n\big) = \sum_{j=0}^{n} \varphi\big(p^j\big) = 1 + \sum_{j=1}^{n} \big(p^j - p^{j-1}\big) = p^n = i\big(p^n\big).$$

□

Bemerkung 3.15
Sowohl die explizite Formel aus Korollar 3.13 wie auch die Rekursionsformel aus Korollar 3.14 können dazu verwendet werden, die Mächtigkeit der Einheitengruppe $\mathbb{Z}_n^*$ zu bestimmen, ohne die Elemente explizit anzugeben. Z.B. ist

$$|\mathbb{Z}_{12}^*| = \varphi(12) = \varphi\big(2^2\big) \cdot \varphi(3) = (4-2) \cdot (3-1) = 4.$$

Aufgrund von Satz 1.12 wissen wir, daß

$$\mathbb{Z}_{12}^* = \left\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\right\}.$$

Wir wollen hier noch einige Werte von φ festhalten:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(n) = \lvert\mathbb{Z}_n^*\rvert$	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Bemerkung 3.16

Wir haben in Korollar 3.14 gesehen, daß die scheinbar uninteressante multiplikative Funktion i die Summatorfunktion der sehr interessanten multiplikativen Funktion φ ist, was wir auch ausdrücken können als

$$\varphi = \mathrm{i} * \mu, \tag{9}$$

d.h. durch Faltung mit μ wird i zu φ. Für die übrigen multiplikativen Funktionen, die wir kennen gelernt haben, gelten ähnliche Beziehungen. In der folgenden Tabelle geben wir für bestimmte multiplikative Funktionen ihre Summatorfunktionen an:

α	φ	i	μ	o	e	$\frac{\mu}{\mathrm{i}}$
$\alpha * e$	i	σ	o	e	τ	$\frac{\varphi}{\mathrm{i}}$

Die Aussage der ersten Spalte ist Korollar 3.14; die der zweiten Spalte folgt aus der Definition von σ; die der dritten Spalte ist Proposition 3.8; die der vierten folgt aus Satz 3.5; die der fünften ergibt sich aus der Definition der Teileranzahlfunktion τ, da

$$(e * e)(z) = \sum_{\substack{1 \leq d \leq z \\ d \mid z}} e(d) * e\left(\frac{z}{d}\right) = \sum_{\substack{1 \leq d \leq z \\ d \mid z}} 1 = \tau(z);$$

und die letzte Spalte ergibt sich aus (9)

$$\varphi(z) = (\mathrm{i} * \mu)(z) = (\mu * \mathrm{i})(z) = \sum_{\substack{1 \leq d \leq z \\ d \mid z}} \mu(d) \cdot \mathrm{i}\left(\frac{z}{d}\right) = \sum_{\substack{1 \leq d \leq z \\ d \mid z}} \mu(d) \cdot \frac{z}{d},$$

indem man beide Seiten durch $\mathrm{i}(z) = z$ teilt:

$$\frac{\varphi}{\mathrm{i}}(z) = \frac{\varphi(z)}{z} = \sum_{\substack{1 \leq d \leq z \\ d \mid z}} \frac{\mu(d)}{d} = \sum_{\substack{1 \leq d \leq z \\ d \mid z}} \frac{\mu}{\mathrm{i}}(d) = \left(\frac{\mu}{\mathrm{i}} * e\right)(z).$$

Dies ist ein Beispiel für multiplikative Funktionen, die keine ganzzahligen Werte annehmen.

Bemerkung 3.17

Für die Definition der Faltung von α und β benötigt man eigentlich nicht, daß die Funktionen *multiplikativ* sind, die Definition funktioniert für beliebige zahlentheoretische Funktionen. Dies gilt analog für die Summatorfunktion. Ferner kann man die Eigenschaften 2)–4) in Satz 3.5 zeigen, wenn man nur voraussetzt, daß die Funktionen α, β und γ dort zahlentheoretisch sind. Die Reduktion auf Primzahlen, die wir für 2) und 3) verwendet haben, ist nicht notwendig. Entsprechend gilt auch der Möbiussche Umkehrsatz für beliebige zahlentheoretische Funktionen. Wir haben auf diese allgemeineren Aussagen verzichtet, da alle Funktionen, die uns in diesem Kapitel interessieren, multiplikativ sind.

Aufgabe 3.18

Die *Liouvillesche* λ*-Funktion* ist definiert durch

$$\lambda : \mathbb{Z}_{>0} \longrightarrow \mathbb{R} : z \mapsto (-1)^{n_{\mathbb{P}}(z)}.$$

Zeige:

a. $\lambda \in \mathcal{Z}$, d.h. λ ist multiplikativ.

b. Für die Summatorfunktion $\Lambda = \lambda * e$ von λ gilt

$$\Lambda(z) = \sum_{\substack{1 \le d \le z \\ d \mid z}} \lambda(d) = \begin{cases} 1, & \text{falls } \exists\, a \in \mathbb{Z} \,:\, z = a^2, \\ 0, & \text{sonst.} \end{cases}$$

Bemerkung 3.19
Die Liouvillesche λ-Funktion ist eng mit *Pólyas Vermutung* in Frage D. der Einleitung verbunden. Mit der dortigen Notation gilt

$$L(n) := \sum_{k=1}^{n} \lambda(k) = g_n - u_n$$

und Pólya vermutete, daß $L(n)$ nie positiv ist.

4 Die Sätze von Euler, Fermat und Wilson

Wir wollen in diesem Kapitel die Eulersche φ-Funktion verwenden, um einen Satz von Euler zu formulieren, aus dem wir dann eine Reihe interessanter Folgerungen ziehen werden. Insbesondere wollen wir Fermats Lösbarkeitsaussage zur diophantischen Gleichung

$$x^2 + y^2 = p$$

für Primzahlen $p \in \mathbb{P}$ beweisen.

Der Beweis des Satzes von Euler ist eine einfache Anwendung des Satzes von Lagrange, den wir bereits in den algebraischen Strukturen kennen gelernt haben. Dazu wollen wir uns an einige Begriffe der Gruppentheorie erinnern.

Bemerkung 4.1
Ist $(G, \cdot)$ eine Gruppe mit neutralem Element e und ist $g \in G$, so ist

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\} \leq G$$

die von g *erzeugte Untergruppe* von G und

$$o(g) = |\langle g \rangle| = \inf \left\{ k \in \mathbb{Z}_{>0} \;\middle|\; g^k = e \right\} \in \mathbb{Z}_{>0} \cup \{\infty\}$$

ist die *Ordnung* von g. Wir wissen, daß

$$g^k = e \iff o(g) \mid k.$$

Zudem impliziert der Satz von Lagrange für eine endliche Gruppe G, daß

$$o(g) \mid |G|$$

und somit

$$g^{|G|} = e. \tag{10}$$

Eine unmittelbare Folgerung aus dem letzten Sachverhalt ist der folgende *Satz von Euler.*

Satz 4.2 (Euler)
Für positive ganze Zahlen $k, n \in \mathbb{Z}_{>0}$ *mit* $\mathrm{ggt}(k, n) = 1$ *gilt*

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

Beweis: Da k und n teilerfremd sind, ist $\overline{k} \in \mathbb{Z}_n^*$ eine Einheit in $\mathbb{Z}_n$. Mithin folgt aus (10)

$$\overline{k}^{\varphi(n)} = \overline{k}^{|\mathbb{Z}_n^*|} = \overline{1},$$

was gleichbedeutend zur Aussage des Satzes ist. □

Bemerkung 4.3
Man kann den Satz von Euler auch verwenden, um eine einfache lineare Kongruenzgleichung der Form

$$a \cdot x \equiv b \pmod{n} \tag{11}$$

zu lösen. Da wir die Kongruenzgleichung auch als Gleichung

$$\overline{a}_n \cdot \overline{x}_n = \overline{b}_n$$

in $\mathbb{Z}_n$ auffassen können, wissen wir, daß sie genau dann für jedes b lösbar ist, wenn $\overline{a}_n \in \mathbb{Z}_n^*$ ist, d.h. wenn $\mathrm{ggt}(a, n) = 1$ (vgl. Bemerkung 2.10). In diesem Fall könnten wir das Inverse von $\overline{a}_n$ mittels des Euklidischen Algorithmus bestimmen und beide Seiten der Gleichung damit multiplizieren.

Alternativ können wir aber auch den Satz von Euler anwenden, der uns das Inverse von $\overline{a}_n$ als

$$\overline{a}_n^{-1} = \overline{a}_n^{\varphi(n)-1}$$

vorgibt. Deshalb gilt also

$$x = a^{\varphi(n)-1} \cdot b$$

löst das Kongruenzgleichungssystem (11).

Wollen wir z.B. die Kongruenzgleichung

$$7 \cdot x \equiv 5 \pmod{12}$$

lösen, so berechnen wir zunächst $\varphi(12) = 4$ und erhalten somit

$$x = 7^{\varphi(12)-1} \cdot 5 = 7^3 \cdot 5 = 1715 = 142 \cdot 12 + 11$$

als eine mögliche Lösung, und wenn wir sie modulo 12 reduzieren, so ist $x = 11$ die eindeutige Lösung zwischen 0 und 11.

Aufgabe 4.4
Es seien $p, q \in \mathbb{P}$ mit $p \neq q$, aber $p - 1 \mid q - 1$. Dann gilt

$$z^{q-1} \;\equiv\; 1 \pmod{pq}$$

für $z \in \mathbb{Z}_{>0}$ mit $\mathrm{ggt}(z, pq) = 1$. □

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

Korollar 4.5 (Kleiner Satz von Fermat)
Ist $p \in \mathbb{P}$ eine Primzahl, so gilt für alle $k \in \mathbb{Z}$

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

Beweis: Wenn p ein Teiler von k ist, so sind beide Seiten der Kongruenzgleichung kongruent zu Null modulo p. Ist p kein Teiler von k, so sind p und k teilerfremd und der Satz von Euler liefert

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

Multipliziert man diese Gleichung mit k, so erhält man die gewünschte Aussage. □

Bemerkung 4.6
Aus dem kleinen Satz von Fermat folgt unmittelbar:

$$p \in \mathbb{P} \quad \Longrightarrow \quad p \mid (2^p - 2). \tag{12}$$

Dies ist die *korrekte* Richtung des vermeintlichen Primzahltestes aus dem alten China, der in Kapitel 1 in Frage F, Teil b. angesprochen wurde. Wir haben bereits angemerkt, daß die Umkehrung nicht gilt, da etwa die zusammengesetzte Zahl $p = 341 = 11 \cdot 31$ ebenfalls diese Eigenschaft hat. Der Nachweis kann mit Hilfe des Satzes von Euler geführt werden, ohne daß dazu $2^{341} - 2$ ausgerechnet werden muß, und ist dem Leser als Übungsaufgabe überlassen.

Wir haben in der Einleitung bereits erwähnt, daß zusammengesetzte Zahlen p für die p ein Teiler von $k^p - k$ ist, *Pseudoprimzahlen zur Basis* k genannt werden. 341 ist deshalb eine *Pseudoprimzahl* zur Basis 2.

Wie in (12) liefert der Satz von Euler eine *Bedingung*, die eine Primzahl *notwendigerweise* erfüllen muß:

$$k^{p-1} \equiv 1 \pmod{p} \quad \text{für alle } 2 \leq k \leq p-1.$$

Diese kann man verwenden, um zu testen, ob eine Zahl möglicherweise eine Primzahl ist. Ist die Kongruenzgleichung für ein k verletzt, so ist p *keine* Primzahl. Andernfalls ist sie entweder eine Primzahl oder eine sehr spezielle zusammengesetzte Zahl, eine sogenannte *Carmichael-Zahl*. Man nennt ein solches Verfahren auch einen *Primzahltest*.

Aufgabe 4.7
Verwende den Satz von Euler, um zu zeigen, daß 341 ein Teiler von $2^{341} - 2$ ist.

Aufgabe 4.8
Verwende den kleinen Satz von Fermat, um zu zeigen, daß jede Mersennesche Zahl $M_q = 2^q - 1$ mit $q \in \mathbb{P}$ eine Pseudoprimzahl zur Basis 2 ist.

Der Satz von Euler impliziert darüber hinaus auch den *Satz von Wilson*. Dazu erinnern wir uns daran, daß ein Polynom vom Grad n über einem Körper K höchstens n Nullstellen in K besitzt.

Korollar 4.9 (Satz von Wilson)
Ist $p \in \mathbb{P}$ *eine Primzahl, so ist*

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

Beweis: Ist $p = 2$, so gilt ohnehin $(2-1)! = 1 \equiv -1 \pmod{2}$, so daß wir p als ungerade voraussetzen können.

Wir betrachten das Polynom

$$f = t^{p-1} - \overline{1} \in \mathbb{Z}_p[t].$$

Da $\mathbb{Z}_p$ nach Satz 1.12 ein Körper ist, besitzt f höchstens $p-1$ verschiedene Nullstellen in $\mathbb{Z}_p$. Zugleich folgt aber aus dem Satz von Euler, daß die Elemente

$$\overline{1}, \ldots, \overline{p-1} \in \mathbb{Z}_p$$

Nullstellen von f sind. Also besitzt f genau $p-1$ verschieden Nullstellen in $\mathbb{Z}_p$ und wir können diese sukzessive abspalten, so daß f vollständig zerfällt:

$$f = \left(t - \overline{1}\right) \cdots \left(t - \overline{p-1}\right).$$

Multiplizieren wir die rechte Seite der Gleichung aus und vergleichen nur den konstanten Koeffizienten, so erhalten wir

$$-\overline{1} = (-1)^{p-1} \cdot \overline{(p-1)!} = \overline{(p-1)!},$$

da p ungerade ist. Diese Gleichung ist aber gleichwertig zur Aussage des Satzes. □

Beispiel 4.10
Die beiden folgenden Beispiele verifizieren die Aussage des Satzes von Wilson:

$$(7-1)! = 720 = 7 \cdot 103 - 1 \equiv -1 \pmod 7$$

und

$$(17-1)! = 20.922.789.888.000 = 17 \cdot 123.0752.346.353 - 1 \equiv -1 \pmod{17}.$$

□

Unser nächstes Ziel ist es, die Lösbarkeit der diophantischen Gleichung

$$x^2 + y^2 = p$$

für Primzahlen $p \in \mathbb{P}$ zu untersuchen, und wir werden sehen, daß diese eng verbunden ist mit der Frage, ob das Polynom

$$t^2 + \overline{1} \in \mathbb{Z}_p[t]$$

eine Nullstelle besitzt oder nicht, sowie mit Frage A, Teil b. der Einleitung. Für den Beweis benötigen wir Dirichlets bekanntes Schubfachprinzip sowie einen sich daraus ergebenden Satz von Thue.

Bemerkung 4.11 (Dirichlets Schubfachprinzip)
Eine Abbildung $\alpha : A \longrightarrow B$ endlicher Mengen mit $|A| > |B|$ ist nicht injektiv.

Etwas anschaulicher ausgedrückt bedeutet dies: Werden n Teile auf weniger als n Schubfächer verteilt, so enthält mindestens ein Schubfach mindestens zwei Teile. □

Satz 4.12 (Thue)
Es sei $n \in \mathbb{Z}_{>0}$ *keine Quadratzahl und* $a \in \mathbb{Z}$ *beliebig. Dann gibt es ein* $(0,0) \neq (x,y) \in \mathbb{Z}^2$ *mit*

$$a \cdot x \equiv y \pmod n \quad \textit{und} \quad -\sqrt{n} < x, y < \sqrt{n}.$$

Beweis: Es sei $m = \min\{k \in \mathbb{Z} \mid \sqrt{n} < k\}$ und

$$A = \{(x, y) \in \mathbb{Z}^2 \mid 0 \leq x, y < \sqrt{n}\}.$$

Wir betrachten die Abbildung

$$\alpha : A \longrightarrow \mathbb{Z}_n : (x, y) \mapsto \overline{a \cdot x - y}.$$

Da nach Voraussetzung n keine Quadratzahl ist, gilt

$$|A| = m^2 > n = |\mathbb{Z}_n|.$$

Nach Dirichlets Schubfachprinzip ist α nicht injektiv, d.h. es gibt zwei verschiedene $(x', y'), (x'', y'') \in A$ mit

$$\overline{a \cdot x' - y'} = \overline{a \cdot x'' - y''} \in \mathbb{Z}_n.$$

Dann gilt aber

$$a \cdot (x' - x'') \equiv y' - y'' \pmod{n}$$

und

$$-\sqrt{n} < x' - x'', y' - y'' < \sqrt{n}.$$

$\square$

Mit dieser Vorbereitung sind wir nun in der Lage, folgenden Satz von Fermat zu beweisen.

Satz 4.13 (Fermat)
Für eine ungerade Primzahl $p \in \mathbb{P}$ *sind folgende Aussagen gleichwertig:*

a. *Die diophantische Gleichung* $x^2 + y^2 = p$ *besitzt eine Lösung* $(x, y) \in \mathbb{Z}^2$.
b. *Das Polynom* $f = t^2 + \overline{1} \in \mathbb{Z}_p[t]$ *hat eine Nullstelle in* $\mathbb{Z}_p$.
c. $p \equiv 1 \pmod{4}$.

Insbesondere ist eine ungerade Primzahl genau dann Summe zweier Quadrate, wenn sie kongruent zu Eins modulo Vier ist.

Beweis: **b.⇒a.:** Sei $a \in \mathbb{Z}$ so, daß $\overline{a}$ eine Nullstelle von f ist, dann ist

$$\overline{a}^2 = -\overline{1} \in \mathbb{Z}_p. \tag{13}$$

Nach dem Satz von Thue 4.12 gibt es $(0, 0) \neq (x, y) \in \mathbb{Z}^2$ mit

$$\overline{a} \cdot \overline{x} = \overline{y} \in \mathbb{Z}_p \quad \text{und} \quad -\sqrt{p} < x, y < \sqrt{p}. \tag{14}$$

Aus (13) und (14) erhalten wir

$$-\overline{x}^2 = \overline{a}^2 \cdot \overline{x}^2 = \overline{y}^2 \in \mathbb{Z}_p$$

und mithin

$$\overline{x^2 + y^2} = \overline{0} \in \mathbb{Z}_p.$$

Es gibt also ein $k \in \mathbb{Z}$, so daß

$$x^2 + y^2 = k \cdot p.$$

Aus (14) folgt aber

$$0 < x^2 + y^2 < 2 \cdot p,$$

so daß $k = 1$ und $x^2 + y^2 = p$.

a.⇒c.: Sind $x, y \in \mathbb{Z}$ mit

$$x^2 + y^2 = p, \tag{15}$$

dann können nicht x und y beide gerade oder beide ungerade sein, da p ungerade ist. Wir können also ohne Einschränkung annehmen, daß x gerade und y ungerade ist, d.h. $x = 2 \cdot k$ und $y = 1 + 2 \cdot l$ für gewisse $k, l \in \mathbb{Z}$. Dann gilt aber

$$p = x^2 + y^2 = 4 \cdot k^2 + 4 \cdot (l^2 + l) + 1 \equiv 1 \pmod 4.$$

c.⇒b.: Ist $p \equiv 1 \pmod 4$, so ist die Zahl

$$n := \frac{p-1}{2}$$

eine gerade Zahl. In $\mathbb{Z}_p$ gilt

$$\overline{p-k} = \overline{-k}$$

für $1 \leq k \leq n$, und aus dem Satz von Wilson 4.9 folgt dann

$$\begin{aligned}
\overline{-1} &= \overline{1} \cdot \overline{2} \cdots \overline{\tfrac{p-1}{2}} \cdot \overline{\tfrac{p+1}{2}} \cdot \overline{\tfrac{p+3}{2}} \cdots \overline{(p-1)} \\
&= \overline{1} \cdot \overline{2} \cdots \overline{\tfrac{p-1}{2}} \cdot \overline{p - \tfrac{p-1}{2}} \cdot \overline{p - \tfrac{p-3}{2}} \cdots \overline{(p-1)} \\
&= \overline{1} \cdot \overline{2} \cdots \overline{\tfrac{p-1}{2}} \cdot \overline{-\tfrac{p-1}{2}} \cdot \overline{-\tfrac{p-3}{2}} \cdots \overline{(-1)} \\
&= (-1)^n \cdot \overline{n!}^2 = \overline{n!}^2.
\end{aligned}$$

Für die letzte Gleichung beachten wir, daß n gerade ist. Insgesamt erhalten wir damit, daß $\overline{n!}$ eine Nullstelle von f ist.

□

Bemerkung 4.14

Der Beweis von Satz 4.13 verwendet das nicht-konstruktive Schubfachprinzip, so daß er keinerlei Hinweis darauf gibt, wie man eine Lösung von $x^2+y^2 = p$ finden könnte, wenn $p \equiv 1 \pmod 4$ ist.

Der Satz macht zudem nur Aussagen über ungerade Primzahlen. Für die einzige gerade Primzahl p gilt jedoch trivialerweise, daß

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

eine Lösung der betrachteten diophantischen Gleichung ist und daß $t^2 + \overline{1} \in \mathbb{Z}_2[t]$ die Nullstelle $\overline{1}$ besitzt, während $p = 2 \not\equiv 1 \pmod 4$. □

Wir wollen uns nun Frage A, Teil b. der Einleitung zuwenden und beweisen, daß es unendlich viele Primzahlen p gibt, die der Bedingung von Satz 4.13 genügen. Dazu erinnern wir uns an die *Reduktion modulo* p, den Ringhomomorphismus

$$\phi_p : \mathbb{Z}[t] \longrightarrow \mathbb{Z}_p[t] : \sum_{k=0}^{n} a_k \cdot t^k \mapsto \sum_{k=0}^{n} \overline{a_k} \cdot t^k,$$

der einem Polynom mit ganzzahligen Koeffizienten ein Polynom in $\mathbb{Z}_p[t]$ zuordnet, indem die Restklassen der Koeffizienten modulo p betrachtet werden. In den algebraischen Strukturen haben wir diesen Ringhomomorphismus für beliebige positive ganze Zahlen p betrachtet, hier können wir uns auf den Fall beschränken, daß p eine Primzahl ist. Wir wollen eine kürzere Notation einführen:

$$f_p := \phi_p(f) \in \mathbb{Z}_p[t].$$

Daß ϕ_p ein Ringhomomorphismus ist, bedeutet unter anderem, daß

$$(f \cdot g)_p = f_p \cdot g_p \quad \text{und} \quad (f+g)_p = f_p + g_p \quad \text{für } f, g \in \mathbb{Z}[t].$$

In der Vorlesung algebraische Strukturen haben wir zudem für Polynome über Körpern gezeigt, daß die Zahl der Nullstellen eines Polynoms durch seinen Grad beschränkt ist, sofern es nicht das Nullpolynom ist. Wir verallgemeinern diese Aussage nun und zeigen, daß ein nicht-konstantes Polynom mit ganzzahligen Koeffizienten jeden Wert nur endlich oft annehmen kann.

Lemma 4.15
Ist $k \in \mathbb{Z}$ und $f \in \mathbb{Z}[t]$ ein nicht-konstantes Polynom vom Grad $\deg(f) = n$, so ist

$$\left|\{z \in \mathbb{Z} \mid f(z) = k\}\right| \leq n.$$

Beweis: Dazu betrachten wir das Polynom

$$g := f - k \in \mathbb{Q}[t]$$

als Polynom mit rationalen Koeffizienten. Dann ist

$$\left|\{z \in \mathbb{Z} \mid f(z) = k\}\right| = \left|\{z \in \mathbb{Z} \mid g(z) = 0\}\right| \leq n,$$

da das Polynom g nicht das Nullpolynom ist und deshalb höchstens $\deg(g) = \deg(f) = n$ Nullstellen hat. Dabei geht ein, daß $\mathbb{Q}$ ein Körper ist. $\square$

Damit können wir den folgenden Satz beweisen, der mit Hilfe des Satzes von Fermat Frage A, Teil b. aus der Einleitung beantwortet.

Satz 4.16
Ist $f \in \mathbb{Z}[t]$ ein nicht-konstantes Polynom, dann gibt es unendlich viele Primzahlen $p \in \mathbb{P}$, so daß die Reduktion $f_p \in \mathbb{Z}_p[t]$ von f modulo p eine Nullstelle in $\mathbb{Z}_p$ hat.

Beweis: Da f nicht konstant ist, hat f die Form

$$f = a_n \cdot t^n + a_{n-1} \cdot t^{n-1} + \cdots + a_1 \cdot t + a_0$$

mit $a_i \in \mathbb{Z}$ und $n = \deg(f) \geq 1$.

Hat f eine Nullstelle $a \in \mathbb{Z}$, so ist $\overline{a}_p \in \mathbb{Z}_p$ eine Nullstelle von f_p für jede Primzahl $p \in \mathbb{P}$. Wir können deshalb annehmen, daß f keine Nullstelle in $\mathbb{Z}$ besitzt. Insbesondere ist dann

$$a_0 = f(0) \neq 0. \tag{16}$$

Wir wollen nun zeigen, wenn $p_1, \ldots, p_k \in \mathbb{P}$ Primzahlen sind, so daß f_{p_i} eine Nullstelle in $\mathbb{Z}_{p_i}$ besitzt, dann gibt es eine Primzahl

$$p \in \mathbb{P} \setminus \{p_1, \ldots, p_k\},$$

so daß auch f_p eine Nullstelle in $\mathbb{Z}_p$ besitzt. Die Aussage des Satzes folgt dann per Induktion.

Seien also $p_1, \ldots, p_k \in \mathbb{P}$ wie oben gegeben. Wir betrachten das Polynom

$$f(a_0 \cdot p_1 \cdots p_k \cdot t) = a_0^n \cdot (p_1 \cdots p_k)^n \cdot a_n \cdot t^n + \ldots + a_0 \cdot (p_1 \cdots p_k) \cdot a_1 \cdot t + a_0 = a_0 \cdot g \in \mathbb{Z}[t],$$

wobei

$$g = b_n \cdot t^n + \ldots b_1 \cdot t + 1 \in \mathbb{Z}[t]$$

mit

$$b_i = a_0^{i-1} \cdot (p_1 \cdots p_k)^i \cdot a_i \in \mathbb{Z}.$$

Man beachte, daß b_i durch p_j teilbar ist für $i = 1, \ldots, n$ und $j = 1, \ldots, k$. Da nach (16) $a_0 \neq 0$ und da $n \geq 1$, ist g kein konstantes Polynom. Wegen Lemma 4.15 gibt es also eine ganze Zahl $z \in \mathbb{Z}$, so daß $g(z) \notin \{-1, 0, 1\}$, und wegen des Fundamentalsatzes der elementaren Zahlentheorie gibt es mithin eine Primzahl $p \in \mathbb{P}$, die die ganze Zahl $g(z)$ teilt, d.h.

$$g_p(\overline{z}_p) = \overline{g(z)}_p = \overline{0}_p \in \mathbb{Z}_p. \tag{17}$$

Dann gilt aber

$$f_p(\overline{a_0 \cdot p_1 \cdots p_k \cdot z}_p) = \overline{a_0}_p \cdot g_p(\overline{z}_p) = \overline{0}_p,$$

und damit hat f_p eine Nullstelle in $\mathbb{Z}_p$. Es bleibt zu zeigen, daß $p \notin \{p_1, \ldots, p_k\}$. Da p_j ein Teiler von b_i ist für alle $j = 1, \ldots, k$ und $i = 1, \ldots, n$, gilt

$$g_{p_j}(\overline{z}_{p_j}) = \overline{b_n}_{p_j} \cdot \overline{z}_{p_j}^n + \ldots + \overline{b_1}_{p_j} \cdot \overline{z}_{p_j} + \overline{1}_{p_j} = \overline{1}_{p_j} \neq \overline{0}_{p_j},$$

so daß wegen (17) $p \neq p_j$ für $j = 1, \ldots, k$. □

Korollar 4.17

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

Beweis: Nach Satz 4.16 gibt es unendlich viele Primzahlen p, so daß die Reduktion von $t^2 + 1$ modulo p eine Nullstelle in $\mathbb{Z}_p$ hat. Aus Satz 4.13 folgt dann, daß es unendlich viele Primzahlen p gibt, deren Rest modulo 4 Eins ist. □

5 Primitivwurzeln modulo n

Wir wollen uns in diesem Kapitel mit den Polynomen der Form

$$t^m - 1$$

beschäftigen. Betrachten wir das Polynom als ein Polynom in $\mathbb{C}[t]$, so ist

$$G = \left\{ e^{\frac{2\cdot\pi\cdot i\cdot k}{m}} \;\middle|\; k = 1, \ldots, m \right\}$$

die Menge der Nullstellen von $t^m - 1$ in $\mathbb{C}$. Man nennt diese auch die m-ten *Einheitswurzeln*. $g, h \in G$ genügen der Gleichung

$$(g \cdot h)^m = g^m \cdot h^m = 1 \cdot 1 = 1,$$

so daß G bezüglich der Multiplikation abgeschlossen ist, d.h. $g \cdot h \in G$. Da G endlich ist, reicht dies, um zu zeigen, daß G eine Untergruppe der multiplikativen Gruppe $(\mathbb{C}^*, \cdot)$ des Körpers $\mathbb{C}$ ist. Die *Gruppe* $(G, \cdot)$ ist zudem zyklisch, da jedes Element von G eine Potenz von $\zeta_m = e^{\frac{2\cdot\pi\cdot i}{m}}$ ist, d.h.

$$G = \left\{ \zeta_m, \zeta_m^2, \ldots, \zeta_m^m \right\} = \langle \zeta_m \rangle .$$

Man nennt einen Erzeuger von G auch eine *primitive* m*-te Einheitswurzel*, und ζ_m ist in aller Regel nicht die einzige. Ist $\mathrm{ggt}(k, m) = 1$, so liefert die Bézout-Identität ganze Zahlen $a, b \in \mathbb{Z}$, so daß

$$1 = a \cdot k + b \cdot m.$$

Folglich ist

$$\zeta_m = \zeta_m^{a\cdot k + b\cdot m} = \left(\zeta_m^k\right)^a \cdot \left(\zeta_m^m\right)^b = \left(\zeta_m^k\right)^a \cdot 1^b = \left(\zeta_m^k\right)^a \in \left\langle \zeta_m^k \right\rangle$$

und damit notwendigerweise auch

$$G = \left\langle \zeta_m^k \right\rangle .$$

Also ist ζ_m^k in diesem Fall eine primitive m-te Einheitswurzel. Ist umgekehrt ζ_m^k eine primitive m-te Einheitswurzel, so hat ζ_m^k die Ordnung m und mit Lemma 5.3 gilt

$$\frac{m}{\mathrm{ggt}(k, m)} = \frac{o(\zeta_m)}{\mathrm{ggt}(k, o(\zeta_m))} = o\left(\zeta_m^k\right) = m.$$

Der größte gemeinsame Teiler von k und m ist also Eins. Wir erhalten damit:

> ζ_m^k ist genau dann eine *primitive* m*-te Einheitswurzel*, wenn $\mathrm{ggt}(k, m) = 1$.

Insbesondere gibt es für jedes $m \in \mathbb{Z}_{>0}$ genau $\varphi(m)$ primitive m-te Einheitswurzeln in $\mathbb{C}$.

Wie sieht das aus, wenn man die komplexen Zahlen $\mathbb{C}$ durch den Ring $\mathbb{Z}_n$ ersetzt? Hat das Polynom

$$t^m - \overline{1} \in \mathbb{Z}_n[t]$$

dann immer noch Nullstellen? Bilden diese immer noch eine Gruppe bezüglich der Multiplikation? Ist diese Gruppe nach wie vor zyklisch? Lassen sich die primitiven Einheitswurzeln also auf $\mathbb{Z}_n$ verallgemeinern?

Bemerkung 5.1
Die Antwort auf zwei der Fragen ist offensichtlich und das mit dem gleichen Argument wie oben. Aus

$$\overline{a}^m = \overline{1}$$

folgt

$$\overline{a} \in \mathbb{Z}_n^*,$$

und wenn $\overline{a}, \overline{b} \in \mathbb{Z}_n^*$ beides Nullstellen von $t^m - \overline{1}$ sind, dann gilt

$$\left(\overline{a} \cdot \overline{b}\right)^m = \overline{a}^m \cdot \overline{b}^m = \overline{1} \cdot \overline{1} = \overline{1},$$

so daß auch $\overline{a} \cdot \overline{b}$ eine Nullstelle von $t^m - \overline{1}$ ist. Mithin ist die Menge

$$G_{m,n} = \left\{\overline{a} \in \mathbb{Z}_n^* \;\middle|\; \overline{a}^m = \overline{1}\right\}$$

der Nullstellen von $t^m - \overline{1} \in \mathbb{Z}_n[t]$ in $\mathbb{Z}_n$ abgeschlossen bezüglich der Multiplikation. Da $\overline{1} \in G_{m,n}$, ist die Menge nicht leer und als endliche Menge damit eine Untergruppe von $(\mathbb{Z}_n^*, \cdot)$, d.h.

$$(G_{m,n}, \cdot) \leq (\mathbb{Z}_n^*, \cdot).$$

Insbesondere hat $t^m - \overline{1}$ also Nullstellen in $\mathbb{Z}_n$.

Uns interessiert im folgenden *nur der Fall*

$$m = \varphi(n),$$

da dann der Satz von Euler 4.2

$$\overline{a}^{\varphi(n)} = \overline{1}$$

für alle $\overline{a} \in \mathbb{Z}_n^*$ impliziert, d.h.

$$G_{\varphi(n),n} = \mathbb{Z}_n^*$$

und $\mathbb{Z}_n^*$ ist genau die Menge der Nullstellen von

$$t^{\varphi(n)} - \overline{1} \in \mathbb{Z}_n[t].$$

Offen bleibt also die Frage, ob $G_{\varphi(n),n} = \mathbb{Z}_n^*$ zyklisch ist und die primitiven $\varphi(n)$-ten Einheitswurzeln sich für diesen Fall verallgemeinern lassen. $\square$

Dies führt uns zu folgender Definition.

Definition 5.2
Eine positive ganze Zahl $a \in \mathbb{Z}_{>0}$ heißt *Primitivwurzel modulo* n, falls

$$\mathbb{Z}_n^* = \left\{\overline{a}^k \;\middle|\; k = 1, \ldots, \varphi(n)\right\} = \langle\overline{a}\rangle.$$

Dies ist gleichwertig dazu, daß $\overline{a}$ in $\mathbb{Z}_n^*$ die Ordnung $\varphi(n)$ hat.

Beachte, daß für eine Primitivwurzel a modulo n zwangsläufig $\mathrm{ggt}(a, n) = 1$ gilt.

Die Frage, ob es eine Primitivwurzel modulo n gibt, ist gleichwertig zur Frage, ob die Gruppe $\mathbb{Z}_n^*$ zyklisch ist. Wir werden uns deshalb zunächst mit Eigenschaften von zyklischen Gruppen auseinandersetzen müssen.

A) **Die Struktur zyklischer Gruppen**

Wir betrachten zunächst, wie sich die Ordnung von Elementen einer Gruppe beim Multiplizieren und Potenzieren verhalten.

Lemma 5.3

Es sei $(G, \cdot)$ *eine Gruppe,* $g, h \in G$ *mit* $o(g), o(h) < \infty$ *und* $k \in \mathbb{Z}$.

a. *Falls* $g \cdot h = h \cdot g$ *und* $\langle g \rangle \cap \langle h \rangle = \{e\}$, *dann ist* $o(g \cdot h) = \text{kgv}\big(o(g), o(h)\big)$.
b. $o\big(g^k\big) = \frac{o(g)}{\text{ggt}(o(g),k)}$.
c. *Ist* $d \mid o(g)$, *so gilt* $\big|\big\{g^l \;\big|\; l \in \mathbb{Z},\ o\big(g^l\big) = d\big\}\big| \geq \varphi(d)$.

Beweis: a. Es sei $k = \text{kgv}\big(o(g), o(h)\big)$ und $m = o(g \cdot h)$. Wir wollen zeigen, daß k ein Teiler von m ist und umgekehrt, dann müssen die beiden positiven Zahlen übereinstimmen.

Für die Ordnung m von $g \cdot h$ gilt

$$e = (g \cdot h)^m = g^m \cdot h^m,$$

da g und h kommutieren. Daraus folgt

$$g^m = h^{-m} \in \langle g \rangle \cap \langle h \rangle = \{e\},$$

und damit $g^m = e$ und $h^m = e^{-1} = e$. Folglich sind $o(g)$ und $o(h)$ Teiler von m, und mithin ist ihr kleinstes gemeinsames Vielfaches k ein Teiler von m.

Umgekehrt läßt sich das kleinste gemeinsame Vielfache k schreiben als $k = a \cdot o(g) = b \cdot o(h)$ für geeignete $a, b \in \mathbb{Z}_{>0}$. Dann gilt aber

$$(g \cdot h)^k = g^k \cdot h^k = \big(g^{o(g)}\big)^a \cdot \big(h^{o(h)}\big)^b = e^a \cdot e^b = e,$$

so daß die Ordnung m von $g \cdot h$ ein Teiler von k sein muß.

b. Der Beweis ist dem Leser als Übungsaufgabe überlassen.

c. Sei $n = o(g)$ und $1 \leq k \leq d$ mit $\text{ggt}(d, k) = 1$. Da $\frac{n}{d}$ ein Teiler von n und von $\frac{k \cdot n}{d}$ ist, gilt $\text{ggt}\left(n, \frac{k \cdot n}{d}\right) = \frac{n}{d} \cdot \text{ggt}(d, k) = \frac{n}{d}$. Aus Teil b. folgt damit

$$o\big(g^{\frac{k \cdot n}{d}}\big) = \frac{n}{\text{ggt}\left(n, \frac{k \cdot n}{d}\right)} = d.$$

Damit gilt

$$\big|\big\{g^l \;\big|\; l \in \mathbb{Z},\ o\big(g^l\big) = d\big\}\big| \geq \left|\left\{g^{\frac{k \cdot n}{d}} \;\middle|\; 1 \leq k \leq d,\ \text{ggt}(d, k) = 1\right\}\right| = \varphi(d),$$

wobei man für die letzte Gleichheit beachten sollte, daß die $g^{\frac{k \cdot n}{d}}$ paarweise verschieden sind, da $1 \leq \frac{k \cdot n}{d} \leq n = o(g)$ für $1 \leq k \leq d$.

$\square$

Aufgabe 5.4
Beweise Lemma 5.3 Teil b.

Lemma 5.5
Es sei $(G, \cdot)$ *eine Gruppe,* $g \in G$*,* $k_1, \ldots, k_n \in \mathbb{Z}$ *und* $k \in \mathrm{ggT}(k_1, \ldots, k_n)$*. Dann gilt*

$$\left\langle g^{k_1}, \ldots, g^{k_n} \right\rangle = \left\langle g^k \right\rangle.$$

Insbesondere ist jede endlich erzeugte Untergruppe einer zyklischen Gruppe zyklisch.

Beweis: Es gibt ganze Zahlen $a_i, c_i \in \mathbb{Z}$, $i = 1, \ldots, n$, so daß $k_i = a_i \cdot k$ und $k = c_1 \cdot k_1 + \ldots + c_n \cdot k_n$. Mithin ist

$$g^k = g^{c_1 \cdot k_1 + \ldots + c_n \cdot k_n} = (g^{k_1})^{c_1} \cdots (g^{k_n})^{c_n} \in \langle g^{k_1}, \ldots, g^{k_n} \rangle$$

und

$$g^{k_i} = g^{a_i \cdot k} = (g^k)^{a_i} \in \langle g^k \rangle$$

für $i = 1, \ldots, n$. Damit stimmen aber die Erzeugnisse von $g^{k_1}, \ldots, g^{k_n}$ bzw. von g^k überein.

Ist $H = \langle h \rangle$ eine zyklische Gruppe und $U = \langle h^{k_1}, \ldots, h^{k_n} \rangle$ eine endlich erzeugte Untergruppe von H, so ist U erzeugt von $h^{\mathrm{ggt}(k_1, \ldots, k_n)}$ und damit zyklisch. □

Bemerkung 5.6
Ist $G = \langle g \rangle$ eine zyklische Gruppe, dann ist die Abbildung

$$\alpha : \mathbb{Z} \longrightarrow G : z \mapsto g^z$$

ein *Gruppenepimorphismus.* α ist genau dann ein Isomorphismus, wenn $o(g) = \infty$. Andernfalls ist $\mathrm{Ker}(\alpha) = n\mathbb{Z}$, wobei $n = o(g) < \infty$. Aufgrund des *Homomorphiesatzes* ist die Abbildung $\overline{\alpha} : \mathbb{Z}/n\mathbb{Z} \longrightarrow G : \overline{z} \mapsto g^z$ dann ein Gruppenisomorphismus. Wir erhalten also

$$G \cong \begin{cases} \mathbb{Z}, & \text{falls } o(g) = \infty, \\ \mathbb{Z}/n\mathbb{Z}, & \text{falls } o(g) = n < \infty. \end{cases}$$

Beachten wir nun noch, daß die Untergruppen der additiven Gruppe $(\mathbb{Z}, +)$ genau die Ideale des Ringes $(\mathbb{Z}, +, \cdot)$ sind, so folgt die Aussage von Lemma 5.5 unmittelbar aus Proposition 2.2, da

$$\overline{\alpha}^{-1}\big(\langle g^{k_1}, \ldots, g^{k_n} \rangle\big) = \langle k_1, \ldots, k_n \rangle_{\mathbb{Z}} = \langle k \rangle_{\mathbb{Z}} = \overline{\alpha}^{-1}\big(\langle g^k \rangle\big)$$

für $k \in \mathrm{ggT}(k_1, \ldots, k_n)$ und da α ein Epimorphismus ist. Zudem folgt damit unmittelbar, daß *jede Untergruppe einer zyklischen Gruppe wieder zyklisch* ist, da $(\mathbb{Z}, +, \cdot)$ ein *Hauptidealring* ist, d.h. die Einschränkung *endlich erzeugt* in Lemma 5.5 ist *unnötig.*

Da wir in diesem Kapitel jedoch an Untergruppen der *multiplikativen* Gruppe $(\mathbb{Z}_n^*, \cdot)$ interessiert sind, wollen unsere Beweise lieber *direkt* als durch den Übergang zur *additiven* Gruppe $(\mathbb{Z}_m, +)$ für ein geeignetes m führen. □

Proposition 5.7
Für eine endliche Gruppe $(G, \cdot)$ *sind die folgenden Aussagen äquivalent:*

a. G *ist zyklisch.*

b. G *hat für jeden Teiler* d *von* $|G|$ *genau* $\varphi(d)$ *Elemente der Ordnung* d.

c. G *hat für jeden Teiler* d *von* $|G|$ *höchstens* $\varphi(d)$ *Elemente der Ordnung* d.

Beweis: Es sei $n = |G|$ die Ordnung von G.

a. ⇒ b.: Wegen des Satzes von Lagrange ist die Ordnung jedes Elementes von G ein Teiler von n, so daß $G = \langle g \rangle$ folgende disjunkte Zerlegung besitzt:

$$G = \dot{\bigcup_{\substack{1 \leq d \leq n \\ d \mid n}}} \{g^l \mid l \in \mathbb{Z},\ o(g^l) = d\}.$$

Nach Lemma 5.3 gilt aber

$$\left|\{g^l \mid l \in \mathbb{Z},\ o(g^l) = d\}\right| \geq \varphi(d), \tag{18}$$

so daß wir unter Berücksichtigung von Korollar 3.14

$$n = |G| = \sum_{\substack{1 \leq d \leq n \\ d \mid n}} \left|\{g^l \mid l \in \mathbb{Z},\ o(g^l) = d\}\right| \geq \sum_{\substack{1 \leq d \leq n \\ d \mid n}} \varphi(d) = n$$

erhalten. Dies ist aber nur möglich, wenn die Ungleichungen (18) für alle d Gleichungen sind. Damit ist b. gezeigt.

b. ⇒ c.: Dies gilt offenbar.

c. ⇒ a.: Nach Voraussetzung gilt

$$\left|\{g \in G \mid\ o(g) = d\}\right| \leq \varphi(d) \tag{19}$$

für alle $d \mid n$. Da

$$G = \dot{\bigcup_{\substack{1 \leq d \leq n \\ d \mid n}}} \{g \in G \mid o(g) = d\}$$

aufgrund des Satzes von Lagrange, gilt mithin

$$n = |G| = \sum_{\substack{1 \leq d \leq n \\ d \mid n}} \left|\{g \in G \mid o(g) = d\}\right| \leq \sum_{\substack{1 \leq d \leq n \\ d \mid n}} \varphi(d) = n.$$

Dies bedingt wieder, daß die Ungleichungen (19) alle Gleichungen sein müssen. Insbesondere bedeutet das, daß G genau $\varphi(n) \geq 1$ Elemente der Ordnung $n = |G|$ enthält, und jedes dieser Elemente muß zwangsläufig ein Erzeuger von G sein. G ist also zyklisch.

□

Da eine endliche Gruppe der Ordnung n genau dann ein Element der Ordnung n enthält, wenn sie zyklisch ist, und da sie nach der gerade gezeigten Proposition dann genau $\varphi(n)$ Elemente der Ordnung n enthält, erhalten wir das folgende Korollar.

Korollar 5.8
Ist G *eine endliche Gruppe der Ordnung* n*, so enthält* G *entweder kein oder genau* $\varphi(n)$ *Elemente der Ordnung* n*.*

Statt eine zyklische Gruppe durch die Anzahl der Elemente zu den nach Lagrange möglichen Ordnungen zu charakterisieren, kann man sie auch durch die Anzahl der möglichen Untergruppen bestimmen.

Satz 5.9
Für eine endliche Gruppe $(G, \cdot)$ *sind die folgenden Aussagen äquivalent:*

a. G *ist zyklisch.*
b. G *hat für jeden Teiler* d *von* $|G|$ *genau eine Untergruppe der Ordnung* d*.*
c. G *hat für jeden Teiler* d *von* $|G|$ *höchstens eine Untergruppe der Ordnung* d*.*

Insbesondere, für $G = \langle g \rangle$ *mit* $o(g) = n$ *ist* $\left\langle g^{\frac{n}{d}} \right\rangle$ die *Untergruppe der Ordnung* d*.*

Beweis: Wir bezeichnen mit $n = |G|$ die Ordnung von G.

a. $\Rightarrow$ b.: Es sei $G = \langle g \rangle$ zyklisch mit $o(g) = |G| = n$ und d sei ein Teiler von n. Nach Lemma 5.3 ist $U = \left\langle g^{\frac{n}{d}} \right\rangle \leq G$ eine Untergruppe von G der Ordnung

$$|U| = o\big(g^{\frac{n}{d}}\big) = \frac{o(g)}{\mathrm{ggt}\left(o(g), \frac{n}{d}\right)} = d,$$

so daß G eine Untergruppe der Ordnung d hat. Zudem enthalten nach Proposition 5.7 sowohl G als auch U genau $\varphi(d)$ Elemente der Ordnung d, so daß jedes Element $h \in G$ der Ordnung d bereits in U enthalten ist. Ist nun $V \leq G$ eine beliebige Untergruppe von G der Ordnung d, so ist V nach Lemma 5.5 zyklisch, also von einem Element h der Ordnung d erzeugt. Wegen $h \in U$ ist auch $V = \langle h \rangle \subseteq U$, und da beide Untergruppen d Elemente enthalten, sind sie gleich. G enthält also genau eine Untergruppe der Ordnung d.

b. $\Rightarrow$ c.: Dies gilt offenbar.

c. $\Rightarrow$ a.: Es sei d ein Teiler von n. Enthält G ein Element h der Ordnung d, so erzeugt dieses eine zyklische Untergruppe $U = \langle h \rangle$ von G. Da G höchstens eine Untergruppe der Ordnung d enthält, muß jedes weitere Element von G mit Ordnung d bereits in U enthalten sein. Mithin ist

$$\big|\{g \in G \mid o(g) = d\}\big| = \big|\{g \in U \mid o(g) = d\}\big| \leq \varphi(d),$$

wobei die letzte Ungleichung aus Korollar 5.8 folgt. Dann ist G aber zyklisch nach Proposition 5.7.

$\square$

Korollar 5.10
Ist G *eine endliche zyklische Gruppe und sind* $U, V \leq G$ *Untergruppen von* G*, so ist* U *genau dann in* V *enthalten, wenn* $|U|$ *ein Teiler von* $|V|$ *ist.*

Beweis: Ist U in V enthalten, so ist die Ordnung von U aufgrund des Satzes von Lagrange ein Teiler der Ordnung von V. Ist umgekehrt die Ordnung von U ein Teiler der Ordnung von V, so besitzt V nach Satz 5.9 eine Untergruppe W der Ordnung $|U|$, da V nach Lemma 5.5 zyklisch ist. W ist aber zugleich eine Untergruppe von G, und da G nach Satz 5.9 nur eine Untergruppe der Ordnung $|U|$ besitzt, muß $U = W$ gelten. Insbesondere ist U also in V enthalten. □

Wir haben in den algebraischen Strukturen gesehen, daß das kartesische Produkt zweier Gruppen mittels der komponentenweisen Operation wieder eine Gruppe ist. Die analoge Aussage für mehr als zwei Gruppen gilt entsprechend. Man spricht dann vom *(äußeren) direkten Produkt* der Gruppen. Es gibt Eigenschaften, die sich von den einzelnen Gruppen auf das direkte Produkt übertragen. Sind alle Gruppen abelsch, so ist das direkte Produkt abelsch. Wenn die einzelnen Faktoren zyklisch, ist dann auch das direkte Produkt zyklisch?

Proposition 5.11

Seien $G_1, \ldots, G_n$ *endliche Gruppen. Genau dann ist das direkte Produkt* $G_1 \times \cdots \times G_n$ *zyklisch, wenn* $G_1, \ldots, G_n$ *zyklisch sind von paarweise teilerfremder Ordnung.*

Beweis: Wir führen den Beweis durch Induktion nach n und betrachten zunächst den Fall $n = 2$.

Es seien $g_1 \in G_1$ und $g_2 \in G_2$, und wir setzen $g = (g_1, e_{G_2}) \in G_1 \times G_2$ und $h = (e_{G_1}, g_2) \in G_1 \times G_2$. Dann gilt $g \cdot h = (g_1, g_2) = h \cdot g$ und

$$\langle g \rangle \cap \langle h \rangle = \big(\langle g_1 \rangle \times \{e_{G_2}\}\big) \cap \big(\{e_{G_1}\} \times \langle g_2 \rangle\big) = \{(e_{G_1}, e_{G_2})\} = \{e_{G_1 \times G_2}\}.$$

Wir können also Lemma 5.3 anwenden und erhalten

$$\begin{aligned} o\big((g_1, g_2)\big) &= o(g \cdot h) = \mathrm{kgv}\,\big(o(g), o(h)\big) \\ &= \frac{o(g) \cdot o(h)}{\mathrm{ggt}(o(g), o(h))} = \frac{o(g_1) \cdot o(g_2)}{\mathrm{ggt}(o(g_1), o(g_2))} \leq |G_1| \cdot |G_2|. \end{aligned} \tag{20}$$

Nun ist $G_1 \times G_2$ genau dann zyklisch, wenn es ein $(g_1, g_2) \in G_1 \times G_2$ mit Ordnung $o(g_1, g_2) = |G_1| \cdot |G_2|$ gibt, und wegen (20) ist das genau dann der Fall, wenn es ein $g_1 \in G_1$ und ein $g_2 \in G_2$ gibt mit $o(g_1) = |G_1|$, $o(g_2) = |G_2|$ und $\mathrm{ggt}\,\big(o(g_1), o(g_2)\big) = 1$, d.h. wenn G_1 und G_2 zyklisch sind mit $\mathrm{ggt}(|G_1|, |G_2|) = 1$.

Sei nun $n \geq 3$. Ist $G_1 \times \cdots \times G_n$ zyklisch, so ist für $i \neq j$ nach Lemma 5.5 auch die Untergruppe

$$\{(g_1, \ldots, g_n) \in G_1 \times \cdots \times G_n \mid g_l = e_{G_l} \text{ für } l \neq i, j\} \cong G_i \times G_j$$

zyklisch. Der Fall $n = 2$ impliziert dann, daß G_i und G_j zyklisch von teilerfremder Ordnung sind. Also sind die G_i zyklisch von paarweise teilerfremder Ordnung.

Sind umgekehrt die G_i zyklisch von paarweise teilerfremder Ordnung, so ist nach Induktion auch $G_1 \times \cdots \times G_{n-1}$ zyklisch und $|G_1 \times \cdots \times G_{n-1}| = |G_1| \cdots |G_{n-1}|$ hat keinen gemeinsamen Teiler mit $|G_n|$. Der Fall $n = 2$ angewandt auf $G_1 \times \cdots \times G_{n-1}$ und G_n impliziert dann, daß auch $G_1 \times \cdots \times G_n$ zyklisch ist. $\square$

B) **Die Struktur von $\mathbb{Z}_n^*$**

Mit den obigen Vorarbeiten wollen wir nun die Struktur der *primen Restklassengruppe* $\mathbb{Z}_n^*$ untersuchen und dabei insbesondere angeben, für welche n *Primitivwurzeln modulo* n existieren und wie man sie ggf. finden kann. Wir betrachten zunächst den Fall, daß n eine Primzahl ist.

Satz 5.12 (Lambert–Euler–Gauß)
Ist $(G, \cdot)$ *eine endliche Untergruppe der multiplikativen Gruppe eines Körpers* $(K, +, \cdot)$*, so ist* G *zyklisch.*

Insbesondere ist $(\mathbb{Z}_p^*, \cdot)$ *zyklisch und es gibt Primitivwurzeln modulo* p *für* $p \in \mathbb{P}$*.*

Beweis: Sei $U \leq G$ eine Untergruppe von G der Ordnung d, wobei d ein Teiler von $|G|$ ist, so gilt nach dem Satz von Lagrange

$$u^d = u^{|U|} = 1$$

für jedes $u \in U$. Damit sind die d Elemente von U Nullstellen des Polynoms

$$t^d - 1 \in K[t].$$

Da dieses Polynom höchstens d Nullstellen besitzt, kann es keine zweite Untergruppe von G der Ordnung d geben. Damit ist G aufgrund von Satz 5.9 zyklisch. $\square$

Bemerkung 5.13
Der Beweis der Existenz von Primitivwurzeln modulo einer Primzahl ist nicht konstruktiv. Um sie zu finden bleibt keine andere Wahl, als die Ordnungen der Elemente von $\mathbb{Z}_p^*$ auszurechnen. Allerdings sollte man dabei geschickt vorgehen. Ist etwa a *keine* Primitivwurzel modulo p, so kann auch keine Potenz von a eine Primitivwurzel modulo p sein. Zudem gibt es aufgrund von Proposition 5.7 zwischen 1 und $p-1$ genau $\varphi(p-1)$ Primitivwurzeln modulo p.

Wir wollen nun eine Primitivwurzel modulo $p = 17$ bestimmen. Die Elemente von $\mathbb{Z}_{17}^*$ sind

$$\overline{1},\ \overline{2},\ \ldots,\ \overline{16}.$$

Aus

$$\overline{2}^4 = \overline{16} = \overline{-1}$$

folgt $\overline{2}^8 = \overline{1}$ und

$$o\big(\overline{2}\big) = 8 < 16 = |\mathbb{Z}_{17}^*|.$$

Mithin sind

$$\overline{2},\ \overline{4} = \overline{2}^2,\ \overline{8} = \overline{2}^3,\ \overline{16} = \overline{2}^4,\ \overline{15} = \overline{2}^5,\ \overline{13} = \overline{2}^6,\ \overline{9} = \overline{2}^7,\quad \text{und}\quad \overline{1} = \overline{2}^8$$

keine Primitivwurzeln modulo 17. Nach Proposition 5.7 gibt es in $\mathbb{Z}_{17}^*$ genau $\varphi(16) = 8$ Erzeuger von $\mathbb{Z}_{17}^*$, so daß

$$\overline{3},\ \overline{5},\ \overline{6},\ \overline{7},\ \overline{10},\ \overline{11},\ \overline{12} \quad \text{und} \quad \overline{14}$$

Ordnung 16 haben. D.h.

$$3,\ 5,\ 6,\ 7,\ 10,\ 11,\ 12 \quad \text{und} \quad 14$$

sind *Primitivwurzeln* modulo 17. □

Als nächstes wollen wir zeigen, wie man aus einer Primitivwurzel modulo p ggf. eine Primitivwurzel modulo einer Potenz von p gewinnen kann. Dazu benötigen wir folgende Hilfsaussagen für die Ordnungen von $\overline{a}_{p^k}$ in $\mathbb{Z}_{p^k}^*$ für diverse p und k.

Lemma 5.14
Es sei $p \in \mathbb{P}$, $k \in \mathbb{Z}_{>0}$ *und* $a \in \mathbb{Z}$ *mit* $\operatorname{ggt}(a, p) = 1$, *dann gilt*

$$o\big(\overline{a}_{p^{k+1}}\big) \in \big\{o\big(\overline{a}_{p^k}\big), p \cdot o\big(\overline{a}_{p^k}\big)\big\}.$$

Aufgabe 5.15
Beweise Lemma 5.14.

Lemma 5.16
Es seien $a \in \mathbb{Z}$, $p \in \mathbb{P}$ *und* $k \in \mathbb{Z}_{>0}$ *mit* $\operatorname{ggt}(a, p) = 1$ *und* $k \cdot p \geq 3$. *Falls* $o\big(\overline{a}_{p^k}\big) = (p-1) \cdot p^m$ *und* $o\big(\overline{a}_{p^{k+1}}\big) = (p-1) \cdot p^{m+1}$, *dann ist*

$$o\big(\overline{a}_{p^{k+2}}\big) = (p-1) \cdot p^{m+2}.$$

Beweis: Aus $o\big(\overline{a}_{p^k}\big) = (p-1) \cdot p^m$ folgt

$$a^{(p-1)\cdot p^m} \equiv 1 \pmod{p^k}, \tag{21}$$

und wegen $o\big(\overline{a}_{p^{k+1}}\big) = (p-1) \cdot p^{m+1}$ gilt

$$a^{(p-1)\cdot p^m} \not\equiv 1 \pmod{p^{k+1}}. \tag{22}$$

Wegen (21) gibt es dann ein $b \in \mathbb{Z}$, so daß

$$a^{(p-1)\cdot p^m} = 1 + b \cdot p^k, \tag{23}$$

und wegen (22) gilt

$$p \not| \, b. \tag{24}$$

Potenzieren wir Gleichung (23) mit p, so erhalten wir

$$a^{(p-1)\cdot p^{m+1}} = \big(1 + b \cdot p^k\big)^p = 1 + b \cdot p^{k+1} + \sum_{j=2}^{p-1} \binom{p}{j} \cdot b^j \cdot p^{j\cdot k} + b^p \cdot p^{k\cdot p}. \tag{25}$$

Für $j = 2, \cdots, p-1$ teilt p den Binomialkoeffizienten $\binom{p}{j}$ und $j \cdot k \geq 2 \cdot k \geq k+1$, so daß

$$\binom{p}{j} \cdot b^j \cdot p^{j\cdot k} \equiv 0 \pmod{p^{k+2}}.$$

Die Voraussetzung $k \cdot p \geq 3$ impliziert zudem $k \cdot p \geq k+2$, so daß auch

$$b^p \cdot p^{k\cdot p} \equiv 0 \pmod{p^{k+2}}.$$

Damit erhalten wir aus (25) und (24)

$$a^{(p-1)\cdot p^{m+1}} \equiv 1 + b \cdot p^{k+1} \not\equiv 1 \pmod{p^{k+2}},$$

da p kein Teiler von b ist. Mithin ist die Ordnung von $\overline{a}_{p^{k+2}}$ ungleich der Ordnung $(p-1)\cdot p^{m+1} = o\big(\overline{a}_{p^{k+1}}\big)$ von $\overline{a}_{p^{k+1}}$, so daß aus Lemma 5.14

$$\overline{a}_{p^{k+2}} = p \cdot o\big(\overline{a}_{p^{k+1}}\big) = (p-1)\cdot p^{m+2}$$

folgt. □

Wir wollen nun zunächst die Existenz von Primitivwurzeln modulo Primzahlquadraten zeigen.

Satz 5.17 (Jacobi)
Es sei $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ sei eine Primitivwurzel modulo p, dann ist a oder $a+p$ eine Primitivwurzel modulo p^2. Insbesondere ist $\mathbb{Z}_{p^2}^*$ zyklisch für alle $p \in \mathbb{P}$.

Beweis: Ist a eine Primitivwurzel modulo p, so gilt insbesondere $\operatorname{ggt}(a,p) = 1$ und aus Lemma 5.14 folgt dann, daß

$$o\big(\overline{a}_{p^2}\big) \in \big\{o\big(\overline{a}_p\big), o\big(\overline{a}_p\big)\cdot p\big\} = \{p-1, (p-1)\cdot p\}.$$

In letzterem Fall ist a eine Primitivwurzel modulo p^2, so daß wir $o\big(\overline{a}_{p^2}\big) = p-1$ annehmen können, d.h.

$$a^{p-1} \equiv 1 \pmod{p^2}. \tag{26}$$

Wir müssen nun zeigen, daß

$$o\big(\overline{a+p}_{p^2}\big) = (p-1)\cdot p.$$

Nehmen wir an, dies sei nicht der Fall. Wegen $a + p \equiv a \pmod{p}$ ist mit a auch $a+p$ eine Primitivwurzel modulo p, und mit dem gleichen Argument wie eben gilt dann auch

$$o\big(\overline{a+p}_{p^2}\big) = (p-1).$$

Übersetzen wir dies in eine Kongruenzgleichung, so erhalten wir modulo p^2

$$\begin{aligned} 1 &\equiv (a+p)^{p-1} = a^{p-1} + (p-1)\cdot p \cdot a^{p-2} + p^2 \cdot \sum_{j=2}^{p-1} \binom{p-1}{j} \cdot p^{j-2} \cdot a^{p-1-j} \\ &\equiv a^{p-1} + (p-1)\cdot p\cdot a^{p-2} \equiv 1 + (p-1)\cdot p \cdot a^{p-2} \pmod{p^2}, \end{aligned}$$

wobei wir für die letzte Kongruenz (26) verwenden. Dies bedingt

$$(p-1)\cdot p \cdot a^{p-2} \equiv 0 \pmod{p^2},$$

so daß p ein Teiler von a^{p-2} ist, im Widerspruch zur Voraussetzung, daß p eine Primzahl und a als Primitivwurzel modulo p teilerfremd zu p ist.

Also ist $a+p$ eine Primitivwurzel modulo p^2. □

Beispiel 5.18
7 ist eine Primitivwurzel modulo 5, da

$$7^2 = 49 \equiv 4 \pmod 5,\quad 7^3 = 343 \equiv 3 \pmod 5 \quad \text{und} \quad 7^4 = 2401 \equiv 1 \pmod 5.$$

Da aber auch

$$7^4 = 2401 \ \equiv \ 1 (\mathrm{mod}\ 25),$$

ist 7 keine Primitivwurzel modulo 25. Aus Satz 5.17 folgt dann aber, daß 12 eine Primitivwurzel modulo 25 ist. □

Ist p eine ungerade Primzahl, so existieren auch Primitivwurzeln modulo allen p^k.

Satz 5.19
Es sei $p \in \mathbb{P}$ *ungerade und* a *sei eine Primitivwurzel modulo* p *und modulo* p^2*, dann ist* a *eine Primitivwurzel modulo* p^k *für alle* $k \in \mathbb{Z}_{>0}$.

Insbesondere ist $\mathbb{Z}_{p^k}$ *zyklisch für* $2 \neq p \in \mathbb{P}$ *und* $k \in \mathbb{Z}_{>0}$.

Beweis: Ist a eine Primitivwurzel modulo p und modulo p^2, so gilt

$$o\big(\overline{a}_p\big) = p - 1 \quad \text{und} \quad o\big(\overline{a}_{p^2}\big) = (p-1)\cdot p.$$

Mittels Induktion folgt dann aus Lemma 5.16

$$o\big(\overline{a}_{p^k}\big) = (p-1)\cdot p^{k-1},$$

d.h. a ist eine Primitivwurzel modulo p^k.

Da es aufgrund der Sätze 5.12 und 5.17 ein $a \in \mathbb{Z}$ gibt, welches Primitivwurzel modulo p und modulo p^2 ist, ist damit $\mathbb{Z}_{p^k}^*$ zyklisch für alle $k \in \mathbb{Z}_{>0}$. □

Beispiel 5.20
Wegen $2 \equiv 7 \pmod 5$ ist 2 nach Beispiel 5.18 eine Primitivwurzel modulo 5. Zudem folgt wegen Lemma 5.14 aus

$$2^4 = 16 \ \not\equiv \ 1 \pmod{25},$$

daß $o\big(\overline{2}_{25}\big) = 5 \cdot o\big(\overline{2}_5\big) = 5 \cdot 4 = \varphi(25)$. 2 ist also auch eine Primitivwurzel modulo 25. Wegen Satz 5.19 ist 2 dann eine Primitivwurzel modulo 5^k für alle $k \in \mathbb{Z}_{>0}$. □

Aufgabe 5.21
Zeige, daß 2 eine Primitivwurzel modulo 3^k für alle $k \in \mathbb{Z}_{>0}$ ist.

Das folgende Beispiel zeigt, daß die Notwendigkeit der Bedingung p *ungerade*.

Beispiel 5.22
Es gilt

$$\mathbb{Z}_8^* = \big\{\overline{1}_8, \overline{3}_8, \overline{5}_8, \overline{7}_8\big\}$$

und

$$\overline{3}_8^2 = \overline{5}_8^2 = \overline{7}_8^2 = \overline{1}_8.$$

Die Gruppe $\mathbb{Z}_8^*$ ist also nicht zyklisch, da sie kein Element der Ordnung 4 enthält. Beachtet man, daß $\overline{7}_8 = -\overline{1}_8$ und $\overline{3}_8 = -\overline{1}_8 \cdot \overline{5}_8$, so gilt

$$\mathbb{Z}_8^* = \big\langle -\overline{1}_8\big\rangle \cdot \big\langle \overline{5}_8\big\rangle.$$

Als nicht-zyklische Gruppe der Ordnung 4 ist $\mathbb{Z}_8^*$ isomorph zur *Kleinschen Vierergruppe* $\mathbb{Z}_2 \times \mathbb{Z}_2$. □

Das Beispiel ist ein Spezialfall des folgenden Satzes.

Satz 5.23
Für $k \geq 3$ *gilt*

$$o\big(\overline{5}_{2^k}\big) = 2^{k-2}$$

und

$$\mathbb{Z}_{2^k}^* = \big\langle -\overline{1}_{2^k}\big\rangle \cdot \big\langle \overline{5}_{2^k}\big\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}.$$

Insbesondere ist $\mathbb{Z}_{2^k}^*$ *nicht zyklisch für* $k \geq 3$.

Beweis: Eine leichte Rechnung zeigt

$$5 \equiv 1 \ (\mathrm{mod}\ 4), \quad 5 \ \equiv \ 5 \ (\mathrm{mod}\ 8), \quad \text{und} \quad 5^2 = 25 \ \equiv \ 1 \ (\mathrm{mod}\ 8),$$

so daß

$$o\big(\overline{5}_{2^2}\big) = 1 = (2-1)\cdot 2^0 \quad \text{und} \quad o\big(\overline{5}_{2^3}\big) = 2 = (2-1)\cdot 2^1.$$

Lemma 5.16 impliziert dann per Induktion nach k, daß

$$o\big(\overline{5}_{2^k}\big) = 2^{k-2}.$$

Wir wollen nun zeigen, daß

$$\big\langle -\overline{1}_{2^k}\big\rangle \cap \big\langle \overline{5}_{2^k}\big\rangle = \big\{\overline{1}_{2^k}\big\}. \tag{27}$$

Da

$$\big\langle -\overline{1}_{2^k}\big\rangle = \big\{\overline{1}_{2^k}, -\overline{1}_{2^k}\big\}$$

reicht es dazu, zu zeigen, daß $-\overline{1}_{2^k} \not\in \big\langle \overline{5}_{2^k}\big\rangle$. Nehmen wir das Gegenteil an, so gilt mit geeigneten $m \in \mathbb{Z}_{>0}$ und $b \in \mathbb{Z}$

$$-1 = 5^m + 2^k \cdot b \equiv 5^m \equiv 1 \ (\mathrm{mod}\ 4),$$

was offenbar falsch ist.

Da $\mathbb{Z}_{2^k}^*$ abelsch ist, ist das Produkt $\big\langle -\overline{1}_{2^k}\big\rangle \cdot \big\langle \overline{5}_{2^k}\big\rangle$ eine Untergruppe von $\mathbb{Z}_{2^k}^*$. Aus der Produktformel folgt dann wegen (27)

$$\big|\big\langle -\overline{1}_{2^k}\big\rangle \cdot \big\langle \overline{5}_{2^k}\big\rangle\big| = \frac{\big|\big\langle -\overline{1}_{2^k}\big\rangle\big| \cdot \big|\big\langle \overline{5}_{2^k}\big\rangle\big|}{\big|\big\langle -\overline{1}_{2^k}\big\rangle \cap \big\langle \overline{5}_{2^k}\big\rangle\big|} = o\big(-\overline{1}_{2^k}\big) \cdot o\big(\overline{5}_{2^k}\big) = 2^{k-1} = |\mathbb{Z}_{2^k}^*|.$$

Mithin ist

$$\mathbb{Z}_{2^k}^* = \big\langle -\overline{1}_{2^k}\big\rangle \cdot \big\langle \overline{5}_{2^k}\big\rangle \tag{28}$$

das innere direkte Produkt einer zyklischen Untergruppe der Ordnung 2 mit einer zyklischen Untergruppe der Ordnung 2^{k-2}.

Wir definieren nun die Abbildung

$$\alpha : \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} \longrightarrow \mathbb{Z}_{2^k}^* : \left(\overline{m}_2, \overline{n}_{2^{k-2}}\right) \mapsto \left(-\overline{1}_{2^k}\right)^m \cdot \left(\overline{5}_{2^k}\right)^n.$$

Man sieht leicht, daß α wohldefiniert ist, sprich nicht von der Wahl der Vertreter für $\overline{m}_2$ bzw. für $\overline{n}_{2^{k-2}}$ abhängt. Zudem ist α ein Gruppenhomomorphismus, da $\mathbb{Z}_{2^k}^*$ abelsch ist und da die Potenzgesetze gelten, und α ist wegen (28) surjektiv. Da sowohl $\mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$, als auch $\mathbb{Z}_{2^k}^*$ genau 2^{k-1} Elemente enthalten, muß α dann bijektiv sein. Die beiden Gruppen sind also isomorph. □

Satz 5.24 (Gauß, Disquisitiones, Art. 92)
Für eine positive ganze Zahl $n \in \mathbb{Z}_{>0}$ mit Primfaktorzerlegung $n = p_1^{n_1} \cdots p_k^{n_k}$ gilt

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{n_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{n_k}}^*.$$

Insbesondere, $\mathbb{Z}_n^*$ ist genau dann zyklisch, wenn

$$n \in \left\{2, 4, p^k, 2 \cdot p^k \;\middle|\; 2 \neq p \in \mathbb{P}, k \in \mathbb{Z}_{>0}\right\}.$$

Es existieren also nur für diese n Primitivwurzeln modulo n, und es gibt jeweils genau $\varphi\big(\varphi(n)\big)$ Primitivwurzeln, die modulo n paarweise nicht kongruent zueinander sind.

Beweis: Aus Satz 3.12 folgt

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{n_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{n_k}}^*$$

mit Induktion nach k. Wegen Proposition 5.11 ist $\mathbb{Z}_n^*$ genau dann zyklisch, wenn die $\mathbb{Z}_{p_i^{n_i}}^*$ alle zyklisch und von paarweise teilerfremder Ordnung sind.

Wegen $|\mathbb{Z}_2^*| = 1$ und wegen der Sätze 5.17 und 5.19 ist $\mathbb{Z}_n^*$ für $n \in \{2, 4, p^k, 2 \cdot p^k \mid p \in \mathbb{P}, k \in \mathbb{Z}_{>0}\}$ mithin zyklisch.

Nehmen wir nun an, daß $\mathbb{Z}_n^*$ zyklisch ist. Falls eines der p_i ungerade ist, dann teilt $p_i - 1$ die Ordnung von $\mathbb{Z}_{p_i^{n_i}}^*$, so daß diese gerade ist. Mithin können keine zwei ungeraden Primteiler in n vorkommen. Da zudem $\mathbb{Z}_{2^k}^*$ nur für $k = 1$ ungerade Ordnung hat und nur für $k \leq 2$ zyklisch ist, muß notwendig

$$n \in \{2, 4, p^k, 2 \cdot p^k \mid p \in \mathbb{P}, k \in \mathbb{Z}_{>0}\}$$

gelten.

Daß es für die angegebenen n jeweils $\varphi(\varphi(n))$ Primitivwurzeln gibt, die paarweise modulo n nicht kongruent zueinander sind, folgt aus Proposition 5.7, da es $\varphi\big(\varphi(n)\big)$ Elemente der Ordnung $\varphi(n)$ in $\mathbb{Z}_n^*$ gibt. □

Die folgende Aufgabe gibt einen Hinweis darauf, wie man Primitivwurzeln modulo $2 \cdot p^k$ finden kann.

Aufgabe 5.25
Es sei $2 \neq p \in \mathbb{P}$, $k \in \mathbb{Z}_{>0}$ und $a \in \mathbb{Z}$ eine Primitivwurzel modulo p^k.

a. Ist a ungerade, so ist a eine Primitivwurzel modulo $2 \cdot p^k$.

b. Ist a gerade, so ist $a + p^k$ eine Primitivwurzel modulo $2 \cdot p^k$.

Aufgabe 5.26

a. Bestimme eine Primitivwurzel modulo $n = 98$.

b. Zeige, daß 2 eine Primitivwurzel modulo $n = 2197$ ist.

6 Das Quadratische Reziprozitätsgesetz

In den Kapiteln 2 und 4 haben wir die Lösbarkeit *linearer Kongruenzgleichungen* der Form

$$a \cdot x + b \equiv 0 \pmod{n} \tag{29}$$

bei gegebenen $a, b \in \mathbb{Z}$, $a \neq 0$, und $n \in \mathbb{Z}_{>0}$ betrachtet. Da Gleichung (29) äquivalent ist zu

$$a \cdot x \equiv -b \pmod{n},$$

ist (29) genau dann lösbar, wenn

$$\mathrm{ggt}(a, n) \mid b.$$

Die Lösung erhalten wir entweder mit Hilfe des Euklidischen Algorithmus (siehe Bemerkungen 2.3 und 2.6) oder durch Anwenden des Satzes von Euler (siehe Bemerkung 4.3).

In diesem Abschnitt wollen wir uns mit *quadratischen Kongruenzgleichungen* in einer Veränderlichen beschäftigen, d.h. mit Gleichungen der Form

$$a \cdot x^2 + b \cdot x + c \equiv 0 \pmod{n} \tag{30}$$

bei gegebenen $a, b, c \in \mathbb{Z}$, $a \neq 0$, und $n \in \mathbb{Z}_{>0}$. Da $4a$ ungleich Null ist, löst x die Gleichung (30) genau dann, wenn x die Gleichung

$$(2a \cdot x + b)^2 + (4ac - b^2) = 4a^2 \cdot x^2 + 4ab \cdot x + 4ac \equiv 0 \pmod{4an} \tag{31}$$

löst. Setzen wir $y = 2ax + b$, $d = b^2 - 4ac$ und $m = 4an$, dann hat (31) die Form[1]

$$y^2 \equiv d \pmod{m}. \tag{32}$$

Gelingt es uns, eine Lösung $y \in \mathbb{Z}$ für (32) zu finden, dann reduziert sich die Lösbarkeit von (30) damit auf die Lösbarkeit der *linearen Kongruenz*

$$2a \cdot x \equiv y - b \pmod{m},$$

d.h. auf die Frage, ob

$$2a = \mathrm{ggt}(2a, m) \mid y - b.$$

Es reicht also, sich für die Frage der Lösbarkeit allgemeiner quadratischer Kongruenzgleichungen mit Gleichungen der Form (32) auseinanderzusetzen.

Der *Chinesische Restsatz* erlaubt es, die Gleichung (32) auf den Fall zu reduzieren, daß m eine *Primzahlpotenz* ist. Hat nämlich m die Primfaktorzerlegung

$$m = p_1^{n_1} \cdots p_k^{n_k},$$

[1]Anmerkung: d ist die *Diskriminante* des Polynoms $ax^2 + bx + c$, und diese ist genau dann Null, wenn das Polynom über den komplexen Zahlen eine doppelte Nullstelle hat. Ist sie größer als Null, kann man über den reellen Zahlen die Lösung von $ax^2 + bx + c = 0$ als $x = \frac{-b \pm \sqrt{d}}{2a}$ angeben. In $\mathbb{Z}_m$ ist das Teilen durch $2a$ sowie das Ziehen von Quadratwurzeln jedoch im allgemeinen nicht zulässig. Die Frage, wann wir in $\mathbb{Z}_m$ durch $2a$ teilen können, haben wir bereits gelöst, und dieses Kapitel beschäftigt sich nun mit der Frage, wann eine Zahl d eine Quadratwurzel in $\mathbb{Z}_m$ besitzt.

so liefert der Isomorphismus

$$\alpha : \mathbb{Z}_m \longrightarrow \mathbb{Z}_{p_1^{n_1}} \times \ldots \times \mathbb{Z}_{p_k^{n_k}} : \overline{z}_m \mapsto \left(\overline{z}_{p_1^{n_1}}, \ldots, \overline{z}_{p_k^{n_k}}\right)$$

des *Chinesischen Restsatzes*, daß es genau dann ein $y \in \mathbb{Z}$ mit

$$y^2 \equiv d \pmod{m}$$

gibt, wenn $y_1, \ldots, y_k \in \mathbb{Z}$ mit

$$y_i^2 \equiv d \left(\mathrm{mod}\ p_i^{n_i}\right)$$

für $i = 1, \ldots, k$ existieren. Denn aus der Existenz von y folgt mit $y_i = y$ die Gleichung

$$\left(\overline{d}_{p_1^{n_1}}, \ldots, \overline{d}_{p_k^{n_k}}\right) = \alpha\left(\overline{d}_m\right) = \alpha\left(\overline{y}_m^2\right) = \left(\overline{y_1}^2_{p_1^{n_1}}, \ldots, \overline{y_k}^2_{p_k^{n_k}}\right),$$

und umgekehrt folgt aus der Existenz von $y_1, \ldots, y_k$ für das Urbild $\overline{y}_m$ von $(\overline{y_1}_{p_1^{n_1}}, \ldots, \overline{y_k}_{p_k^{n_k}})$ unter α unmittelbar

$$\alpha\left(\overline{y}_m^2\right) = \left(\overline{y_1}^2_{p_1^{n_1}}, \ldots, \overline{y_k}^2_{p_k^{n_k}}\right) = \left(\overline{d}_{p_1^{n_1}}, \ldots, \overline{d}_{p_k^{n_k}}\right) = \alpha\left(\overline{d}_m\right),$$

so daß die Bijektivität von α uns $y^2 \equiv d \pmod{m}$ liefert.

Wir haben die Eingangsfrage der Lösbarkeit einer *allgemeinen quadratischen Kongruenzgleichung* in einer Veränderlichen (30) nun im wesentlichen reduziert auf die Betrachtung der Lösbarkeit einer quadratischer Gleichungen der Form

$$x^2 \equiv a \left(\mathrm{mod}\ p^k\right) \tag{33}$$

für eine ganze Zahl $a \in \mathbb{Z}$, $p \in \mathbb{P}$ eine Primzahl und $k \in \mathbb{Z}_{>0}$.

Die folgende Aufgabe zeigt, daß es dabei reicht, den Fall $\mathrm{ggt}(a, p) = 1$ in den Griff zu bekommen.

Aufgabe 6.1
Es sei $p \in \mathbb{P}$ eine Primzahl, $k \in \mathbb{Z}_{>0}$ und $a = p^m \cdot b \in \mathbb{Z}$ mit $\mathrm{ggt}(b, p) = 1$.

a. Ist $m \geq k$, so hat die Gleichung $x^2 \equiv a \pmod{p^k}$ eine Lösung in $\mathbb{Z}$.
b. Ist $0 \leq m < k$, so sind die folgenden Aussagen gleichwertig:
   (i) $x^2 \equiv a \pmod{p^k}$ hat eine Lösung in $\mathbb{Z}$.
   (ii) m ist gerade und die Gleichung $y^2 \equiv b \pmod{p^{k-m}}$ ist in $\mathbb{Z}$ lösbar.

Im weiteren Verlauf des Kapitels beschränken wir uns deshalb auf die Frage nach der Lösbarkeit von (33) im Fall, daß die Primzahl p *kein* Teiler von a ist. Dies führt zu folgender Definition, bei der die Bedingung $\mathrm{ggt}(a, n) = 1$ für $n = p^k$ genau der Bedingung $p \not| a$ entspricht.

Definition 6.2
Es sei $n \in \mathbb{Z}_{>0}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggt}(a, n) = 1$. Die Zahl a heißt *quadratischer Rest modulo* n, falls die Gleichung

$$x^2 \equiv a \pmod{n}$$

eine Lösung $x \in \mathbb{Z}$ besitzt. Andernfalls heißt a ein *quadratischer Nichtrest modulo* n. Wir bezeichnen mit

$$\mathrm{QR}_n = \left\{\overline{a}_n \in \mathbb{Z}_n^* \;\middle|\; a \text{ ist quadratischer Rest modulo } n\right\} = \left\{\overline{x}^2 \;\middle|\; \overline{x} \in \mathbb{Z}_n^*\right\}$$

die *Menge der Quadrate* in $\mathbb{Z}_n^*$ und mit

$$\mathrm{QNR}_n = \left\{\overline{a}_n \in \mathbb{Z}_n^* \;\middle|\; a \text{ ist quadratischer Nichtrest modulo } n\right\}$$

die *Menge der Nichtquadrate* in $\mathbb{Z}_n^*$.

Bemerkung 6.3
Man beachte, daß aufgrund der Definition die Restklasse jedes quadratischen Restes bzw. Nichtrestes a modulo n in $\mathbb{Z}_n$ eine Einheit ist, da $\mathrm{ggt}(a, n) = 1$ vorausgesetzt wird, und daß

$$\mathrm{QNR}_n = \mathbb{Z}_n^* \setminus \mathrm{QR}_n\,.$$

Zudem ist Gleichung (33) *für den Fall* $\mathrm{ggt}(a, p) = 1$ *genau dann lösbar, wenn* a *ein quadratischer Rest modulo* p^k *ist.*

Die Primzahl 2 spielt wie so oft eine gesonderte Rolle, die jedoch einen vergleichsweise einfachen Zugang erlaubt. Die Lösbarkeit von (33) für den Fall $p = 2$ und $\mathrm{ggt}(a, p) = 1$ wird durch die folgende Aufgabe vollständig beantwortet.

Aufgabe 6.4

a. a ist genau dann quadratischer Rest modulo 2, wenn a ungerade ist.

b. a ist genau dann quadratischer Rest modulo 4, wenn $a \equiv 1 \pmod 4$.

c. Für $a \in \mathbb{Z}$ sind die folgenden Aussagen gleichwertig:
   (i) a ist ein quadratischer Rest modulo 2^k für alle $k \geq 3$.
   (ii) a ist ein quadratischer Rest modulo 8.
   (iii) $a \equiv 1 \pmod 8$.

Da die Lösbarkeit von (33) für die Primzahl 2 durch die Aufgaben 6.1 und 6.4 vollständig gelöst ist, können wir uns von jetzt an auf die Betrachtung *ungerader* Primzahlen beschränken. Der folgende Satz gibt Kriterien, die es erlauben, die Lösbarkeit von (33) für ungerade Primzahlen zu entscheiden. Allerdings sind diese Kriterien weit weniger explizit als die Kriterien in Aufgabe 6.4.

Satz 6.5 (Primitivwurzelkriterium)
Es sei $p \in \mathbb{P}$ *eine ungerade Primzahl,* $a \in \mathbb{Z}$ *mit* $\mathrm{ggt}(a, p) = 1$ *und* $k \in \mathbb{Z}_{>0}$.

a. *Die folgenden Aussagen sind gleichwertig:*
   (i) a *ist quadratischer Rest modulo* p^k*, d.h.* $\overline{a}_{p^k} \in \mathrm{QR}_{p^k}$.
   (ii) *Für jede Primitivwurzel* b *modulo* p^k *gibt es ein* $m \in \mathbb{Z}$*, so daß* $\overline{a}_{p^k} = \overline{b}_{p^k}^{2m}$.
   (iii) *Es gibt eine Primitivwurzel* b *modulo* p^k *und ein* $m \in \mathbb{Z}$*, so daß* $\overline{a}_{p^k} = \overline{b}_{p^k}^{2m}$.

(iv) *Die Ordnung von* $\overline{a}_{p^k}$ *in* $\mathbb{Z}_{p^k}^*$ *teilt* $\frac{p-1}{2} \cdot p^{k-1}$*, d.h.*

$$a^{\frac{(p-1)\cdot p^{k-1}}{2}} \equiv 1 \left(\text{mod } p^k\right).$$

Insbesondere gilt für jede Primitivwurzel b *modulo* p^k

$$\mathrm{QR}_{p^k} = \left\{ \overline{b}^{2m} \;\middle|\; 1 \le m \le \frac{p-1}{2} \cdot p^{k-1} \right\}.$$

b. a *ist genau dann ein quadratischer Rest modulo* p^k*, wenn* a *ein quadratischer Rest modulo* p *ist.*

Beweis: a. **(i)⇒(ii):** Ist a ein quadratischer Rest modulo p^k, so gibt es ein $x \in \mathbb{Z}$ mit

$$\overline{x}^2 = \overline{a} \in \mathbb{Z}_{p^k}^*,$$

und ist b eine Primitivwurzel modulo p^k, so gibt es ein $m \in \mathbb{Z}$ mit

$$\overline{x} = \overline{b}^m \in \mathbb{Z}_{p^k}^*.$$

Damit gilt

$$\overline{a} = \overline{x}^2 = \overline{b}^{2m}.$$

(ii)⇒(iii): Dies gilt offenbar, da p ungerade ist und es nach Satz 5.19 Primitivwurzeln modulo p^k gibt.

(iii)⇒(iv): Ist b eine Primitivwurzel modulo p^k und $\overline{a} = \overline{b}^{2m}$, so gilt

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

Für die letzte Gleichung beachten wir, daß $\varphi(p^k) = (p-1)\cdot p^{k-1}$ die Ordnung der Gruppe $\mathbb{Z}_{p^k}^*$ ist.

(iv)⇒(i): Es sei $n = (p-1)\cdot p^{k-1} = \varphi(p^k)$. Nach Voraussetzung ist $o(\overline{a})$ ein Teiler von $\frac{p-1}{2} \cdot p^{k-1} = \frac{n}{2}$, so daß es eine ganze Zahl $c \in \mathbb{Z}$ gibt mit

$$n = 2 \cdot c \cdot o\left(\overline{a}\right).$$

Da p ungerade ist, gibt es eine Primitivwurzel b modulo p^k und ein $l \in \mathbb{Z}$, so daß

$$\overline{a} = \overline{b}^l \in \mathbb{Z}_{p^k}^*.$$

Aus Lemma 5.3 folgt

$$\mathrm{ggt}(n, l) = \frac{n}{o(\overline{a})} = 2 \cdot c,$$

so daß l eine gerade Zahl ist, d.h. $l = 2 \cdot m$ für ein $m \in \mathbb{Z}$. Damit gilt dann für $x = b^m$

$$x^2 = b^{2m} = b^l \equiv a \left(\text{mod } p^k\right),$$

und a ist ein quadratischer Rest modulo p^k.

b. Ist a ein quadratischer Rest modulo p^k, so gibt es $x, c \in \mathbb{Z}$ mit

$$a = x^2 + c \cdot p^k \equiv x^2 \pmod{p},$$

so daß a auch ein quadratischer Rest modulo p ist.

Ist nun a umgekehrt ein quadratischer Rest modulo p, so ist die Ordnung von $\overline{a}_p$ nach Teil a. ein Teiler von $\frac{p-1}{2}$ und aus Lemma 5.14 folgt dann mit Induktion nach k, daß es ein $1 \leq l \leq k-1$ gibt mit

$$o(\overline{a}_{p^k}) = o(\overline{a}_p) \cdot p^l \mid \frac{p-1}{2} \cdot p^{k-1}.$$

Deshalb ist a nach Teil a. ein quadratischer Rest modulo p^k.

□

Bemerkung 6.6

Teil b. in Satz 6.5 reduziert das reduzierte Eingangsproblem (33) für ungerade Primzahlen p und für Zahlen a mit $\mathrm{ggt}(a, p) = 1$ nochmals, da es nun reicht zu testen, ob a ein quadratischer Rest modulo p ist, um die Antwort zugleich für alle Potenzen von p zu erhalten.

Für große Primzahlen p sind die Kriterien, die der Satz liefert aber nicht praktikabel:

- Primitivwurzeln modulo p zu finden und $\overline{a}_p$ als Potenz einer solchen darzustellen, ist zu aufwendig, da keine guten Algorithmen dafür bekannt sind, und
- $a^{\frac{p-1}{2}}$ modulo p zu bestimmen ist nicht unbedingt leichter.

Qualitativ unterscheiden sich die Kriterien in Teil (iii) und in Teil (iv) wesentlich. Prüft man das Kriterium in Teil (iii) nach und findet eine Primitivwurzel b und den zugehörigen Exponenten m, so hat man eine Lösung $x = b^m$ der Gleichung $x^2 \equiv a \pmod{p}$ gefunden. Prüft man hingegen für Teil (iv) nach, daß

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

so weiß man lediglich, daß die Gleichung $x^2 \equiv a \pmod{p}$ lösbar ist, man hat jedoch keinerlei Hinweis auf eine Lösung.

Wir wollen uns im weiteren Verlauf des Kapitels mit der Frage der *Lösbarkeit* beschäftigen, ohne uns um eine Methode zur Findung einer Lösung zu kümmern. D.h. *wir suchen ein einfaches Verfahren, das es uns erlaubt, zu entscheiden, ob ein gegebenes a ein quadratischer Rest modulo einer ungeraden Primzahl p ist oder nicht.* □

Wieviele Quadrate und Nichtquadrate gibt es modulo einer ungeraden Primzahl?

Satz 6.7

Ist $p \in \mathbb{P}$ eine ungerade Primzahl, so ist die Menge der Quadrate $(\mathrm{QR}_p, \cdot)$ eine Untergruppe von $(\mathbb{Z}_p^*, \cdot)$, und es gibt genau

$$|\,\mathrm{QR}_p\,| = |\,\mathrm{QNR}_p\,| = \frac{\varphi(p)}{2} = \frac{p-1}{2}$$

quadratische Reste modulo p und ebensoviele quadratische Nichtreste.

Beweis: Da die Gruppe $(\mathbb{Z}_p^*, \cdot)$ abelsch ist, ist die Abbildung

$$\alpha : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^* : \overline{x} \mapsto \overline{x}^2$$

ein Gruppenhomomorphismus, dessen Bild $\mathrm{Im}(\alpha)$ die Menge QR_p der Quadrate in $\mathbb{Z}_p^*$ ist. Damit ist QR_p eine Untergruppe von $\mathbb{Z}_p^*$.

Zudem ist $\overline{x}$ genau dann in $\mathrm{Ker}(\alpha)$, wenn $\overline{x}^2 = \overline{1}$, d.h. wenn $\overline{x}$ eine Nullstelle des Polynoms $t^2 - \overline{1} = (t - \overline{1}) \cdot (t + \overline{1})$ ist. Da $\mathbb{Z}_p$ ein Körper ist, hat dieses Polynom nur die Nullstellen $\overline{1}$ und $-\overline{1}$, und diese sind verschieden, da p ungerade ist. Somit gilt

$$|\,\mathrm{Ker}(\alpha)| = \left|\{\overline{1}, -\overline{1}\}\right| = 2,$$

und aus dem Homomorphiesatz

$$|\,\mathrm{QR}_p\,| = |\,\mathrm{Im}(\alpha)| = \frac{|\mathbb{Z}_p^*|}{|\,\mathrm{Ker}(\alpha)|} = \frac{p-1}{2}$$

folgt die Behauptung, da

$$|\,\mathrm{QNR}_p\,| = |\mathbb{Z}_p^*| - |\,\mathrm{QR}_p\,| = \frac{p-1}{2}.$$

□

Wir führen nun das *Legendre-Symbol* ein, das ein nützliches Hilfsmittel bei der Betrachtung quadratischer Reste und Nichtreste ist.

Definition 6.8

Es sei $p \in \mathbb{P}$ eine Primzahl und $a \in \mathbb{Z}$. Wir definieren das *Legendre-Symbol* a *nach* p durch

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{falls } \overline{a}_p \in \mathrm{QR}_p, \\ -1, & \text{falls } \overline{a}_p \in \mathrm{QNR}_p, \\ 0, & \text{falls } p \mid a. \end{cases}$$

Das Legendre-Symbol gibt also an, ob a ein quadratischer Rest modulo p ist oder nicht. Es reicht deshalb, eine effiziente Methode zur Berechnung des Legendre-Symbols finden.

Beispiel 6.9

Für $p = 11$ gilt

$$1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16 \equiv 5 \ (\mathrm{mod}\ 11), \quad 5^2 = 25 \equiv 3 \ (\mathrm{mod}\ 11)$$

und $|\,\mathrm{QR}_{11}\,| = \frac{\varphi(11)}{2} = 5$. Mithin ist

$$\mathrm{QR}_{11} = \{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}$$

und für das Legendre-Symbol gilt:

a	0	1	2	3	4	5	6	7	8	9	10
$\left(\frac{a}{11}\right)$	0	1	−1	1	1	1	−1	−1	−1	1	−1

Eines der Kriterien in Satz 6.5 formuliert sich mit Hilfe des Legendre-Symbols wie folgt und geht auf Leonard Euler zurück.

Satz 6.10 (Euler-Kriterium)
Es sei $p \in \mathbb{P}$ *eine ungerade Primzahl und* $a \in \mathbb{Z}$*, dann gilt*

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

Beweis: Ist p ein Teiler von a, so sind beide Seiten der Kongruenzgleichung kongruent zu Null modulo p, so daß wir davon ausgehen können, daß p kein Teiler von a ist.

Nach Definition ist $\left(\frac{a}{p}\right)$ genau dann Eins, wenn a ein quadratischer Rest modulo p ist, und dieses ist nach Satz 6.5 genau dann der Fall, wenn $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ist. Andernfalls ist $\left(\frac{a}{p}\right) = -1$ und

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

da $\overline{a}^{\frac{p-1}{2}}$ nach dem Satz von Euler 4.2 eine der beiden Nullstellen $\overline{1}$ oder $-\overline{1}$ des Polynoms $t^2 - \overline{1} \in \mathbb{Z}_p[t]$ ist und nicht $\overline{1}$ sein kann. □

Bemerkung 6.11
Bei gegebenem $p \in \mathbb{P}$ können wir das Legendre-Symbol als Abbildung

$$\left(\frac{\cdot}{p}\right) : \mathbb{Z} \longrightarrow \mathbb{R} : a \mapsto \left(\frac{a}{p}\right) \tag{34}$$

auffassen. Schränken wir sie auf $\mathbb{Z}_{>0}$ ein, so ist sie für ungerade p eine multiplikative zahlentheoretische Funktion im Sinne von Definition 3.1, wie wir in der folgenden Proposition zeigen. □

Wir wollen einige elementare Eigenschaften des Legendre-Symbols herleiten.

Korollar 6.12
Es seien $p \in \mathbb{P}$ *und* $a, b \in \mathbb{Z}$*. Dann gelten*

a. *Falls* $a \equiv b \pmod{p}$*, so ist* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

b. *Falls* $\mathrm{ggt}(a, p) = 1$*, so ist* $\left(\frac{a^2}{p}\right) = 1$.

c. *Ist* p *eine ungerade Primzahl, so gilt*

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Insbesondere ist die Funktion

$$(\mathbb{Z}_p^*, \cdot) \longrightarrow (\{1, -1\}, \cdot) : \overline{a}_p \mapsto \left(\frac{a}{p}\right)$$

ein Gruppenhomomorphismus, dessen Kern QR_p *ist.*

d. *Hat* a *die Primfaktorzerlegung* $a = p_1^{n_1} \cdots p_k^{n_k}$ *und ist* $p \in \mathbb{P}$ *eine ungerade Primzahl mit* $\mathrm{ggt}(a, p) = 1$*, so ist*

$$\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right)^{n_1} \cdots \left(\frac{p_k}{p}\right)^{n_k}.$$

Beweis: Teil a. ist klar, da das Legendre-Symbol von a nach p nach Definition nur von der Klasse $\overline{a} \in \mathbb{Z}_p$ abhängt, und Teil b. ist ebenfalls klar, da a^2 ein quadratischer Rest modulo p ist, sobald p kein Teiler von a ist.

Aus dem Euler-Kriterium 6.10 folgt

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

und da p eine ungerade Primzahl ist, so daß $1 \not\equiv -1 \pmod{p}$, folgt

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Damit ist die Multiplikativität in Teil c. gezeigt. Man beachte auch, daß die Abbildung

$$(\mathbb{Z}_p^*, \cdot) \longrightarrow \big(\{1, -1\}, \cdot\big) : \overline{a}_p \mapsto \left(\frac{a}{p}\right)$$

wegen Teil a. wohldefiniert ist und wegen der Multiplikativität ein Gruppenhomomorphismus ist, dessen Kern nach Definition des Legendre-Symbols genau die Quadrate in $\mathbb{Z}_p^*$ sind. Teil d. folgt aus Teil c. mittels Induktion. □

Bemerkung 6.13
Jede Gruppe mit zwei Elementen ist isomorph zur Gruppe $(\{1, -1\}, \cdot)$, wobei das neutrale Element auf 1 abgebildet werden muß. Da QR_p eine Untergruppe von $\mathbb{Z}_p^*$ vom Index $\frac{|\mathbb{Z}_p^*|}{|\mathrm{QR}_p|} = 2$ ist, hat die Faktorgruppe $\mathbb{Z}_p^*/\,\mathrm{QR}_p$ genau zwei Elemente und die Abbildung

$$\alpha : \mathbb{Z}_p^*/\,\mathrm{QR}_p \longrightarrow \{1, -1\} : \overline{a} \cdot \mathrm{QR}_p \mapsto \begin{cases} 1, & \text{falls } \overline{a} \in \mathrm{QR}_p, \\ -1, & \text{falls } \overline{a} \notin \mathrm{QR}_p, \text{ d.h. } \overline{a} \in \mathrm{QNR}_p, \end{cases}$$

ist ein Gruppenisomorphismus. Verknüpfen wir α mit der Restklassenabbildung

$$\nu : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^*/\,\mathrm{QR}_p : \overline{a} \mapsto \overline{a} \cdot \mathrm{QR}_p,$$

die ihrerseits ein Gruppenhomomorphismus ist, so erhalten wir wieder einen Gruppenhomomorphismus

$$\alpha \circ \nu : \mathbb{Z}_p^* \longrightarrow \mathrm{QR}_p : \overline{a} \mapsto \left(\frac{a}{p}\right).$$

Dies ist ein konzeptionellerer Beweis für die Aussage in Teil c. von Korollar 6.12 in dem Fall, daß p weder a noch b teilt. □

Indem wir für ungerade Primzahlen den Term $(-1)^{\frac{p-1}{2}}$ betrachten, erhalten wir aus dem Euler-Kriterium den *Ersten Ergänzungssatz zum Quadratischen Reziprozitätsgesetz*, welcher uns das Legendre-Symbol zu -1 berechnet.

Korollar 6.14 (Erster Ergänzungsatz zum Quadratischen Reziprozitätsgesetz)
Ist $p \in \mathbb{P}$, so gilt

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \textit{falls } p \equiv 1 \pmod 4 \textit{ oder } p = 2, \\ -1, & \textit{falls } p \equiv 3 \pmod 4. \end{cases}$$

Bemerkung 6.15
Alternativ hätte man das Korollar auch aus dem Satz von Fermat 4.13 ableiten können, der besagt, daß das Polynom $t^2 + \overline{1} \in \mathbb{Z}_p[t]$ genau dann eine Nullstelle in $\mathbb{Z}_p$ besitzt, wenn $p \equiv 1 \pmod 4$ ist. Daß $t^2 + \overline{1} \in \mathbb{Z}_p[t]$ eine Nullstelle in $\mathbb{Z}_p$ besitzt, heißt aber gerade, daß $-\overline{1}$ ein Quadrat in $\mathbb{Z}_p$ ist, daß also -1 ein Quadratischer Rest modulo p ist.

Das letzte Argument zeigt, daß man umgekehrt auch Korollar 6.14 verwenden kann, um einen alternativen Beweis für die Äquivalenz von Teil b. und c. im Satz von Fermat 4.13 zu geben. □

Wir suchen nach wie vor eine bessere Möglichkeit, Legendre-Symbole berechnen zu können.

Bisher haben wir in aller Regel die Zahlen $1, 2, \ldots, p-1$ als Vertretersystem für die Restklassen in $\mathbb{Z}_p^*$ betrachtet. Für die folgenden Überlegungen ist es aber besser, die Vertreter symmetrisch verteilt um den Nullpunkt zu wählen.

Definition 6.16
Es sei $p \in \mathbb{P}$ eine ungerade Primzahl und $k = \frac{p-1}{2}$. Wir bezeichnen die Menge

$$\mathrm{MR}_p = \{-k, -k+1, \ldots, -1, 1, 2, \ldots, k\} = \{\pm r \mid 1 \leq r \leq k\}.$$

als Menge der *Minimalreste modulo* p. Sie ist ein Vertretersystem von $\mathbb{Z}_p^*$, d.h. jedes Element von $\mathbb{Z}_p^*$ ist Restklasse genau eines Elementes in MR_p.

Ist $a \in \mathbb{Z}$ mit $\mathrm{ggt}(a, p) = 1$ und ist $1 \leq n \leq \frac{p-1}{2}$, so gibt es genau ein $r_{a,n} \in \mathrm{MR}_p$ mit

$$n \cdot a \equiv r_{a,n} \pmod p,$$

und wir setzen

$$\varepsilon_{a,n} = \mathrm{sign}(r_{a,n}) = \begin{cases} 1, & \text{falls } r_{a,n} > 0, \\ -1, & \text{falls } r_{a,n} < 0 \end{cases}$$

sowie

$$\nu_{a,p} = \left| \left\{ n \;\middle|\; \varepsilon_{a,n} = -1, n = 1, \ldots, \frac{p-1}{2} \right\} \right|.$$

□

Beispiel 6.17
Wir betrachten $p = 11$ und $a = 3$.

$$\mathrm{MR}_{11} = \{-5, -4, -3, -2, -1, 1, 2, 3, 4, 5\}$$

ist die Menge der Minimalreste modulo 11, und es gilt:

$$\begin{array}{rclclcl} 1 \cdot 3 & \equiv & 3 \pmod{11} & \Longrightarrow & r_{3,1} = 3 & \Longrightarrow & \varepsilon_{3,1} = 1 \\ 2 \cdot 3 & \equiv & -5 \pmod{11} & \Longrightarrow & r_{3,2} = -5 & \Longrightarrow & \varepsilon_{3,2} = -1 \\ 3 \cdot 3 & \equiv & -2 \pmod{11} & \Longrightarrow & r_{3,3} = -2 & \Longrightarrow & \varepsilon_{3,3} = -1 \\ 4 \cdot 3 & \equiv & 1 \pmod{11} & \Longrightarrow & r_{3,4} = 1 & \Longrightarrow & \varepsilon_{3,4} = 1 \\ 5 \cdot 3 & \equiv & 4 \pmod{11} & \Longrightarrow & r_{3,5} = 4 & \Longrightarrow & \varepsilon_{3,5} = 1 \end{array}$$

Insbesondere gilt damit $\nu_{3,11} = 2$. □

Mit obiger Notation können wir folgende Formel von Gauß zur Berechnung des Legendre-Symbols formulieren.

Satz 6.18 (Lemma von Gauß)
Ist $p \in \mathbb{P}$ *eine ungerade Primzahl und* $a \in \mathbb{Z}$ *mit* $\mathrm{ggt}(a, p) = 1$*, so gilt*

$$\left(\frac{a}{p}\right) = \varepsilon_{a,1} \cdot \varepsilon_{a,2} \cdots \varepsilon_{a,\frac{p-1}{2}} = (-1)^{\nu_{a,p}}.$$

Beweis: Es sei $k = \frac{p-1}{2}$.

Wir beachten zunächst, daß $-n \cdot a \equiv -r_{a,n} \pmod p$ und daß die Abbildung

$$\mu_a : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^* : \overline{n} \mapsto \overline{n} \cdot \overline{a} = \overline{na}$$

bijektiv ist, da $\overline{a}$ in $\mathbb{Z}_p$ invertierbar ist. Das Bild von μ_a ist

$$\begin{aligned} \mathbb{Z}_p^* = \mathrm{Im}(\mu_a) &= \{\overline{a \cdot r} \mid r \in \mathrm{MR}_p\} \\ &= \left\{\overline{a \cdot n}, -\overline{a \cdot n} \;\middle|\; 1 \le n \le k\right\} \\ &= \left\{\overline{r_{a,n}}, -\overline{r_{a,n}} \;\middle|\; 1 \le n \le k\right\}. \end{aligned}$$

Da die Menge $p - 1$ Elemente enthalten muß, muß notwendigerweise

$$\{-r_{a,n}, r_{a,n} \mid 1 \le n \le k\} = \mathrm{MR}_p = \{-k, \ldots, -1, 1, \ldots, k\}$$

gelten. Das ist aber nur möglich, wenn

$$\left\{|r_{a,n}| \;\middle|\; 1 \le n \le k\right\} = \{1, 2, \ldots, k\}$$

gilt, und damit erhalten wir

$$k! = 1 \cdot 2 \cdots (k-1) \cdot k = \prod_{n=1}^{k} |r_{a,n}|.$$

Modulo p impliziert diese Gleichung

$$k! \cdot a^k = \prod_{n=1}^{k} na \equiv \prod_{n=1}^{k} r_{a,n} = \prod_{n=1}^{k} |r_{a,n}| \cdot \prod_{n=1}^{k} \varepsilon_{a,n} = k! \cdot \prod_{n=1}^{k} \varepsilon_{a,n}.$$

Da p kein Teiler von $k!$ ist, ist $k!$ invertierbar modulo p, und wir erhalten modulo p

$$a^k \equiv \prod_{n=1}^{k} \varepsilon_{a,n} \pmod p.$$

Aus dem Euler-Kriterium folgt deshalb

$$\left(\frac{a}{p}\right) = \prod_{n=1}^{k} \varepsilon_{a,n} = (-1)^{\nu_{a,p}},$$

da $1 \not\equiv -1 \pmod p$. □

Beispiel 6.19
Aus Beispiel 6.17 erhalten wir mit Hilfe des Lemmas von Gauß, daß

$$\left(\frac{3}{11}\right) = \varepsilon_{3,1} \cdot \varepsilon_{3,2} \cdot \varepsilon_{3,3} \cdot \varepsilon_{3,4} \cdot \varepsilon_{3,5} = (-1)^2 = 1.$$

3 ist also ein quadratischer Rest modulo 11, was wir in Beispiel 6.9 bereits gesehen haben.

Korollar 6.20 (Zweiter Ergänzungsatz zum Quadratischen Reziprozitätsgesetz)
Ist $p \in \mathbb{P}$ eine ungerade Primzahl, so gilt

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

Beweis: Der Beweis ist dem Leser als Übungsaufgabe überlassen.

□

Mit Hilfe des Lemmas von Gauß können wir eine weitere Formel für die Berechnung des Legendre-Symbols angeben, die uns schließlich den Beweis des zentralen Ergebnisses dieses Kapitels, des Quadratischen Reziprozitätsgesetzes, erlaubt. Dazu benötigen wir folgende Notation.

Definition 6.21
Für eine reelle Zahl $r \in \mathbb{R}$ definieren wir den *ganzen Anteil* oder die *Abrundung* von r als

$$\lfloor r \rfloor = \max\{z \in \mathbb{Z} \mid z \leq r\} \in \mathbb{Z}.$$

Ist $p \in \mathbb{P}$ eine ungerade Primzahl und $a \in \mathbb{Z}$, so setzen wir

$$S_{a,p} = \sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{an}{p} \right\rfloor .$$

Im Beweis des folgenden Lemmas verwenden wir die offensichtliche Beziehung

$$\lfloor z + r \rfloor = z + \lfloor r \rfloor \tag{35}$$

für $z \in \mathbb{Z}$ und $r \in \mathbb{R}$.

Lemma 6.22
Es sei $p \in \mathbb{P}$ eine ungerade Primzahl und $a \in \mathbb{Z}$ mit $\mathrm{ggt}(a,p) = 1$. *Dann gilt*

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

und falls a ungerade ist, gilt zudem

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

Beweis: Für den ersten Teil der Behauptung reicht es wegen des Lemmas von Gauß 6.18 zu zeigen, daß

$$\varepsilon_{a,n} = (-1)^{\left\lfloor \frac{2an}{p} \right\rfloor}$$

für $n = 1, \ldots, \frac{p-1}{2}$.

Mit Hilfe von (35) sehen wir

$$\left\lfloor \frac{2an}{p} \right\rfloor = \left\lfloor 2 \cdot \left\lfloor \frac{an}{p} \right\rfloor + 2 \cdot \left(\frac{an}{p} - \left\lfloor \frac{an}{p} \right\rfloor \right) \right\rfloor = 2 \cdot \left\lfloor \frac{an}{p} \right\rfloor + \left\lfloor 2 \cdot \left(\frac{an}{p} - \left\lfloor \frac{an}{p} \right\rfloor \right) \right\rfloor.$$

Da der zweite Summand nur die Werte Null und Eins annehmen kann, ist diese Zahl genau dann gerade, wenn der zweite Summand Null ist, d.h. wenn

$$2 \cdot \left(\frac{an}{p} - \left\lfloor \frac{an}{p} \right\rfloor \right) < 1,$$

was gleichwertig ist zu

$$an - p \cdot \left\lfloor \frac{an}{p} \right\rfloor < \frac{p}{2}. \tag{36}$$

Da $an - p \cdot \left\lfloor \frac{an}{p} \right\rfloor$ der Rest von an bei Division mit Rest durch p ist und da $\frac{p}{2}$ keine ganze Zahl ist, ist (36) wiederum gleichwertig zu

$$r_{a,n} > 0,$$

d.h. $\varepsilon_{a,n} = 1$. Der erste Teil der Aussage ist damit gezeigt.

Für den zweiten Teil der Aussage betrachten wir zunächst

$$\begin{aligned} S_{a+p,p} &= \sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{(a+p) \cdot n}{p} \right\rfloor = \sum_{n=1}^{\frac{p-1}{2}} \left(\left\lfloor \frac{an}{p} \right\rfloor + n \right) \\ &= \sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{an}{p} \right\rfloor + \sum_{n=1}^{\frac{p-1}{2}} n = S_{a,p} + \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = S_{a,p} + \frac{p^2-1}{8}. \end{aligned}$$

Da a ungerade ist, ist $a + p$ gerade und $\frac{a+p}{2} \in \mathbb{Z}$. Mit Hilfe der Rechenregeln für das Legendre-Symbol und dem bereits bewiesenen ersten Teil des Lemmas erhalten wir damit:

$$\begin{aligned} \left(\frac{2}{p}\right) \cdot \left(\frac{a}{p}\right) &= \left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4 \cdot \frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right) \cdot \left(\frac{\frac{a+p}{2}}{p}\right) \\ &= \left(\frac{\frac{a+p}{2}}{p}\right) = (-1)^{S_{a+p,p}} = (-1)^{S_{a,p}} \cdot (-1)^{\frac{p^2-1}{8}}. \end{aligned}$$

Aus dem zweiten Ergänzungssatz 6.20 folgt dann

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

$\square$

Nun sind wir endlich in der Lage, das Quadratische Reziprozitätsgesetz zu zeigen. Die Aussage war bereits Euler bekannt, der jedoch keinen Beweis für ihre Korrektheit geben konnte. Legendre gelang es, einige Spezialfälle zu beweisen, bevor schließlich Gauß 1796 einen ersten vollständigen Beweis lieferte. Die Aussage faszinierte Gauß so sehr, daß er im Laufe der Jahre sieben weitere Beweise dafür gab. Nach Gauß haben viele andere Mathematiker weitere Beweise für dieses Gesetz gefunden und die dabei entwickelten Methoden haben die Zahlentheorie wesentlich voran gebracht. Diese Tatsache trägt vielleicht mehr zur Bedeutung des Quadratischen Reziprozitätsgesetztes bei, als die eigentliche Aussage selbst.

Das Quadratische Reziprozitätsgesetz ist im Gegensatz zu den beiden bereits bewiesenen Ergänzungssätzen keine explizite Formel zur Berechnung eines Legendre-Symbols. Vielmehr beschreibt es die Beziehung zwischen den Legendre-Symbolen $\left(\frac{q}{p}\right)$ und $\left(\frac{p}{q}\right)$ für zwei Primzahlen p und q. Allerdings kann man dann unter Zuhilfenahme der Rechenregeln 6.12 ein beliebiges Legendre-Symbol rasch auf bekannte Spezialfälle reduzieren.

Satz 6.23 (Quadratisches Reziprozitätsgesetz)
Es seien $p, q \in \mathbb{P}$ *zwei verschiedene ungerade Primzahlen. Dann gilt*

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

Insbesondere gilt also

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

Beweis: Wenden wir die zweite Formel in Lemma 6.22 auf die beiden Legendre-Symbole $\left(\frac{p}{q}\right)$ und $\left(\frac{q}{p}\right)$ an, so erhalten wir

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{S_{p,q}} \cdot (-1)^{S_{q,p}} = (-1)^{S_{p,q}+S_{q,p}}.$$

Es reicht deshalb,

$$S_{p,q} + S_{q,p} = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

zu zeigen. Dazu betrachten wir die Menge

$$M = \left\{ qn - pm \;\middle|\; 1 \leq n \leq \frac{p-1}{2},\ 1 \leq m \leq \frac{q-1}{2} \right\}.$$

Wir wollen zunächst zeigen, daß M genau $\frac{p-1}{2} \cdot \frac{q-1}{2}$ Elemente enthält.

Sind $1 \leq n, n' \leq \frac{p-1}{2}$ und $1 \leq m, m' \leq \frac{q-1}{2}$ mit $qn - pm = qn' - pm'$, so gilt

$$p \cdot (m' - m) = q \cdot (n' - n)$$

mit

$$0 \leq |m' - m| \leq \frac{q-3}{2} \quad \text{und} \quad 0 \leq |n' - n| \leq \frac{p-3}{2}.$$

Da die Primzahl p kein Teiler von q ist, muß deshalb $n' - n = 0$ gelten und damit

$$n' = n \quad \text{und} \quad m' = m.$$

Wir erhalten daraus, daß

$$|M| = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Das gleiche Argument liefert auch

$$0 \notin M.$$

Wir zerlegen die Menge M nun in ihren negativen und ihren positiven Teil,

$$P = \{z \in M \mid z < 0\} \quad \text{und} \quad Q = \{z \in M \mid z > 0\}.$$

Damit erhalten wir

$$qn - pm \in P \iff n < \frac{pm}{q} \notin \mathbb{Z} \iff 1 \leq n \leq \left\lfloor \frac{pm}{q} \right\rfloor,$$

wobei wir für die letzte Äquivalenz beachten, daß $\frac{pm}{q} \notin \mathbb{Z}$. Wir können P deshalb seinerseits folgendermaßen disjunkt zerlegen:

$$P = \dot{\bigcup_{m=1}^{\frac{q-1}{2}}} \left\{ qn - pm \;\middle|\; 1 \leq n \leq \left\lfloor \frac{pm}{q} \right\rfloor \right\}.$$

Damit gilt dann

$$|P| = \sum_{m=1}^{\frac{q-1}{2}} \left\lfloor \frac{pm}{q} \right\rfloor = S_{p,q},$$

und analog erhält man

$$|Q| = \sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{qn}{p} \right\rfloor = S_{q,p}.$$

Insgesamt haben wir wie gefordert gezeigt, daß

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = |M| = |P| + |Q| = S_{p,q} + S_{q,p}.$$

$\square$

Beispiel 6.24

Ist 62 ein quadratischer Rest modulo 131? Da 131 eine Primzahl ist und 62 die Primfaktorzerlegung $62 = 2 \cdot 31$ hat, gilt

$$\left(\frac{62}{131}\right) = \left(\frac{2}{131}\right) \cdot \left(\frac{31}{131}\right).$$

Aus dem Zweiten Ergänzungssatz zum Quadratischen Reziprozitätsgesetz 6.20 folgt

$$\left(\frac{2}{131}\right) = -1,$$

da $131 = 16 \cdot 8 + 3 \equiv 3 \pmod 8$. Um $\left(\frac{31}{131}\right)$ auszurechnen, wollen wir das Quadratische Reziprozitätsgesetz 6.23 sowie die Rechenregeln 6.12 anwenden. Danach gilt

$$\left(\frac{31}{131}\right) = -\left(\frac{131}{31}\right) = -\left(\frac{7}{31}\right) = \left(\frac{31}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1,$$

wobei wir folgende Kongruenzen ausnutzen: $131 \equiv 3 \pmod 4$, $31 \equiv 3 \pmod 4$, $131 \equiv 7 \pmod{31}$, $7 \equiv 3 \pmod 4$, $31 \equiv 3 \pmod 7$ und $7 \equiv 1 \pmod 3$.

Insgesamt erhalten wir also

$$\left(\frac{62}{131}\right) = (-1) \cdot (-1) = 1,$$

so daß 62 ein quadratischer Rest modulo 131 ist. Insbesondere gibt es also eine ganze Zahl $x \in \mathbb{Z}$ mit

$$x^2 \equiv 62 \pmod{131}.$$

Es ist ein weit schwierigeres Unterfangen, ein solches x zu finden, während es wieder leicht ist, zu überprüfen, daß $x = 18$ und $x = 113$ mögliche Lösungen sind:

$$18^2 = 324 = 2 \cdot 131 + 62 \equiv 62 \pmod{131}$$

und

$$113^2 = 12769 = 97 \cdot 131 + 62 \equiv 62 \pmod{131}.$$

Es sind die beiden einzigen Lösungen zwischen 1 und 131. □

Wir wollen das Kapitel mit einem Beispiel abschließen, in dem wir eine allgemeine quadratische Kongruenzgleichung mit den Eingangsüberlegungen des Kapitels sowie den hier entwickelten Methoden auf Lösbarkeit überprüfen und lösen.

Beispiel 6.25
Ist die Kongruenzgleichung

$$3 \cdot x^2 + x + 4 \equiv 0 \pmod{126} \tag{37}$$

lösbar? Durch quadratische Ergänzung transformieren wir die Gleichung zu

$$y^2 \equiv -47 \pmod{1512} \tag{38}$$

mit $y \equiv 6x + 1 \pmod{1512}$.

Da $m = 1512$ die Primfaktorzerlegung

$$m = 1512 = 2^3 \cdot 3^3 \cdot 7$$

besitzt, wenden wir uns nun also den folgenden drei Kongruenzgleichungen zu:

$$y^2 \equiv -47 \equiv 1 \pmod 8, \tag{39}$$

$$y^2 \equiv -47 \equiv 7 \pmod{27}, \tag{40}$$

und

$$y^2 \equiv -47 \equiv 2 \pmod 7. \tag{41}$$

Gleichung (39) ist nach Aufgabe 6.4 lösbar und offenbar ist $y_1 = 1$ eine Lösung.

Um zu sehen, daß (40) ebenfalls lösbar ist, reicht es wegen Satz 6.5, das Legendre-Symbol $\left(\frac{7}{3}\right)$ zu berechnen, für das gilt

$$\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Damit ist 7 ein quadratischer Rest modulo 3 und mithin modulo 27. Um eine Lösung y_2 von (40) zu bestimmen, müssen wir 7 aber als Potenz einer Primitivwurzel modulo 27 darstellen. Nach Aufgabe 5.21 ist 2 eine Primitivwurzel modulo 27 und man rechnet nach, daß

$$2^{16} = 65536 = 2427 \cdot 27 + 7 \equiv 7 \pmod{27}$$

ist. Damit ist $y_2 = 13 \equiv 256 = 2^8 \pmod{27}$ eine Lösung von (40).

Nach dem Zweiten Ergänzungssatz 6.20 gilt $\left(\frac{2}{7}\right) = 1$, da $7 \equiv -1 \pmod{8}$, und mithin ist (41) lösbar. Außerdem gilt für $y_3 = 3$ offenbar

$$y_3^2 = 9 \equiv 2 \pmod{7}.$$

Wir wollen nun das Tripel $(y_1, y_2, y_3) = (1, 13, 3)$ mittels des Chinesischen Restsatzes von $\mathbb{Z}_8 \times \mathbb{Z}_{27} \times \mathbb{Z}_7$ nach $\mathbb{Z}_{1512}$ liften. Dazu bestimmen wir zunächst die Inversen von $N_1 = 27 \cdot 7 = 189$ modulo $n_1 = 8$, $N_2 = 8 \cdot 7 = 56$ modulo $n_2 = 27$ und $N_3 = 8 \cdot 27 = 216$ modulo $n_3 = 7$. Da in $\mathbb{Z}_8^*$ jedes Element selbstinvers ist, ist

$$x_1 = 5 \equiv 189 \pmod{8}$$

das Inverse zu N_1 modulo n_1. Ferner gilt

$$N_2 = 56 \equiv 2 \pmod{27} \quad \text{und} \quad 2 \cdot 14 = 28 \equiv 1 \pmod{27},$$

so daß $x_2 = 14$ das Inverse von N_2 modulo n_2 ist. Schließlich gilt

$$N_3 = 216 \equiv 6 \pmod{7} \quad \text{und} \quad 6 \cdot 6 = 36 \equiv 1 \pmod{7},$$

so daß N_3 modulo n_3 wieder selbstinvers ist und $x_3 = 6$ als Inverses verwendet werden kann.

Der Chinesische Restsatz liefert dann

$$\begin{aligned} y_1 \cdot x_1 \cdot N_1 + y_2 \cdot x_2 \cdot N_2 + y_3 \cdot x_3 \cdot N_3 &= 1 \cdot 5 \cdot 189 + 13 \cdot 14 \cdot 56 + 3 \cdot 6 \cdot 216 \\ &= 945 + 10192 + 3888 = 15025 \equiv -95 = y \pmod{1512} \end{aligned}$$

als Lösung der Kongruenzgleichung (38)

$$y^2 \equiv -47 \pmod{1512}$$

liefert.

Nun müssen wir uns noch mit der Lösung der linearen Kongruenzgleichung

$$6x + 1 \equiv y = -95 \pmod{1512}$$

befassen. Diese ist gleichwertig zu

$$6x \equiv -96 \pmod{1512}. \tag{42}$$

Wir wissen bereits, daß 6 der größte gemeinsame Teiler von 6 und 1512 ist, und für die Lösbarkeit ist also zu prüfen, ob 6 ein Teiler von -96 ist. Da dies der Fall ist, ist Gleichung (42) lösbar und

$$x = \frac{-96}{6} = -16$$

ist eine Lösung von (42) und damit von (37). Da wir wissen, daß mit x auch $x+k\cdot 126$ für jedes $k \in \mathbb{Z}$ eine Lösung von (37) ist, liefert uns x die Lösung

$$x \equiv 110 \pmod{126}$$

von (37) in $\{0, \ldots, 125\}$. Es ist nicht die einzige Lösung der Gleichung. Zwischen 0 und 125 hat (37) genau die *vier* Lösungen

$$11, \quad 47, \quad 74 \quad \text{und} \quad 110.$$

Man beachte, daß das Polynom

$$\overline{3} \cdot t^2 + t + \overline{4} \in \mathbb{Z}_{126}[t]$$

vom Grad zwei damit mehr als zwei Nullstellen hat. Dies ist möglich, da $\mathbb{Z}_{126}$ Nullteiler enthält (vgl. Lemma 4.15). □

Aufgabe 6.26
Ist die Fermatsche Zahl $F_n = 2^{(2^n)} + 1$ eine Primzahl, so gilt

$$3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}.$$

Aufgabe 6.27

a. Zeige mit Hilfe des Primitivwurzelkriteriums, daß $a = 77$ ein quadratischer Rest modulo $n = 2197$ ist und finde eine Lösung von $x^2 \equiv a \pmod{2197}$.

b. Zeige mit Hilfe des Quadratischen Reziprozitätsgesetzes, daß $a = 77$ ein quadratischer Rest modulo $n = 2197$ ist.

c. Ist 195 ein quadratischer Rest modulo 1901?

Aufgabe 6.28
Es sei $p \in \mathbb{P}$ eine ungerade Primzahl und $a \in \mathbb{Z}_{>0}$ mit $\operatorname{ggt}(a, p) = 1$. Zeige:

a. $\mu_a : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^* : \overline{z} \mapsto \overline{a} \cdot \overline{z}$ ist bijektiv, d.h.

$$\mu_a \in \mathrm{Sym}(\mathbb{Z}_p^*) \cong \mathbb{S}_{p-1}.$$

b. Für das Signum der Permutation μ_a gilt

$$\mathrm{sgn}(\mu_a) = \left(\frac{a}{p}\right).$$

Aufgabe 6.29
Die Menge

$$\{p \in \mathbb{P} \mid p \equiv \pm 1 \pmod{8}\}$$

enthält unendlich viele Elemente.

Aufgabe 6.30

Es sei $p \in \mathbb{P}$ eine ungerade Primzahl und $k, m \in \mathbb{Z}$ mit $\operatorname{ggt}(p, km) = 1$. Falls die diophantische Gleichung

$$x^2 - m \cdot y^2 = k \cdot p$$

eine Lösung hat, dann ist das Legendre-Symbol $\left(\frac{m}{p}\right) = 1$.

7 Quadratische Zahlkörper

Ausgangspunkt für die Betrachtungen dieses Kapitels sollen die diophantischen Gleichungen

$$x^2 - m \cdot y^2 = n$$

für gegebene Zahlen $m, n \in \mathbb{Z}$ sein. Die linke Seite der Gleichung läßt sich über den komplexen Zahlen zerlegen als

$$x^2 - m \cdot y^2 = \left(x - \sqrt{m} \cdot y\right) \cdot \left(x + \sqrt{m} \cdot y\right),$$

wobei

$$\sqrt{m} \in \mathbb{C}$$

eine der beiden Nullstellen des Polynoms

$$t^2 - m \in \mathbb{C}[t]$$

ist, d.h. eine der beiden komplexen Quadratwurzeln aus m. Dies führt uns dazu, Zahlen der Form

$$x + \sqrt{m} \cdot y \quad \text{mit} \quad x, y \in \mathbb{Z}$$

zu betrachten.

Wir wollen im folgenden die Konvention verwenden, daß für eine *positive* Zahl m mit $\sqrt{m}$ die *positive reelle Quadratwurzel* von m bezeichnet wird, und für eine *negative* Zahl m bezeichnet $\sqrt{m}$ die *komplexe Quadratwurzel* von m *in der oberen Halbebene.*

A) **Der Ring der ganzen Zahlen in** $\mathbb{Q}\left[\sqrt{m}\right]$

Bemerkung 7.1
Es sei S ein kommutativer Ring mit Eins und $R \subseteq S$ sei ein Unterring von S. Ist $\omega \in S$ Nullstelle eines Polynoms

$$f = t^n + \alpha_{n-1} \cdot t^{n-1} + \ldots + \alpha_1 \cdot t + \alpha_0 \in R[t],$$

dann wissen wir aus der Vorlesung algebraische Strukturen, daß

$$R[\omega] = \left\{a_0 + a_1 \cdot \omega + \cdots + a_{n-1} \cdot \omega^{n-1} \;\middle|\; a_0, \ldots, a_{n-1} \in R\right\}$$

das Bild des Einsetzhomomorphismus

$$\varphi_\omega : R[t] \longrightarrow S : f \mapsto f(\omega)$$

und damit ein Unterring von S ist.

Korollar 7.2
Es sei $m \in \mathbb{Z}$ *keine Quadratzahl, dann ist*

$$\mathbb{Q}\left[\sqrt{m}\right] = \left\{a + b \cdot \sqrt{m} \;\middle|\; a, b \in \mathbb{Q}\right\}$$

ein Unterkörper von $\mathbb{C}$ *und*

$$\mathbb{Z}\left[\sqrt{m}\right] = \left\{a + b \cdot \sqrt{m} \;\middle|\; a, b \in \mathbb{Z}\right\}$$

ein Unterring von $\mathbb{Q}\big[\sqrt{m}\big]$.

Beweis: $\sqrt{m}$ ist Nullstelle des quadratischen Polynoms

$$t^2 - m \in \mathbb{Z}[t] \subset \mathbb{C}[t]$$

Nach Bemerkung 7.1 ist $\mathbb{Q}\big[\sqrt{m}\big]$ damit ein Unterring von $\mathbb{C}$ und wir müssen nur zeigen, daß das multiplikative Inverse von $0 \neq x = a + b \cdot \sqrt{m} \in \mathbb{Q}\big[\sqrt{m}\big]$ wieder in $\mathbb{Q}\big[\sqrt{m}\big]$ liegt. Da m keine Quadratzahl ist und $(a, b) \neq (0, 0)$, ist $a^2 \neq b^2 \cdot m$ und

$$\frac{1}{x} = \frac{a}{a^2 - b^2 \cdot m} - \frac{b}{a^2 - b^2 \cdot m} \cdot \sqrt{m} \in \mathbb{Q}\big[\sqrt{m}\big].$$

Mithin ist $\mathbb{Q}\big[\sqrt{m}\big]$ ein Unterkörper von $\mathbb{C}$. Damit ist dann $\mathbb{Z}\big[\sqrt{m}\big]$ nach Bemerkung 7.1 seinerseits ein Unterring von $\mathbb{Q}\big[\sqrt{m}\big]$, da

$$t^2 - m \in \mathbb{Z}[t] \subset \mathbb{Q}\big[\sqrt{m}\big][t].$$

□

Definition 7.3
Es ein $m \in \mathbb{Z}$ keine Quadratzahl. Ist $m < 0$, so nennen wir den Körper $\mathbb{Q}\big[\sqrt{m}\big]$ einen *imaginär-quadratischen Zahlkörper*, und ist $m > 0$ so nennen wir ihn einen *reell-quadratischen Zahlkörper*.

Wir wollen in diesem Kapitel die Ringe $\mathbb{Z}\big[\sqrt{m}\big]$ als Unterringe von $\mathbb{Q}\big[\sqrt{m}\big]$ untersuchen. Dabei stellt sich heraus, daß sie nicht immer die erstrebenswerten Eigenschaften besitzen. Falls m eine quadratfreie Zahl mit Rest Eins bei Division durch Vier ist, so sollte man lieber zu einem etwas größeren Unterring von $\mathbb{Q}\big[\sqrt{m}\big]$ wechseln, wie wir in Satz 7.16 sehen werden.

Korollar 7.4
Es sei $1 \neq m \in \mathbb{Z}$ *eine quadratfreie Zahl und*

$$\omega_m = \begin{cases} \sqrt{m}, & \textit{falls } m \equiv 2, 3 \pmod 4, \\ \frac{1+\sqrt{m}}{2}, & \textit{falls } m \equiv 1 \pmod 4. \end{cases}$$

Dann ist

$$\mathbb{Z}[\omega_m] = \big\{a + b \cdot \omega_m \;\big|\; a, b \in \mathbb{Z}\big\}$$

ein Unterring von $\mathbb{Q}\big[\sqrt{m}\big]$*, der* $\mathbb{Z}\big[\sqrt{m}\big]$ *enthält.*

Beweis: Wir können annehmen, daß $m \equiv 1 \pmod 4$ gilt, da die Aussage ansonsten bereits aus Korollar 7.2 folgt. Dann gibt es aber eine ganze Zahl $k \in \mathbb{Z}$, so daß $m = 4 \cdot k + 1$, und deshalb ist

$$\omega_m^2 - \omega_m - k = \frac{1 + 2 \cdot \sqrt{m} + m}{4} - \frac{1 + \sqrt{m}}{2} - k = 0,$$

d.h. $\omega_m \notin \mathbb{Q}$ ist dann Nullstelle des quadratischen Polynoms

$$t^2 - t - k \in \mathbb{Z}[t] \subset \mathbb{Q}[t].$$

Also ist $\mathbb{Z}[\omega_m]$ nach Bemerkung 7.1 ein Unterring von $\mathbb{Q}\left[\sqrt{m}\right]$. Für $a + b \cdot \sqrt{m} \in \mathbb{Z}\left[\sqrt{m}\right]$ mit $a, b \in \mathbb{Z}$ gilt zudem

$$a + b \cdot \sqrt{m} = (a - b) + 2b \cdot \omega_m \in \mathbb{Z}[\omega_m],$$

so daß $\mathbb{Z}[\omega_m]$ den Ring $\mathbb{Z}\left[\sqrt{m}\right]$ enthält. □

Beispiel 7.5

a. Ist $m = -1$, so ist $\sqrt{-1} = i$ die imaginäre Einheit und

$$\mathbb{Z}[i] = \mathbb{Z}\left[\sqrt{-1}\right] = \mathbb{Z}[\omega_{-1}] = \{a + b \cdot i \mid a, b \in \mathbb{Z}\}$$

ist der Ring der *ganzen Gaußschen Zahlen*.

b. Ist $m = 2$, so ist

$$\mathbb{Z}\left[\sqrt{2}\right] = \mathbb{Z}[\omega_2] = \left\{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Z}\right\}.$$

c. Ist $m = 5$, so ist

$$\mathbb{Z}\left[\sqrt{5}\right] = \left\{a + b \cdot \sqrt{5} \mid a, b \in \mathbb{Z}\right\} \subsetneqq \left\{a + b \cdot \frac{1 + \sqrt{5}}{2} \;\middle|\; a, b \in \mathbb{Z}\right\} = \mathbb{Z}[\omega_5].$$

□

Bemerkung 7.6

Ein $\mathbb{Q}$-Vektorraum $(V, +, \cdot)$ mit einer Multiplikation

$$\circ : V \times V \longrightarrow V,$$

so daß $(V, +, \circ)$ ein Ring wird und so daß das verallgemeinerte Assoziativgesetz

$$q \cdot (x \circ y) = (q \cdot x) \circ y$$

für $q \in \mathbb{Q}$ und $x, y \in V$ gilt, heißt eine $\mathbb{Q}$-*Algebra*. Die Dimension als $\mathbb{Q}$-Vektorraum nennt man die Dimension der $\mathbb{Q}$-Algebra, und eine Basis von V als $\mathbb{Q}$-Vektorraum nennt man ein Basis der $\mathbb{Q}$-Algebra. Jeder Körper, der $\mathbb{Q}$ als Unterkörper enthält, ist offenbar eine $\mathbb{Q}$-Algebra.

Wie bei allen algebraischen Strukturen fordert man auch bei *Algebrenhomomorphismen*, daß sie mit der gegebenen Struktur verträglich sind, d.h. sie sollten mit der Addition, der Skalarmultiplikation und der Multiplikation verträglich sein und die Eins auf die Eins abbilden. Ist ein Algebrenhomomorphismus $\varphi : V \longrightarrow V$ bijektiv, so nennt man ihn einen *Algebrenautomorphismus*. □

Bislang haben wir an keiner Stelle verwendet, daß die Zahl m keine Quadratzahl oder gar quadratfrei ist. Dies ist erstmals für die Aussage in folgendem Korollar wichtig und dann für Definition 7.8.

Korollar 7.7

Ist $m \in \mathbb{Z}$ keine Quadratzahl, dann ist $\mathbb{Q}\left[\sqrt{m}\right]$ eine 2-dimensionale $\mathbb{Q}$-Algebra mit Basis

$$\left\{1, \sqrt{m}\right\}.$$

Insbesondere sind die Zahlen a *und* b *in der Darstellung eines Elementes* $a+b\cdot\sqrt{m}$ *in* $\mathbb{Q}\big[\sqrt{m}\big]$, $\mathbb{Z}\big[\sqrt{m}\big]$ *bzw.* $\mathbb{Z}[\omega_m]$ *eindeutig bestimmt.*

Beweis: Nach Bemerkung 7.6 ist $\mathbb{Q}\big[\sqrt{m}\big]$ eine $\mathbb{Q}$-Algebra, da $\mathbb{Q}$ ein Unterkörper von $\mathbb{Q}\big[\sqrt{m}\big]$ ist. Zudem ist $\big\{1,\sqrt{m}\big\}$ offenbar ein Erzeugendensystem von

$$\mathbb{Q}\big[\sqrt{m}\big]=\big\{a\cdot 1+b\cdot\sqrt{m}\;\big|\;a,b\in\mathbb{Q}\big\}$$

als $\mathbb{Q}$-Vektorraum, da jedes Element von $\mathbb{Q}\big[\sqrt{m}\big]$ eine $\mathbb{Q}$-Linearkombination von 1 und $\sqrt{m}$ ist.

Es bleibt zu zeigen, daß diese beiden Zahlen linear unabhängig über $\mathbb{Q}$ sind. Seien dazu $a,b\in\mathbb{Q}$ mit

$$a\cdot 1+b\cdot\sqrt{m}=0.$$

Wäre $b\neq 0$, so wäre

$$\sqrt{m}=-\frac{a}{b}\in\mathbb{Q}$$

im Widerspruch dazu, daß m keine Quadratzahl ist. Also ist $b=0$, und damit auch

$$0=a\cdot 1+b\cdot\sqrt{m}=a.$$

Wir haben also gezeigt, daß 1 und $\sqrt{m}$ linear unabhängig über $\mathbb{Q}$ sind. Als Erzeugendensystem von $\mathbb{Q}\big[\sqrt{m}\big]$ ist $\big\{1,\sqrt{m}\big\}$ damit eine Basis, und $\mathbb{Q}\big[\sqrt{m}\big]$ hat insbesondere die Dimension zwei. □

Wir führen nun auf $\mathbb{Q}\big[\sqrt{m}\big]$ und damit auch auf $\mathbb{Z}\big[\sqrt{m}\big]$ drei Operationen ein, die bei den folgenden Betrachtungen eine wesentliche Rolle spielen werden: die *Konjugation*, die *Spur* und die *Norm*.

Definition 7.8
Es sei $m\in\mathbb{Z}$ keine Quadratzahl.

a. Die Abbildung

$$K:\mathbb{Q}\big[\sqrt{m}\big]\longrightarrow\mathbb{Q}\big[\sqrt{m}\big]:a+b\cdot\sqrt{m}\mapsto a-b\cdot\sqrt{m}$$

heißt die *Konjugation* auf $\mathbb{Q}\big[\sqrt{m}\big]$. Sie ist wohldefiniert, weil die Darstellung eines Elementes in $\mathbb{Q}\big[\sqrt{m}\big]$ als $a+b\cdot\sqrt{m}$ eindeutig ist!

b. Die Abbildung

$$S:\mathbb{Q}\big[\sqrt{m}\big]\longrightarrow\mathbb{Q}:x\mapsto x+K(x)$$

heißt die *Spur* auf $\mathbb{Q}\big[\sqrt{m}\big]$, d.h.

$$S\left(a+b\cdot\sqrt{m}\right)=2\cdot a\in\mathbb{Q}.$$

c. Die Abbildung

$$N:\mathbb{Q}\big[\sqrt{m}\big]\longrightarrow\mathbb{Q}:x\mapsto x\cdot K(x)$$

heißt die *Norm* auf $\mathbb{Q}\big[\sqrt{m}\big]$, d.h.

$$N\left(a+b\cdot\sqrt{m}\right)=a^2-m\cdot b^2\in\mathbb{Q}.$$

d. Für $x \in \mathbb{Q}\left[\sqrt{m}\right]$ nennen wir das Polynom

$$\chi_x = (t - x) \cdot \big(t - K(x)\big) = t^2 - S(x) \cdot t + N(x) \in \mathbb{Q}[t]$$

das *charakteristische Polynom* von a.

Bemerkung 7.9

Ist $m < 0$, so ist die Konjugation genau die komplexe Konjugation, d.h.

$$K(x) = \overline{x},$$

die Spur ist das Doppelte des Realteils, d.h.

$$S(x) = 2 \cdot \mathrm{Re}(x),$$

und die Norm ist dann das Betragsquadrat, d.h.

$$N(x) = |x|^2.$$

Das gilt nicht, wenn $m > 0$ ist, da dann $\mathbb{Q}\left[\sqrt{m}\right] \subset \mathbb{R}$. □

Bemerkung 7.10

Betrachten wir $\mathbb{Q}\left[\sqrt{m}\right]$ als $\mathbb{Q}$-Vektorraum und ist $x = a + b \cdot \sqrt{m} \in \mathbb{Q}\left[\sqrt{m}\right]$, so ist die Abbildung

$$F_x : \mathbb{Q}\left[\sqrt{m}\right] \longrightarrow \mathbb{Q}\left[\sqrt{m}\right] : y \mapsto x \cdot y$$

eine $\mathbb{Q}$-lineare Abbildung. Wir können also die Matrixdarstellung von F_x bezüglich der Basis $B = \left\{1, \sqrt{m}\right\}$ bestimmen:

$$F_x(1) = x \cdot 1 = x = a \cdot 1 + b \cdot \sqrt{m}$$

und

$$F_x\left(\sqrt{m}\right) = x \cdot \sqrt{m} = mb \cdot 1 + a \cdot \sqrt{m}.$$

Wir erhalten als Matrixdarstellung deshalb die Matrix

$$M_B^B(F_x) = \begin{pmatrix} a & mb \\ b & a \end{pmatrix}.$$

Für die Spur und die Determinante der linearen Abbildung F_x, d.h. dieser Matrix, gilt

$$\mathrm{Spur}(F_x) = \mathrm{Spur}\left(M_B^B(F_x)\right) = 2 \cdot a = S(x)$$

und

$$\det(F_x) = \det\left(M_B^B(F_x)\right) = a^2 - m \cdot b^2 = N(x).$$

Außerdem gilt für das charakteristische Polynom χ_A einer 2×2-Matrix A

$$\chi_A = t^2 - \mathrm{Spur}(A) \cdot t + \det(A),$$

so daß wir insbesondere

$$\chi_{F_x} = \chi_{M_B^B(F_x)} = t^2 - S(x) \cdot t + N(x) = \chi_x$$

erhalten. Wir haben in Definition 7.8 also eigentlich keine neuen Begriffe eingeführt, wir haben lediglich Begriffe, die aus der linearen Algebra bekannt sind, neu interpretiert.

Diese Interpretation liefert uns eine wichtige Eigenschaft der Norm frei Haus:

$$N(x) = 0 \quad \Longleftrightarrow \quad x = 0,$$

denn $\mathbb{Q}\left[\sqrt{m}\right]$ ist ein Körper, so daß x genau dann ungleich Null ist, wenn die Multiplikation F_x mit x eine bijektive Abbildung ist, was wiederum gleichwertig dazu ist, daß die Determinante $\det(F_x) = N(x)$ nicht Null ist. Wir geben unten einen alternativen Beweis. □

Die folgenden Eigenschaften der Konjugation, der Spur und der Norm sind einfach zu sehen und für spätere Rechnungen sehr hilfreich.

Proposition 7.11
Es sei $m \in \mathbb{Z}$ *keine Quadratzahl.*

a. K *ist ein selbst-inverser* $\mathbb{Q}$*-Algebrenautomorphismus, d.h.*

$$\begin{array}{rcl} K(x+y) & = & K(x)+K(y), \\ K(x\cdot y) & = & K(x)\cdot K(y), \\ K(a\cdot x) & = & a\cdot K(x), \\ K\big(K(x)\big) & = & x \end{array}$$

für $x, y \in \mathbb{Q}\big[\sqrt{m}\big]$ *und* $a \in \mathbb{Q}$.

b. $\mathbb{Q} = \mathrm{Eig}(K, 1)$ *ist der Eigenraum von* K *zum Eigenwert* 1*, d.h.*

$$K(x) = x \quad\Longleftrightarrow\quad x \in \mathbb{Q}.$$

c. *Die Spur ist eine* $\mathbb{Q}$*-lineare Abbildung.*

d. *Die Norm ist multiplikativ, d.h.* $N(x\cdot y) = N(x)\cdot N(y)$ *für* $x, y \in \mathbb{Q}\big[\sqrt{m}\big]$.

e. *Für* $x \in \mathbb{Q}\big[\sqrt{m}\big]$ *gilt*

$$N(x) = 0 \quad\Longleftrightarrow\quad x = 0.$$

f. $K\big(\mathbb{Z}\big[\sqrt{m}\big]\big) \subseteq \mathbb{Z}\big[\sqrt{m}\big]$ *und* $K\big(\mathbb{Z}[\omega_m]\big) \subseteq \mathbb{Z}[\omega_m]$.

Beweis: a. Die vier Eigenschaften erhält man unmittelbar durch Einsetzen der Definition.

b. Sei $x = a + b\cdot\sqrt{m} \in \mathbb{Q}\big[\sqrt{m}\big]$ gegeben, dann gilt

$$K(x) = x \iff -b\cdot\sqrt{m} = b\cdot\sqrt{m} \iff b = 0 \iff x \in \mathbb{Q},$$

wobei wir für die letzte Äquivalenz ausnutzen, daß $\sqrt{m} \notin \mathbb{Q}$.

c. Dies folgt unmittelbar aus der Definition.

d. Es seien $x, y \in \mathbb{Q}\big[\sqrt{m}\big]$. Dann gilt mit Teil a.

$$N(x\cdot y) = x\cdot y\cdot K(x\cdot y) = x\cdot y\cdot K(x)\cdot K(y) = N(x)\cdot N(y).$$

e. Da $\mathbb{Q}\big[\sqrt{m}\big]$ ein Körper ist, gilt für $x \in \mathbb{Q}\big[\sqrt{m}\big]$

$$x\cdot K(x) = N(x) = 0 \iff (x = 0 \text{ oder } K(x) = 0) \iff x = 0,$$

wobei wir für die letzte Äquivalenz ausnutzen, daß K bijektiv ist.

f. Die Aussage für $\mathbb{Z}\big[\sqrt{m}\big]$ ist offensichtlich, so daß wir nur noch $\mathbb{Z}[\omega_m]$ mit $m \equiv 1 \pmod 4$ betrachten müssen. Ist $x = a + b\cdot\omega_m \in \mathbb{Z}[\omega_m]$, so ist

$$x = \frac{2a+b}{2} + \frac{b}{2}\cdot\sqrt{m}$$

und

$$K(x) = \frac{2a+b}{2} - \frac{b}{2}\cdot\sqrt{m} = (a+b) - b\cdot\omega_m \in \mathbb{Z}[\omega_m].$$

□

Definition 7.12
Eine Zahl $x \in \mathbb{Q}\left[\sqrt{m}\right]$ heißt *ganz* oder *ganz algebraisch* oder *ganz über* $\mathbb{Z}$, falls

$$\chi_x = t^2 - S(x) \cdot t + N(x) \in \mathbb{Z}[t],$$

d.h. falls

$$S(x) \in \mathbb{Z} \quad \text{und} \quad N(x) \in \mathbb{Z}.$$

Beispiel 7.13
Die Zahl $\omega_5 = \frac{1}{2} + \frac{1}{2} \cdot \sqrt{5} \in \mathbb{Q}\left[\sqrt{5}\right]$ ist ganz, da

$$S(\omega_5) = 2 \cdot \frac{1}{2} \in \mathbb{Z} \quad \text{und} \quad N(\omega_5) = \frac{1}{4} - 5 \cdot \frac{1}{4} = -1 \in \mathbb{Z},$$

dagegen ist die Zahl $x = \frac{1}{2} \in \mathbb{Q}\left[\sqrt{5}\right]$ nicht ganz, da

$$N(x) = \frac{1}{4} \notin \mathbb{Z}.$$

Bemerkung 7.14
In der Vorlesung Einführung in die Algebra nennt man eine Zahl $x \in \mathbb{C}$ *algebraisch* über $\mathbb{Q}$, wenn es ein Polynom $0 \neq f \in \mathbb{Q}[t]$ mit Koeffizienten in $\mathbb{Q}$ gibt, so daß x eine Nullstelle von f ist. Die Menge aller Polynome, die x als Nullstelle haben, bilden ein Ideal, und da $\mathbb{Q}[t]$ ein Hauptidealring ist, gibt es genau ein Polynom μ_x mit *Höchstkoeffizient Eins*, das dieses Ideal erzeugt, d.h.

$$\langle \mu_x \rangle_{\mathbb{Q}[t]} = \{f \in \mathbb{Q}[t] \mid f(x) = 0\}.$$

Man nennt μ_x das *Minimalpolynom* von x, und es teilt jedes andere Polynom in $\mathbb{Q}[t]$, das x als Nullstelle hat. Insbesondere ist μ_x also *irreduzibel*.

Ist $x \in \mathbb{Q}\left[\sqrt{m}\right]$ für ein Nicht-Quadrat m, so wissen wir, daß x eine Nullstelle des charakteristischen Polynoms $\chi_x \in \mathbb{Q}[t]$ ist. Die Elemente von $\mathbb{Q}\left[\sqrt{m}\right]$ sind also alle *algebraisch* über $\mathbb{Q}$ und das Minimalpolynom μ_x von x teilt χ_x. Da χ_x Grad Zwei hat, gilt offenbar

$$\chi_x \neq \mu_x \iff \mu_x = t - x \iff x \in \mathbb{Q}. \tag{43}$$

Man möchte mit dem Begriff *ganz algebraisch* die Theorie der algebraischen Elemente vom Körper $\mathbb{Q}$ auf den Ring $\mathbb{Z}$ übertragen. Das führt zu Problemen. Da $\mathbb{Q}$ ein Körper ist, kann man über $\mathbb{Q}$ jedes Polynom durch Multiplikation mit dem Inversen des Höchstkoeffizienten in ein Polynom überführen, welches Höchstkoeffizient Eins hat, ohne die Nullstellen des Polynoms zu verändern. Für Polynome mit ganzzahligen Koeffizienten gilt das nicht mehr. Dividiert man die Koeffizienten, so werden sie im allgemeinen nicht mehr ganzzahlig sein.

Allgemein nennt man eine komplexe Zahl deshalb *ganz* oder *ganz algebraisch* über $\mathbb{Z}$, wenn es ein Polynom $0 \neq f = t^n + a_{n-1} \cdot t^{n-1} + \ldots + a_0 \in \mathbb{Z}[t]$ mit *Höchstkoeffizient Eins* gibt, so daß x eine Nullstelle von f ist. Da wir f als Polynom in $\mathbb{Q}[t]$ auffassen können, ist x dann algebraisch und μ_x teilt f in $\mathbb{Q}[t]$. Andererseits können wir unter den $0 \neq f \in \mathbb{Z}[t]$ mit x als Nullstelle ein f von minimalem Grad wählen. Dann muß f in $\mathbb{Z}[t]$ irreduzibel sein, und ein Ergebnis der Algebra, das als *Lemma von Gauß* bekannt ist (aber nichts mit dem Lemma von Gauß 6.18 zu tun hat), besagt dann, daß f bereits irreduzibel in $\mathbb{Q}[t]$ ist. Da μ_x ein Teiler des irreduziblen Polynoms f ist, müssen diese notwendigerweise *assoziiert* sein, daß heißt sie unterscheiden sich nur um einen Faktor $a \in \mathbb{Q}^*$, und da beide Höchstkoeffizient Eins haben, muß $a = 1$ gelten, d.h. $\mu_x = f \in \mathbb{Z}[t]$. Aus diesem hier nur zitierten Lemma von Gauß folgt also

$$x \in \mathbb{C} \text{ ist ganz über } \mathbb{Z} \iff \mu_x \in \mathbb{Z}[t].$$

Für den Fall $x \in \mathbb{Q}\left[\sqrt{m}\right]$, an dem wir in dieser Vorlesung interessiert sind, folgt dann mit (43)

$$x \in \mathbb{Q}\left[\sqrt{m}\right] \text{ ist } \textit{ganz} \text{ über } \mathbb{Z} \iff \mu_x \in \mathbb{Z}[t] \iff \chi_x \in \mathbb{Z}[t].$$

Dies zeigt, daß unsere Definition 7.12 gleichwertig zu der allgemeineren Definition ist, die nur fordert, daß x Nullstelle *irgendeines* Polynoms in $\mathbb{Z}[t]$ mit Höchstkoeffizient Eins sein soll.

Ziel der Bemerkung war allein diese Erkenntnis, die für unsere Vorlesung eigentlich irrelevant ist. Sie soll dazu dienen, die Ergebnisse in späteren Semestern besser einordnen zu können. □

Bemerkung 7.15
Wir haben bislang meist vorausgesetzt, daß die Zahl m keine Quadratzahl ist. Um die Ringe $\mathbb{Q}\left[\sqrt{m}\right]$ zu untersuchen, kann man sich jedoch auf den Fall zurück ziehen, daß m quadratfrei und ungleich 1 ist. Denn jede ganze Zahl m läßt sich zerlegen als

$$m = k^2 \cdot n$$

mit $k \in \mathbb{Z}$ und n quadratfrei, und ist m keine Quadratzahl, so ist n zudem ungleich Eins. Dann gilt aber offenbar

$$\mathbb{Q}\left[\sqrt{m}\right] = \mathbb{Q}\left[\sqrt{n}\right],$$

da

$$a + b \cdot \sqrt{m} = a + b \cdot k \cdot \sqrt{n}.$$

Wir werden uns im folgenden deshalb meist darauf beschränken, den Fall einer quadratfreien Zahl $m \neq 1$ zu betrachten. Man beachte übrigens, daß die Konjugation, die Norm, die Spur und das charakteristische Polynom eines Elementes nur vom quadratischen Zahlkörper, nicht aber von seiner Darstellung als $\mathbb{Q}\left[\sqrt{m}\right]$ oder $\mathbb{Q}\left[\sqrt{n}\right]$ abhängen!

Satz 7.16
Ist $1 \neq m \in \mathbb{Z}$ *eine quadratfreie ganze Zahl, so ist*

$$\mathbb{Z}[\omega_m] = \left\{x \in \mathbb{Q}\left[\sqrt{m}\right] \;\middle|\; x \textit{ ist ganz}\right\}.$$

Insbesondere ist die Menge der ganzen Zahlen in $\mathbb{Q}\left[\sqrt{m}\right]$ *ein Unterring von* $\mathbb{Q}\left[\sqrt{m}\right]$, *den man auch als* ganzen Abschluß *von* $\mathbb{Z}$ *in* $\mathbb{Q}\left[\sqrt{m}\right]$ *bezeichnet oder als den* Ring der ganzen Zahlen in $\mathbb{Q}\left[\sqrt{m}\right]$.

Beweis: Es sei zunächst $x = a + b \cdot \sqrt{m} \in \mathbb{Q}\left[\sqrt{m}\right]$ ganz. Dann gilt

$$2 \cdot a = S(x) \in \mathbb{Z} \quad \text{und} \quad a^2 - m \cdot b^2 = N(x) \in \mathbb{Z}.$$

Es muß also eine ganze Zahl $c \in \mathbb{Z}$ geben mit

$$a = \frac{c}{2},$$

und da dann $4 \cdot a^2 = c^2 \in \mathbb{Z}$, erhalten wir mit $b = \frac{u}{v} \in \mathbb{Q}$ zudem

$$\frac{4 \cdot m \cdot u^2}{v^2} = 4 \cdot m \cdot b^2 = -4 \cdot \left(a^2 - m \cdot b^2\right) + 4 \cdot a^2 \in \mathbb{Z}.$$

Da m quadratfrei ist, muß jeder Primteiler p von v zugleich ein Teiler von $4 \cdot u^2$ und damit von $2 \cdot u$ sein. Dann teilt p^2 aber $4 \cdot u^2$ und wir können p^2 kürzen. Mit

Induktion nach der Zahl der Primteiler von ν erhalten wir, daß ν ein Teiler von $2 \cdot u$ ist, und es gibt mithin eine ganze Zahl $d = \frac{2 \cdot u}{\nu} \in \mathbb{Z}$, so daß

$$b = \frac{d}{2}.$$

Für die Norm von x erhalten wir also

$$\frac{c^2 - m \cdot d^2}{4} = a^2 - m \cdot b^2 = N(x) \in \mathbb{Z},$$

so daß die ganze Zahl $c^2 - m \cdot d^2$ durch 4 teilbar sein muß, d.h.

$$c^2 - m \cdot d^2 \ \equiv \ 0 \ (\text{mod } 4). \tag{44}$$

Wir schreiben nun

$$c = \gamma + 2 \cdot k \quad \text{und} \quad d = \delta + 2 \cdot l$$

mit $k, l \in \mathbb{Z}$ und $\gamma, \delta \in \{0, 1\}$. Man beachte, daß $\gamma^2 = \gamma$ und $\delta^2 = \delta$. (44) nimmt dann die Form

$$0 \ \equiv \ c^2 - md^2 = \gamma - m\delta + 4 \cdot \left(\gamma k + k^2 - m\delta l - ml^2\right) \ \equiv \ \gamma - m \cdot \delta \ (\text{mod } 4)$$

an, d.h.

$$\gamma \ \equiv \ m \cdot \delta \ (\text{mod } 4). \tag{45}$$

Nun wollen wir die verschiedenen Möglichkeiten für den Rest von m bei Division mit Rest durch 4 betrachten:

1. Fall: $m \equiv 1$ (mod 4)**:** Dann ist

$$\gamma \ \equiv \ m \cdot \delta \ \equiv \ \delta \ (\text{mod } 4),$$

und da $\gamma, \delta \in \{0, 1\}$ muß notwendigerweise $\gamma = \delta$ gelten. Es folgt

$$x = \frac{c - d}{2} + d \cdot \frac{1 + \sqrt{m}}{2} = (k - l) + d \cdot \omega_m \in \mathbb{Z}[\omega_m].$$

2. Fall: $m \equiv 2$ (mod 4) **oder** $m \equiv 3$ (mod 4)**:** Dann gilt

$$\gamma \ \equiv \ m \cdot \delta \ \equiv \ 2 \cdot \delta \ (\text{mod } 4)$$

bzw.

$$\gamma \ \equiv \ m \cdot \delta \ \equiv \ 3 \cdot \delta \ (\text{mod } 4),$$

was für $\gamma, \delta \in \{0, 1\}$ nur möglich ist, wenn $\gamma = 0 = \delta$. In diesem Fall gilt

$$x = \frac{c}{2} + \frac{d}{2} \cdot \sqrt{m} = k + l \cdot \omega_m \in \mathbb{Z}\left[\sqrt{m}\right] = \mathbb{Z}[\omega_m].$$

Da der Fall $m \equiv 0$ (mod 4) für ein quadratfreies m nicht auftreten kann, ist damit gezeigt, daß die ganzen Elemente von $\mathbb{Q}\left[\sqrt{m}\right]$ in $\mathbb{Z}[\omega_m]$ enthalten sind.

Sei nun umgekehrt $a + b \cdot \omega_m \in \mathbb{Z}[\omega_m]$, $a, b \in \mathbb{Z}$. Wir müssen zeigen, daß $S(x)$ und $N(x)$ ganze Zahlen sind, dann ist x ein ganzes Element in $\mathbb{Q}\left[\sqrt{m}\right]$.

1. Fall: $m \equiv 1 \pmod 4$**:** Dann gilt

$$S(x) = S\left(\frac{2a+b}{2} + \frac{b}{2} \cdot \sqrt{m}\right) = 2a + b \in \mathbb{Z}$$

und

$$N(x) = \frac{(2a+b)^2}{4} - m \cdot \frac{b^2}{4} = (a^2 + ab) + \frac{1-m}{4} \cdot b^2 \in \mathbb{Z},$$

da $1 - m$ nach Voraussetzung durch 4 teilbar ist.

2. Fall: $m \equiv 2 \pmod 4$ **oder** $m \equiv 3 \pmod 4$**:** Dann gilt

$$S(x) = 2 \cdot a \in \mathbb{Z} \quad \text{und} \quad N(x) = a^2 - m \cdot b^2 \in \mathbb{Z}.$$

In beiden Fällen ist $x = a + b \cdot \omega_m$ also ganz. □

Bemerkung 7.17

Wir haben in Bemerkung 7.14 für beliebige komplexe Zahlen definiert, wann sie ganz über $\mathbb{Z}$ heißen. Ist R ein Unterring von $\mathbb{C}$ so kann man ganz allgemein zeigen, daß die ganzen Elemente in R einen Unterring von R bilden, den man wieder den ganzen Abschluß von $\mathbb{Z}$ in R nennt. Dies verallgemeinert die Aussage von Satz 7.16. Für den Beweis verwendet man eine geeignete Fassung des Satzes von Cayley-Hamilton und erspart sich damit, den ganzen Abschluß von $\mathbb{Z}$ in R konkret auszurechnen, was meist ein weit schwierigeres Unterfangen ist. □

Wir haben dieses Kapitel mit der Frage begonnen, wann eine diophantische Gleichung der Form

$$x^2 - m \cdot y^2 = n$$

bei gegebenem m und n lösbar ist. Mit der eingeführten Notation läßt sich die Frage wie folgt umformulieren, wobei wir $z = x + y \cdot \sqrt{m}$ für $x, y \in \mathbb{Z}$ betrachten.

Bemerkung 7.18

Für $m \in \mathbb{Z}$ kein Quadrat und $n \in \mathbb{Z}$ sind folgende Aussagen gleichwertig:

a. Die diophantische Gleichung $x^2 - m \cdot y^2 = n$ besitzt eine Lösung.

b. Es gibt ein $z \in \mathbb{Z}\left[\sqrt{m}\right]$ mit $N(z) = n$.

Wir können diese Aussage umgekehrt auch verwenden, um aus der Lösbarkeit der diophantischen Gleichung Rückschlüsse auf die ganzen Zahlen zu ziehen, die als Norm eines ganzen Elementes von $\mathbb{Q}\left[\sqrt{m}\right]$ auftreten können. Wenden wir dieses Korollar etwa mit $m = -1$ und einer ungeraden Primzahl $n \in \mathbb{P}$ an, so ist $\mathbb{Z}[\omega_m]$ der Ring der ganzen Gaußschen Zahlen und unter Berücksichtigung des Satzes von Fermat 4.13 erhalten wir das folgende Korollar.

Korollar 7.19

Für eine ungerade Primzahl $p \in \mathbb{P}$ *sind die folgenden Aussagen gleichwertig:*

a. *Es gibt ein* $z \in \mathbb{Z}[i]$ *mit* $N(z) = p$.

b. *Die diophantische Gleichung* $x^2 + y^2 = p$ *ist lösbar.*

c. $p \equiv 1 \pmod 4$.

B) Die Einheiten in $\mathbb{Z}[\omega_m]$

Wenn man interessante Ringe wie die Ringe der ganzen Zahlen in $\mathbb{Q}\left[\sqrt{m}\right]$ gefunden hat, dann möchte ein Algebraiker auch ihre Struktur näher untersuchen. Dazu gehört zu allererst, daß er ihre Einheiten finden möchte. Diese sind auf interessante Weise mit den *Pellschen Gleichungen* der Einleitung (siehe S. 25) verknüpft, wie wir am Ende dieses Abschnitts sehen werden.

Zunächst beschreiben wir die Einheiten von $\mathbb{Z}[\omega_m]$ durch eine Eigenschaft, die die Norm involviert. Diese können wir dann ausnutzen, um $\mathbb{Z}[\omega_m]^*$ für negative m vollständig zu beschreiben.

Satz 7.20
Es sei $1 \neq m \in \mathbb{Z}$ eine quadratfreie ganze Zahl. Dann ist

$$\mathbb{Z}[\omega_m]^* = \{x \in \mathbb{Z}[\omega_m] \mid N(x) = \pm 1\}$$

die Gruppe der Einheiten in $\mathbb{Z}[\omega_m]$.

Beweis: Ist $x \in \mathbb{Z}[\omega_m]^*$ eine Einheit, so gibt es ein $y \in \mathbb{Z}[\omega_m]^*$ mit $x \cdot y = 1$. Da x und y ganz sind, ist $N(x), N(y) \in \mathbb{Z}$ und außerdem gilt

$$1 = N(1) = N(x \cdot y) = N(x) \cdot N(y).$$

Dies zeigt, daß $N(x) \in \mathbb{Z}^* = \{1, -1\}$ eine Einheit in $\mathbb{Z}$ ist, also $N(x) = \pm 1$.

Ist umgekehrt $x \in \mathbb{Z}[\omega_m]$ mit $N(x) = \pm 1$, dann ist

$$y = \frac{K(x)}{N(x)} = \pm K(x) \in \mathbb{Z}[\omega_m]$$

und

$$x \cdot y = \frac{x \cdot K(x)}{N(x)} = 1.$$

Mithin ist x eine Einheit in $\mathbb{Z}[\omega_m]$. □

Beispiel 7.21

a. Wir betrachten $m = 3$ und $u = 2 - \sqrt{3} \in \mathbb{Z}\left[\sqrt{m}\right]$. Dann ist

$$N(u) = u \cdot K(u) = \left(2 - \sqrt{3}\right) \cdot \left(2 + \sqrt{3}\right) = 1,$$

so daß u ein Einheit in $Z\left[\sqrt{m}\right]$ ist. Zudem gilt

$$u^{-1} = K(u) = 2 + \sqrt{3}.$$

b. Ist $m = -3$ und

$$\omega_m = \frac{1 + \sqrt{-3}}{2} \in \mathbb{Z}[\omega_m],$$

dann gilt

$$N(\omega_m) = \frac{1^2 - m \cdot 1^2}{4} = 1,$$

so daß ω_m in diesem Fall eine Einheit in $\mathbb{Z}[\omega_m]$ ist. Das Inverse von ω_m ist

$$\omega_m^{-1} = K(\omega_m) = \frac{1 - \sqrt{-3}}{2} = -\omega_m^2,$$

und damit gilt

$$\omega_m^6 = 1.$$

ω_m ist also eine primitive sechste Einheitswurzel (vgl. S. 48).

Für negative m, d.h. im imaginär-quadratischen Fall, stellt sich die Gruppe der Einheiten als sehr einfach heraus. Sie ist stets endlich und besteht meist nur aus den trivialen Elementen 1 und -1.

Korollar 7.22

Es sei $m \in \mathbb{Z}_{<0}$ *eine negative quadratfreie ganze Zahl. Dann gilt*

$$\mathbb{Z}[\omega_m]^* = \begin{cases} \{1,-1,i,-i\} = \langle i \rangle, & \textit{falls } m = -1, \\ \left\{1,-1,\omega_m,-\omega_m,\omega_m^2,-\omega_m^2\right\} = \langle \omega_m \rangle, & \textit{falls } m = -3, \\ \{1,-1\} = \langle -1 \rangle, & \textit{sonst.} \end{cases}$$

Insbesondere, die Einheitengruppe $\mathbb{Z}[\omega_m]^*$ *ist zyklisch.*

Beweis: Der Beweis ist dem Leser als Übungsaufgabe überlassen.

□

Der reell-quadratische Fall, d.h. $m > 0$, den man zunächst als einfacher wähnen könnte, da er nur reelle Zahlen involviert und nicht der Erweiterung auf die komplexen Zahlen bedarf, erweist sich als weitaus schwieriger. Die Einheitengruppe ist in diesem Fall unendlich, genauer gesagt ist sie das direkte Produkt einer unendlichen zyklischen Gruppe mit einer Gruppe der Ordnung 2, wie der Leser in Aufgabe 7.27 zeigen darf. Daß der reell-quadratische Fall der schwierigere ist, gilt aber nicht nur für die Einheiten, diese Tatsache wird uns auch im folgenden Abschnitt wieder begegnen.

Korollar 7.23

Ist $m \in \mathbb{Z}_{>1}$ *kein Quadrat, dann gibt es unendlich viele Zahlen in* $\mathbb{Z}\left[\sqrt{m}\right]$ *mit Norm Eins. Insbesondere gilt für eine quadratfreie positive Zahl* $m \in \mathbb{Z}_{>0}$

$$\left|\mathbb{Z}[\omega_m]^*\right| = \infty.$$

Die Hauptarbeit im folgenden Beweis besteht darin, überhaupt eine Zahl $\varepsilon \in \mathbb{Z}$ mit Norm Eins zu finden, die nicht ± 1 ist. Dabei ist die Grundidee, die irrationale Zahl $\sqrt{m}$ durch eine Folge rationaler Zahlen $\frac{a_n}{b_n}$ zu approximieren. Wir werden im wesentlichen

$$\left|\frac{a_n}{b_n} - \sqrt{m}\right| < \frac{1}{n^2}$$

fordern. Daß dies möglich ist, ist naheliegend, da $\mathbb{Q}$ dicht in $\mathbb{R}$ liegt. Wir wollen dann zeigen, daß eine Teilfolge der $x_n = a_n + b_n \cdot \sqrt{m}$ konstante Norm hat und paarweise verschiedenen Betrag. Unter den Folgengliedern dieser Teilfolge finden wir schließlich zwei x_k und x_l so, daß

$$\varepsilon = \frac{x_k}{x_l} \in \mathbb{Q}\left[\sqrt{m}\right]$$

die gesuchte Zahl ist. Unklar ist dabei lediglich, warum ε wirklich in $\mathbb{Z}\left[\sqrt{m}\right]$ liegt. Die Potenzen von ε stellen sich als paarweise verschieden heraus, so daß damit letztendlich die unendlich vielen Einheiten in $\mathbb{Z}[\omega_m]$ gefunden sind.

Beweis: Da jedes Element von $\mathbb{Z}\left[\sqrt{m}\right] \subseteq \mathbb{Z}[\omega_m]$ mit Norm Eins eine Einheit in $\mathbb{Z}[\omega_m]$ ist, reicht es zu zeigen, daß es unendlich viele Elemente in $\mathbb{Z}\left[\sqrt{m}\right]$ mit Norm Eins gibt. Die wesentliche Arbeit dabei wird sein, überhaupt ein Element

$$\varepsilon \in \mathbb{Z}\left[\sqrt{m}\right] \setminus \{1, -1\}$$

von Norm Eins zu finden. Da der Beweis sehr umfangreich ist, zerlegen wir ihn in mehrere Schritte. Dabei verwenden wir die Abbildung

$$I : \mathbb{Z}\left[\sqrt{m}\right] \longrightarrow \mathbb{Z}\left[\sqrt{m}\right] : a + b \cdot \sqrt{m} \mapsto b,$$

die es uns erlaubt eine Zahl $x = a + b \cdot \sqrt{m}$ als

$$x = a - b\sqrt{m} + 2 \cdot b\sqrt{m} = K(x) + 2 \cdot I(x) \cdot \sqrt{m} \tag{46}$$

zu schreiben.

1. **Schritt:** $\exists\ (x_n)_{n=1}^{\infty} \subset \mathbb{Z}\left[\sqrt{m}\right]\ :\ |K(x_n)| \leq \frac{1}{n}$ **und** $0 < I(x_n) \leq n$**:**
Für $k = 0, \ldots, n$ betrachten wir die reellen Zahlen

$$r_k = k \cdot \sqrt{m} - \left\lfloor k \cdot \sqrt{m} \right\rfloor \in [0, 1)$$

im halb-offenen Intervall $[0, 1)$. Wir können dieses Intervall äquidistant in n Teilintervalle der Länge $\frac{1}{n}$ zerlegen

$$[0, 1) = \dot{\bigcup_{j=0}^{n-1}} \left[\frac{j}{n}, \frac{j+1}{n}\right).$$

Dann muß mindestens eines der n Teilintervalle mindestens zwei der $n+1$ Zahlen $r_0, \ldots, r_n$ enthalten. Sind r_l und r_k, $0 \leq l < k \leq n$, im gleichen Teilintervall, so ist ihr Abstand echt kleiner als $\frac{1}{n}$, und mit

$$b_n = k - l \in \mathbb{Z} \quad \text{und} \quad a_n = \left\lfloor k \cdot \sqrt{m} \right\rfloor - \left\lfloor l \cdot \sqrt{m} \right\rfloor \in \mathbb{Z}$$

folgt

$$\left|a_n - b_n \cdot \sqrt{m}\right| = \left|(l - k) \cdot \sqrt{m} - \left(\left\lfloor l \cdot \sqrt{m} \right\rfloor - \left\lfloor k \cdot \sqrt{m} \right\rfloor\right)\right| = |r_l - r_k| < \frac{1}{n}$$

und

$$0 < b_n \leq n.$$

Setzen wir $x_n = a_n + b_n \cdot \sqrt{m}$, so haben wir unsere Folge gefunden.

2. Schritt: $\forall\, n = 1, \dots, \infty \;:\; |N(x_n)| \le \frac{1}{n} \cdot |x_n| \le 1 + 2 \cdot \sqrt{m}$**:**
Dies folgt aus einer einfachen Rechnung, bei der wir im zweitletzten Schritt $I(x_n) \le n$ ausnutzen sowie mehrfach, daß $|K(x_n)| \le \frac{1}{n}$:

$$\begin{aligned} |N(x_n)| =& |K(x_n) \cdot x_n| = |K(x_n)| \cdot |x_n| \\ \le& \frac{1}{n} \cdot |x_n| \overset{(46)}{=} \frac{1}{n} \left|K(x_n) + 2 \cdot I(x_n) \cdot \sqrt{m}\right| \\ \le& \frac{1}{n} \cdot \left(|K(x_n)| + 2 \cdot I(x_n) \cdot \sqrt{m}\right) \\ \le& \frac{1}{n^2} + 2 \cdot \sqrt{m} \le 1 + 2 \cdot \sqrt{m}. \end{aligned}$$

3. Schritt: $\forall\, z \in \mathbb{Z}\left[\sqrt{m}\right] \;:\; |\{x_n \mid x_n = \pm z\}| < \infty$**:**
Nehmen wir im Gegenteil an, daß für ein festes $z \in \mathbb{Z}\left[\sqrt{m}\right]$ eine Teilfolge $(x_{n_l})_{l=1}^{\infty}$ gibt mit $x_{n_l} = \pm z$ für alle l, so folgt

$$|N(z)| = |N(\pm x_{n_l})| = |N(x_{n_l})| \le \frac{1}{n_l} \cdot |x_{n_l}| = \frac{1}{n_l} \cdot |z| \overset{l \mapsto \infty}{\longrightarrow} 0,$$

d.h.

$$N(x_{n_1}) = N(z) = 0,$$

und damit $x_{n_1} = 0$, im Widerspruch zu $I(x_{n_1}) \neq 0$.

4. Schritt: $\exists\, (z_k)_{k=1}^{\infty} \subset \mathbb{Z}\left[\sqrt{m}\right] \;:\; \forall\, i \neq j$ **gilt** $z_i \neq \pm z_j$, **aber** $N(z_i) = N(z_j)$**:**
Wir wollen die Folge $(z_k)_{k=1}^{\infty}$ als Teilfolge der Folge $(x_n)_{n=1}^{\infty}$ finden. Dazu beachten wir, daß nach dem 2. Schritt

$$N(x_n) \in \left[-1 - \sqrt{m}, 1 + \sqrt{m}\right] \cap \mathbb{Z}$$

eine ganze Zahl im beschränkten Intervall $\left[-1 - \sqrt{m}, 1 + \sqrt{m}\right]$ ist. Da es in diesem Intervall nur endlich viele Zahlen gibt, müssen unendlich viele der x_n die gleiche Norm haben. D.h. es gibt eine Teilfolge $(y_l)_{l=1}^{\infty}$ von $(x_n)_{n=1}^{\infty}$, so daß

$$N(y_i) = N(y_j)$$

für alle $i, j = 1, \dots, \infty$. Nach dem 3. Schritt kann es für jedes der y_l nur endlich viele andere y_i geben kann mit $y_l = \pm y_i$. Es muß also eine Teilfolge $(z_k)_{k=1}^{\infty}$ von $(y_l)_{l=1}^{\infty}$ geben, so daß

$$z_i \neq \pm z_j$$

für $i \neq j$. Man kann sie wie folgt konstruieren: wähle $z_1 = y_1$ und setze $i_1 = 1$, wähle dann rekursiv für $l \ge 2$ ein $i_l \ge i_{l-1}$ so, daß

$$\{y_i \mid y_i = \pm z_{l-1}\} \subseteq \{y_1, \dots, y_{i_l - 1}\}$$

und setze $z_l = y_{i_l}$.

5. Schritt: $\exists\, \varepsilon \in \mathbb{Z}\big[\sqrt{m}\big] \setminus \{1,-1\} \;:\; N(\varepsilon) = 1$**:**
Wir setzen $n = N(z_1)$ und betrachten die Abbildung

$$\{z_l \mid l = 1, \ldots, \infty\} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_n : a + b \cdot \sqrt{m} \mapsto \big(\overline{a}, \overline{b}\big).$$

Wegen Schritt 4 ist der Definitionsbereich der Abbildung unendlich, der Zielbereich enthält aber nur n^2 Elemente. Mithin muß es zwei Folgenglieder $z_i = a + b \cdot \sqrt{m}$ und $z_j = c + d \cdot \sqrt{m}$, $i \neq j$, geben, deren Bilder in $\mathbb{Z}_n \times \mathbb{Z}_n$ übereinstimmen, d.h.

$$a \equiv c \pmod{n} \quad \text{und} \quad b \equiv d \pmod{n}. \tag{47}$$

Wir wollen nun zeigen, daß

$$\varepsilon = \frac{z_i}{z_j} = \frac{z_i \cdot K(z_j)}{N(z_j)} = \frac{ac - mbd}{n} + \frac{bc - ad}{n} \cdot \sqrt{m} \in \mathbb{Q}\big[\sqrt{m}\big]$$

in der Tat ein Element in $\mathbb{Z}\big[\sqrt{m}\big] \setminus \{1,-1\}$ von Norm Eins ist.
Dazu beachten wir, daß modulo n

$$ac - mbd \overset{(47)}{\equiv} a^2 - m \cdot b^2 = N(z_i) = n \equiv 0 \pmod{n}$$

und

$$bc - ad \overset{(47)}{\equiv} ba - ab = 0 \pmod{n}.$$

Also sind die ganzen Zahlen $ac - mbd$ und $bc - ad$ durch n teilbar und

$$\varepsilon \in \mathbb{Z}\big[\sqrt{m}\big].$$

Zudem folgt aus der Multiplikativität der Norm

$$N(\varepsilon) = \frac{N(z_i)}{N(z_j)} = \frac{n}{n} = 1$$

und da nach dem 4. Schritt $z_i \neq \pm z_j$ gilt zudem $\varepsilon \neq \pm 1$.

6. Schritt: $\Big|\big\{x \in \mathbb{Z}\big[\sqrt{m}\big] \;\big|\; N(x) = 1\big\}\Big| = \infty$**:**
Wir wollen nun zeigen, daß die $\varepsilon^n \in \mathbb{Z}\big[\sqrt{m}\big]$, $n = 1, \ldots, \infty$, paarweise verschiedene Elemente von $\mathbb{Z}\big[\sqrt{m}\big]$ mit Norm Eins sind. Aus der Multiplikativität der Norm folgt unmittelbar

$$N\big(\varepsilon^n\big) = N(\varepsilon)^n = 1^n = 1.$$

Nehmen wir nun

$$\varepsilon^k = \varepsilon^l$$

für ein Paar (k, l) mit $k > l \geq 1$ an. Dann gilt

$$\varepsilon^{k-l} = 1,$$

und da $\varepsilon \in \mathbb{R}$ und da Eins in $\mathbb{R}$ bestenfalls die $k - l$-ten Wurzeln 1 und -1 besitzt, muß $\varepsilon = \pm 1$ gelten. Das steht aber im Widerspruch zur Wahl von ε im 5. Schritt. Also sind die ε^n, $n = 1, \ldots, \infty$, paarweise verschiedene Elemente in $\mathbb{Z}\big[\sqrt{m}\big]$ der Norm Eins.

$\square$

Bemerkung 7.24
Die Hauptaussage von Korollar 7.23 besteht darin, daß es unendlich viele Element in $\mathbb{Z}\big[\sqrt{m}\big]$ von Norm Eins gibt. Dabei haben wir für m nur vorausgesetzt, daß m *kein Quadrat* ist, so daß $\sqrt{m}$ eine irrationale Zahl ist. Die Aussage ist damit gleichwertig zu folgendem Korollar über die Anzahl der Lösungen der *Pellschen Gleichung*

$$x^2 - m \cdot y^2 = 1,$$

mit der wir uns bereits in der Einleitung in Frage K beschäftigt haben (siehe S. 25).

Obwohl die Gleichungen von Euler dem englischen Mathematiker Pell zugeschrieben wurden, scheint sich letzterer nie mit ihnen beschäftigt zu haben. Sie gehen wohl vielmehr auf Fermat zurück und werden von manchen Autoren deshalb auch *Fermat-Pellsche Gleichungen* genannt. Unter diesem Namen verbergen sich neben den oben genannten Gleichungen auch die Gleichungen der Form

$$x^2 - m \cdot y^2 = -1,$$

deren Lösung zu Elementen der Norm -1 in $\mathbb{Z}\big[\sqrt{m}\big]$ gehören. Auch von diesen gibt es unendlich viele, was wir in dieser Vorlesung aber nicht zeigen wollen.

Korollar 7.25
Es sei $m \in \mathbb{Z}_{>0}$ eine positive Zahl, die kein Quadrat ist, dann hat die Pellsche Gleichung

$$x^2 - m \cdot y^2 = 1$$

unendlich viele Lösungen.

Bemerkung 7.26
Der Beweis von Korollar 7.23 ist konstruktiv und man kann aus ihm einen Algorithmus zum Finden einer Einheit in $\mathbb{Z}[\omega_m]^*$ mit Norm Eins ableiten, d.h. einen Algorithmus zur Lösung der Pellschen Gleichung $x^2 - m \cdot y^2 = 1$.

Dazu berechnet man sukzessive für $n \in \mathbb{N}$, ganze Zahlen $a_n \in \mathbb{Z}$ und $0 < b_n \leq n$ so, daß $|a_n - b_n \cdot \sqrt{m}| = |K(x_n)| \leq \frac{1}{n}$. Da man für ein festes n nur endlich viele b_n zu testen hat, kommen auch nur endlich viele a_n in Frage. Man tut dies solange, bis man ein Paar $x_i = a_i + b_i \cdot \sqrt{m}$ und $x_j = a_j + b_j \cdot \sqrt{m}$ gefunden hat, so daß $x_i \neq \pm x_j$, $N(x_i) = N(x_j)$, $a_i \equiv a_j \pmod{N(x_i)}$ und $b_i \equiv b_j \pmod{N(x_i)}$. Dabei muß man im Prinzip im n-ten Schritt x_n mit allen vorherigen x_i vergleichen. Dieser Algorithmus ist ganz offensichtlich nicht effizient.

Lösungen der Pellschen Gleichungen und damit Einheiten in $\mathbb{Z}[\omega_m]^*$ mit Norm ± 1 berechnet man besser mit Hilfe einer *Kettenbruchentwicklung* von $\sqrt{m}$, ein Thema, auf das wir aus Zeitgründen in dieser Vorlesung nicht eingehen können. □

Die folgende Aufgabe beschreibt die Struktur der Einheitengruppe $\mathbb{Z}[\omega_m]$ für ein quadratfreies positives m vollständig. Die Hauptarbeit besteht dabei darin, zu zeigen, daß das Minimum

$$\min\left\{x \in \mathbb{Z}[\omega_m]^* \;\middle|\; x > 1\right\}$$

existiert. Diese kleinste Einheit, die größer als Eins ist, wird *Fundamentaleinheit* in $\mathbb{Z}[\omega_m]$ genannt, da sie alle anderen erzeugt.

Aufgabe 7.27
Es sei $m \in \mathbb{Z}_{>1}$ eine quadratfreie Zahl, dann bilden die positiven Einheiten in $\mathbb{Z}[\omega_m]$ eine zyklische Gruppe

$$\mathbb{Z}[\omega_m]^*_{>0} = \left\{x \in \mathbb{Z}[\omega_m]^* \;\middle|\; x > 0\right\},$$

die von der kleinsten Einheit größer Eins, der sogenannten *Fundamentaleinheit* erzeugt wird, d.h. von

$$\varepsilon = \min\left\{x \in \mathbb{Z}[\omega_m]^* \;\middle|\; x > 1\right\}.$$

Zudem gilt

$$\mathbb{Z}[\omega_m]^* = \left\{ \pm \varepsilon^n \;\middle|\; n \in \mathbb{Z}\right\} = \{1, -1\} \cdot \mathbb{Z}[\omega_m]^*_{>0} \cong \mathbb{Z}_2 \times \mathbb{Z},$$

d.h. $\mathbb{Z}[\omega_m]^*$ ist das direkte Produkt einer zyklischen Gruppe der Ordnung zwei und einer unendlichen zyklischen Gruppe.

Bemerkung 7.28
Um zu zeigen, daß es eine Fundamentaleinheit in $\mathbb{Z}[\omega_m]$ für ein quadratfreies $m > 1$ gibt, haben wir die Existenz einer Einheit von Norm Eins ausgenutzt. Dies bedeutet jedoch nicht, daß die Fundamentaleinheit Norm Eins haben muß.

Die Beweise von Korollar 7.23 und Aufgabe 7.27 sind konstruktiv, so daß man auf diesem Weg im Prinzip eine Fundamentaleinheit bestimmen könnte. Allerdings ist der resultierende Algorithmus nicht effizient. Die folgende Aufgabe liefert einen weit besseren Ansatz zur Suche nach einer Fundamentaleinheit.

Aufgabe 7.29
Es sei $m \in \mathbb{Z}_{>1}$ quadratfrei.

a. Ist $m \equiv 2, 3 \pmod 4$ und $\varepsilon = a + b \cdot \sqrt{m} \in \mathbb{Z}[\omega_m]$, $a, b \in \mathbb{Z}$, eine Fundamentaleinheit von $\mathbb{Z}[\omega_m]$, dann sind $a, b > 0$ und
$$b = \min\left\{y \in \mathbb{Z}_{>0} \;\middle|\; \exists\, x \in \mathbb{Z} \,:\, x^2 - m \cdot y^2 = \pm 1\right\}.$$
b. Ist $m \equiv 1 \pmod 4$ und $\varepsilon = \frac{a+b\cdot\sqrt{m}}{2} \in \mathbb{Z}[\omega_m]$, $a, b \in \mathbb{Z}$, eine Fundamentaleinheit von $\mathbb{Z}[\omega_m]$, dann sind $a, b > 0$ und
$$b = \min\left\{y \in \mathbb{Z}_{>0} \;\middle|\; \exists\, x \in \mathbb{Z} \,:\, x^2 - m \cdot y^2 = \pm 4\right\}.$$

Bemerkung 7.30
Die Aufgabe zeigt uns unter anderem, daß Fundamentaleinheiten sehr groß sein können. In der Einleitung (siehe S. 25) haben wir die Pellsche Gleichung

$$x^2 - 1141 \cdot y^2 = 1$$

betrachtet und angemerkt, daß

$$(x, y) = (1036782394157223963237125215,\ 30693385322765657197397208)$$

die Lösung mit minimalem positiven y ist. Die Pellsche Gleichung

$$x^2 - 1141 \cdot y^2 = -1$$

hat in diesem Fall *keine* Lösung, wie man mit Hilfe von Kettenbruchkriterien zeigen kann. Die Fundamentaleinheit in $\mathbb{Z}[\omega_{1141}]$ ist deshalb

$$\varepsilon = 1036782394157223963237125215 + 30693385322765657197397208 \cdot \sqrt{1141}.$$

Sie liegt übrigens in $\mathbb{Z}\big[\sqrt{1141}\big]$, obwohl $1141 \equiv 1$ (mod 4).

Wer glaubt, ε sei eine ungewöhnlich *große* Fundamentaleinheit, der sollte es mit $m = 1.000.099$ versuchen. In diesem Fall hat in der Fundamentaleinheit $a + b \cdot \sqrt{m}$ die Zahl b 1115 Ziffern. □

C) Primfaktorzerlegung in $\mathbb{Z}[\omega_m]$

Unser Ziel ist es nach wie vor, die Struktur der Ringe der ganzen Zahlen $\mathbb{Z}[\omega_m]$ besser zu verstehen. In den algebraischen Strukturen haben wir uns mit zwei anderen Ringen beschäftigt, mit den ganzen Zahlen $\mathbb{Z}$ und mit Polynomringen über Körpern. Die wesentliche Strukturaussage dort war die Existenz einer *Primfaktorzerlegung*. Die Bedeutung dieser Strukturaussage für $\mathbb{Z}$ zeigt sich darin, daß die ganze Vorlesung *Elementare Zahlentheorie* auf diesem zentralen Ergebnis basiert. Es wird deshalb zurecht *Fundamentalsatz der elementaren Zahlentheorie* genannt. Gibt es in den Ringen der ganzen Zahlen $\mathbb{Z}[\omega_m]$ ebenfalls eine Primfaktorzerlegung?

Bevor wir uns dieser Frage widmen, wollen wir einige Begriffe aus den algebraischen Strukturen in Erinnerung rufen (vgl. auch S. 1ff.).

Bemerkung 7.31
Ein Integritätsbereich R heißt *euklidisch*, wenn es eine Funktion

$$\nu : R \setminus \{0\} \longrightarrow \mathbb{N}$$

gibt, so daß es für alle $x, y \in R \setminus \{0\}$ eine *Division mit Rest* der Form

$$x = q \cdot y + r$$

mit $q, r \in R$ gibt, wobei entweder $r = 0$ oder $\nu(r) < \nu(y)$. Wir nennen ν dann eine *euklidische Funktion* von R.

Ein Integritätsbereich R heißt *faktoriell*, falls jedes $0 \neq x \in R \setminus R^*$ sich als Produkt von endlich vielen Primelementen schreiben läßt, d.h.

$$x = p_1^{n_1} \cdots p_k^{n_k}, \tag{48}$$

$p_1, \ldots, p_k$ prim, $\langle p_i \rangle_R \neq \langle p_j \rangle_R$ für $i \neq j$ und $n_1, \ldots, n_k \in \mathbb{Z}_{>0}$. Man nennt die Darstellung (48) dann die *Primfaktorzerlegung* von x. Sie ist im wesentlichen eindeutig, d.h. bis auf die Reihenfolge sind die Ideale $\langle p_i \rangle$ und die Exponenten n_i eindeutig bestimmt. Daß für das Primelement p_i nur sein Ideal eindeutig bestimmt ist, heißt, daß p_i bis auf das Produkt mit einer Einheit festgelegt ist. Bei $\mathbb{Z}$ hieß dies, daß p_i bis auf sein Vorzeichen feststand, bei $K[t]$ bis auf ein Skalar ungleich Null, bei den Ringen $\mathbb{Z}[\omega_m]$ wird das von m abhängen, wie wir im letzten Abschnitt gezeigt haben. $\square$

Ein zentrales Ergebnis der Vorlesung algebraische Strukturen besagt, daß *jeder euklidische Ring faktoriell ist*, und wir haben dieses Ergebnis verwendet, um die Existenz der Primfaktorzerlegung in $\mathbb{Z}$ und in Polynomringen zu beweisen. Es ist also naheliegend, auch bei den $\mathbb{Z}[\omega_m]$ zunächst zu fragen, ob sie euklidisch sind. Für den Ring der ganzen Gaußschen Zahlen $\mathbb{Z}[i] = \mathbb{Z}[\omega_{-1}]$ wissen wir das bereits aus den Übungen zur Vorlesung algebraische Strukturen. Wir wiederholen den Beweis hier und verallgemeinern ihn ein wenig, so daß er einige andere $\mathbb{Z}[\omega_m]$ einschließt.

Satz 7.32
Für $m \in \{-2, -1, 2, 3\}$ ist der Ring $\mathbb{Z}[\omega_m]$ euklidisch mit dem Normbetrag

$$|N| : \mathbb{Z}[\omega_m] \longrightarrow \mathbb{N} : x \mapsto |N(x)|$$

als euklidischer Funktion. Insbesondere ist $\mathbb{Z}[\omega_m]$ dann auch faktoriell.

Beweis: Wir müssen die Existenz einer Division mit Rest zeigen. Seien dazu $x, y \in \mathbb{Z}[\omega_m] \setminus \{0\}$ gegeben, dann ist

$$\frac{x}{y} = a + b \cdot \sqrt{m} \in \mathbb{Q}\left[\sqrt{m}\right]$$

mit $a, b \in \mathbb{Q} \subset \mathbb{R}$. Da eine reelle Zahl höchstens den Abstand $\frac{1}{2}$ von der nächstgelegenen ganzen Zahl haben kann, gibt es ganze Zahlen $c, d \in \mathbb{Z}$ mit

$$|a - c| \leq \frac{1}{2} \quad \text{und} \quad |b - d| \leq \frac{1}{2}. \tag{49}$$

Wir setzen nun

$$q = c + d \cdot \sqrt{m} \in \mathbb{Z}\left[\sqrt{m}\right] \subseteq \mathbb{Z}[\omega_m]$$

und

$$r = x - q \cdot y \in \mathbb{Z}[\omega_m].$$

Damit gilt zunächst offenbar

$$x = q \cdot y + r,$$

und wir müssen nur noch zeigen, daß

$$0 \leq |N(r)| < |N(y)|.$$

Dabei beachte man, daß $|N(r)| = 0$ gleichbedeutend mit $r = 0$ ist.

Unter Ausnutzung der Multiplikativität der Norm und des Betrages gilt

$$\begin{aligned} |N(r)| =& \left| N\left(y \cdot \left(\frac{x}{y} - q\right)\right)\right| = |N(y)| \cdot \left| N\left(\frac{x}{y} - q\right)\right| \\ =& |N(y)| \cdot \left|N\left((a-c) + (b-d) \cdot \sqrt{m}\right)\right| \\ =& |N(y)| \cdot \left|(a-c)^2 - m \cdot (b-d)^2\right| \end{aligned}$$

Ist $m \in \{-1,-2\}$, so erhalten wir

$$|N(r)| = |N(y)| \cdot \left((a-c)^2 + |m| \cdot (b-d)^2\right) \overset{(49)}{\leq} |N(y)| \cdot \frac{3}{4} < |N(y)|,$$

und für $m \in \{2,3\}$ erhalten wir

$$|N(r)| \leq |N(y)| \cdot \max\left\{(a-c)^2,\ m \cdot (b-d)^2\right\} \overset{(49)}{\leq} |N(y)| \cdot \frac{3}{4} < |N(y)|.$$

Also ist $\mathbb{Z}[\omega_m]$ euklidisch mit dem Normbetrag als euklidischer Funktion. □

Man kann den Beweis des obigen Satzes so anpassen, daß er auf einige weitere Fälle anwendbar wird.

Aufgabe 7.33
Für $m \in \{-3,-7,-11\}$ ist der Ring $\mathbb{Z}[\omega_m]$ euklidisch mit dem Normbetrag

$$|N| : \mathbb{Z}[\omega_m] \longrightarrow \mathbb{N} : x \mapsto |N(x)|$$

als euklidischer Funktion. Insbesondere ist $\mathbb{Z}[\omega_m]$ dann auch faktoriell.

Aufgabe 7.34
Es sei $1 \neq m \in \mathbb{Z}$ eine quadratfreie Zahl

a. 2 in $\mathbb{Z}\left[\sqrt{m}\right]$ kein Primelement.
b. Falls $m \leq -3$ oder $m \equiv 1 \pmod 4$, dann ist 2 irreduzibel in $\mathbb{Z}\left[\sqrt{m}\right]$.
c. Für $m < 0$ ist $\mathbb{Z}\left[\sqrt{m}\right]$ genau dann faktoriell, wenn $m = -1$ oder $m = -2$.
d. Für $m \equiv 1 \pmod 4$ ist $\mathbb{Z}\left[\sqrt{m}\right]$ nie faktoriell.

Bemerkung 7.35
Der Beweis von Satz 7.32 funktioniert in der gegebenen Form nicht mehr für betragsgrößere m, und wir wissen aus der Vorlesung algebraische Strukturen auch schon, daß er sicher nicht für alle m durch ein besseres Argument ersetzt werden kann. Denn wir haben in den algebraischen Strukturen gezeigt, daß

$$\mathbb{Z}\left[\sqrt{-5}\right] = \mathbb{Z}[\omega_{-5}]$$

nicht faktoriell ist und mithin kein euklidischer Ring sein kann, weder mit dem Normbetrag als euklidischer Funktion noch mit einer anderen.

Ist einer der Ringe $\mathbb{Z}[\omega_m]$ ein euklidischer Ring mit dem Normbetrag als euklidischer Funktion, sagt man auch, $\mathbb{Z}[\omega_m]$ sei N-*euklidisch*. □

Wir werden in dieser Vorlesung für keine weiteren Ringe ganzer Zahlen $\mathbb{Z}[\omega_m]$ zeigen, ob sie euklidisch sind bzw. auch nur faktoriell sind. In den beiden folgenden Bemerkungen wollen wir aber die wesentlichen Ergebnisse festhalten, die zu dieser Frage bekannt sind. Dabei werden wir sehen, daß durchaus in etlichen der Ringe $\mathbb{Z}[\omega_m]$ eine Primfaktorzerlegung existiert, so daß es sinnvoll ist, im weiteren Verlauf des Abschnitts die Struktur der faktoriellen $\mathbb{Z}[\omega_m]$ weiter zu untersuchen, indem wir uns ihren elementaren Bausteinen, den *Primelementen* zuwenden.

Was die angesprochenen Ergebnisse betrifft, so unterscheiden sie sich für $m < 0$ und $m > 0$ wesentlich, so daß wir diese getrennt auflisten wollen. Zudem ist der imaginär-quadratische Fall wieder leichter und vollständig verstanden.

Bemerkung 7.36
Es sei $m < 0$ eine quadratfreie negative ganze Zahl. Dann gilt:

$$\begin{aligned} \mathbb{Z}[\omega_m] \text{ ist euklidisch} &\iff \mathbb{Z}[\omega_m] \text{ ist N-euklidisch} \\ &\iff m \in \{-1, -2, -3, -7, -11\}. \end{aligned}$$

Für den Fall $m \not\equiv 1 \pmod 4$ gilt zudem, daß es keine weiteren faktoriellen $\mathbb{Z}[\omega_m]$ gibt, d.h. für diese ist euklidisch äquivalent zu faktoriell. Für $m \equiv 1 \pmod 4$ gibt es aber noch einige faktorielle Ringe, die nicht euklidisch sind. Für den Beweis würde man ausnutzen, daß für $m < 0$ gilt:

$$\mathbb{Z}[\omega_m] \text{ ist faktoriell} \iff \mathbb{Z}[\omega_m] \text{ ist ein Hauptidealring.}$$

Nach einer mühsamen Kleinarbeit kann man dann für $m < 0$ zeigen:

$$\mathbb{Z}[\omega_m] \text{ ist faktoriell} \iff m \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Daß für diese Werte von m der Ring $\mathbb{Z}[\omega_m]$ faktoriell ist, wußte schon Gauß und er vermutete auch, daß dies für keine anderen Werte $m < 0$ der Fall ist. Der Beweis gelang aber erst Stark in den 1960er Jahren (siehe [Sta67]). □

Bemerkung 7.37
Es sei $m > 1$ eine quadratfreie positive ganze Zahl. Dann gilt:

$$\mathbb{Z}[\omega_m] \text{ ist N-euklidisch} \Leftrightarrow m \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Dieses Ergebnis wurde von Chatland und Davenport 1950 gezeigt, wobei es Davenport gelang zu zeigen, daß $\mathbb{Z}[\omega_m]$ für $m > 2^{14}$ nicht N-euklidisch ist, und Chatland dann die *wenigen tausend* Ringe für $m \leq 2^{14}$ im gleichen Jahr überprüfte.

Es ist nicht bekannt, ob es ein euklidisches $\mathbb{Z}[\omega_m]$ gibt, das nicht N-euklidisch ist. Bruns (siehe [Bru00]) gibt $\mathbb{Z}[\omega_{14}]$ als das kleinste denkbare Beispiel an. Der Ring ist nicht N-euklidisch, aber faktoriell. Er könnte euklidisch sein, Ihr müßt nur eine euklidische Funktion finden – oder alternativ zeigen, daß es keine gibt.

Anders als im imaginär-quadratischen Fall vermutete Gauß, daß unendlich viele der $\mathbb{Z}[\omega_m]$ für $m > 0$ faktoriell seien. Auch diese Vermutung konnte bislang weder bewiesen noch widerlegt werden. Für $m \leq 100$ sind 38 der Ringe $\mathbb{Z}[\omega_m]$ faktoriell. □

Bemerkung 7.38
An dieser Stelle sollte man vielleicht erwähnen, daß die Ringe $\mathbb{Z}\left[\sqrt{m}\right]$ für $m \equiv 1 \pmod 4$ nie faktoriell sind, ganz egal, ob m positiv oder negativ ist. Das ist einer der Gründe dafür, daß man sich mehr für die Ringe $\mathbb{Z}[\omega_m]$ interessiert als für $\mathbb{Z}\left[\sqrt{m}\right]$. Ein zweiter Grund ist, daß die Charakterisierung von $\mathbb{Z}[\omega_m]$ als ganzer Abschluß von $\mathbb{Z}$ in $\mathbb{Q}\left[\sqrt{m}\right]$ intrinsisch und basisunabhängig ist.

Für $m < 0$ ist $\mathbb{Z}\left[\sqrt{m}\right]$ übrigens genau dann N-euklidisch, wenn $m \in \{-1, -2\}$, wie man durch eine etwas genauer Betrachtung des Beweises von Satz 7.32 sieht. □

In einigen der Ringe $\mathbb{Z}[\omega_m]$ gibt es eine eindeutige Primfaktorzerlegung, in anderen gibt es sie nicht. Die folgende Aufgabe zeigt, daß man in letzteren aber zumindest immer eine Zerlegung in ein Produkt von irreduziblen Elementen erreichen kann. Nur ist diese im allgemeinen nicht eindeutig.

Aufgabe 7.39
Es sei $1 \neq m \in \mathbb{Z}$ eine quadratfreie ganze Zahl und $x \in \mathbb{Z}[\omega_m]$.

a. Ist x eine Einheit in $\mathbb{Z}[\omega_m]$, so ist $K(x)$ eine Einheit in $\mathbb{Z}[\omega_m]$.
b. Ist x irreduzibel in $\mathbb{Z}[\omega_m]$, so ist $K(x)$ irreduzibel in $\mathbb{Z}[\omega_m]$.
c. Ist $N(x)$ in $\mathbb{Z}$ eine Primzahl, so ist x irreduzibel in $\mathbb{Z}[\omega_m]$.

d. Jedes Element $0 \neq x \in \mathbb{Z}[\omega_m] \setminus \mathbb{Z}[\omega_m]^*$ läßt sich als Produkt von endlich vielen irreduziblen Elementen schreiben.

Betrachten wir eine Ringerweiterung $R \subseteq S$ und ein Element $p \in R$, so kann p als Element von R prim sein, ohne daß es deshalb auch als Element von S prim ist. Ist etwa $R = \mathbb{Z}$ und $S = \mathbb{Q}$, so ist die Primzahl $p = 2$ prim in $\mathbb{Z}$, aber eine Einheit in $\mathbb{Q}$. Der erste Teil der obigen Aufgabe hilft uns bei der Frage, welche Eigenschaften Primzahlen $p \in \mathbb{P}$ als Elemente eines Rings $\mathbb{Z}[\omega_m]$ besitzen.

Proposition 7.40
Es sei $1 \neq m \in \mathbb{Z}$ *quadratfrei und* $p \in \mathbb{P}$ *eine Primzahl.*

Entweder ist p *auch irreduzibel in* $\mathbb{Z}[\omega_m]$ *oder es gibt ein irreduzibles* $\pi \in \mathbb{Z}[\omega_m]$ *mit* $p \in \{\pi \cdot K(\pi), -\pi \cdot K(\pi)\}$.

Beweis: Ist p nicht irreduzibel in $\mathbb{Z}[\omega_m]$, so ist

$$p = x \cdot y$$

das Produkt von Nichteinheiten $x, y \in \mathbb{Z}[\omega_m] \setminus \mathbb{Z}[\omega_m]^*$. Berechnen wir die Norm von p, so gilt

$$p^2 = N(p) = N(x) \cdot N(y)$$

mit $N(x), N(y) \in \mathbb{Z}$. Da x und y keine Einheiten sind, ist ihre Norm ungleich ± 1 und aus der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ erhalten wir

$$N(x) = N(y) \in \{p, -p\}.$$

Für $\pi = x$ gilt also

$$p = N(\pi) = \pi \cdot K(\pi) \quad \text{oder} \quad p = -N(\pi) = -\pi \cdot K(\pi).$$

Wegen Aufgabe 7.39 ist π irreduzibel in $\mathbb{Z}[\omega_m]$, da $N(x) = p$ eine Primzahl ist. □

Wegen Proposition 7.40 erfüllt jede Primzahl $p \in \mathbb{P}$ als Element eines Ringes ganzer Zahlen $\mathbb{Z}[\omega_m]$ genau eine der Bedingungen in der folgenden Definition. Wir sprechen dabei vom *Zerlegungsverhalten* von p in $\mathbb{Z}[\omega_m]$.

Definition 7.41
Ist $1 \neq m \in \mathbb{Z}$ quadratfrei und $p \in \mathbb{P}$ eine Primzahl, so sagen wir:

a. p ist *träge* in $\mathbb{Z}[\omega_m]$, falls p irreduzibel in $\mathbb{Z}[\omega_m]$ ist.

b. p ist *verzweigt* in $\mathbb{Z}[\omega_m]$, falls es ein $\pi \in \mathbb{Z}[\omega_m]$ gibt, so daß $p = \pm N(\pi) = \pm\pi \cdot K(\pi)$ und $\frac{\pi}{K(\pi)} \in \mathbb{Z}[\omega_m]^*$.

c. p ist *unverzweigt* in $\mathbb{Z}[\omega_m]$, falls es ein $\pi \in \mathbb{Z}[\omega_m]$ gibt, so daß $p = \pm N(\pi) = \pm\pi \cdot K(\pi)$ und $\frac{\pi}{K(\pi)} \notin \mathbb{Z}[\omega_m]^*$.

Bemerkung 7.42
Wegen Proposition 7.40 erfüllt p genau eine der drei Bedingungen, und falls p eine der Bedingungen b. oder c. erfüllt, so ist die dort angegebene Zahl π irreduzibel in $\mathbb{Z}[\omega_m]$.

Man beachte auch, daß die Bedingung

$$\frac{\pi}{K(\pi)} \in \mathbb{Z}[\omega_m]^*$$

gleichbedeutend dazu ist, daß es eine Einheit $u \in \mathbb{Z}[\omega_m]^*$ gibt mit

$$\pi = u \cdot K(\pi).$$

Aus der Vorlesung algebraische Strukturen wissen wir aber, daß letzteres äquivalent dazu ist, daß die von π bzw. von $K(\pi)$ erzeugten Ideale übereinstimmen, d.h.

$$\langle \pi \rangle_{\mathbb{Z}[\omega_m]} = \langle K(\pi) \rangle_{\mathbb{Z}[\omega_m]}.$$

Man nennt π und $K(\pi)$ dann auch *assoziiert*.

Beispiel 7.43
Für $m = 3$ ist $R = \mathbb{Z}[\omega_m] = \mathbb{Z}\big[\sqrt{3}\big]$ ein faktorieller Ring.

5 ist träge in R: Wäre 5 nicht träge, dann wäre

$$\pm 5 = \pi \cdot K(\pi) = x^2 - 3 \cdot y^2$$

für ein $\pi = x + y \cdot \sqrt{3}$ mit ganzen Zahlen $x, y \in \mathbb{Z}$. Damit hätte die diophantischen Gleichung $x^2 - 3y^2 = \pm 5$ eine Lösung und nach Aufgabe 6.30 muß dann das Legendre-Symbol $\left(\frac{3}{5}\right)$ Eins sein. Es gilt aber

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

also muß 5 träge sein.

2 ist verzweigt in R: Setzen wir $\pi = -1 + \sqrt{3}$, so gilt

$$2 = -\pi \cdot K(\pi)$$

und

$$u := \frac{\pi}{K(\pi)} = \frac{\pi^2}{N(\pi)} = \frac{4 - 2 \cdot \sqrt{3}}{-2} \in \mathbb{Z}\left[\sqrt{3}\right]^*$$

ist eine Einheit in $\mathbb{Z}\big[\sqrt{3}\big]$, da $N(u) = 1$.

11 ist unverzweigt in R: Wir betrachten $\pi = 1 + 2 \cdot \sqrt{3}$, so daß

$$11 = -\pi \cdot K(\pi)$$

und

$$\frac{\pi}{K(\pi)} = \frac{\pi^2}{N(\pi)} = -\frac{13 + 4 \cdot \sqrt{3}}{11} \not\in \mathbb{Z}\left[\sqrt{3}\right].$$

□

In Teil a. unseres Beispiels haben wir gesehen, daß es einen Zusammenhang zwischen dem Legendre-Symbol und der Trägheit einer Primzahl gibt. Diesen Zusammenhang wollen wir genauer untersuchen.

Satz 7.44 (Zerlegungssatz)
Es sei $1 \neq m \in \mathbb{Z}$ quadratfrei, so daß $\mathbb{Z}[\omega_m]$ faktoriell ist, und $p \in \mathbb{P}$ sei eine ungerade Primzahl. Dann tritt genau einer der folgenden drei Fälle auf:

a. p *ist genau dann verzweigt, wenn* $\left(\frac{m}{p}\right) = 0$.

b. p *ist genau dann unverzweigt, wenn* $\left(\frac{m}{p}\right) = 1$.

c. p *ist genau dann träge, wenn* $\left(\frac{m}{p}\right) = -1$.

Im Beweis dieses Satzes verwenden wir das folgende Zerlegungslemma.

Lemma 7.45 (Zerlegungslemma)
Sei $1 \neq m \in \mathbb{Z}$ *quadratfrei,* $\pi \in \mathbb{Z}[\omega_m]$ *prim und* $p \in \mathbb{P}$ *ungerade mit* $p = \pm\pi \cdot K(\pi)$. *Genau dann ist* $\frac{\pi}{K(\pi)} \in \mathbb{Z}[\omega_m]^*$, *wenn* p *ein Teiler von* m *ist.*

Beweis: Seien $a, b \in \mathbb{Z}$ so, daß

$$\pi = \begin{cases} a + b \cdot \sqrt{m}, & \text{falls } m \equiv 2, 3 \pmod 4, \\ \frac{a}{2} + \frac{b}{2} \cdot \sqrt{m}, & \text{falls } m \equiv 1 \pmod 4. \end{cases}$$

“$\Longleftarrow$”: Nach Voraussetzung gibt es eine ganze Zahl $c \in \mathbb{Z}$ mit $p \cdot c = m$, so daß π ein Teiler von

$$\pm\pi \cdot K(\pi) \cdot c = p \cdot c = m = \sqrt{m} \cdot \sqrt{m}$$

in $\mathbb{Z}[\omega_m]$ ist. Da π nach Voraussetzung ein Primelement ist, ist π auch ein Teiler von $\sqrt{m}$ in $\mathbb{Z}[\omega_m]$. Aber dann teilt π auch jedes Vielfache von $\sqrt{m}$ und damit

$$\pi - K(\pi) = \begin{cases} 2 \cdot b \cdot \sqrt{m}, & \text{falls } m \equiv 2, 3 \pmod 4, \\ b \cdot \sqrt{m}, & \text{falls } m \equiv 1 \pmod 4. \end{cases}$$

Da π zudem ein Teiler von π ist, ist π also auch ein Teiler von $K(\pi)$. Nach Aufgabe 7.39 ist $K(\pi)$ aber irreduzibel, und aus der Vorlesung algebraische Strukturen wissen wir, daß sich π und $K(\pi)$ dann nur um eine Einheit unterscheiden, d.h. $\frac{\pi}{K(\pi)}$ ist eine Einheit in $\mathbb{Z}[\omega_m]^*$.

“$\Longrightarrow$”: Nach Voraussetzung gilt

$$a^2 - m \cdot b^2 = \begin{cases} \pi \cdot K(\pi) = \pm p, & \text{falls } m \equiv 2, 3 \pmod 4, \\ 4 \cdot \pi \cdot K(\pi) = \pm 4p, & \text{falls } m \equiv 1 \pmod 4. \end{cases} \tag{50}$$

Damit ist p ein Teiler von $a^2 - m \cdot b^2$.
Wäre p auch ein Teiler von b, so wäre p als Teiler von

$$a^2 = \left(a^2 - m \cdot b^2\right) + m \cdot b^2$$

ein Teiler von a und damit wäre p^2 ein Teiler von $a^2 - m \cdot b^2$ im Widerspruch zur Primfaktorzerlegung von $a^2 - m \cdot b^2$ in (50) – hierbei beachten wir, daß p eine ungerade Primzahl ist. Also ist p kein Teiler von b.
Nach Voraussetzung gilt zudem

$$\mathbb{Z}[\omega_m]^* \ni \pm\frac{\pi}{K(\pi)} = \frac{\pi^2}{p} = \begin{cases} \frac{a^2+m\cdot b^2}{p} + \frac{2\cdot a\cdot b}{p} \cdot \sqrt{m}, & \text{falls } m \equiv 2, 3 \pmod 4, \\ \frac{a^2+m\cdot b^2}{4p} + \frac{2\cdot a\cdot b}{4p} \cdot \sqrt{m}, & \text{falls } m \equiv 1 \pmod 4. \end{cases}$$

Aus der Beschreibung der Elemente von $\mathbb{Z}[\omega_m]$ und aus der Tatsache, daß p eine ungerade Primzahl ist, erhalten wir, daß p die ganze Zahl $2 \cdot a \cdot b$ teilen muß, und da p kein Teiler von 2 und kein Teiler von b ist, muß p ein Teiler von a sein. Aber dann gilt

$$p \mid a^2 - \left(a^2 - m \cdot b^2\right) = m \cdot b^2,$$

und da p kein Teiler von b ist, muß p ein Teiler von m sein.

□

Beweis von Satz 7.44: Da die Bedingungen an das Zerlegungsverhalten von p sich genauso gegenseitig ausschließen, wie die Bedingungen an den Wert des Legendre-Symbols, und da damit jeweils alle möglichen Fälle abgedeckt sind, reicht es, jeweils aus dem Wert des Legendre-Symbols das angegebene Verzweigungsverhalten von p herzuleiten.

Bevor wir uns dieser Aufgabe zuwenden, wollen wir die folgende Aussage zeigen:

$$\exists\, x \in \mathbb{Z} \, : \, p \mid x^2 - m \quad \Longrightarrow \quad p \text{ ist nicht träge.}$$

Nehmen wir an, daß dennoch träge ist, so ist p irreduzibel in $\mathbb{Z}[\omega_m]$ und damit ein Primelement von $\mathbb{Z}[\omega_m]$, da $\mathbb{Z}[\omega_m]$ nach Voraussetzung faktoriell ist. Wegen

$$p \mid x^2 - m = \left(x - \sqrt{m}\right) \cdot \left(x + \sqrt{m}\right)$$

muß p mithin ein Teiler von $x - \sqrt{m}$ oder von $x + \sqrt{m}$ in $\mathbb{Z}[\omega_m]$ sein, so daß

$$\frac{x}{p} - \frac{1}{p} \cdot \sqrt{m} \in \mathbb{Z}[\omega_m] \quad \text{oder} \quad \frac{x}{p} + \frac{1}{p} \cdot \sqrt{m} \in \mathbb{Z}[\omega_m].$$

Elemente dieser Gestalt gibt es in $\mathbb{Z}[\omega_m]$ aber nicht – hierbei beachten wir, daß p eine ungerade Primzahl ist.

Wir können uns nun der Betrachtung der verschiedenen Fälle widmen.

1. **Fall:** $\left(\frac{m}{p}\right) = -1$**:** Wegen Aufgabe 6.30 und da p ungerade ist, besitzen die Gleichungen

$$x^2 - m \cdot y^2 = \pm p$$

und

$$x^2 - m \cdot y^2 = \pm 4 \cdot p$$

keine Lösung $x, y \in \mathbb{Z}$. Daraus folgt aber, daß es in $\mathbb{Z}[\omega_m]$ kein Element

$$\pi = x + y \cdot \sqrt{m} = x + y \cdot \omega_m \quad (\text{ falls } p \equiv 2, 3 \ (\mathrm{mod}\ 4))$$

bzw.

$$\pi = \frac{x}{2} + \frac{y}{2} \cdot \sqrt{m} = \frac{x - y}{2} + \frac{y}{2} \cdot \omega_m \quad (\text{ falls } p \equiv 1 \ (\mathrm{mod}\ 4))$$

mit Norm $\pm p$ gibt. Aus Proposition 7.40 folgt dann, daß p irreduzibel in $\mathbb{Z}[\omega_m]$ und damit träge ist.

2. Fall: $\left(\frac{m}{p}\right) = 1$**:** Nach Voraussetzung ist m ein quadratischer Rest modulo p, d.h. es gibt ein $x \in \mathbb{Z}$ mit $p \mid x^2 - m$. Nach obiger Vorüberlegung ist p dann nicht träge. Nach Proposition 7.40 gibt es ein irreduzibles Element $\pi \in \mathbb{Z}[\omega_m]$ mit $p = \pm\pi \cdot K(\pi)$. Da $\mathbb{Z}[\omega_m]$ faktoriell ist, ist dieses ein Primelement, und da $\left(\frac{m}{p}\right) = 1$, ist p kein Teiler von m. Die Voraussetzungen des Zerlegungslemmas 7.45 sind erfüllt, so daß wir aus $p \not| m$ schließen, daß $\frac{\pi}{K(\pi)}$ keine Einheit in $\mathbb{Z}[\omega_m]$ ist. Also ist p unverzweigt.

3. Fall: $\left(\frac{m}{p}\right) = 0$**:** Nach Voraussetzung ist p ein Teiler von m und somit gilt $p \mid 0^2 - m$. Nach obiger Vorüberlegung ist p dann nicht träge. Nach Proposition 7.40 gibt es ein irreduzibles Element $\pi \in \mathbb{Z}[\omega_m]$ mit $p = \pm\pi \cdot K(\pi)$. Da $\mathbb{Z}[\omega_m]$ faktoriell ist, ist dieses ein Primelement. Die Voraussetzungen des Zerlegungslemmas 7.45 sind wieder erfüllt, so daß wir aus $p \mid m$ diesmal schließen, daß $\frac{\pi}{K(\pi)}$ eine Einheit in $\mathbb{Z}[\omega_m]$ ist. Also ist p verzweigt.

□

Wir sind nun in der Lage, die Primelemente in $\mathbb{Z}[\omega_m]$ genau zu beschreiben, wenn $\mathbb{Z}[\omega_m]$ faktoriell ist. Die Primelemente sind in diesem Fall die Elementarbausteine, aus denen alle anderen Zahlen in $\mathbb{Z}[\omega_m]$ aufgebaut sind. Überraschenderweise tauchen alle Primelemente von $\mathbb{Z}[\omega_m]$ aber bereits als Teiler der Primzahlen $p \in \mathbb{P}$ auf. Das ist ein Ergebnis, das in dieser Form nicht zu erwarten war.

Korollar 7.46
Es sei $1 \neq m \in \mathbb{Z}$ quadratfrei, so daß $\mathbb{Z}[\omega_m]$ faktoriell ist.

a. *Ist $\pi \in \mathbb{Z}[\omega_m]$ prim, so teilt π genau eine Primzahl $p \in \mathbb{P}$ und es gilt*
$$N(\pi) \in \left\{p, -p, p^2, -p^2\right\}.$$

b. *Die Menge der Primelemente in $\mathbb{Z}[\omega_m]$ ist genau die Menge*
$$\{p \in \mathbb{P} \mid p \text{ ist träge}\} \,\dot\cup\, \left\{\pi \;\middle|\; |\pi \cdot K(\pi)| \in \mathbb{P} \text{ ist verzweigt oder unverzweigt}\right\}$$
der Primfaktoren von Primzahlen $p \in \mathbb{P}$.

Beweis: a. Da π prim ist, ist π weder Null noch eine Einheit, und nach Satz 7.20 ist mithin
$$N(\pi) \in \mathbb{Z} \setminus \{0, 1, -1\}$$
eine ganze Zahl, die sich nach dem Fundamentalsatz der Elementaren Zahlentheorie als Produkt von Primzahlen schreiben läßt, d.h. es gibt Primzahlen $p_1, \ldots, p_k \in \mathbb{P}$ mit
$$\pi \cdot K(\pi) = N(\pi) = \pm p_1 \ldots p_k.$$
Da π dieses Produkt in $\mathbb{Z}[\omega_m]$ teilt, muß π auch eines der p_i teilen, d.h. es gibt ein $x \in \mathbb{Z}[\omega_m]$ mit
$$p_i = \pi \cdot x.$$

Durch Anwenden der Norm erhalten wir

$$N(\pi) \cdot N(x) = N(p_i) = p_i^2$$

und damit

$$N(\pi) \in \left\{p_i, -p_i, p_i^2, -p_i^2\right\},$$

da $N(\pi) \neq \pm 1$. Dies zeigt, daß π eine Primzahl teilt, und daß die Norm von π für diese die angegebene Bedingung erfüllt.
Es bleibt zu zeigen, daß π keine zwei verschiedenen Primzahlen $p, q \in \mathbb{P}$ teilen kann. Die Bézout Identität liefert die Existenz zweier ganzer Zahlen $a, b \in \mathbb{Z}$ mit

$$a \cdot p + b \cdot q = 1,$$

und wäre π ein Teiler sowohl von p, als auch von q, so würde diese Gleichung π als Teiler der Eins erweisen, d.h. π wäre eine Einheit im Widerspruch zur Wahl von π als Primelement. Also teilt π keine zwei verschiedenen Primzahlen.

b. Unter Berücksichtigung von Proposition 7.40 sind die Elemente der beiden angegebenen Mengen Primelemente und die Mengen sind disjunkt. Es bleibt zu zeigen, daß jedes Primelement $\pi \in \mathbb{Z}[\omega_m]$ in eine dieser beiden Mengen gehört, und dazu reicht es zu zeigen, daß π Teiler einer Primzahl $p \in \mathbb{P}$ ist. Dies folgt aber aus Teil a. dieses Satzes – dabei beachten wir, daß für eine Primzahl der Form $\pm\pi \cdot K(\pi) \in \mathbb{P}$ diese Zerlegung ihre Primfaktorzerlegung ist.

□

Ausgangspunkt des Kapitels war die Betrachtung von diophantischen Gleichungen der Form

$$x^2 - m \cdot y^2 = n$$

mit beliebigem n. Ist n eine Primzahl, so können wir den Zerlegungssatz anwenden, um die Lösbarkeit der Gleichung auf die Berechnung von Legendre-Symbolen zurückzuführen (vgl. auch Aufgaben 7.39).

Aufgabe 7.47
Es sei $p \in \mathbb{P}$ eine ungerade Primzahl.

a. Die diophantische Gleichung $x^2 + 2 \cdot y^2 = p$ hat genau dann eine Lösung, wenn $\left(\frac{-2}{p}\right) = 1$, d.h. wenn

$$p \equiv 1 \pmod 8 \quad \text{oder} \quad p \equiv 3 \pmod 8.$$

b. Die diophantische Gleichung $x^2 - 2 \cdot y^2 = p$ hat genau dann eine Lösung, wenn $\left(\frac{2}{p}\right) = 1$, d.h. wenn

$$p \equiv 1 \pmod 8 \quad \text{oder} \quad p \equiv -1 \pmod 8.$$

Im Zerlegungssatz haben wir das Zerlegungsverhalten von ungeraden Primzahlen beschrieben. Analog kann man auch das Zerlegungverhalten der Primzahl 2 in Abhängigkeit beschreiben.

Aufgabe 7.48
Es sei $1 \neq m \in \mathbb{Z}$ eine quadratfrei Zahl, so daß $\mathbb{Z}[\omega_m]$ faktoriell ist. Dann tritt genau einer der folgenden drei Fälle ein:

a. 2 ist genau dann verzweigt, wenn $m \equiv 2, 3 \pmod 4$.

b. 2 ist genau dann unverzweigt, wenn $m \equiv 1 \pmod 8$.

c. 2 ist genau dann träge, wenn $m \equiv 5 \pmod 8$.

Bemerkung 7.49
Nicht alle Ringe $\mathbb{Z}[\omega_m]$ ganzer Zahlen von quadratischen Zahlkörpern sind faktoriell, d.h. nicht in jedem dieser Ringe hat man eine eindeutige Primfaktorzerlegung der *Elemente*. Führt man aber den Begriff des *Primideals* ein, so kann man zeigen, daß sich jedes Ideal in eindeutiger Weise als Produkt von Primidealen schreiben läßt. Ringe mit dieser Eigenschaft nennt man *Dedekindbereiche* und sie verallgemeinern den Begriff des faktoriellen Ringes in natürlicher Weise. Die in diesem Kapitel untersuchten Ringe $\mathbb{Z}[\omega_m]$ sind die grundlegendsten Beispiele von Dedekindbereichen, und man kann das Verzweigungsverhalten einer Primzahl $p \in \mathbb{P}$ dann in ähnlicher Weise wie im Zerlegungssatz beschreiben, indem man von die Zerlegung des Ideals $\langle p \rangle_{\mathbb{Z}[\omega_m]}$ in $\mathbb{Z}[\omega_m]$ betrachtet. Dazu sei auf die Vorlesungen kommutative Algebra sowie Zahlentheorie aus dem Kanon der Arbeitsgruppe Algebra, Geometrie und Computeralgebra verwiesen.

D) **Summen zweier Quadrate**

In Kapitel 1 haben wir in Frage H wissen wollen, welche Zahlen sich als Summe zweier Quadrate schreiben lassen, und in Kapitel 4 haben wir eine erste Antwort mit dem Satz von Fermat 4.13 gegeben, der zeigt, daß eine *Primzahl* $p \in \mathbb{P}$ genau dann Summe zweier Quadrate ist, wenn sie kongruent zu Eins modulo Vier ist. In Korollar 7.19 haben wir daraus eine Aussage über die Norm von Elementen im Ring der ganzen Gaußschen Zahlen abgeleitet. Diesen Ansatz wollen wir im vorliegenden Abschnitt auf alle positiven Zahlen n erweitern und genau angeben, wann sie Summe zweier Quadratzahlen sind.

Satz 7.50 (Fermat)
Es sei $n \in \mathbb{Z}_0$ eine positive ganze Zahl.
Genau dann ist n Summe zweier Quadratzahlen, wenn jeder Primteiler q von n mit $q \equiv 3 \pmod 4$ in der Primfaktorzerlegung von n mit geradem Exponenten vorkommt, d.h. wenn die Primfaktorzerlegung von n die Form

$$n = 2^{\alpha} \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot q_1^{2\beta_1} \cdots q_l^{2\beta_l} \tag{51}$$

besitzt mit

$$p_i \equiv 1 \pmod 4$$

und

$$q_i \equiv 3 \pmod 4.$$

Beweis: Für den Beweis beachten wir zunächst, daß die Primzahl 2 verzweigt ist, da

$$2 = (1 + i) \cdot (1 - i) = -i \cdot (1 + i)^2$$

und

$$\frac{1 + i}{1 - i} = i \in \mathbb{Z}[i]^*.$$

n ist genau dann Summe zweier Quadrate, wenn es ganze Zahlen $x, y \in \mathbb{Z}$ gibt mit

$$n = x^2 + y^2 = N(x + iy).$$

Gibt es solche Zahlen x und y, so können wir die Primfaktorzerlegung von $z = x + iy \in \mathbb{Z}[i]$ in den ganzen Gaußschen Zahlen betrachten und erhalten

$$x + iy = \eta \cdot (1 + i)^\alpha \cdot \pi_1^{\alpha_1} \cdots \pi_k^{\alpha_k} \cdot q_1^{\beta_1} \ldots q_l^{\beta_l}$$

mit ungeraden Primzahlen $q_1, \ldots, q_l$, die in $\mathbb{Z}[i]$ träge sind, und Primelementen $\pi_1, \ldots, \pi_k$, für die $p_j = |\pi_j \cdot K(\pi_j)| \in \mathbb{P}$ eine in $\mathbb{Z}[i]$ verzweigte oder unverzweigte ungerade Primzahl ist. Wenden wir die Norm an, so erhalten wir

$$\begin{aligned} n = N(x + iy) =& N(\eta) \cdot N(1 + i)^\alpha \cdot N(\pi_1)^{\alpha_1} \cdots N(\pi_k)^{\alpha_k} \cdot N(q_1)^{\beta_1} \cdots N(q_l)^{\beta_l} \\ =& \pm 2^\alpha \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot q_1^{2\beta_1} \cdots q_l^{2\beta_l}. \end{aligned}$$

Das Vorzeichen muß dabei positiv sein, da n positiv ist. Wir wenden nun den Zerlegungssatz 7.44 an. Da die q_j träge sind in $\mathbb{Z}[i]$ gilt $\left(\frac{-1}{q_j}\right) = -1$, d.h.

$$q_j \equiv 3 \pmod 4.$$

Die p_j sind unverzweigt, da p_j kein Teiler von -1 ist, und mithin ist $\left(\frac{-1}{p_j}\right) = 1$, d.h.

$$p_j \equiv 1 \pmod 4.$$

Besitzt umgekehrt n eine Zerlegung der Form (51) mit den gegebenen Kongruenzbedingungen, so besitzen die p_j nach dem Zerlegungssatz eine Primfaktorzerlegung der Form

$$p_j = \pi_j \cdot K(\pi_j)$$

und die q_j sind träge in $\mathbb{Z}[i]$ – man beachte dabei, daß $p_j = -\pi_j \cdot K(\pi_j)$ nicht möglich ist, da dann die linke Seite positiv und die rechte negativ wäre. Betrachten wir nun

$$z = (1 + i)^\alpha \cdot \pi_1^{\alpha_1} \cdots \pi_k^{\alpha_k} \cdot q_1^{\beta_1} \cdots q_l^{\beta_l} \in \mathbb{Z}[i],$$

so gibt es ganze Zahlen $x, y \in \mathbb{Z}$ mit $z = x + iy$ und es gilt

$$n = N(z) = x^2 + y^2.$$

□

Beispiel 7.51
Die Zahl $n = 2 \cdot 5 \cdot 3^2 = 90$ läßt sich schreiben als

$$n = 90 = 9 + 81 = 3^2 + 9^2.$$

□

Aus Satz 7.50 folgt unmittelbar, daß bei Frage H in der Tabelle auf Seite 21 die vierte, siebte und achte Spalte leer bleiben mußte, wie das folgende Korollar zeigt.

Korollar 7.52

Ist $z \in \mathbb{Z}_{>0}$ *Summe zweier Quadratzahlen und* $z \equiv r \pmod 8$ *mit* $0 \le r \le 7$*, so ist*

$$r \in \{0, 1, 2, 4, 5\}.$$

Beweis: Ist $q = 3 + 4 \cdot k \equiv 3 \pmod 4$, so ist

$$q^2 = 9 + 24 \cdot k + 16 \cdot k^2 \ \equiv \ 1 \pmod 8.$$

Eine Summe z zweier Quadratzahlen hat eine Primfaktorzerlegung der Form

$$z = 2^\alpha \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot q_1^{2\beta_1} \cdots q_l^{2\beta_l},$$

wobei $p_i \equiv 1 \pmod 4$ und $q_i \equiv 3 \pmod 4$. Da die q_i alle mit geraden Exponenten vorkommen erhalten wir modulo 8 also

$$z \ \equiv \ 2^\alpha \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k} \pmod 8.$$

Für die p_i gilt

$$p_i \ \equiv \ 1 \pmod 8 \quad \text{oder} \quad p_i \ \equiv \ 5 \pmod 8,$$

so daß auch

$$p^{\alpha_i} \ \equiv \ 1 \pmod 8 \quad \text{oder} \quad p^{\alpha_i} \ \equiv \ 5 \pmod 8,$$

da $5^2 = 25 \equiv 1 \pmod 8$. Also gilt

$$z \ \equiv \ 2^\alpha \pmod 8 \quad \text{oder} \quad z \ \equiv \ 2^\alpha \cdot 5 \pmod 8,$$

so daß

$$r \in \{0, 1, 2, 4, 5\}.$$

□

Bemerkung 7.53

Man kann in Satz 7.50 auch die Anzahl der Lösungen von

$$x^2 + y^2 = n$$

bestimmen, wobei man nur die substantiell verschiedenen Lösungen zählen möchte, d.h. eine Lösung (r, s) wird man nicht von den Lösungen

$$(r, -s), (-r, -s), (-r, s), (s, r), (-s, r), (s, -r), (-s, -r)$$

unterscheiden. Dies führt zu einer Äquivalenzrelation und die Anzahl der Äquivalenzklassen ist die Anzahl der substantiell verschiedenen Lösungen. Hat n die Primfaktorzerlegung in (51), so gibt es genau

$$\left\lfloor \frac{(\alpha_1 + 1) \cdots (\alpha_k + 1) + 1}{2} \right\rfloor$$

solcher Äquivalenzklassen, wie man durch eine genau Betrachtung der möglichen Primfaktorzerlegungen in $\mathbb{Z}[\omega_m]$, die zu diesem n führen, sehen kann.

Will man nun etwa wissen, was die kleinste natürliche Zahl ist, die auf mindestens drei Arten als Summe zweier Quadrate zu schreiben ist, so sucht man Zahlen α_i mit

$$3 \leq \frac{(\alpha_1+1)\cdots(\alpha_k+1)+1}{2} < 4$$

Dabei kommen dann nur

$$k=2 \quad \text{und} \quad (\alpha_1,\alpha_2) \in \{(1,2),(2,1)\}$$

oder

$$k=1 \quad \text{und} \quad \alpha_1 \in \{4,5\}$$

in Frage. Die kleinstmöglichen Primzahlen p mit $p \equiv 1 \pmod 4$ sind 5 und 13, so daß die kleinstmöglichen n, die obiger Bedingung genügen die Zahlen

$$5^2 \cdot 13 \quad \text{bzw.} \quad 5^4 \quad \text{bzw.} \quad 5^5$$

sind. Die kleinste unter diesen ist

$$n = 5^2 \cdot 13 = 325,$$

und es gilt

$$325 = 1^2 + 18^2 = 6^2 + 17^2 = 10^2 + 15^2.$$

$\square$

Literatur

[Bru00] Winfried Bruns, *Zahlentheorie*, OSM, Reihe V, no. 146, FB Mathematik/Informatik, Universität Osnabrück, 2000.

[Bur07] David Burton, *Elementary number theory*, 6 ed., Mc Graw Hill, 2007.

[GPY05] Dan A. Goldston, Janos Pintz, and Cem Y. Yildirim, *Primes in tupels I*, arXiv:math/0508185, 2005.

[Has58] Colin Brian Haselgrove, *A disproof of a conjecture of Pólya*, Mathematika **5** (1958), no. 141–145.

[Mal06] Gunter Malle, *Elementare Zahlentheorie*, Vorlesungsmitschrift, 2006.

[Pol19] George Polya, *Verschiedene Bemerkungen zur Zahlentheorie*, Jahresbericht der deutschen Math.-Vereinigung **28** (1919), 31–40.

[RU95] Reinhold Remmert and Peter Ullrich, *Elementare Zahlentheorie*, 2 ed., Springer, 1995.

[Sta67] Harold Mead Stark, *A complete determination of the complex qudratic fields of class-number one*, Mich. Math. J. **14** (1967), 1–27.

[Sta98] ———, *An introduction to number theory*, 10 ed., MIT Press, 1998.

[Tan80] Minoru Tanaka, *A numerical investigation on cumulative sum of the Liouville function*, Tokyo Journal of Mathematics **3** (1980), 187–189.