Skript zur Vorlesung Algebra und Zahlentheorie für Lehramtsstudierende

Friedrich-Schiller-Universität Jena

Sommersemester 2021

Hans Franzen

Stand: 16. Juli 2021

1. Teilbarkeit

1.1. Vollständige Induktion.

Bemerkung 1.1.1. Wir benutzen folgende Konventionen und Notationen:

- $\mathbb{N} = \{1, 2, 3, \ldots\}$ bezeichne die Menge der natürlichen Zahlen,
- $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$,
- $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$ bezeichne die Menge der ganzen Zahlen.

Axiom 1.1.2 (Wohlordnung der natürlichen Zahlen)**.** Jede nicht-leere Teilmenge $M \subseteq \mathbb{N}$ besitzt ein kleinstes Element.

Bemerkung 1.1.3. Analog besitzt auch jede nicht-leere Teilmenge von $\mathbb{N}_0$ ein kleinstes Element, also auch $\mathbb{N}_0$ ist wohlgeordnet.

Lemma 1.1.4 (Prinzip der vollständigen Induktion)**.** *Für jedes $n \in \mathbb{N}$ sei $A(n)$ eine Aussage. Es gelte:*

(a) Die Aussage $A(1)$ ist wahr.
(b) Für jedes $n \in \mathbb{N}$ gilt: falls $A(n)$ wahr ist, so ist auch $A(n+1)$ wahr.

Dann ist $A(n)$ wahr für alle $n \in \mathbb{N}$.

Beweis. Sei $M = \{n \in \mathbb{N} \mid A(n) \text{ ist falsch}\}$. Wir müssen zeigen, dass $M = \emptyset$ ist. Angenommen $M \neq \emptyset$. Dann gäbe es nach Axiom 1.1.2 ein kleinstes Element von M; nennen wir es n. Da $A(1)$ wahr ist, ist $n > 1$. Nach Konstruktion ist $n-1 \notin M$, also ist $A(n-1)$ wahr. Gemäß (b) ist dann aber $A(n)$ auch wahr. Also ist $n \notin M$. Ein Widerspruch. $\square$

Bemerkung 1.1.5. Es gibt folgende Varianten des Prinzips der vollständigen Induktion:

(1) Vollständige Induktion über $\mathbb{N}_0$: Sei $A(n)$ eine Aussage für jedes $n \in \mathbb{N}_0$. Ist $A(0)$ wahr, und ist für jedes $n \in \mathbb{N}_0$ mit $A(n)$ auch $A(n+1)$ wahr, so folgt, dass $A(n)$ wahr ist für alle $n \in \mathbb{N}_0$.
(2) Ist $A(n)$ eine Aussage für jedes $n \in \mathbb{N}$. Es gelte:
   (a) $A(1)$ ist wahr.
   (b) Für alle $n \in \mathbb{N}$ gilt: falls $A(1), A(2), \ldots, A(n)$ alle wahr sind, so ist auch $A(n+1)$ wahr.

   Dann ist $A(n)$ wahr für alle $n \in \mathbb{N}$.

1.2. Division mit Rest.

Definition 1.2.1. Seien $a, b \in \mathbb{Z}$. Wir sagen a *teilt* b, wenn es ein $q \in \mathbb{Z}$ mit $b = aq$ gibt.

Bemerkung 1.2.2. Zu Sprechweisen und Notationen:

(1) Für „a teilt b“ benutzt man das Symbol $a \mid b$. Das Symbol $a \nmid b$ bedeutet a teilt b nicht.
(2) Andere Sprechweisen für „a teilt b“ sind:
   - a ist ein Teiler von b,
   - b wird von a geteilt,
   - b ist ein Vielfaches von a.

Beispiel 1.2.3. $17 \mid 51$, $4 \nmid 18$

Lemma 1.2.4. *Seien $a, b, c \in \mathbb{Z}$.*

(1) Stets gelten $1 \mid a$*,* $a \mid a$ *und* $a \mid 0$*.*
(2) Genau dann gilt $a \mid b$*, wenn* $-a \mid b$ *gilt.*
(3) Falls $a \mid b$ *und* $b \mid c$*, so gilt* $a \mid c$*.*
(4) Falls $0 \mid a$*, so ist* $a = 0$*.*
(5) Falls $a \mid b$ *und* $b \mid a$*, so ist* $b = \pm a$*.*
(6) Falls $a \mid b$ *und* $b \neq 0$ *gelten, ist* $|a| \leq |b|$

Beweis.

(1) Da $a = 1 \cdot a$, folgt $1 \mid a$. Wegen $a = a \cdot 1$, gilt $a \mid a$ und aus $0 = a \cdot 0$, folgt $a \mid 0$.
(2) Es gelte $a \mid b$. Dann existiert $q \in \mathbb{Z}$ mit $b = aq$. Dann ist $b = (-a)(-q)$, also auch $-a \mid b$. Falls umgekehrt $-a \mid b$ gilt, so folgt aus der Hinrichtung $a = -(-a)$ teilt b.
(3) Da $a \mid b$, existiert ein $q \in \mathbb{Z}$ mit $b = aq$. Genauso existiert wegen $b \mid c$ ein $p \in \mathbb{Z}$ mit $c = bp$. Also ist $c = bp = aqp$ und deshalb folgt $a \mid c$.
(4) Es gibt ein $q \in \mathbb{Z}$ mit $a = 0 \cdot q$. Also ist $a = 0$.
(5) Ist $a = 0$, so folgt $b = 0$ und umgekehrt. Deshalb dürfen wir $a, b \neq 0$ annehmen. Nach Voraussetzung existieren $q, p \in \mathbb{Z}$, so dass $b = aq$ und $a = bp$. Dann ist $b = aq = bpq$. Da $b \neq 0$ ist, ist $pq = 1$ und daher $q = p = \pm 1$. Das impliziert $b = \pm a$.
(6) Es gibt ein $q \in \mathbb{Z}$ mit $b = aq$. Wegen $b \neq 0$ ist $q \neq 0$. Dann ist $|b| = |a| \cdot |q| \geq |a|$. □

Lemma 1.2.5 (Division mit Rest)**.** *Seien* $b \in \mathbb{Z}$ *und* $a \in \mathbb{N}$*. Dann gibt es eindeutig bestimmte Zahlen* $q \in \mathbb{Z}$ *und* $r \in \{0, \ldots, a-1\}$*, so dass*

$$b = aq + r.$$

Beweis. Zur Existenz: Sei $R = \{b - aq \mid q \in \mathbb{Z}\}$. Dann ist $R \cap \mathbb{N}_0 \neq \emptyset$, denn für $q \leq b/a$ ist $b - aq \geq 0$ (beachte, dass $a > 0$ ist). Also besitzt $R \cap \mathbb{N}_0$, nach dem Wohlordnungsaxiom für $\mathbb{N}_0$, ein kleinstes Element r. Insbesondere ist $r \in R$, also existiert $q \in \mathbb{Z}$, so dass $r = b - aq$, oder äquivalent

$$b = aq + r.$$

Es genügt zu zeigen, dass $r \leq a - 1$ ist. Angenommen $r \geq a$. Dann ist $r' := r - a \geq 0$ und

$$r' = r - a = b - aq - a = b - a(q+1) \in R$$

also ist $r' \in R \cap \mathbb{N}_0$ und $r' < r$. Das ist ein Widerspruch zur Minimalität von r.
Zur Eindeutigkeit: Seien $q, q' \in \mathbb{Z}$ und $r, r' \in \{0, \ldots, a-1\}$, so dass $b = aq + r = aq' + r'$. Angenommen $q \neq q'$. O.E. gelte $q < q'$. Dann ist

$$r - r' = a(q' - q) \geq a$$

was aber nicht sein kann, denn $0 \leq r, r' < a$. Also ist $q = q'$ und deshalb auch $r = r'$. □

Bemerkung 1.2.6. Der Beweis liefert einen Algorithmus zur Bestimmung von q und r:

```
q := 0
r := b
while (r >= a){
        r = r-a
        q = q+1
```

```
        }
        while (r < 0){
                r = r+a
                q = q-1
        }
        return (q,r)
```

Beispiel 1.2.7. Seien $b = 99$ und $a = 7$. Dann ist $q = 14$ und $r = 1$; tatsächlich $7 \cdot 14 + 1 = 98 + 1 = 99$.

1.3. **Ideale.**

Definition 1.3.1. Eine Teilmenge $I \subseteq \mathbb{Z}$ heißt *Ideal* falls folgende Eigenschaften gelten:

(I.1) $0 \in I$.
(I.2) Für alle $a, b \in I$ ist $a + b \in I$.
(I.3) Für alle $a \in I$ und alle $n \in \mathbb{Z}$ ist $na \in I$.

Beispiel 1.3.2.

(1) Die Menge aller geraden ganzen Zahlen ist ein Ideal!
(2) Die Menge aller ungeraden ganzen Zahlen ist kein Ideal (alle drei Axiome sind verletzt).
(3) Die Menge $\mathbb{N}_0$ ist kein Ideal (zwar sind (I.1) und (I.2) erfüllt, aber (I.3) nicht: es gilt $2 \in \mathbb{N}_0$, aber $-2 = (-1) \cdot 2 \notin \mathbb{N}_0$).

Definition 1.3.3. Seien $n_1, \ldots, n_t \in \mathbb{Z}$. Wir definieren

$$(n_1, \ldots, n_t) := \{a_1 n_1 + \ldots + a_t n_t \mid a_1, \ldots, a_t \in \mathbb{Z}\}.$$

Man nennt $(n_1, \ldots, n_t)$ das *von $n_1, \ldots, n_t$ erzeugte Ideal.* (Diese Bezeichnung wird durch das nächste Lemma gerechtfertigt.)

Lemma 1.3.4. *Seien $n_1, \ldots, n_t \in \mathbb{Z}$. Dann ist $(n_1, \ldots, n_t)$ ein Ideal.*

Beweis. Schreibe $I := (n_1, \ldots, n_t)$. Wir weisen die Axiome nach:

(I.1) $0 = 0n_1 + \ldots + 0n_t \in I$.
(I.2) Seien $a = a_1 n_1 + \ldots + a_t n_t, b = b_1 n_1 + \ldots + b_t n_t \in I$. Dann ist $a + b = (a_1 + b_1)n_1 + \ldots + (a_t + b_t)n_t \in I$.
(I.3) Sei $a = a_1 n_1 + \ldots + a_t n_t \in I$ und $m \in \mathbb{Z}$. Dann ist $ma = (ma_1)n_1 + \ldots + (ma_t)n_t \in I$. □

Bemerkung 1.3.5. Sei $n \in \mathbb{Z}$. Dann ist $(n) = \{an \mid a \in \mathbb{Z}\}$ die Menge aller Vielfachen von n. Schreibe auch $n\mathbb{Z} := (n)$.

Lemma 1.3.6. *Sei $I \subseteq \mathbb{Z}$ ein Ideal. Dann existiert ein eindeutig bestimmtes $n \in \mathbb{N}_0$ mit $I = (n)$.*

Beweis. Wir beweisen Existenz und Eindeutigkeit.

- Existenz: Ist $I = \{0\}$, so ist $I = (0)$ und $n := 0$ ist das gesuchte Element. Angenommen $I \neq \{0\}$. Dann ist $I \cap \mathbb{N} \neq \emptyset$, denn nach Annahme existiert ein $a \in I$ mit $a \neq 0$. Ist a bereits positiv, so ist $a \in I \cap \mathbb{N}$. Ist $a < 0$, so ist

$-a = (-1)a \in I$ nach Eigenschaft (I.3). Da $I \cap \mathbb{N}$ nicht-leer ist, gibt es nach dem Wohlordnungsaxiom (Axiom 1.1.2) ein kleinstes Element $n \in I \cap \mathbb{N}$. Wir zeigen

$$I = (n).$$

Zu „$\supseteq$“: Sei $b \in (n)$. Dann existiert $a \in \mathbb{Z}$ mit $b = an$. Da $n \in I$ ist, folgt aus (I.3), dass auch $b = an \in I$ ist.
Zu „$\subseteq$“: Sei $b \in I$. Führe Division mit Rest durch. Es exisieren $q \in \mathbb{Z}$ und $r \in \{0, \ldots, n-1\}$, so dass $b = nq + r$. Dann ist

$$r = b - nq \in I.$$

Wäre $r \neq 0$, so wäre $r \in \mathbb{N}$ und $r < n$. Das würde einen Widerspruch zur Minimalität von n ergeben. Also muss $r = 0$ sein. Demnach ist $b = nq \in (n)$.

- Eindeutigkeit: Seien $n, m \in \mathbb{N}_0$, so dass $(n) = I = (m)$. Es folgt $m|n$ und $n|m$ nach Bemerkung 1.3.5. Lemma 1.2.4(5) impliziert $m = \pm n$. Da $m, n \geq 0$ sind, folgt daraus $m = n$. □

Definition 1.3.7. Sei $I \subseteq \mathbb{Z}$ ein Ideal. Das nach Lemma 1.3.6 eindeutig bestimmte Element $n \in \mathbb{N}_0$ mit $I = (n)$ heißt der *nicht-negative Erzeuger* von I.

Lemma 1.3.8 (Operationen auf Idealen)**.** *Seien $I, J \subseteq \mathbb{Z}$ Ideale. Dann ist*

$$I + J := \{a + b \mid a \in I, b \in J\}$$

ein Ideal. Ebenso ist der Durchschnitt $I \cap J$ ein Ideal.

Beweis. Wir rechnen die Axiome nach.

(I.1) $0 = 0 + 0 \in I + J$.

(I.2) Seien $x, y \in I + J$. Dann gibt es $a, a' \in I$ und $b, b' \in J$ mit $x = a + b$ und $y = a' + b'$. Dann ist $x + y = (a + a') + (b + b') \in I + J$.

(I.3) Sei $x \in I + J$, also $x = a + b$ für $a \in I$ und $b \in J$ und sei $m \in \mathbb{Z}$. Dann ist $mx = ma + mb \in I + J$.

Für den Durchschnitt läuft der Beweis ähnlich. □

Lemma 1.3.9. *Seien $n_1, \ldots, n_t, m_1, \ldots, m_s \in \mathbb{Z}$. Dann ist*

$$(n_1, \ldots, n_t) + (m_1, \ldots, m_s) = (n_1, \ldots, n_t, m_1, \ldots, m_s).$$

Beweis. Sei $I := (n_1, \ldots, n_t)$, $J := (m_1, \ldots, m_s)$ und $K := (n_1, \ldots, n_t, m_1, \ldots, m_s)$.
Zu „$\subseteq$“: Sei $x \in I + J$, also $x = a + b$ für $a \in I$ und $b \in J$. Dann gibt es $a_1, \ldots, a_t \in \mathbb{Z}$ und $b_1, \ldots, b_s \in \mathbb{Z}$ mit $a = a_1 n_1 + \ldots + a_t n_t$ und $b = b_1 m_1 + \ldots + b_s m_s$. Dann ist

$$x = a + b = a_1 n_1 + \ldots + a_t n_t + b_1 m_1 + \ldots + b_s m_s \in K.$$

Zu „$\supseteq$“: Ebenso offensichtlich wie „$\subseteq$“. □

1.4. **Größter gemeinsamer Teiler.**

Definition 1.4.1. Seien $n_1, \ldots, n_t \in \mathbb{Z}$. Ein $d \in \mathbb{Z}$, für das $d \mid n_i$ gilt (alle $i = 1, \ldots, t$) heißt ein *gemeinsamer Teiler* von $n_1, \ldots, n_t$. Es sei

$$T(n_1, \ldots, n_t) := \{d \in \mathbb{Z} \mid d \text{ gemeinsamer Teiler von } n_1, \ldots, n_t\}.$$

Lemma 1.4.2. *Seien $n_1, \ldots, n_t \in \mathbb{Z}$ nicht alle 0. Dann ist $T(n_1, \ldots, n_t)$ eine endliche Menge.*

Beweis. Ohne Einschränkung gelte $n_1 \neq 0$. Für jedes $d \in T(n_1, \ldots, n_t)$ gilt insbesondere $d \mid n_1$, also folgt aus Lemma 1.2.4(vi), dass $|d| \leq |n_1|$ ist. Deswegen ist $T(n_1, \ldots, n_t) \subseteq \{-|n_1|, \ldots, |n_1|\}$. □

Definition 1.4.3. Seien $n_1, \ldots, n_t \in \mathbb{Z}$ nicht alle 0. Dann heißt $\mathrm{ggT}(n_1, \ldots, n_t) := \max T(n_1, \ldots, n_t)$ der *größte gemeinsame Teiler* von $n_1, \ldots, n_t$.

Bemerkung 1.4.4. Seien $n_1, \ldots, n_t \in \mathbb{Z}$ nicht alle 0. Wegen $1 \in T(n_1, \ldots, n_t)$ ist $\mathrm{ggT}(n_1, \ldots, n_t) \in \mathbb{N}$.

Lemma 1.4.5. *Seien $n_1, \ldots, n_t \in \mathbb{Z}$ nicht alle 0. Dann ist $\mathrm{ggT}(n_1, \ldots, n_t)$ der nicht-negative Erzeuger des Ideals $(n_1, \ldots, n_t)$.*

Beweis. Sei $d := \mathrm{ggT}(n_1, \ldots, n_t)$ und sei n der nicht-negative Erzeuger von $(n_1, \ldots, n_t)$. Wir zeigen $d = n$, indem wir $d \leq n$ und $n \leq d$ zeigen.
Zu $d \leq n$: Insbesondere ist $n \in (n_1, \ldots, n_t)$. Deshalb existieren $a_1, \ldots, a_t \in \mathbb{Z}$ mit $n = a_1 n_1 + \ldots + a_t n_t$. Da d ein gemeinsamer Teiler der $n_1, \ldots, n_t$ ist, existieren $q_1, \ldots, q_t \in \mathbb{Z}$ mit $n_i = q_i d$ für alle $i = 1, \ldots, r$. Damit ist

$$n = a_1 q_1 d + \ldots + a_t q_t d = (a_1 q_1 + \ldots + a_t q_t) d$$

ein Vielfaches von d. Aus Lemma 1.2.4(vi) folgt dann $d = |d| \leq |n| = n$.
Zu $n \leq d$: Es gilt $n_1, \ldots, n_t \in (n)$, also ist jedes n_i ein Vielfaches von n; mit anderen Worten n ist ein gemeinsamer Teiler von $n_1, \ldots, n_t$. Da d der größte gemeinsame Teiler von $n_1, \ldots, n_t$ ist, folgt $n \leq d$. □

Korollar 1.4.6 (Bézouts Lemma)**.** *Seien $n_1, \ldots, n_t \in \mathbb{Z}$ nicht alle 0 und sei $d = \mathrm{ggT}(n_1, \ldots, n_t)$. Dann existieren $a_1, \ldots, a_t \in \mathbb{Z}$, so dass $d = a_1 n_1 + \ldots + a_t n_t$.*

Beweis. Nach Lemma 1.4.5 ist insbesondere $d \in (n_1, \ldots, n_t)$. Nach Definition des Ideals $(n_1, \ldots, n_t)$ existieren also $a_1, \ldots, a_t$ wie gefordert. □

Beispiel 1.4.7. $\mathrm{ggT}(40, 12) = 4 = 1 \cdot 40 + (-3) \cdot 12$

1.5. **Euklidischer Algorithmus.**

Ziel. Bestimme algorithmisch den größten gemeinsamen Teiler von gegebenen ganzen Zahlen $n_1, \ldots, n_t$ (nicht alle 0), sowie die Koeffizienten aus dem Lemma von Bézout.

Lemma 1.5.1. *Seien $n_1, \ldots, n_t \in \mathbb{Z}$. Für alle $i, j \in \{1, \ldots, t\}$ gilt:*

(1) $(n_1, \ldots, n_i, \ldots, n_t) = (n_1, \ldots, -n_i, \ldots, n_t)$
(2) Ist $n_i = 0$, so ist $(n_1, \ldots, n_i, \ldots, n_t) = (n_1, \ldots, n_{i-1}, n_{i+1}, \ldots, n_t)$.
(3) $(n_1, \ldots, n_i, \ldots, n_j, \ldots, n_t) = (n_1, \ldots, n_j, \ldots, n_i, \ldots, n_t)$
(4) Falls $j \neq i$ ist gilt für jedes $a \in \mathbb{Z}$:

$$(n_1, \ldots, n_i, \ldots, n_j, \ldots, n_t) = (n_1, \ldots, n_i + a n_j, \ldots, n_j, \ldots, n_t).$$

Beweis. Wir beweisen exemplarisch (4). Die restlichen Aussagen zeigen wir analog. Sei $I := (n_1, \ldots, n_i, \ldots, n_j, \ldots, n_t)$ und $J := (n_1, \ldots, n_i + a n_j, \ldots, n_j, \ldots, n_t)$.

Zu „$\subseteq$“: Sei $x \in I$. Dann existieren $a_1, \ldots, a_t \in \mathbb{Z}$, so dass $x = a_1 n_1 + \ldots + a_t n_t$. Definiere $b_1, \ldots, b_t$ durch $b_i := a_i$, $b_j := a_j - aa_i$ und $b_k := a_k$ (für $k \neq i, j$). Dann ist

$$\begin{aligned} & b_1 n_1 + \ldots + b_i(n_i + an_j) + \ldots + b_j n_j + \ldots + b_t n_t \\ = & a_1 n_1 + \ldots + a_i(n_i + an_j) + \ldots + (a_j - aa_i) n_j + \ldots + a_t n_t \\ = & a_1 n_1 + \ldots + a_i n_i + \ldots + (aa_i + a_j - aa_i) n_j + \ldots + a_t n_t \\ = & x, \end{aligned}$$

sprich $x \in J$.
Zu „$\supseteq$“: Sei $x = b_1 n_1 + \ldots + b_i(n_i + an_j) + \ldots + b_j n_j + \ldots + b_t n_t$ und definiere $a_i = b_i$, $a_j = b_j + ab_i$ und $a_k = b_k$ (für $k \neq i, j$). Dann rechnet man nach, dass $x = a_1 n_1 + \ldots + a_t n_t$ ist. □

Algorithmus 1.5.2 (Euklidischer Algorithmus)**.** Gegeben $n_1, \ldots, n_t \in \mathbb{Z}$ nicht alle 0. Der Algorithmus berechnet $d := \mathrm{ggT}(n_1, \ldots, n_t)$. Wende dazu, unter Verwendung von Lemma 1.5.1, die folgenden Operationen auf das Ideal $I = (n_1, \ldots, n_t)$ an:
Reduktionsschritte:

(1) Falls ein $n_i = 0$, streiche es aus der Liste. Wir dürfen ohne Einschränkung annehmen $n_1, \ldots, n_t \neq 0$
(2) Falls $n_i < 0$, ersetze es durch $-n_i$. Wir dürfen ohne Einschränkung $n_1, \ldots, n_t > 0$ annehmen.
(3) Sortiere die Zahlen so um, dass $n_1 \geq n_2 \geq \ldots \geq n_t$.
(4) Falls $n_i = n_{i+1}$, ersetze n_i durch $n_i - n_{i+1} = 0$ und streiche es aus der Liste. Wir dürfen daher $n_1 > n_2 > \ldots > n_t$ annehmen.

Nun wende folgende Iteration auf $n_1, \ldots, n_t$ an:

- Falls $t = 1$, dann sind wir fertig und $d = n_1$.
- Falls $t \geq 2$, dann dividiere n_1 durch n_t mit Rest. Wir finden also $q \in \mathbb{Z}$ und $r \in \{0, \ldots, n_t - 1\}$, so dass $n_1 = qn_t + r$. Dann ist $(n_1, \ldots, n_t) = (n_2, \ldots, n_t, r)$. Falls $r = 0$ ist, eliminiere es aus der Liste. Wiederhole die Iteration mit $n_2, \ldots, n_t, r$.

Diese Iteration terminiert nach endlich vielen Schritten, da in jeder Anwendung die Gesamtsumme $n_1 + \ldots + n_t$ verkleinert wird.

Beispiel 1.5.3. Bestimme $\mathrm{ggT}(51, 33, 21)$. Wir können direkt zur Iteration gehen.

- $51 = 2 \cdot 21 + 9$. Erhalte $33, 21, 9$.
- $33 = 3 \cdot 9 + 6$. Erhalte $21, 9, 6$.
- $21 = 3 \cdot 6 + 3$. Erhalte $9, 6, 3$. (Spätestens hier sehen wir was rauskommt; wir führen trotzdem den Algorithmus zu Ende aus.)
- $9 = 3 \cdot 3 + 0$. Erhalte $6, 3$.
- $6 = 2 \cdot 3 + 0$. Erhalte 3.

Also $\mathrm{ggT}(51, 33, 21) = 3$.

Lemma 1.5.4. *Seien $n_1, \ldots, n_t, m_1, \ldots, m_s \in \mathbb{Z}$ und $n_1, \ldots, n_t$ nicht alle 0. Dann gilt*

$$(n_1, \ldots, n_t, m_1, \ldots, m_s) = (\mathrm{ggT}(n_1, \ldots, n_t), m_1, \ldots, m_s).$$

Beweis. Sei $d := \mathrm{ggT}(n_1, \ldots, n_t)$. Unter Verwendung der Lemmata 1.4.5 und 1.3.9 sehen wir

$$\begin{aligned}(n_1, \ldots, n_t, m_1, \ldots, m_s) &= (n_1, \ldots, n_t) + (m_1, \ldots, m_s) \\ &= (d) + (m_1, \ldots, m_s) \\ &= (d, m_1, \ldots, m_s).\end{aligned}$$

□

Bemerkung 1.5.5. Seien $n_1, \ldots, n_t \in \mathbb{Z} \setminus \{0\}$. Nach Lemma 1.5.4 gilt

$$(n_1, \ldots, n_t) = (\mathrm{ggT}(n_1, \ldots, n_{t-1}), n_t)$$

und deshalb auch

$$\mathrm{ggT}(n_1, \ldots, n_t) = \mathrm{ggT}(\mathrm{ggT}(n_1, \ldots, n_{t-1}), n_t).$$

Sei $d := \mathrm{ggT}(n_1, \ldots, n_t)$ und $d' := \mathrm{ggT}(n_1, \ldots, n_{t-1})$. Seien $a_1, \ldots, a_{t-1} \in \mathbb{Z}$, so dass $d' = a_1 n_1 + \ldots + a_{t-1} n_{t-1}$ gemäß Bézouts Lemma. Seien $b, c \in \mathbb{Z}$, so dass $d = bd' + cn_t$, wiederum nach Bézout. Dann ist

$$d = bd' + cn_t = ba_1 n_1 + \ldots + ba_{t-1} n_{t-1} + cn_t.$$

Es genügt also tatsächlich induktiv die Koeffizienten aus Bézouts Lemma immer nur für zwei ganze Zahlen zu bestimmen.

Algorithmus 1.5.6 (Erweiterter euklidischer Algorithmus)**.** Seien $n, m \in \mathbb{N}$. Der Algorithmus liefert $\mathrm{ggT}(n, m)$ und Zahlen $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(n, m) = an + bm$.
Definiere $i := 1$ und

$$\begin{aligned} x_0 &:= 1 & y_0 &:= 0 & z_0 &:= n \\ x_1 &:= 0 & y_1 &:= 1 & z_1 &:= m. \end{aligned}$$

Schritt i: Seien x_i, y_i und z_i bereits bestimmt.
Falls $z_i = 0$, dann brich ab. In diesem Fall ist

$$\mathrm{ggT}(n, m) = z_{i-1} \qquad a = x_{i-1} \qquad b = y_{i-1}.$$

Falls $z_i \neq 0$, dann teile z_{i-1} durch z_i mit Rest. Erhalte $q_i \in \mathbb{Z}$ und $r_i \in \{0, \ldots, z_i - 1\}$, so dass $z_{i-1} = q_i z_i + r_i$. Definiere

$$x_{i+1} := x_{i-1} - q_i x_i \qquad y_{i+1} := y_{i-1} - q_i y_i \qquad z_{i+1} := r_i.$$

Fahre mit Schritt $i + 1$ fort.

Satz 1.5.7. *Der erweiterte euklidische Algorithmus bricht nach endlich vielen Schritten ab und liefert* $\mathrm{ggT}(n, m)$*, sowie* $a, b \in \mathbb{Z}$ *mit* $\mathrm{ggT}(n, m) = an + bm$.

Beweis. Zeige, dass das Verfahren abbricht. Dazu beobachten wir, dass für jedes $i \geq 1$ mit $z_i \neq 0$ nach Konstruktion gilt $z_{i+1} < z_i$.
Zeige, dass $z_{i-1} = \mathrm{ggT}(n, m)$ ist, falls $z_i = 0$ gilt. Zeige dazu per Induktion, dass für jedes $j \leq i$ gilt $\mathrm{ggT}(z_{j-1}, z_j) = \mathrm{ggT}(n, m)$.
$j = 1$. Gilt per Definition von z_0 und z_1.
$j \to j + 1$. Angenommen $\mathrm{ggT}(z_{j-1}, z_j) = \mathrm{ggT}(n, m)$. Nach Definition ist $z_{j-1} = q_j z_j + z_{j+1}$. Deshalb ist

$$\mathrm{ggT}(z_j, z_{j+1}) = \mathrm{ggT}(z_{j-1}, z_j) = \mathrm{ggT}(n, m).$$

Schließlich zum Beweis, dass $\mathrm{ggT}(n,m) = an + bm$ gilt. Dazu zeigen wir per Induktion, dass für alle $j \leq i$ gilt $z_j = x_j n + y_j m$.
$j = 0, j = 1$. Gelten per Definition.
$j \geq 2$. Angenommen die Behauptung gelten für $j-1$ und $j-2$. Wir berechnen

$$\begin{aligned} x_j n + y_j m &= (x_{j-2} - q_{j-1}x_{j-1})n + (y_{j-2} - q_{j-1}y_{j-1})m \\ &= \underbrace{x_{j-2}n + y_{j-2}m}_{=z_{j-2}} - q_{j-1}(\underbrace{x_{j-1}n + y_{j-1}m}_{=z_{j-1}}) \\ &= z_{j-2} - q_{j-1}z_{j-1} \\ &= z_j. \end{aligned}$$

□

Beispiel 1.5.8. Bestimme $\mathrm{ggT}(136, 51)$.

i	x_i	y_i	z_i	$z_{i-1} = q_i z_i + r_i$	q_i
0	1	0	136		
1	0	1	51	$136 = 2 \cdot 51 + 34$	2
2	1	-2	34	$51 = 1 \cdot 34 + 17$	1
3	-1	3	17	$34 = 2 \cdot 17 + 0$	2
4			0		

Also $\mathrm{ggT}(136, 51) = 17$, $a = -1$ und $b = 3$. Probe: $(-1) \cdot 136 + 3 \cdot 51 = 17$.

1.6. **Kleinstes gemeinsames Vielfaches.**

Definition 1.6.1. Seien $n_1, \ldots, n_t \in \mathbb{Z}$. Ein $v \in \mathbb{Z}$ heißt *gemeinsames Vielfaches* der $n_1, \ldots, n_t$, wenn $n_i \mid v$ (alle $i = 1, \ldots, t$).

Bemerkung 1.6.2. Seien $n_1, \ldots, n_t \in \mathbb{Z}$. Dann ist $(n_1) \cap \ldots \cap (n_t)$ die Menge der gemeinsamen Vielfachen von $n_1, \ldots, n_t$. Insbesondere ist die Menge der gemeinsamen Vielfachen ein Ideal nach Lemma 1.3.8.

Lemma 1.6.3. *Seien $n_1, \ldots, n_t \neq 0$. Dann ist $(n_1) \cap \ldots \cap (n_t) \cap \mathbb{N} \neq \emptyset$.*

Beweis. Es gilt $|n_1 \cdot \ldots \cdot n_t| \in (n_1) \cap \ldots \cap (n_t) \cap \mathbb{N}$. □

Definition 1.6.4. Seien $n_1, \ldots, n_t \in \mathbb{Z} \backslash \{0\}$. Das kleinste Element von $(n_1) \cap \ldots \cap (n_t) \cap \mathbb{N}$ heißt das *kleinste gemeinsame Vielfache* von $n_1, \ldots, n_t$ und wird mit $\mathrm{kgV}(n_1, \ldots, n_t)$ bezeichnet.

Lemma 1.6.5. *Seien $n_1, \ldots, n_t \in \mathbb{Z} \setminus \{0\}$. Sei $v := \mathrm{kgV}(n_1, \ldots, n_t)$. Dann ist*

$$(n_1) \cap \ldots \cap (n_t) = (v).$$

Beweis. Sei $I := (n_1) \cap \ldots \cap (n_t)$. Wir beobachten, dass $v \in I$ ist. Wir zeigen $I = (v)$.
Zu „$\subseteq$“: Sei $x \in I$, also x ein gemeinsames Vielfaches der $n_1, \ldots, n_t$. Führe Division mit Rest durch. Es gibt dann $q \in \mathbb{Z}$ und $r \in \{0, \ldots, v-1\}$, so dass $x = qv + r$. Dann ist $r = x - qv \in I$. Wäre $r \neq 0$, so wäre $r \in I \cap \mathbb{N}$ echt kleiner als v; das geht nicht. Also ist $x = qv \in (v)$.
Zu „$\supseteq$“: Sei $x \in (v)$, sagen wir $x = av$. Da $v \in I$ und I ein Ideal ist, folgt $x \in I$. □

Satz 1.6.6. *Seien $n, m \in \mathbb{Z} \setminus \{0\}$. Dann ist $\mathrm{ggT}(n,m) \cdot \mathrm{kgV}(n,m) = |n \cdot m|$.*

Beweis. Ohne Einschränkung seien $n, m > 0$. Sei $d := \mathrm{ggT}(n, m)$. Wir zeigen, dass

$$v := \frac{nm}{d}$$

das kleinste gemeinsame Vielfache von n und m ist. Zunächst ist d ein Teiler von n und m, also ist $v = n(m/d) = m(n/d)$ ein Vielfaches sowohl von n als auch von m. Sei nun $w \in \mathbb{N}$ ein weiteres gemeinsames Vielfaches von n und m. Dann gibt es $a, b \in \mathbb{Z}$ mit $w = an = bm$. Nach dem Lemma von Bézout existieren $r, s \in \mathbb{Z}$, so dass $d = rn + sm$. Multipliziere diese Identität mit a und erhalte

$$ad = r\underbrace{an}_{=bm} + sam = (\underbrace{rb + sa}_{=:c})m$$

Somit ist $a = c(m/d)$ und damit $w = an = c(m/d)n = cv$. Es gilt also $v \mid w$. Da $w > 0$ ist, folgt $v < w$. Daher ist v das kleinste gemeinsame Vielfache von n und m. $\square$

Bemerkung 1.6.7. Für mehr als 2 Zahlen gilt keine Vergleichbare Identität. So ist zum Beispiel $\mathrm{ggT}(2, 2, 2) \cdot \mathrm{kgV}(2, 2, 2) = 2 \cdot 2 = 4$.

2. Primfaktorzerlegung

2.1. Primzahlen.

Definition 2.1.1. Eine Zahl $p \in \mathbb{N} \setminus \{1\}$ heißt *Primzahl*, wenn ihre einzigen Teiler ± 1 und $\pm p$ sind. Mit $\mathbb{P}$ bezeichnen wir die Menge der Primzahlen.

Bemerkung 2.1.2. Die ersten paar Primzahlen sind $2, 3, 5, 7, 11, 13, 17, \ldots$.

Definition 2.1.3. Sei $a \in \mathbb{Z}$. Eine Primzahl p mit $p \mid a$ heißt ein *Primfaktor* von a.

Lemma 2.1.4. *Jedes $a \in \mathbb{Z} \setminus \{\pm 1\}$ hat einen Primfaktor.*

Beweis. Jede Primzahl ist ein Primfaktor von 0. Ohne Einschränkung sei also $a > 1$. Betrachte die Menge $M = \{d \in \mathbb{N} \setminus \{1\} \mid d \text{ teilt } a\}$. Dann ist $a \in M$, also insbesondere $M \neq \emptyset$. Sei p das kleinste Element von M. Angenommen p wäre keine Primzahl, so hätte p einen Teiler b mit $1 < b < p$. Dann wäre b aber auch ein Teiler von a und damit $b \in M$. Ein Widerspruch zur Minimalität von p. □

Satz 2.1.5. *Sei $p \in \mathbb{N} \setminus \{1\}$. Dann sind folgende Aussagen äquivalent:*

(1) p ist eine Primzahl.
(2) Sind $a, b \in \mathbb{Z}$, so dass $p \mid ab$, so folgt $p \mid a$ oder $p \mid b$.

Beweis. Zu „(1) $\Rightarrow$ (2)“: Seien $a, b \in \mathbb{Z}$ mit $p \mid ab$ und $p \nmid a$. Wir müssen zeigen, dass $p \mid b$. Weil $p \mid ab$ existiert ein $c \in \mathbb{Z}$ mit $cp = ab$. Wegen $p \nmid a$ folgt $\mathrm{ggT}(p, a) = 1$. Nach Bézouts Lemma finden wir also $r, s \in \mathbb{Z}$, so dass $1 = rp + sa$. Dann ist

$$b = brp + bsa = brp + scp = (br + sc)p$$

also $p \mid b$.
Zu „(2) $\Rightarrow$ (1)“: Sei $1 \leq d < p$ ein Teiler von p. Dann ist $p = cd$ für ein $c \in \mathbb{Z}$. Da $p \nmid d$, muss $p \mid c$ gelten. Andererseits gilt auch $c \mid p$. Daher ist $c = p$ und damit $d = 1$. □

Satz 2.1.6 (Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Seien $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen. Definieren wir $m := p_1 \cdot \ldots \cdot p_r + 1$. Nach Lemma 2.1.4, hat m einen Primfaktor p. Da $p_i \nmid m$ für alle $i = 1, \ldots, r$ gilt, folgt $p \notin \{p_1, \ldots, p_r\}$. □

2.2. Existenz der Primfaktorzerlegung.

Satz 2.2.1 (Primfaktorzerlegung)**.** *Sei $a \in \mathbb{N} \setminus \{1\}$.*

(1) Es gibt Primzahlen $p_1, \ldots, p_r$, so dass

$$a = p_1 \ldots p_r.$$

(2) Seien $p_1, \ldots, p_r$ und $q_1, \ldots, q_s$ Primzahlen, so dass

$$a = p_1 \ldots p_r = q_1 \ldots q_s.$$

Dann ist $r = s$ und, nach Umnummerieren der q_j's, gilt $p_i = q_i$ für $i = 1, \ldots, r$.

Beweis. (1) Beweis per Induktion nach $a \geq 2$. Der Induktionsanfang $a = 2$ ist klar. Im Induktionsschritt nehmen wir an, jedes $b < a$ mit $b \geq 2$ habe eine Primfaktorzerlegung. Nach Lemma 2.1.4 hat a einen Primfaktor p. Sei $b := a/p$. Dann ist entweder $b = 1$ und damit $a = p$ eine Primzahl (dann sind wir fertig), oder

$b \geq 2$. Im letzeren Fall gibt es nach Induktionsannahme eine Primfaktorzerlegung $b = p_2 \dots p_r$. Dann ist $a = p \cdot p_2 \dots p_r$.

(2) Wieder per Induktion nach $a \geq 2$. Der Induktionsanfang ist wiederum klar. Zum Induktionsschritt. Da $p_1 \dots p_r = q_1 \dots q_s$, folgt $p_1 \mid q_1 \dots q_s$. Nach Satz 2.1.5 folgt dann $p_1 \mid q_j$ für ein j. Nach Umnummerieren können wir annehmen $j = 1$, also $p_1 \mid q_1$. Da q_1 eine Primzahl ist, folgt $p_1 = q_1$ und damit auch $p_2 \dots p_r = q_2 \dots q_s =: b$. Nach Induktionssannahme ist deshalb $r - 1 = s - 1$ und, nach Umnummerieren, $p_2 = q_2, \dots, p_r = q_r$. □

Korollar 2.2.2 (Primfaktorzerlegung, zweite Formulierung)**.** *Zu jeder Zahl $a \in \mathbb{N} \setminus \{1\}$ gibt es eindeutig bestimmte Primzahlen $p_1 < \dots < p_r$ und eindeutig bestimmte Zahlen $n_1, \dots, n_r \in \mathbb{N}$, so dass*

$$a = p_1^{n_1} \dots p_r^{n_r}.$$

Korollar 2.2.3 (Primfaktorzerlegung, dritte Formulierung)**.** *Zu jeder Zahl $a \in \mathbb{N}$ gibt es eindeutig bestimmte Zahlen $n_p \in \mathbb{N}_0$ für alle $p \in \mathbb{P}$, so dass alle außer endlich vielen $n_p = 0$ sind und, so dass*

$$a = \prod_{p \in \mathbb{P}} p^{n_p}.$$

Definition 2.2.4. Die Darstellungen von a aus Satz 2.2.1 und den Korollaren 2.2.2 und 2.2.3 heißen *Primfaktorzerlegung* von a.

Bemerkung 2.2.5. Wir fassen $1 = \prod_{p \in \mathbb{P}} p^0$ auch als Primfaktorzerlegung auf.

Beispiel 2.2.6. $360 = 2^3 \cdot 3^2 \cdot 5$.

Lemma 2.2.7. *Seien $a, b \in \mathbb{N}$ und seien $a = \prod_{p \in \mathbb{P}} p^{n_p}$ und $b = \prod_{p \in \mathbb{P}} p^{m_p}$ ihre Primfaktorzerlegungen. Dann gilt $a \mid b$ genau dann wenn $n_p \leq m_p$ für alle $p \in \mathbb{P}$ ist.*

Beweis. Zu „$\Rightarrow$“: Gelte $a \mid b$. Sei $p \in \mathbb{P}$ mit $n_p \geq 1$. Dann folgt $p \mid b$ (also $m_p \geq 1$) und es gilt $(a/p) \mid (b/p)$. Induktiv sehen wir, dass $n_p - 1 \leq m_p - 1$ ist.
Zu „$\Leftarrow$“: Klar. □

Korollar 2.2.8. *Seien $a, b \in \mathbb{N}$ und seien $a = \prod_{p \in \mathbb{P}} p^{n_p}$ und $b = \prod_{p \in \mathbb{P}} p^{m_p}$ ihre Primfaktorzerlegungen. Dann gilt*

$$\mathrm{ggT}(a, b) = \prod_{p \in \mathbb{P}} p^{\min\{n_p, m_p\}}$$
$$\mathrm{kgV}(a, b) = \prod_{p \in \mathbb{P}} p^{\max\{n_p, m_p\}}.$$

Beweis. Nur für den ggT. Sei $d := \mathrm{ggT}(a, b)$ und sei $d = \prod_{p \in \mathbb{P}} p^{x_p}$ seine Primfaktorzerlegung. Nach Lemma 2.2.7 folgt $x_p \leq n_p$ und $x_p \leq m_p$. Andererseits ist $\prod_{p \in \mathbb{P}} p^{\min\{n_p, m_p\}}$ ein gemeinsamer Teiler von a und b (wieder wegen Lemma 2.2.7). Also muss $x_p = \min\{n_p, m_p\}$ sein. □

2.3. **Sieb des Eratosthenes.**

Lemma 2.3.1. *Sei $n \in \mathbb{N} \setminus \{1\}$ keine Primzahl. Dann gibt es einen Primfaktor p von n mit $p \leq \sqrt{n}$.*

Beweis. Da n nicht prim ist, existieren $x, y \in \mathbb{N} \setminus \{1\}$, so dass $n = xy$. Ohne Einschränkung gelte $x \leq y$. Dann ist $x^2 \leq xy = n$, also $x \leq \sqrt{n}$. Sei p ein Primfaktor von x. Dann ist p auch ein Primfaktor von n und es gilt $p \leq x \leq \sqrt{n}$. □

Algorithmus 2.3.2 (Sieb des Eratosthenes)**.** Sei $N \in \mathbb{N} \setminus \{1\}$. Der Algorithmus bestimmt alle Primzahlen zwischen 2 und N.

(1) Schreibe alle Zahlen $2, \ldots, N$ aufsteigend in eine Liste L.
(2) Lege eine leere Liste P an.
(3) Falls $L = \emptyset$, brich ab.
Falls $L \neq \emptyset$, dann wähle das kleinste Element p aus L. Speichere es in P.
(4) Streiche alle Vielfachen von p aus L. Fahre fort mit Schritt 3.

Am Ende des Algorithmus ist P die Liste aller Primzahlen zwischen $2, \ldots, N$.

Satz 2.3.3. *Das Sieb des Eratosthenes terminiert und bestimmt genau die Primzahlen zwischen 2 und N.*

Beweis. Da in jedem Durchlauf in dem $L \neq \emptyset$ ist mindestens ein Element gestrichen wird, muss der Algorithmus nach endlich vielen Schritten terminieren.
Wir zeigen, dass am Ende des Algorithmus $P = \{2, \ldots, N\} \cap \mathbb{P}$ gilt.
Zu „$\subseteq$“: Sei $p \in P$. Dann muss in einem Schritt p das kleinste Element von L sein. Dann ist p eine Primzahl, denn wäre sie keine, so wäre sie in einem früheren Schritt gestrichen worden.
Zu „$\supseteq$“: Sei p eine Primzahl zwischen 2 und N. Dann gilt in jedem Schritt: ist $q < p$ das kleinste Element von L, so gilt $q \nmid p$, also wird p in diesem Schritt nicht gestrichen. Somit ist in irgendwann p das kleinste Element von L und damit in P. □

Bemerkung 2.3.4. Beim Sieb von Eratosthenes reicht es die Schritte durchzuführen, bis das kleinste Element $p > \sqrt{N}$ ist. Dann ist wegen Lemma 2.3.1 jedes $n \in L$, das noch nicht gestrichen wurde eine Primzahl.

Beispiel 2.3.5. Hier ist das Resultat des Siebs des Eratosthenes für $N = 100$. Die durchgestrichenen Zahlen sind gestrichen und nicht in P. Die übrigen Zahlen sind in P.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

2.4. **Gauß-Klammer, b-adische Entwicklung und Primfaktorzerlegung von Fakultäten.**

Bemerkung 2.4.1. Für große Zahlen N ist es im Allgemeinen aufwendig die Primfaktorzerlegung zu bestimmen. Wenn man allerdings bereits eine Faktorisierung von N kennt, etwa $N = n_1 \dots n_t$, so muß für jeden Primfaktor p von N bereits gelten, dass p eines der n_i teilt. Das wenden wir auf Fakultäten an. Für $N = n! = 1 \cdot 2 \cdot \ldots \cdot n$ und eine Primzahl p mit $p \mid n!$ gibt es ein $m \leq n$, so dass $p \mid m$. Insbesondere gilt also $p \leq n$. Das Ziel dieses Abschnitts ist die Primfaktorzerlegung von $n!$ explizit zu bestimmen.

Definition 2.4.2. Sei $x \in \mathbb{R}$. Wir definieren die *Gauß-Klammer* $\lfloor x \rfloor$ von x als

$$\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}.$$

Bemerkung 2.4.3. Anschaulich ist $\lfloor x \rfloor$ die Abrundung von x, also die größte ganze Zahl die kleiner oder gleich x ist. Es gilt offensichtlich $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

Lemma 2.4.4. *Seien $n, b \in \mathbb{N}$. Dann sind aus $\{1, 2, \ldots, n\}$ genau $\lfloor n/b \rfloor$ Zahlen durch b teilbar.*

Beweis. Die durch b teilbaren Zahlen aus $\{1, \ldots, n\}$ sind genau $\{kb \mid k \in \mathbb{N},\ kb \leq n\}$ und $kb \leq n$ ist äquivalent zu $k \leq \lfloor n/b \rfloor$. □

Satz 2.4.5. *Sei $n \in \mathbb{N}$ und sei p eine Primzahl. Sei $m \in \mathbb{N}_0$ die größte Zahl, so dass $p^m \mid n!$. Dann gilt*

$$m = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

Beweis. Für $a \in \mathbb{N}$ sei $m(a) = \max\{k \in \mathbb{N}_0 \mid p^k \text{ teilt } a\}$. Also $m = m(n!)$. Dann ist $a = p^{m(a)} \cdot r_a$, wobei $p \nmid r_a$. Es gilt

$$\begin{aligned} n! &= p^m \cdot r_{n!} \\ n! &= 1 \cdot 2 \cdot \ldots \cdot n \\ &= \prod_{a=1}^{n} (p^{m(a)} \cdot r_a) \\ &= p^{\sum_{a=1}^{n} m(a)} \cdot \prod_{a=1}^{n} r_a \end{aligned}$$

und deshalb ist $m = \sum_{a=1}^{n} m(a)$. Nun ist

$$\begin{aligned} \{a \in \{1, \ldots, n\} \mid p \text{ teilt } a\} &= \{a \in \{1, \ldots, n\} \mid m(a) \geq 1\} \qquad \text{Anzahl: } \left\lfloor \frac{n}{p} \right\rfloor \\ \{a \in \{1, \ldots, n\} \mid p^2 \text{ teilt } a\} &= \{a \in \{1, \ldots, n\} \mid m(a) \geq 2\} \qquad \text{Anzahl: } \left\lfloor \frac{n}{p^2} \right\rfloor \\ &\vdots \end{aligned}$$

Damit gilt

$$m = \sum_{a=1}^{n} m(a) = \sum_{i=1}^{\infty} |\{a \in \{1, \ldots, n\} \mid m(a) \geq i\}| = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

□

Korollar 2.4.6. *Sei $n \in \mathbb{N}$. Dann ist die Primfaktorzerlegung von $n!$ gegeben durch $n! = \prod_{p \in \mathbb{P}} p^{m_p}$, wobei $m_p = \sum_{i=1}^{\infty} \lfloor n/(p^i) \rfloor$ ist. Insbesondere ist $m_p = 0$, falls $p > n$ ist.*

Lemma 2.4.7 (Existenz der b-adischen Entwicklung)**.** *Sei $b \in \mathbb{N} \setminus \{1\}$. Zu jeder Zahl $n \in \mathbb{N}_0$ existieren eindeutig bestimmte $r_0, r_1, r_2, \ldots \in \{0, \ldots, b-1\}$, so dass alle außer endlich viele $r_i = 0$ und so dass*

$$n = \sum_{i=0}^{\infty} r_i b^i.$$

Beweis. Zur Existenz: Induktion über n.
$n = 0$. Es gilt $0 = \sum_{i=0}^{\infty} 0 \cdot b^i$.
$n > 0$. Laut Induktionsannahme besitze jedes $m < n$ eine b-adische Entwicklung. Führe Division von n durch b mit Rest durch. Erhalte $n = qb + r_0$ für eindeutig bestimmte $q \in \mathbb{N}$ und $r_0 \in \{0, \ldots, b-1\}$. Nach Induktionsannahme existieren $r_1, r_2, \ldots \in \{0, \ldots, b-1\}$, nur endlich viele $\neq 0$, so dass $q = \sum_{i=0}^{\infty} r_{i+1} b^i$. Dann ist

$$n = r_0 + qb = r_0 + \sum_{i=0}^{\infty} r_{i+1} b^{i+1} = \sum_{i=0}^{\infty} r_i b^i.$$

Zur Eindeutigkeit: Wieder Induktion über n.
$n = 0$. Klar.
$n > 0$. Angenommen die Eindeutigkeit gelte für jedes $m < n$. Seien $r_0, r_1, r_2, \ldots \in \{0, \ldots, b-1\}$ und $s_0, s_1, s_2, \ldots \in \{0, \ldots, b-1\}$, jeweils nur endlich viele $\neq 0$, so dass $n = \sum_{i=0}^{\infty} r_i b^i = \sum_{i=0}^{\infty} s_i b^i$. Es gilt dann

$$n = r_0 + b(\sum_{i=i}^{\infty} r_i b^{i-1}) = s_0 + b(\sum_{i=1}^{\infty} s_i b^{i-1}),$$

also sind beides Divisionen von n durch b mit Rest. Da die Division mit Rest eindeutig ist, folgt $r_0 = s_0$ und $\sum_{i=i}^{\infty} r_i b^{i-1} = \sum_{i=1}^{\infty} s_i b^{i-1} =: m$. Es gilt $m < n$. Da die Eindeutigkeit für m nach Induktionsannahme gilt, folgt $r_i = s_i$ für alle $i = 1, 2, \ldots$. □

Definition 2.4.8. Die Darstellung von n aus dem obigen Lemma nennt man die *b-adische Entwicklung* von n.

Bemerkung 2.4.9. Der Beweis liefert einen Algorithmus zur Bestimmung der b-adischen Entwicklung. Wir erhalten $r_0, r_1, r_2, \ldots$ durch sukzessive Division durch b mit Rest:

$$\begin{aligned} n &= q_0 b + r_0 \\ q_0 &= q_1 b + r_1 \\ q_1 &= q_2 b + r_2 \\ &\vdots \end{aligned}$$

Dieses Verfahren bricht ab, wenn $q_i = 0$ wird.

Beispiel 2.4.10. Sei $b = 3$ und $n = 100$.

$$\begin{aligned} 100 &= 33 \cdot 3 + 1 \\ 33 &= 11 \cdot 3 + 0 \\ 11 &= 3 \cdot 3 + 2 \\ 3 &= 1 \cdot 3 + 0 \\ 1 &= 0 \cdot 3 + 1. \end{aligned}$$

Also $100 = 1 \cdot 3^0 + 0 \cdot 3^1 + 2 \cdot 3^2 + 0 \cdot 3^3 + 1 \cdot 3^4$.

Definition 2.4.11. Sei $b \in \mathbb{N} \setminus \{1\}$ und sei $n \in \mathbb{N}_0$ mit b-adischer Entwicklung $n = \sum_{i=0}^{\infty} r_i b^i$. Wir definieren

$$\begin{aligned} s_b(n) &:= \sum_{i=0}^{\infty} r_i \\ a_b(n) &:= \sum_{i=0}^{\infty} (-1)^i r_i. \end{aligned}$$

Man nennt $s_b(n)$ die *b-adische Quersumme* von n und $a_b(n)$ die *b-adische alternierende Summe* von n.

Beispiel 2.4.12. (1) $s_3(100) = 1+0+2+0+1 = 5$ und $a_3(100) = 1-0+2-0+1 = 5$.
(2) $s_{10}(1000) = 0 + 0 + 0 + 1 = 1$ und $a_{10}(1000) = 0 - 0 + 0 - 1 = -1$.

Satz 2.4.13. *Sei $n \in \mathbb{N}$, sei p eine Primzahl und sei $m \in \mathbb{N}_0$ die größte Zahl, so dass $p^m \mid n!$. Dann gilt*

$$m = \frac{n - s_p(n)}{p - 1}.$$

Beweis. Wir wissen bereits aus Satz 2.4.5, dass $m = \sum_{j=1}^{\infty} \lfloor n/(p^j) \rfloor$ ist. Sei $n = \sum_{i=0}^{\infty} r_i p^i$ die p-adische Entwicklung von n. Dann ist

$$\begin{aligned} \frac{n}{p} &= \frac{r_0}{p} + \sum_{i=1}^{\infty} r_i p^{i-1} \\ \frac{n}{p^2} &= \frac{r_0 + r_1 p}{p^2} + \sum_{i=2}^{\infty} r_i p^{i-2} \\ &\vdots \\ \frac{n}{p^j} &= \frac{r_0 + r_1 p + \ldots + r_{j-1} p^{j-1}}{p^j} + \sum_{i=j}^{\infty} r_i p^{i-j} \end{aligned}$$

Da $r_i \leq p-1$ sind, folgt

$$\begin{aligned} r_0 + r_1 p + \ldots + r_{j-1} p^{j-1} &\leq (p-1) + (p-1)p + \ldots + (p-1)p^{j-1} \\ &= (p-1)(1 + p + \ldots + p^{j-1}) \\ &= (p-1)\frac{p^j - 1}{p-1} \\ &= p^j - 1, \end{aligned}$$

und deshalb ist

$$\left\lfloor \frac{n}{p^j} \right\rfloor = \sum_{i=j}^{\infty} r_i p^{i-j}.$$

Wir berechnen

$$\begin{aligned} m &= \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor \\ &= \sum_{j=1}^{\infty} \sum_{i=j}^{\infty} r_i p^{i-j} \\ &= r_1 + r_2 p + r_3 p^2 + r_4 p^3 + \ldots \\ &\qquad + r_2 \quad + r_3 p \quad + r_4 p^2 + \ldots \\ &\qquad\qquad + r_3 \quad + r_4 p \quad + \ldots \\ &\qquad\qquad\qquad + r_4 \quad + \ldots \\ &\qquad\qquad\qquad\qquad + \ldots \\ &= r_1 + r_2(1+p) + r_3(1+p+p^2) + r_4(1+p+p^3) + \ldots \\ &= r_1 \frac{p-1}{p-1} + r_2 \frac{p^2-1}{p-1} + r_3 \frac{p^3-1}{p-1} + r_4 \frac{p^4-1}{p-1} + \ldots \\ &= \frac{(r_0 + r_1 p + r_2 p^2 + r_3 p^3 + \ldots) - (r_0 + r_1 + r_2 + r_3 + \ldots)}{p-1} \\ &= \frac{n - s_p(n)}{p-1}. \end{aligned}$$

□

Korollar 2.4.14. *Sei $n \in \mathbb{N}$. Dann ist*

$$n! = \prod_{p \in \mathbb{P}} p^{\frac{n - s_p(n)}{p-1}}.$$

Beispiel 2.4.15. Die größte Zahl m, so dass $3^m \mid 100!$ ist $m = \frac{100 - s_3(100)}{3-1} = \frac{96}{2} = 48$.

3. Kongruenzen

3.1. Äquivalenzrelationen.

Definition 3.1.1. Sei X eine Menge. Sei $R \subseteq X \times X$ eine Teilmenge. Für $x, y \in X$ schreiben wir $x \sim_R y$, falls $(x, y) \in R$. Wir nennen R eine *Äquivalenzrelation*, wenn folgende Axiome gelten:

(1) Reflexivität: Für alle $x \in X$ gilt $x \sim_R x$.
(2) Symmetrie: Für alle $x, y \in X$ mit $x \sim_R y$ gilt auch $y \sim_R x$.
(3) Transitivität: Für alle $x, y, z \in X$, so dass $x \sim_R y$ und $y \sim_R z$ gelten, folgt $x \sim_R z$.

Definition 3.1.2. Sei R eine Äquivalenzrelation auf X. Eine Teilmenge $K \subseteq X$ heißt *Äquivalenzklasse* bezüglich R, wenn gilt:

(1) $K \neq \emptyset$
(2) Für alle $x, y \in K$ gilt $x \sim_R y$.
(3) Für alle $x \in K$ und alle $y \in X$ mit $x \sim_R y$ ist $y \in K$.

Mit X/R bezeichnen wir die Menge der Äquivalenzklassen bezüglich R.

Lemma 3.1.3. *Sei R eine Äquivalenzrelation auf X.*

(1) Für jedes $x \in X$ ist $[x]_R := \{y \in X \mid x \sim_R y\}$ eine Äquivalenzklasse bezüglich R.
(2) Ist K eine Äquivalenzklasse und $x \in K$, so ist $K = [x]_R$.
(3) Sind K, K' Äquivalenzklassen und $K \cap K' \neq \emptyset$, so ist $K = K'$.

Insbesondere ist $X = \bigcup_{K \in X/R} K$ und diese Vereinigung ist disjunkt.

3.2. Kongruenz modulo m.

Definition 3.2.1. Sei $m \in \mathbb{N}_0$. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen *kongruent modulo m*, symbolisch $a \equiv b \pmod{m}$, wenn $m \mid b - a$.

Bemerkung 3.2.2. Für $a, b \in \mathbb{Z}$ gilt genau dann $a \equiv b \pmod{m}$, wenn $b - a$ im Ideal $m\mathbb{Z} = (m)$ liegt.

Bemerkung 3.2.3. Es gilt $a \equiv b \pmod{0}$ genau dann wenn $a = b$ und stets gilt $a \equiv b \pmod{1}$.

Lemma 3.2.4. *Sei $m \in \mathbb{N}_0$. Die Relation Kongruenz modulo m ist eine Äquivalenzrelation auf $\mathbb{Z}$.*

Beweis. Zeige, dass Kongruenz reflexiv, symmetrisch und transitiv ist.

- Reflexivität: Sei $a \in \mathbb{Z}$. Da $m \mid a - a = 0$, folgt $a \equiv a \pmod{m}$.
- Symmetrie: Seien $a, b \in \mathbb{Z}$ und es gelte $a \equiv b \pmod{m}$. Das bedeutet $m \mid b - a$. Dann folgt aber auch, dass $m \mid a - b = -(b - a)$ und damit $b \equiv a \pmod{m}$.
- Transitivität: Seien $a, b, c \in \mathbb{Z}$ und gelte $a \equiv b \pmod{m}$, sowie $b \equiv c \pmod{m}$. Wir wollen zeigen, dass $a \equiv c \pmod{m}$ gilt. Es gilt $m \mid b - a$, sowie $m \mid c - b$. Dann teilt m aber auch die Summe $(c - b) + (b - a) = c - a$. Somit gilt $a \equiv c \pmod{m}$. $\square$

Bemerkung 3.2.5. Sei $m \in \mathbb{N}_0$ und $a \in \mathbb{Z}$. Eine Äquivalenzklasse bezüglich Kongruenz modulo m nennt man Restklasse modulo m. Die Restklase von a modulo m ist die Menge

$$\{b \in \mathbb{Z} \mid a \equiv b \pmod{m}\} = \{a + rm \mid r \in \mathbb{Z}\}.$$

Wir bezeichnen deshalb die Restklasse von a mit $a + m\mathbb{Z}$. Die Restklasse von 0 ist also das Ideal $m\mathbb{Z}$.
Die Menge der Restklassen modulo m werde mit $\mathbb{Z}/m\mathbb{Z}$ bezeichnet. Falls $m > 0$, ist $\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\}$.

Lemma 3.2.6. *Seien $m \in \mathbb{N}_0$ und $a, a', b, b' \in \mathbb{Z}$. Gelte $a \equiv b \pmod{m}$ und $a' \equiv b' \pmod{m}$. Dann gelten auch:*

(1) $a + a' \equiv b + b' \pmod{m}$
(2) $aa' \equiv bb' \pmod{m}$

Beweis. Es gilt $b - a, b' - a' \in m\mathbb{Z}$.

(1) Da $m\mathbb{Z}$ ein Ideal ist, liegt auch $(b-a) + (b'-a') = (b+b') - (a-a')$ in $m\mathbb{Z}$. Das beweist (1).
(2) Es gilt

$$bb' - aa' = bb' - ba' + ba' - aa' = b(b' - a') + (b - a)a' \in m\mathbb{Z}$$

denn $m\mathbb{Z}$ ist ein Ideal. Also folgt (2). □

Lemma 3.2.7 (Teilbarkeitstests)**.** *Sei $m \in \mathbb{N}$ und $b \in \mathbb{N} \setminus \{1\}$, so dass $b \equiv 1 \pmod{m}$. Sei $n \in \mathbb{N}_0$. Genau dann ist n durch m teilbar, wenn die b-adische Quersumme $s_b(n)$ durch m teilbar ist.*

Beweis. Sei $n = \sum_{i=0}^{\infty} r_i b^i$ die b-adische Entwicklung. Da $b \equiv 1 \pmod{m}$, folgt aus Lemma 3.2.6, dass auch $b^i \equiv 1 \pmod{m}$ gilt. Wiederum mit Lemma 3.2.6 ist

$$n = \sum_{i=0}^{\infty} r_i b^i \equiv \sum_{i=0}^{\infty} r_i = s_b(n) \pmod{m}.$$

□

Beispiel 3.2.8. Das vorige Lemma zeigt, dass eine Zahl $n \in \mathbb{N}_0$ genau dann durch 3 bzw. 9 teilbar ist, wenn ihre (10-adische) Quersumme durch 3 bzw. 9 teilbar ist.

3.3. **Kleiner Satz von Fermat.**

Lemma 3.3.1. *Sei p eine Primzahl. Seien $a, b \in \mathbb{Z}$. Dann gilt $(a+b)^p \equiv a^p + b^p \pmod{p}$.*

Beweis. Wir berechnen mit der binomischen Formel

$$(*) \qquad (a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + b^p.$$

Für $i \in \{1, \ldots, p-1\}$ gilt

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}.$$

Da $p \mid p!$, aber $p \nmid i!$ und $p \nmid (p-i)!$, ist p ein Teiler von $\binom{p}{i}$. Mit anderen Worten $\binom{p}{i} \equiv 0 \pmod{p}$. Damit fällt die mittlere Summe in der Gleichung (*) weg und die Behauptung folgt. □

Satz 3.3.2 (Kleiner Satz von Fermat)**.** *Sei p eine Primzahl und $a \in \mathbb{Z}$. Stets gilt $a^p \equiv a$ (mod p).*

Beweis. Wir unterscheiden die Fälle $a \geq 0$ und $a < 0$.
Zunächst sei $a \geq 0$. Beweise die Behauptung per Induktion nach a. Für $a = 0$ ist die Behauptung klar. Angenommen die Aussage gelte für a. Wir wollen sie für $a+1$ zeigen. Wir berechnen

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$$

nach Lemma 3.3.1 und der Induktionsannahme.
Nun sei $a < 0$. Dann ist $-a > 0$, also gilt $(-a)^p \equiv -a \pmod{p}$ und daraus folgt

$$a^p \equiv (-1)^{p+1} a \pmod{p}$$

Ist p ungerade, so ist $(-1)^{p+1}a = a$ und die Behauptung ist gezeigt. Es bleibt der Fall $p = 2$. Dort erhalten wir $a^2 \equiv -a \pmod{2}$. Aber $a \equiv -a \pmod{2}$, also folgt die Behauptung auch hier. □

Korollar 3.3.3. *Sei p eine Primzahl und $a \in \mathbb{Z}$ sei nicht durch p teilbar. Dann gilt $a^{p-1} \equiv 1$ (mod p).*

Beweis. Nach dem kleinen Satz von Fermat ist p ein Teiler von $a^p - a = a(a^{p-1} - 1)$. Da $p \nmid a$ und p eine Primzahl ist, muss $p \mid (a^{p-1} - 1)$ gelten. □

3.4. **Lösbarkeit von linearen Kongruenzen.**

Lemma 3.4.1. *Seien $a, x, y \in \mathbb{Z}$ und $m \in \mathbb{N}$. Sei $d := \mathrm{ggT}(a, m)$. Genau dann ist $ax \equiv ay$ (mod m), wenn $x \equiv y$ (mod m/d).*

Beweis. Seien $m' := m/d$ und $a' := a/d$.
Zu „$\Rightarrow$“: Es gelte $ax \equiv ay \pmod{m}$, also $a(y-x) \in m\mathbb{Z}$. Es gibt also ein $z \in \mathbb{Z}$, so dass

$$da'(y-x) = a(y-x) = mz = dm'z$$

Dann ist auch $a'(y-x) = m'z$. Es gilt $\mathrm{ggT}(a', m') = 1$. Also existieren nach dem Lemma von Bézout Zahlen $u, v \in \mathbb{Z}$, so dass $ua' + vm' = 1$. Also

$$\begin{aligned} y - x &= (ua' + vm')(y-x) \\ &= ua'(y-x) + vm'(y-x) \\ &= um'z + vm'(y-x) \\ &= m'(uz + v(y-x)) \in m'\mathbb{Z} \end{aligned}$$

und deswegen gilt $x \equiv y \pmod{m'}$.
Zu „$\Leftarrow$“: Gelte $x \equiv y \pmod{m'}$. Dann ist $y - x = m'z$ für ein $z \in \mathbb{Z}$. Also ist

$$ay - ax = a(y-x) = a'dm'z = a'mz \in m\mathbb{Z}$$

und somit $ax \equiv ay \pmod{m}$. □

Satz 3.4.2. *Seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Sei $d := \mathrm{ggT}(a, m)$.*

(1) Genau dann gibt es ein $x \in \mathbb{Z}$, so dass $ax \equiv b \pmod{m}$, wenn $d \mid b$.
(2) Falls $d \mid b$, so ist $\{x \in \mathbb{Z} \mid ax \equiv b \pmod{m}\}$ eine Restklasse modulo m/d.

Beweis. Seien $m' := m/d$ und $a' := a/d$.

(1) Zu „$\Rightarrow$“: Gelte $ax \equiv b \pmod{m}$. Dann gibt es ein $z \in \mathbb{Z}$ mit $ax - b = mz$. Also $da'x - b = dm'z$ und damit
$$b = d(a'x - m'z).$$
Zu „$\Leftarrow$“: Gelte $d \mid b$. Sei $b' := b/d$. Es gilt $\mathrm{ggT}(a', m') = 1$. Nach dem Lemma von Bézout existieren $u, v \in \mathbb{Z}$ mit $ua' + vm' = 1$. Dann ist $b' = ua'b' + vm'b'$. Das stellen wir um zu $a'ub' = b' - vm'b'$. Multiplizieren wir diese Gleichung mit d, so erhalten wir
$$aub' = b - vmb' \equiv b \pmod{m}$$
also ist $x := ub'$ eine Lösung.

(2) Da $d \mid b$ gibt es nach (1) ein $x \in \mathbb{Z}$ mit $ax \equiv b \pmod{m}$. Sei $y \in \mathbb{Z}$.
Falls $ay \equiv b \pmod{m}$ gilt, so ist $ax \equiv ay \pmod{m}$. Das ist nach Lemma 3.4.1 äquivalent zu $x \equiv y \pmod{m'}$, also ist $y \in x + m'\mathbb{Z}$.
Ist umgekehrt $y \in x + m'\mathbb{Z}$, so gilt $x \equiv y \pmod{m'}$, was nach 3.4.1 äquivalent ist zu $ax \equiv ay \pmod{m}$. Da $ax \equiv b \pmod{m}$, folgt deshalb auch $ay \equiv b \pmod{m}$. □

Algorithmus 3.4.3. Der Beweis liefert einen Algorithmus zur Bestimmung der Lösungsmenge L der linearen Kongruenz $ax \equiv b \pmod{m}$.

(1) Bestimme $d = \mathrm{ggT}(a, m)$, sowie $u, v \in \mathbb{Z}$ mit $ua + vm = d$ mithilfe des erweiterten Euklidischen Algorithmus.
(2) Falls $d \nmid b$, so ist $L = \emptyset$.
Falls $d \mid b$, ist $x := ub/d$ eine spezielle Lösung. Die Lösungsmenge der Kongruenz ist $L = x + (m/d)\mathbb{Z}$.

Beispiel 3.4.4. Wir bestimmen die Lösungsmenge von $22x \equiv 14 \pmod{100}$.

(1) Erweiterter Euklidischer Algorithmus:

i	x_i	y_i	z_i	$z_{i-1} = q_i z_i + r_i$	q_i
0	1	0	100		
1	0	1	22	$100 = 4 \cdot 22 + 12$	4
2	1	-4	12	$22 = 1 \cdot 12 + 10$	1
3	-1	5	10	$12 = 1 \cdot 10 + 2$	1
4	2	-9	2	$10 = 5 \cdot 2 + 0$	5
5			0		

Also $\mathrm{ggT}(100, 22) = 2 = 2 \cdot 100 + (-9) \cdot 22$. Also $d = 2$, $u = -9$ und $v = 2$.

(2) Da $2 \mid 14$ ist die Kongruenz lösbar. Eine spezielle Lösung ist $x = (-9) \cdot 14/2 = -63$. Erhalte $L = -63 + 50\mathbb{Z} = -13 + 50\mathbb{Z}$.
Probe: $22 \cdot (-13) = -286 \equiv 14 \pmod{100}$.

Beispiel 3.4.5. In der chromatischen Tonleiter besteht eine Oktave aus 12 Halbtonschritten (siehe Abbildung 1). Von C nach Fis sind es 6 Halbtonschritte. Eine Quinte

[1]Quelle: Public Domain, https://commons.wikimedia.org/w/index.php?curid=543460

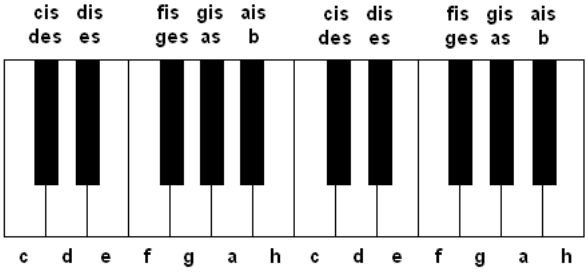

Abbildung 1. Tonbelegung Tastatur mit mitteltöniger Stimmung[1]

umfasst 7 Halbtonschritte. Wie viele Quinten muss man auf dem Klavier greifen, um von C zu einem Fis zu gelangen? Das kann man als Kongruenzgleichung formulieren:

$$7x \equiv 6 \pmod{12}$$

Es gilt $\mathrm{ggT}(7, 12) = 1$ und $1 \mid 6$, also ist die Gleichung lösbar. Wir erhalten mit erweitertem Euklidischen Algorithmus $1 = (-5) \cdot 7 + 3 \cdot 12$. Dann ist $x = (-5) \cdot 6 = -30$ eine spezielle Lösung und $L = -30 + 12\mathbb{Z} = 6 + 12\mathbb{Z}$ die Lösungsmenge. Also kommt man mit $6 + 12k$ Quinten ($k \in \mathbb{Z}$) von C zu einem Fis.
Eine große Terz umfasst 4 Halbtonschritte. Wir fragen uns, ob man mit großen Terzen von C nach Fis gelangen kann. Das führt zur Kongruenzgleichung

$$4x \equiv 6 \pmod{12}$$

Da $\mathrm{ggT}(4, 12) = 4$ ist und $4 \nmid 6$, ist das nicht möglich. Das sieht man auch anschaulich sehr leicht.

4. Gruppen und Ringe

4.1. Gruppen.

Definition 4.1.1. Eine *Gruppe* besteht aus einer Menge G und einer Abbildung $* : G \times G \to G,\ (a,b) \mapsto a * b$, so dass folgende Eigenschaften gelten:

(G.1) Assoziativität: $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$.
(G.2) Neutrales Element: Es gibt ein $e \in G$, so dass $a * e = e * a = a$ für jedes $a \in G$.
(G.3) Inverse: Sei e ein neutrales Element von G. Dann gibt es zu jedem $a \in G$ ein $\tilde{a} \in G$ mit $\tilde{a} * a = a * \tilde{a} = e$.

Falls zusätzlich $a * b = b * a$ für alle $a, b \in G$ gilt, nennt man G eine *abelsche Gruppe.*

Bemerkung 4.1.2. Sei $(G, *)$ eine Gruppe.

(1) Eine Gruppe besitzt genau ein neutrales Element. Wir schreiben manchmal e_G dafür.
(2) Zu jedem Element $a \in G$ gibt es genau ein inverses Element. Wir bezeichnen es mit a^{-1}.

Bemerkung 4.1.3. Schreibweisen für Gruppen.

(1) Oft werden Gruppen multiplikativ geschrieben, das bedeutet wir schreiben $\cdot$ statt $*$ und 1 statt e.
(2) Abelsche Gruppen werden oft additiv geschrieben, das heißt wir schreiben $+$ statt $*$, 0 statt e und $-a$ statt a^{-1}.

Definition 4.1.4. Seien $(G, *_G)$ und $(H, *_H)$ Gruppen. Ein *Gruppenhomomorphismus* ist eine Abbildung $f : G \to H$, so dass für alle $a, b \in G$ gilt

$$f(a *_G b) = f(a) *_H f(b).$$

Ein bijektiver Gruppenhomomorphismus heißt *Gruppenisomorphismus.*

Lemma 4.1.5. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt*

(1) $f(e_G) = e_H$
(2) Für alle $a \in G$ ist $f(a^{-1}) = f(a)^{-1}$.

Beweis.

(1) Es gilt $e_H * f(e_G) = f(e_G) = f(e_G * e_G) = f(e_G) * f(e_G)$. Multipliziere mit dem Inversen von $f(e_G)$ von rechts und erhalte $e_H = f(e_G)$.
(2) Wir haben $f(a) * f(a^{-1}) = f(a * a^{-1}) = f(e_G) = e_H$. Nun multipliziere beide Seiten von links mit $f(a)^{-1}$ und erhalte die Behauptung. □

4.2. Ringe.

Definition 4.2.1. Ein *Ring* besteht aus einer Menge A zusammen mit zwei Abbildungen $+ : A \times A \to A,\ (a,b) \mapsto a + b$ und $\cdot : A \times A \to A,\ (a,b) \mapsto a \cdot b$, so dass folgende Axiome gelten:

(R.1) $(R, +)$ ist eine abelsche Gruppe; ihr neutrales Element werde mit $0 = 0_A$ bezeichnet.
(R.2) Assoziativität der Multiplikation: Für alle $a, b, c \in A$ gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(R.3) Distributivgesetze: Für alle $a, b, c \in A$ gelten

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c,$$

wobei die Konvention „Punkt vor Strich“ gelte.

(R.4) Einselement: Es gibt ein Element $1 \in A$, so dass für alle $a \in A$ gilt $1 \cdot a = a \cdot 1 = a$.

(R.5) Kommutativität der Multiplikation: Für alle $a, b \in A$ gilt $a \cdot b = b \cdot a$.

Bemerkung 4.2.2. Ein Element 1 wie im Axiom (R.4) ist eindeutig bestimmt. Es heißt das Einselement von A. Wir schreiben manchmal auch 1_A.

Bemerkung 4.2.3. In einem Ring A gilt $a \cdot 0 = 0 \cdot a = 0$ für jedes $a \in A$.

Bemerkung 4.2.4. Der Begriff Ring ist in der Literatur nicht einheitlich definiert. Oft werden von einem Ring nur die Axiome (R.1)–(R.4) verlangt, manchmal sogar nur (R.1)–(R.3).

Beispiel 4.2.5. Einige Beispiele für Ringe.

(1) $\mathbb{Z}$ ist mit der Addition und Multiplikation von ganzen Zahlen ein Ring.

(2) $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind mit der Addition und Multiplikation von rationalen/rellen/komplexen Zahlen ebenfalls Ringe.

(3) Sei $I \subseteq \mathbb{R}$ ein offenes Intervall. Sei $\mathscr{C}(I) := \{f : I \to \mathbb{R} \mid f \text{ stetig}\}$. Auf $\mathscr{C}(I)$ definieren wir die Operationen $+ : \mathscr{C}(I) \times \mathscr{C}(I) \to \mathscr{C}(I)$ und $\cdot : \mathscr{C}(I) \times \mathscr{C}(I) \to \mathscr{C}(I)$ durch

$$f + g : I \to \mathbb{R},\ x \mapsto f(x) + g(x)$$
$$f \cdot g : I \to \mathbb{R},\ x \mapsto f(x) \cdot g(x).$$

Dann sind $+$ und $\cdot$ wohldefiniert, denn $f + g$ und $f \cdot g$ sind stetige Abbildungen. So wird $\mathscr{C}(I)$ zu einem Ring. (Axiome verifizieren!)

(4) Die Menge $2\mathbb{Z}$ der geraden ganzen Zahlen mit der Addition und Multiplikation von ganzen Zahlen erfüllt die Axiome (R.1)–(R.3) und (R.5), nicht aber (R.4).

(5) Sei $n \geq 2$. Die Menge $M_{n \times n}(\mathbb{R})$ mit der üblichen Addition und der Matrixmultiplikation erfüllt die Axiome (R.1)–(R.4), aber nicht (R.5).

Bemerkung 4.2.6. Die Menge $\{0\}$ ist mit den eindeutig bestimmten Abbildungen $+, \cdot : \{0\} \times \{0\} \to \{0\}$ ein Ring, der sogenannte Nullring. Im Nullring gilt $1 = 0$. Ist umgekehrt A ein Ring in dem $1_A = 0_A$ gilt, so ist A der Nullring.

Definition 4.2.7. Seien A und B Ringe. Ein *Ringhomomorphismus* ist eine Abbildung $f : A \to B$, so dass für alle $a, a' \in A$ gelten:

(H.1) $f(a + a') = f(a) + f(a')$

(H.2) $f(a \cdot a') = f(a \cdot a')$

(H.3) $f(1_A) = 1_B$.

Ein bijektiver Ringhomomorphismus heißt *Ringisomorphismus*.

Bemerkung 4.2.8. Da ein Ringhomomorphismus $f : A \to B$ insbesondere ein Gruppenhomomorphismus $f : (A, +) \to (B, +)$ ist, folgt $f(0_A) = 0_B$ aus Lemma 4.1.5.

Beispiel 4.2.9. Für Ringhomomorphismen.

(1) Die Teilmengeninklusionen $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$ sind Ringhomomorphismen.
(2) Sei I ein Intervall und sei $x_0 \in I$. Die Abbildung $\mathscr{C}(I) \to \mathbb{R}$ definiert durch $f \mapsto f(x_0)$ ist ein Ringhomomorphismus.

Definition 4.2.10. Sei $f : A \to B$ ein Ringhomomorphismus. Man nennt $\ker(f) := \{a \in A \mid f(a) = 0\}$ den *Kern* von f und $\operatorname{im}(f) := f(A)$ das *Bild* von f.

Lemma 4.2.11. *Genau dann ist ein Rinhomomorphismus $f : A \to B$ injektiv, wenn $\ker(f) = \{0\}$ ist.*

Beweis. Zu „$\Rightarrow$“: Klar.
Zu „$\Leftarrow$“: Gelte $\ker(f) = \{0\}$. Seien $a, a' \in A$ mit $f(a) = f(a')$. Dann ist $0 = f(a) - f(a') = f(a - a')$, also $a - a' \in \ker(f)$. Dann ist aber $a - a' = 0$ und deshalb $a = a'$. □

4.3. **Der Restklassenring $\mathbb{Z}/m\mathbb{Z}$.**

Lemma 4.3.1. *Sei $m \in \mathbb{N}_0$. Dann sind die Abbildungen*

$$+ : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ (a + m\mathbb{Z}, b + m\mathbb{Z}) \mapsto (a + b) + m\mathbb{Z}$$
$$\cdot : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ (a + m\mathbb{Z}, b + m\mathbb{Z}) \mapsto (ab) + m\mathbb{Z}$$

wohldefiniert. Auf diese Art ist $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein Ring; es gilt $0_{\mathbb{Z}/m\mathbb{Z}} = 0 + m\mathbb{Z}$ und $1_{\mathbb{Z}/m\mathbb{Z}} = 1 + m\mathbb{Z}$.

Beweis. Zur Wohldefiniertheit: Wir müssen prüfen, dass die Definition von $+$ und $\cdot$ unabhängig von der Wahl der Repräsentanten der Restklassen ist. Dazu seien $a, a' \in \mathbb{Z}$, sowie $b, b' \in \mathbb{Z}$ jeweils Repräsentanten derselben Restklasse, d.h. $a + m\mathbb{Z} = a' + m\mathbb{Z}$ und $b + m\mathbb{Z} = b' + m\mathbb{Z}$. Also $a \equiv a' \pmod{m}$, sowie $b \equiv b' \pmod{m}$. Dann folgt aus Lemma 3.2.6 $a + b \equiv a' + b'$ und $ab \equiv a'b'$. Das bedeutet

$$(a + b) + m\mathbb{Z} = (a' + b') + m\mathbb{Z} \qquad (ab) + m\mathbb{Z} = (a'b') + m\mathbb{Z}$$

und damit folgt die Wohldefiniertheit.
Wir müssen alle Ringaxiome prüfen. Die ergeben sich jeweils aus den entsprechenden Ringaxiomen für $\mathbb{Z}$. Wir weisen examplarisch eines der Distributivgesetze nach. Seien $a, b, c \in \mathbb{Z}$. Es gilt

$$\begin{aligned}
(a + m\mathbb{Z}) \cdot ((b + m\mathbb{Z}) + (c + m\mathbb{Z})) &= (a + m\mathbb{Z}) \cdot ((b + c) + m\mathbb{Z}) \\
&= (a(b + c)) + m\mathbb{Z} \\
&= (ab + ac) + m\mathbb{Z} \\
&= ((ab) + m\mathbb{Z}) + ((ac) + m\mathbb{Z}) \\
&= (a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) + (a + m\mathbb{Z}) \cdot (c + m\mathbb{Z}).
\end{aligned}$$

Alle anderen Axiome rechnet man analog nach. □

Definition 4.3.2. Sei $m \in \mathbb{N}_0$. Man nennt $\mathbb{Z}/m\mathbb{Z}$ mit der Ringstruktur aus Lemma 4.3.1 den *Restklassenring* modulo m.

Beispiel 4.3.3. Additions- und Multiplikationstafeln von $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/5\mathbb{Z}$.

(1) Schreibe $\bar{i} := i + 4\mathbb{Z}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(2) Schreibe $\overline{i} := i + 5\mathbb{Z}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

4.4. **Chinesischer Restsatz.**

Ziel. Gegeben $m_1, \ldots, m_n \in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{Z}$, wollen wir die Lösungsmenge des Systems von simultanen Kongruenzen

$$x \equiv a_i \pmod{m_i}$$

bestimmen.

Lemma 4.4.1. *Seien $A_1, \ldots, A_n$ Ringe. Auf dem kartesische Produkt $\prod_{i=1}^n A_i$ erklären wir folgende Operationen*

$$\begin{aligned} + : \Big(\prod_{i=1}^n A_i\Big) \times \Big(\prod_{i=1}^n A_i\Big) &\to \prod_{i=1}^n A_i, \\ ((a_1, \ldots, a_n), (b_1, \ldots, b_n)) &\mapsto (a_1 + b_1, \ldots, a_n + b_n) \\ \cdot : \Big(\prod_{i=1}^n A_i\Big) \times \Big(\prod_{i=1}^n A_i\Big) &\to \prod_{i=1}^n A_i, \\ ((a_1, \ldots, a_n), (b_1, \ldots, b_n)) &\mapsto (a_1 b_1, \ldots, a_n b_n) \end{aligned}$$

So wird $(\prod_{i=1}^n A_i, +, \cdot)$ zu einem Ring. Es gilt $0 = (0, \ldots, 0)$ und $1 = (1, \ldots, 1)$.

Beweis. Prüfe exemplarisch die Assoziativität der Multiplikation. Seien $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$ und $c = (c_1, \ldots, c_n)$ Elemente von $\prod_{i=1}^n A_i$. Dann gilt

$$\begin{aligned} a \cdot (b \cdot c) &= (a_1, \ldots, a_n) \cdot ((b_1, \ldots, b_n) \cdot (c_1, \ldots, c_n)) \\ &= (a_1, \ldots, a_n) \cdot (b_1 c_1, \ldots, b_n c_n) \\ &= (a_1(b_1 c_1), \ldots, a_n(b_n c_n)) \\ &= ((a_1 b_1)c_1, \ldots, (a_n b_n)c_n) \\ &= \ldots \\ &= (a \cdot b) \cdot c. \end{aligned}$$

□

Lemma 4.4.2. *Seien $m_1, \ldots, m_r, m \in \mathbb{N}$. Dann ist*

$$\mathrm{ggT}(\mathrm{kgV}(m_1, \ldots, m_r), m) = \mathrm{kgV}(\mathrm{ggT}(m_1, m), \ldots, \mathrm{ggT}(m_r, m)).$$

Beweis. Wir betrachten die Primfaktorzerlegungen der Zahlen m_i und m. Sei p eine Primzahl. Sei $k_i \in \mathbb{N}_0$ die Multiplizität von p in m_i und sei $k \in \mathbb{N}_0$ die Multiplizität von p in m. Dann gilt

$$\begin{aligned}
\text{Mult. von } p \text{ in } \operatorname{kgV}(m_1, \dots, m_r) &= \max\{k_1, \dots, k_r\} \\
\text{Mult. von } p \text{ in } \operatorname{ggT}(\operatorname{kgV}(m_1, \dots, m_r), m) &= \min\{\max\{k_1, \dots, k_r\}, k\} \\
\text{Mult. von } p \text{ in } \operatorname{ggT}(m_i, m) &= \min\{k_i, k\} \\
\text{Mult. von } p \text{ in } \operatorname{kgV}(\operatorname{ggT}(m_1, m), \dots, \operatorname{ggT}(m_r, m)) &= \max\{\min\{k_1, k\}, \dots, \min\{k_r, k\}\}.
\end{aligned}$$

Offensichtlich ist aber

$$\min\{\max\{k_1, \dots, k_r\}, k\} = \max\{\min\{k_1, k\}, \dots, \min\{k_r, k\}\}$$

und deswegen stimmt die Multiplizität von p in beiden Zahlen überein. Da p aber eine beliebige Primzahl war, sind die Primfaktorzerlegungen der natürlichen Zahlen $\operatorname{ggT}(\operatorname{kgV}(m_1, \dots, m_r), m)$ und $\operatorname{kgV}(\operatorname{ggT}(m_1, m), \dots, \operatorname{ggT}(m_r, m))$ gleich. Damit stimmen sie überein. □

Satz 4.4.3 (Chinesischer Restsatz)**.** *Seien $m_1, \dots, m_n \in \mathbb{N}$. Betrachte die Abbildung*

$$\varphi : \mathbb{Z} \to \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$$

definiert durch $\varphi(a) := (a + m_1\mathbb{Z}, \dots, a + m_n\mathbb{Z})$. Dann gilt:

(1) φ ist ein Ringhomomorphismus.

(2) Ein Element $(a_1 + m_1\mathbb{Z}, \dots, a_n + m_n\mathbb{Z}) \in \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$ liegt genau dann in $\operatorname{im}(\varphi)$, wenn

$$a_i \equiv a_j \pmod{\operatorname{ggT}(m_i, m_j)}$$

gilt für alle $i, j = 1, \dots, n$.

(3) Sei $v = \operatorname{kgV}(m_1, \dots, m_n)$. Dann ist

$$\ker(\varphi) = \bigcap_{i=1}^{n} m_i\mathbb{Z} = v\mathbb{Z}.$$

Beweis.

(1) Nachrechnen.

(2) Zu „$\subseteq$“: Sei $(a_1 + m_1\mathbb{Z}, \dots, a_n + m_n\mathbb{Z}) \in \operatorname{im}(\varphi)$. Dann existiert ein $x \in \mathbb{Z}$ mit

$$\varphi(x) = (x + m_1\mathbb{Z}, \dots, x + m_n\mathbb{Z}) = (a_1 + m_1\mathbb{Z}, \dots, a_n + m_n\mathbb{Z}),$$

also ist $x - a_i \in m_i\mathbb{Z}$ für jedes $i = 1, \dots, n$. Damit folgt

$$a_i - a_j = (-1)(x - a_i) + (x - a_j) \in m_i\mathbb{Z} + m_j\mathbb{Z}$$

und das Ideal $m_i\mathbb{Z} + m_j\mathbb{Z}$ wird nach Lemma 1.4.5 erzeugt von $\operatorname{ggT}(m_i, m_j)$. Somit gilt $a_i \equiv a_j \pmod{\operatorname{ggT}(m_i, m_j)}$ wie gefordert.

Zu „$\supseteq$“: Sei $(a_1 + m_1\mathbb{Z}, \dots, a_n + m_n\mathbb{Z}) \in \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$, so dass $a_i \equiv a_j \pmod{\operatorname{ggT}(m_i, m_j)}$ für alle i, j. Schreibe abkürzend $d_{ij} := \operatorname{ggT}(m_i, m_j)$. Wir behaupten die Existenz von $x \in \mathbb{Z}$, so dass

$$x \equiv a_i \pmod{m_i}$$

für alle $i = 1, \ldots, n$. Wir beweisen diese Behauptung per Induktion nach n. Im Fall $n = 1$ ist nichts zu zeigen. Sei also $n > 1$. Nach Induktionsvoraussetzung existiert ein $y \in \mathbb{Z}$ mit $y \equiv a_i \pmod{m_i}$ für alle $i = 1, \ldots, n-1$. Wir sehen

$$\begin{aligned} a_i - y &\in m_i\mathbb{Z} \subseteq m_i\mathbb{Z} + m_n\mathbb{Z} \\ a_n - a_i &\in m_i\mathbb{Z} + m_n\mathbb{Z} \end{aligned}$$

für $i = 1, \ldots, n-1$. Deswegen liegt auch $a_n - y = (a_n - a_i) + (a_i - y) \in m_i\mathbb{Z} + m_n\mathbb{Z}$ für jedes $i = 1, \ldots, n-1$. Das impliziert

$$\begin{aligned} a_n - y \in & \bigcap_{i=1}^{n-1} (m_i\mathbb{Z} + m_n\mathbb{Z}) \\ &= \mathrm{kgV}(\mathrm{ggT}(m_1, m_n), \ldots, \mathrm{ggT}(m_{n-1}, m_n))\mathbb{Z} \\ &= \mathrm{ggT}(\mathrm{kgV}(m_1, \ldots, m_{n-1}), m_n)\mathbb{Z}. \end{aligned}$$

Hierbei haben wir die Lemmata 1.4.5, 1.6.5 und 4.4.2 verwendet. Sei $u := \mathrm{kgV}(m_1, \ldots, m_{n-1})$ und $d := \mathrm{ggT}(u, m_n)$. Dann gilt $a_n - y \in d\mathbb{Z}$, also existiert ein $q \in \mathbb{Z}$ mit $a_n - y = qd$. Ferner existieren nach dem Lemma von Bézout $r, s \in \mathbb{Z}$ mit $d = ru + sm_n$. Somit ist

$$a_n - y = qd = qru + qsm_n.$$

Definiere $x := y + qru$. Dann gelten

$$\begin{aligned} x &= a_n - qsm_n \\ &\equiv a_n \pmod{m_n} \\ x &= y + qru \\ &\equiv y \pmod{m_i} \\ &\equiv a_i \pmod{m_i} \end{aligned}$$

für jedes $i = 1, \ldots, n-1$, denn m_i ist ein Teiler von u.

(3) Sei $x \in \mathbb{Z}$. Es gelten folgende Äquivalenzen:

$$\begin{aligned} x \in \ker(\varphi) &\Leftrightarrow (x + m_1\mathbb{Z}, \ldots, x + m_n\mathbb{Z}) = (0 + m_1\mathbb{Z}, \ldots, 0 + m_n\mathbb{Z}) \\ &\Leftrightarrow x \in m_i\mathbb{Z} \text{ für alle } i = 1, \ldots, n \\ &\Leftrightarrow x \in \bigcap_{i=1}^{n} m_i\mathbb{Z}. \end{aligned}$$

Also ist $\ker(\varphi) = \bigcap_{i=1}^{n} m_i\mathbb{Z}$ gezeigt. Dass $\bigcap_{i=1}^{n} m_i\mathbb{Z} = v\mathbb{Z}$ ist, haben wir bereits in Lemma 1.6.5 gezeigt. □

Satz 4.4.4 (Chinesischer Restsatz, alternative Formulierung)**.** *Seien $m_1, \ldots, m_n \in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{Z}$.*

(1) Genau dann existiert ein $x \in \mathbb{Z}$ mit

$$x \equiv a_i \quad (\mathit{mod}\ m_i)$$

für alle $i = 1, \ldots, n$, wenn

$$a_i \equiv a_j \quad (\mathit{mod}\ \mathrm{ggT}(m_i, m_j))$$

für alle $i, j \in \{1, \ldots, n\}$ gilt.

(2) *Falls eine der beiden äquivalenten Bedingungen aus (1) gilt, so ist die Lösungsmenge*

$$\{x \in \mathbb{Z} \mid x \equiv a_i \pmod{m_i} \text{ für alle } i = 1, \ldots, n\}$$

eine Restklasse modulo $\mathrm{kgV}(m_1, \ldots, m_n)$.

Beweis.

(1) Genau dann existiert ein $x \in \mathbb{Z}$ wie gefordert, wenn es ein $x \in \mathbb{Z}$ mit

$$(x + m_1\mathbb{Z}, \ldots, x + m_n\mathbb{Z}) = (a_1 + m_1\mathbb{Z}, \ldots, a_n + m_n\mathbb{Z})$$

gibt. Das ist aber äquivalent zur Aussage $(a_1 + m_1\mathbb{Z}, \ldots, a_n + m_n\mathbb{Z}) \in \mathrm{im}(\varphi)$. Nach Satz 4.4.3(2) ist das aber äquivalent zu $a_i \equiv a_j \pmod{\mathrm{ggT}(m_i, m_j)}$ für alle $i, j = 1, \ldots, n$.

(2) Wir nehmen an, es gebe eine Lösung x_0 der simultanen Kongruenz. Sei L die gesamte Lösungsmenge. Wir zeigen

$$L = x_0 + v\mathbb{Z},$$

wobei $v := \mathrm{kgV}(m_1, \ldots, m_n)$ sei.
Zu „$\subseteq$“: Ist $x \in \mathbb{Z}$ eine beliebige Lösung der Kongruenz, so gilt $x \equiv a_i \equiv x_0 \pmod{m_i}$ für alle $i = 1, \ldots, n$. Deshalb ist $\varphi(x) = \varphi(x_0)$ und damit $x - x_0 \in \ker(\varphi) = v\mathbb{Z}$ (nach Satz 4.4.3(1 und 3)). Deshalb ist $x \in x_0 + v\mathbb{Z}$.
Zu „$\supseteq$“: Sei $x \in x_0 + v\mathbb{Z}$. Dann ist $x - x_0 \in \ker(\varphi)$ nach Satz 4.4.3(3). Es gilt also $\varphi(x) = \varphi(x_0)$, denn φ ist ein Ringhomomorphismus. Damit ist $x \equiv x_0 \equiv a_i \pmod{m_i}$ für jedes $i = 1, \ldots, n$. □

Korollar 4.4.5. *Seien $m_1, \ldots, m_n \in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{Z}$. Falls $m_1, \ldots, m_n$ paarweise teilerfremd sind, so existiert ein $x \in \mathbb{Z}$ mit $x \equiv a_i \pmod{m_i}$ für alle $i = 1, \ldots, n$.*

Algorithmus 4.4.6. Gegeben $m_1, \ldots, m_n \in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{Z}$ bestimmt der Algorithmus die Lösungsmenge der simultanen Kongruenzen $x \equiv a_i \pmod{m_i}$, alle $i = 1, \ldots, n$.
Iteration über i.
Schritt 1: Definiere $x_1 := a_1$ und $u_1 := m_1$. Fahre fort mit nächstem Schritt.
Schritt i. Angenommen ein $x_{i-1} \in \mathbb{Z}$, für das $x_{i-1} \equiv a_j \pmod{m_j}$ für alle $j = 1, \ldots, i-1$ gilt, ist bereits bestimmt. Ferner sei $u_{i-1} = \mathrm{kgV}(m_1, \ldots, m_{i-1})$ bereits bestimmt. Betrachte die Kongruenz

$$\begin{aligned} x_{i-1} + u_{i-1}z &\equiv a_i \pmod{m_i} \\ \Leftrightarrow u_{i-1}z &\equiv a_i - x_{i-1} \pmod{m_i}. \end{aligned}$$

Bestimme $\mathrm{ggT}(u_{i-1}, m_i)$ mit dem Euklidischen Algorithmus.
Falls $\mathrm{ggT}(u_{i-1}, m_i) \nmid a_i - x_{i-1}$, so ist $L = \emptyset$. Stop.
Falls $\mathrm{ggT}(u_{i-1}, m_i) \mid a_i - x_{i-1}$, so bestimme eine spezielle Lösung z mithilfe des Algorithmus 3.4.3 und setze

$$\begin{aligned} x_i &:= x_{i-1} + u_{i-1}z \\ u_i &:= \frac{u_{i-1}m_i}{\mathrm{ggT}(u_{i-1}, m_i)} \end{aligned}$$

Fahre fort mit Schritt $i+1$.
Falls die Iteration am Ende nicht gestoppt hat, so ist x_n eine spezielle Lösung, $u_n = \mathrm{kgV}(m_1, \ldots, m_n)$ und die Lösungsmenge ist

$$L = x_n + u_n\mathbb{Z}.$$

Satz 4.4.7. *Algorithmus 4.4.6 bestimmt die Lösungsmenge der simultanen Kongruenzen $x \equiv a_i \pmod{m_i}$ $(i = 1, \ldots, n)$.*

Beweis. Wir zeigen per Induktion über $i \in \{1, \ldots, n\}$, dass $x_i \equiv a_j \pmod{m_j}$ gilt für $j = 1, \ldots, i$ und $u_i = \mathrm{kgV}(m_1, \ldots, m_i)$.
Für $i = 1$ ist das offensichtlich. Gelte also $i > 1$ und die Behauptung sei richtig für $i-1$.
Für eine Lösung z der Kongruenz $u_{i-1}z \equiv a_i - x_{i-1} \pmod{m_i}$ und $x_i = x_{i-1} + u_{i-1}z$ gilt dann

$$\begin{aligned} x_i = x_{i-1} + u_{i-1}z &\equiv x_{i-1} + (a_i - x_{i-1}) \pmod{m_i} \\ &= a_i \\ x_i = x_{i-1} + u_{i-1}z &\equiv x_{i-1} \pmod{m_j} \\ &\equiv a_j \pmod{m_j} \end{aligned}$$

denn u_{i-1} ist ein Vielfaches von m_j. Außerdem gilt

$$\begin{aligned} u_i &= \frac{u_{i-1}m_i}{\mathrm{ggT}(u_{i-1}m_i)} \\ &= \mathrm{kgV}(u_{i-1}, m_i) \\ &= \mathrm{kgV}(\mathrm{kgV}(m_1, \ldots, m_{i-1}), m_i) \\ &= \mathrm{kgV}(m_1, \ldots, m_i). \end{aligned}$$

□

Beispiel 4.4.8. Finde alle $x \in \mathbb{Z}$ mit

$$\begin{aligned} x &\equiv 2 \pmod{10} \\ x &\equiv 7 \pmod{15} \\ x &\equiv 4 \pmod{21}. \end{aligned}$$

Schritt 1: Setze $x_1 = 2$, $u_1 = 10$.
Schritt 2: Löse $10z \equiv 7 - 2 = 5 \pmod{15}$. Es gilt $\mathrm{ggT}(10, 15) = 5 = (-1) \cdot 10 + 1 \cdot 15$. Also ist $z = -1$ eine Lösung. Setze $x_2 = 2 + 10 \cdot (-1) = -8$ und $u_2 = 30$.
Schritt 3. Löse $30z \equiv 4 - (-8) = 12 \pmod{21}$. Da $\mathrm{ggT}(30, 21) = 3 = (-2) \cdot 30 + 3 \cdot 21$, ist $z = (-2) \cdot 12/3 = -8$ eine Lösung. Setze $x_3 = -8 + 30 \cdot (-8) = -248$ und $u_3 = 210$.
Erhalten

$$L = -248 + 210\mathbb{Z} = -38 + 210\mathbb{Z}.$$

Probe:

$$\begin{aligned} -38 &\equiv 2 \pmod{10} \\ -38 &\equiv 7 \pmod{15} \\ -38 &\equiv 4 \pmod{21}. \end{aligned}$$

4.5. **Einheiten und Körper.**

Definition 4.5.1. Sei A ein Ring. Ein Element $u \in A$ heißt *Einheit* von A, wenn es ein $\tilde{u} \in A$ mit $u\tilde{u} = \tilde{u}u = 1$ gibt. Wir bezeichnen die Menge der Einheiten von A mit $A^\times$.

Lemma 4.5.2. *Sei A ein Ring.*

(1) 1 ist stets eine Einheit.
(2) Das Produkt von zwei Einheiten ist eine Einheit.
(3) Die Menge $A^\times$ wird mit der Abbildung $\cdot : A^\times \times A^\times \to A^\times,\ (u, v) \mapsto uv$ (also der Einschränkung der Ringmultiplikation) eine abelsche Gruppe.

Beweis.

(1) $1 \cdot 1 = 1$.
(2) Seien $u, v \in A^\times$. Dann gibt es $\tilde{u}, \tilde{v} \in A$ wie in Definition 4.5.1. Daher ist
$$(\tilde{v}\tilde{u})(uv) = (\tilde{v}(\tilde{u}u))v = \tilde{v}v = 1.$$
(Natürlich gilt auch $(uv)(\tilde{v}\tilde{u}) = 1$.)
(3) Die Abbildung $\cdot$ ist wohldefiniert wegen (2). Die Multiplikation ist assoziativ, also ist (G.1) erfüllt. 1 ist ein neutrales Element; das zeigt (G.2). Für (G.3) sei $u \in A^\times$ und sei $\tilde{u} \in A$ mit $\tilde{u}u = u\tilde{u} = 1$. Dann ist $\tilde{u} \in A^\times$ und ist damit ein Inverses zu u. Somit ist $(A^\times, \cdot)$ eine Gruppe. Da der Ring kommutativ ist, ist die Gruppe auch abelsch. □

Definition 4.5.3. Wir nennen $(A^\times, \cdot)$ die *Einheitengruppe* von A.

Bemerkung 4.5.4. Da das Inverse Element zu $u \in A^\times$eindeutig bestimmt ist, ist das Element $\tilde{u}$ aus Definition 4.5.1 eindeutig. Wir schreiben $u^{-1} := \tilde{u}$.

Bemerkung 4.5.5. Im Nullring 0 ist $1 = 0$, also ist 0 dort eine Einheit. In jedem anderen Ring ist 0 keine Einheit.

Lemma 4.5.6. *Sei A ein Ring und sei $a \in A$. Falls es ein $b \in A \setminus \{0\}$ mit $ab = 0$ gibt, ist a keine Einheit von A.*

Beweis. Angenommen a wäre eine Einheit. Dann gäbe es $\tilde{a} \in A$ mit $\tilde{a}a = 1$. Dann wäre aber $b = \tilde{a}ab = \tilde{a} \cdot 0 = 0$. □

Satz 4.5.7 (Einheiten im Restklassenring)**.** *Sei $m \in \mathbb{N}$. Sei $a \in \mathbb{Z}$. Genau dann ist $a + m\mathbb{Z}$ eine Einheit in $\mathbb{Z}/m\mathbb{Z}$, wenn* $\mathrm{ggT}(a, m) = 1$ *ist.*

Beweis. Zu „$\Rightarrow$“: Sei $a+m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$. Dann existiert ein $b \in \mathbb{Z}$ mit $ab+m\mathbb{Z} = 1+m\mathbb{Z}$, also $ab \equiv 1 \pmod{m}$. Damit existiert ein $q \in \mathbb{Z}$, so dass $ab-1 = qm$ und damit $1 \in (a, m)$. Somit ist $(a, m) = (1)$ und deshalb $\mathrm{ggT}(a, m) = 1$.
Zu „$\Leftarrow$“: Gelte $\mathrm{ggT}(a, m) = 1$. Dann gibt es nach Bézout $u, v \in \mathbb{Z}$ mit $1 = ua + vm$. Dann ist aber $ua \equiv 1 \pmod{m}$ und deshalb $(u + m\mathbb{Z})(a + m\mathbb{Z}) = 1 + m\mathbb{Z}$. □

Algorithmus 4.5.8. Der Beweis liefert einen Algorithmus, der prüft, ob $a + m\mathbb{Z}$ eine Einheit von $\mathbb{Z}/m\mathbb{Z}$ ist und ggf. das Inverse bestimmt. Sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$.

(1) Wende den erweiterten Euklidischen Algorithmus an, um $d = \mathrm{ggT}(a, m)$ und $u, v \in \mathbb{Z}$ mit $d = ua + vm$ zu erhalten.

(2) Falls $d \geq 2$ ist, ist $a + m\mathbb{Z} \notin (\mathbb{Z} + m\mathbb{Z})^\times$.
Falls $d = 1$, so ist $(a + m\mathbb{Z})^{-1} = u + m\mathbb{Z}$.

Beispiel 4.5.9. Prüfe, ob $13 + 20\mathbb{Z} \in (\mathbb{Z}/20\mathbb{Z})^\times$ ist und bestimme ggf. das Inverse.

(1) Erweiterter Euklidischer Algorithmus:

i	x_i	y_i	z_i	$z_{i-1} = q_i z_i + r_i$	q_i
0	1	0	20		
1	0	1	13	$20 = 1 \cdot 13 + 7$	1
2	1	-1	7	$13 = 1 \cdot 7 + 6$	1
3	-1	2	6	$7 = 1 \cdot 6 + 1$	1
4	2	-3	1	$6 = 6 \cdot 1 + 0$	6
5			0		

Also gilt $\mathrm{ggT}(13, 20) = 1 = (-3) \cdot 13 + 2 \cdot 20$.

(2) Wir erhalten $13 + 20\mathbb{Z} \in (\mathbb{Z}/20\mathbb{Z})^{-1}$ und $(13 + 20\mathbb{Z})^{-1} = -3 + 20\mathbb{Z} = 17 + 20\mathbb{Z}$.

Definition 4.5.10. Sei A ein Ring. Wir nennen A einen *Körper*, wenn $A^\times = A \setminus \{0\}$ ist.

Beispiel 4.5.11. Beispiele und Nicht-Beispiele für Körper.

(1) Der Nullring ist kein Körper, denn $\{0\}^\times = \{0\} \neq \{0\} \setminus \{0\} = \emptyset$.
(2) $\mathbb{Z}$ ist kein Körper, denn $\mathbb{Z}^\times = \{\pm 1\}$.
(3) $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper.

Satz 4.5.12. *Sei $m \in \mathbb{N}_0$. Genau dann ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper, wenn m eine Primzahl ist.*

Beweis. Für $m = 0$ ist $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}$ kein Körper. Für $m = 1$ ist $\mathbb{Z}/m\mathbb{Z}$ der Nullring; auch kein Körper. Also gehen wir zum Fall $m \geq 2$ über.
Zu „$\Rightarrow$“: Sei $\mathbb{Z}/m\mathbb{Z}$ ein Körper. Angenommen m ist keine Primzahl. Dann existieren $a, b \in \{2, \ldots, m-1\}$ mit $m = ab$. Es gilt $a, b \notin m\mathbb{Z}$, also $(a+m\mathbb{Z}), (b+m\mathbb{Z}) \in (\mathbb{Z}/m\mathbb{Z}) \setminus \{0+m\mathbb{Z}\}$, aber $(a + m\mathbb{Z})(b + m\mathbb{Z}) = 0 + m\mathbb{Z}$. Damit sind $a + m\mathbb{Z}$ und $b + m\mathbb{Z}$ keine Einheiten nach Lemma 4.5.6.
Zu „$\Leftarrow$“: Sei $m = p$ eine Primzahl und $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Dann ist $\mathrm{ggT}(a, p) = 1$, also ist $a + p\mathbb{Z}$ eine Einheit ist $\mathbb{Z}/p\mathbb{Z}$ nach Satz 4.5.7. □

Lemma 4.5.13. *Sei K ein Körper. Ist $x \in K \setminus \{0, 1, -1\}$, so ist $x^{-1} \neq x$.*

Beweis. Angenommen $x^{-1} = x$. Dann ist $x^2 = 1$. Also $0 = x^2 - 1 = (x - 1)(x + 1)$ und damit $x = 1$ oder $x = -1$. □

Satz 4.5.14 (Wilson)**.** *Sei $m \in \mathbb{N} \setminus \{1\}$. Genau dann ist m eine Primzahl, wenn gilt $(m - 1)! \equiv -1$ (mod m).*

Beweis. Zu „$\Rightarrow$“: Sei $m = p$ eine Primzahl. Betrachte zunächst die Fälle $p = 2$ und $p = 3$ separat. Es gilt $(2 - 1)! = 1 \equiv -1 \pmod 2$ und $(3 - 1)! = 2 \equiv -1 \pmod 3$.
Nun sei $p \geq 5$. Da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, gilt $(\mathbb{Z}/p\mathbb{Z})^\times = \{1+p\mathbb{Z}, \ldots, p-1+p\mathbb{Z}\}$. Betrachte das Produkt

$$(2 + p\mathbb{Z}) \cdot (3 + p\mathbb{Z}) \cdot \ldots \cdot (p - 2 + p\mathbb{Z}).$$

Nach Lemma 4.5.13 wird in diesem Produkt jede Zahl mit ihrem Inversen multipliziert. Also ist das obige Produkt $1 + p\mathbb{Z}$. Damit ist

$$(p-1)! + p\mathbb{Z} = (2 + p\mathbb{Z}) \cdot (3 + p\mathbb{Z}) \cdot \ldots \cdot (p - 2 + p\mathbb{Z}) \cdot (p - 1 + p\mathbb{Z}) = p - 1 + p\mathbb{Z}$$

und damit $(p-1)! \equiv p - 1 \equiv -1 \pmod{p}$.
Zu „$\Leftarrow$“: Sei $m \neq 1$ keine Primzahl. Dann existieren $a, b \in \{2, \ldots, m-1\}$ mit $m = ab$. Unterscheide 3 Fälle:

(1) Falls $a \neq b$ ist, gelte ohne Einschränkung $a < b$. Dann ist $m = ab$ ein Teiler von $(m-1)!$. Also $(m-1)! \equiv 0 \not\equiv -1 \pmod{m}$.
(2) Falls $a = b = 2$ ist $m = 4$ und es gilt $3! = 6 \equiv 2 \not\equiv -1 \pmod{4}$.
(3) Falls $a = b > 2$, so ist $2a < m$ und $2m = a \cdot (2a)$ ein Teiler von $(m-1)!$. Also wieder $(m-1)! \equiv 0 \not\equiv -1 \pmod{m}$. $\square$

5. Die Eulersche φ-Funktion und Ordnungen von Gruppenelementen

5.1. Die Eulersche φ-Funktion.

Definition 5.1.1. Die Funktion $\varphi : \mathbb{N} \to \mathbb{N}$, definiert durch

$$\varphi(m) := \left|(\mathbb{Z}/m\mathbb{Z})^\times\right|$$

heißt die *Eulersche φ-Funktion.*

Lemma 5.1.2. *Sei $m \in \mathbb{N}$. Dann gilt*

$$\varphi(m) = |\{a \in \{0, \dots, m-1\} \mid \mathrm{ggT}(a, m) = 1\}|$$

Beweis. Es gilt $\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}\}$. Sei $a \in \{0, \dots, m-1\}$. Nach Satz 4.5.7 gilt genau dann $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$, wenn $\mathrm{ggT}(a, m) = 1$ ist. □

Beispiel 5.1.3. Hier sind die ersten 6 Werte von φ:

- $\varphi(1) = 1$, denn $(\mathbb{Z}/1\mathbb{Z})^\times = \{0 + 1\mathbb{Z}\}$.
- $\varphi(2) = 1$, denn $(\mathbb{Z}/2\mathbb{Z})^\times = \{1 + 2\mathbb{Z}\}$.
- $\varphi(3) = 2$, denn $(\mathbb{Z}/3\mathbb{Z})^\times = \{1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$.
- $\varphi(4) = 2$, denn $(\mathbb{Z}/4\mathbb{Z})^\times = \{1 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$.
- $\varphi(5) = 4$, denn $(\mathbb{Z}/5\mathbb{Z})^\times = \{1 + 5\mathbb{Z}, \dots, 4 + 5\mathbb{Z}\}$.
- $\varphi(6) = 2$, denn $(\mathbb{Z}/6\mathbb{Z})^\times = \{1 + 6\mathbb{Z}, 5 + 6\mathbb{Z}\}$.

Bemerkung 5.1.4. Sei p eine Primzahl. Dann ist $\mathbb{Z}/p\mathbb{Z}$ nach Satz 4.5.7 ein Körper. Also ist $\varphi(p) = p - 1$.

Lemma 5.1.5. *Sei p eine Primzahl und $r \in \mathbb{N}$. Dann ist $\varphi(p^r) = p^{r-1}(p-1)$.*

Beweis. Für $a \in \mathbb{Z}$ gilt genau dann $\mathrm{ggT}(a, p) = 1$, wenn $p \nmid a$. Also ist

$$\varphi(p^r) = |\{a \in \{0, \dots, p^r - 1\} \mid p \text{ teilt nicht } a\}|.$$

Nach Lemma 2.4.4 sind genau $\lfloor p^r/p \rfloor$ Zahlen aus $\{0, \dots, p^r - 1\}$ durch p teilbar. Also folgt

$$\varphi(p^r) = p^r - \left\lfloor \frac{p^r}{p} \right\rfloor = p^r - p^{r-1} = p^{r-1}(p-1).$$

□

Lemma 5.1.6. *Seien A, B Ringe und $f : A \to B$ ein Ringhomomorphismus. Dann gilt:*

(1) $f(A^\times) \subseteq B^\times$.
(2) $f^\times : A^\times \to B^\times,\ a \mapsto f(a)$ ist ein Gruppenhomomorphismus.
(3) Ist f ein Ringisomorphismus, so ist $f^\times : A^\times \to B^\times$ ein Gruppenisomorphismus.

Beweis.

(1) Übung.
(2) Nach (1) ist $f^\times$ wohldefiniert. Ferner gilt für $a, a' \in A^\times$ per Definition $f^\times(aa') = f(aa') = f(a)f(a') = f^\times(a)f^\times(a')$.
(3) Da f injektiv ist, ist auch $f^\times$ injektiv. Zur Surjektivität von $f^\times$. Sei $b \in B^\times$. Da f surjektiv ist, existiert ein $a \in A$ mit $f(a) = b$. Genauso existiert ein $a' \in A$ mit $f(a') = b^{-1}$. Dann ist $f(aa') = f(a)f(a') = bb^{-1} = 1 = f(1)$. Da f injektiv ist, ist $aa' = 1$ und damit $a \in A^\times$. Somit ist $b = f(a) = f^\times(a)$. □

Lemma 5.1.7. *Seien A, B Ringe. Betrachte den Produktring $A \times B$ aus Lemma 4.4.1. Es gilt $(A \times B)^\times = A^\times \times B^\times$.*

Beweis. Sei $(a, b) \in A \times B$. Genau dann ist $(a, b) \in (A \times B)^\times$, wenn es $(\tilde{a}, \tilde{b}) \in A \times B$ gibt mit

$$(a, b) \cdot (\tilde{a}, \tilde{b}) = (a\tilde{a}, b\tilde{b}) = (1, 1),$$

also $a\tilde{a} = 1$ und $b\tilde{b} = 1$. Das ist genau dann der Fall, wenn $a \in A^\times$ und $b \in B^\times$ ist. □

Lemma 5.1.8. *Sei B ein Ring und sei $f : \mathbb{Z} \to B$ ein Ringhomomorphismus. Dann gilt:*

(1) $\ker(f)$ *ist ein Ideal von* $\mathbb{Z}$.
(2) Es gibt genau ein $m \in \mathbb{N}_0$ mit $\ker(f) = m\mathbb{Z}$.
(3) Es gibt genau einen Ringhomomorphismus $\overline{f} : \mathbb{Z}/m\mathbb{Z} \to B$, so dass

$$\overline{f}(a + m\mathbb{Z}) = f(a)$$

für alle $a \in \mathbb{Z}$.
(4) $\overline{f}$ ist injektiv und $\operatorname{im}(\overline{f}) = \operatorname{im}(f)$.

Beweis.

(1) Weise die Axiome nach:
(I.1) $f(0) = 0$.
(I.2) Seien $a, b \in \ker(f)$, d.h. $f(a) = f(b) = 0$. Dann $f(a + b) = f(a) + f(b) = 0$.
(I.3) Sei $a \in \ker(f)$ und $n \in \mathbb{Z}$. Dann ist $f(na) = f(n)f(a) = f(n) \cdot 0 = 0$.
(2) Da $\ker(f)$ ein Ideal von $\mathbb{Z}$ ist, existiert nach Lemma 1.3.6 ein eindeutig bestimmtes $m \in \mathbb{N}_0$ mit $\ker(f) = m\mathbb{Z}$.
(3) Zur Existenz. Definiere $\overline{f} : \mathbb{Z}/m\mathbb{Z} \to B$ durch $\overline{f}(a + m\mathbb{Z}) = f(a)$. Dann ist $\overline{f}$ wohldefiniert, denn für $a, a' \in \mathbb{Z}$ mit $a + m\mathbb{Z} = a' + m\mathbb{Z}$ ist $a - a' \in m\mathbb{Z} = \ker(f)$. Also gilt $0 = f(a - a')$ und deshalb $f(a) = f(a')$. Man sieht sofort, dass $\overline{f}$ ein Rinhomomorphismus ist (Axiome nachrechnen). Zur Eindeutigkeit: $\overline{f}$ ist bereits durch f eindeutig festgelegt.
(4) Sei $a + m\mathbb{Z}$ mit $\overline{f}(a + m\mathbb{Z}) = 0$. Nach Definition ist $\overline{f}(a + m\mathbb{Z}) = f(a)$, also ist $a \in \ker(f) = m\mathbb{Z}$. Damit ist $a + m\mathbb{Z} = 0 + m\mathbb{Z}$.
Sei $b \in B$. Dann gilt

$$\begin{aligned} b \in \operatorname{im}(f) &\Leftrightarrow \text{ex. } a \in \mathbb{Z} \text{ mit } f(a) = b \\ &\Leftrightarrow \text{ex. } a + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z} \text{ mit } \overline{f}(a + m\mathbb{Z}) = b \\ &\Leftrightarrow b \in \operatorname{im}(\overline{f}). \end{aligned}$$

□

Bemerkung 5.1.9. Sei B ein Ring. Dann existiert genau ein Ringhomomorphismus $f : \mathbb{Z} \to B$.

Beweis. Da f ein Ringhomomorphismus sein soll, muss $f(1) = 1$ und $f(0) = 0$ gelten. Ist nun $n \in \mathbb{N}$, so muss

$$f(n) = f(n \cdot 1) = f(\underbrace{1 + \ldots + 1}_{n \text{ Mal}}) = \underbrace{f(1) + \ldots + f(1)}_{n \text{ Mal}}$$

gelten. Für $n \in \mathbb{Z}_{<0}$ ist $-n > 0$ und es muss

$$f(n) = -f(-n)$$

sein. Auf diese Weise ist f eindeutig festgelegt. Man rechnet nach, dass f ein Ringhomomorphismus ist. □

Lemma 5.1.10. *Seien $m, n \in \mathbb{Z}$ mit $\mathrm{ggT}(m,n) = 1$. Dann ist $\varphi(mn) = \varphi(m)\varphi(n)$.*

Beweis. Betrachte die Abbildung $f : \mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ definiert durch $f(a) = (a + m\mathbb{Z}, a + n\mathbb{Z})$; in Satz 4.4.3(1) haben wir bereits bewiesen, dass f ein Ringhomomorphismus ist. Da $\mathrm{ggT}(m,n) = 1$, ist f surjektiv nach Satz 4.4.3(2). Ferner ist $\ker(f) = \mathrm{kgV}(m,n)\mathbb{Z} = mn\mathbb{Z}$ nach Satz 4.4.3(3). Gemäß Lemma 5.1.8 existiert ein bijektiver Ringhomomorphismus

$$\overline{f} : \mathbb{Z}/mn\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),$$

sprich ein Ringisomorphismus. Nach Lemmata 5.1.6 und 5.1.7 gibt es einen Isomorphismus von Gruppen

$$f^\times : (\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

Somit folgt

$$\varphi(mn) = \varphi(m)\varphi(n).$$

□

Satz 5.1.11. *Sei $m \in \mathbb{N}$, seien $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen und seien $n_1, \ldots, n_r > 0$ mit $m = \prod_{i=1}^r p_i^{n_i}$ (also die Primfaktorzerlegung von m). Dann gilt*

$$\varphi(m) = \prod_{i=1}^r p_i^{n_i - 1}(p_i - 1).$$

Beweis. Die Zahlen $a := p_1^{n_1} \ldots p_{r-1}^{n_{r-1}}$ und $b := p_r^{n_r}$ sind teilerfremd. Somit ist $\varphi(m) = \varphi(a)\varphi(b)$ nach Lemma 5.1.10. Induktiv sehen wir

$$\varphi(m) = \prod_{i=1}^r \varphi(p_i^{n_i}) = \prod_{i=1}^r p_i^{n_i - 1}(p_i - 1).$$

□

Beispiel 5.1.12. $\varphi(1000) = \varphi(2^3 \cdot 5^3) = 2^2(2-1) \cdot 5^2 \cdot (5-1) = 400.$

Satz 5.1.13. *Sei $m \in \mathbb{N}$. Dann ist*

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

Beweis. Sei $D(m) := \{d \in \{1, \ldots, m\} \mid d \text{ teilt } m\}$. Dann ist die Abbildung $D(m) \to D(m),\ d \mapsto m/d$ bijektiv. Deshalb ist

$$\sum_{d \in D(m)} \varphi(d) = \sum_{d \in D(m)} \varphi(\frac{m}{d}).$$

Für jedes $d \in D(m)$ betrachten wir die Menge $G_d(m) := \{a \in \{1, \ldots, m\} \mid \mathrm{ggT}(a, m) = d\}$. Diese Mengen sind paarweise disjunkt, also $G_d(m) \cap G_{d'}(m) = \emptyset$ für alle $d \neq d'$. Ferner gilt

$$\bigcup_{d \in D(m)} G_d(m) = \{1, \ldots, m\}.$$

Also ist $\sum_{d \in D(m)} |G_d(m)| = m$.
Für eine Zahl a gilt aber genau dann $\mathrm{ggT}(a, m) = d$, wenn $d \mid a$ und $\mathrm{ggT}(a/d, m/d) = 1$ ist. Also ist $G_d(m) \to G_1(m/d),\ a \mapsto a/d$ eine Bijektion. Aber

$$|G_1(\frac{m}{d})| = |\{b \in \{1, \ldots, \frac{m}{d}\} \mid \mathrm{ggT}(b, \frac{m}{d}) = 1\}| = \varphi(\frac{m}{d}).$$

Somit folgt

$$\sum_{d \in D(m)} \varphi(d) = \sum_{d \in D(m)} \varphi(\frac{m}{d}) = \sum_{d \in D(m)} |G_1(\frac{m}{d})| = \sum_{d \in D(m)} |G_d(m)| = m.$$

□

5.2. **Ordnungen von Gruppenelementen.**

Konvention. In diesem und den folgenden Unterabschnitten sei G eine multiplikativ geschriebene Gruppe.

Definition 5.2.1. Sei G eine endliche Gruppe. Man nennt $\operatorname{ord} G := |G|$ die *Ordnung* von G.

Lemma 5.2.2. *Sei G eine endliche Gruppe und sei $g \in G$. Dann existiert ein $n \in \mathbb{N}$ mit $g^n = e$.*

Beweis. Betrachte die Menge $\{g^n \mid n \in \mathbb{N}\} \subseteq G$. Da G endlich ist, existieren nach dem Schubfachprinzip Zahlen $r, s \in \mathbb{N}$ mit $r < s$ und $g^r = g^s$. Dann ist $g^{s-r} = e$. □

Definition 5.2.3. Sei G eine endliche Gruppe und sei $g \in G$. Die Zahl $\operatorname{ord}_G(g) := \operatorname{ord}(g) := \min\{n \in \mathbb{N} \mid g^n = e\}$ heißt die *Ordnung* von g (in G).

Beispiel 5.2.4. Betrachte die Gruppe $(\mathbb{Z}/7\mathbb{Z})^\times$. Schreibe $\bar{i} := i + 7\mathbb{Z}$. Bestimme die Ordnungen $\operatorname{ord}(\bar{i}) := \operatorname{ord}_{(\mathbb{Z}/7\mathbb{Z})^\times}(\bar{i})$ von $\bar{i}$.

- $\operatorname{ord}(\bar{1}) = 1$
- $\operatorname{ord}(\bar{2}) = 3$, denn $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{1}$.
- $\operatorname{ord}(\bar{3}) = 6$, denn $\bar{3}^2 = \bar{2}$, $\bar{3}^3 = \bar{6}$, $\bar{3}^4 = \bar{2}^2 = \bar{4}$, $\bar{3}^5 = \bar{4} \cdot \bar{3} = \bar{5}$, $\bar{3}^6 = \bar{5} \cdot \bar{3} = \bar{1}$.
- $\operatorname{ord}(\bar{4}) = 3$, denn $\bar{4}^2 = \bar{2}$, $\bar{4}^3 = \bar{2} \cdot \bar{4} = \bar{1}$.
- $\operatorname{ord}(\bar{5}) = 6$, denn $\bar{5}^2 = \bar{4}$, $\bar{5}^3 = \bar{4} \cdot \bar{5} = \bar{6}$, $\bar{5}^4 = \bar{4}^2 = \bar{2}$, $\bar{5}^5 = \bar{2} \cdot \bar{5} = \bar{3}$, $\bar{5}^6 = \bar{3} \cdot \bar{5} = \bar{1}$.
- $\operatorname{ord}(\bar{6}) = 2$, denn $\bar{6}^2 = 1$.

Lemma 5.2.5. *Sei $g \in G$. Dann ist die Menge*

$$\mathrm{Ann}(g) := \{n \in \mathbb{Z} \mid g^n = e\}$$

ein Ideal von $\mathbb{Z}$.

Beweis. Sei $I := \mathrm{Ann}(g)$.
(I.1) $g^0 = e$

(I.2) Gelte $g^m = g^n = e$. Dann ist auch $g^{m+n} = g^m g^n = e$.
(I.3) Gelte $g^m = e$ und sei $a \in \mathbb{Z}$. Dann ist $g^{am} = (g^m)^a = e$. □

Lemma 5.2.6. *Sei G eine endliche Gruppe und sei $g \in G$. Dann ist* $\mathrm{Ann}(g) = \mathrm{ord}(g)\mathbb{Z}$.

Beweis. Nach Lemma 5.2.2 ist $\mathrm{Ann}(g) \neq \{0\}$. Sei d der nicht-negative Erzeuger von $\mathrm{Ann}(g)$. Nach dem Beweis von Lemma 1.3.6 ist

$$d = \min(\mathrm{Ann}(g) \cap \mathbb{N}) = \mathrm{ord}(g).$$

□

Korollar 5.2.7. *Seien G eine endliche Gruppe, $g \in G$ und $m \in \mathbb{Z}$. Genau dann ist $g^m = e$, wenn* $\mathrm{ord}(g) \mid m$.

Beweis. Sei $d = \mathrm{ord}(g)$. Also ist $\mathrm{Ann}(g) = d\mathbb{Z}$ nach Lemma 5.2.6. Somit gilt für jedes $m \in \mathbb{Z}$

$$g^m = e \Leftrightarrow m \in d\mathbb{Z} \Leftrightarrow d \mid m.$$

□

5.3. **Untergruppen.**

Definition 5.3.1. Sei G eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt *Untergruppe* von G, wenn gelten:
(U.1) $e \in H$
(U.2) $ab \in H$ für alle $a, b \in H$
(U.3) $a^{-1} \in H$ für alle $a \in H$

Bemerkung 5.3.2. Untergruppen von $(\mathbb{Z}, +)$ sind genau Ideale von $\mathbb{Z}$.

Beweis. Übung. □

Beispiel 5.3.3. Betrachte den Restklassenring $\mathbb{Z}/8\mathbb{Z}$. Schreibe $\overline{i} := i + 8\mathbb{Z}$. Es gilt

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

mit folgender Gruppentafel:

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

Damit hat $(\mathbb{Z}/8\mathbb{Z})^\times$ folgende Untergruppen:

$$\{\overline{1}\} \qquad \{\overline{1}, \overline{3}\} \qquad \{\overline{1}, \overline{5}\} \qquad \{\overline{1}, \overline{7}\} \qquad (\mathbb{Z}/8\mathbb{Z})^\times.$$

Man sieht sofort, dass alle oben genannten Teilmengen Untergruppen sind. Tatsächlich sind das alle Untergruppen. Zunächst muss jede Untergruppe $e = \overline{1}$ enthalten. Ist H eine Untergruppe von $(\mathbb{Z}/8\mathbb{Z})^\times$, die $x, y \in \{\overline{3}, \overline{5}, \overline{7}\}$ mit $x \neq y$ enthält, so ist auch $z = xy \in H$, wobei z das Element mit $\{x, y, z\} = \{\overline{3}, \overline{5}, \overline{7}\}$ sei. Damit ist $H = (\mathbb{Z}/8\mathbb{Z})^\times$.

Lemma 5.3.4. *Sei G eine Gruppe und H eine Untergruppe von G. Dann ist H zusammen mit $\cdot : H \times H \to H,\ (a, b) \mapsto ab$ selbst eine Gruppe.*

Beweis. Da $ab \in H$ ist für alle $a, b \in H$, ist die Abbildung $\cdot : H \times H \to H$ wohldefiniert. Da die Gruppenverknüpfung von G assoziativ ist, gilt auch in $(H, \cdot)$ das Assoziativgesetz. Das Untergruppenaxiom (U.1) impliziert, dass $(H, \cdot)$ ein neutrales Element, nämlich e_G, besitzt. Sei $a \in H$. Dann ist das Inverse a^{-1} (in G) auch ein Element von H und es gilt $aa^{-1} = a^{-1}a = e$. Somit ist auch das Axiom (G.3) für $(H, \cdot)$ erfüllt. □

Lemma 5.3.5. *Sei H eine Untergruppe von G. Für $a, b \in G$ definieren wir die Relation*

$$a \sim_H b :\Leftrightarrow a^{-1}b \in H.$$

Dann ist $\sim_H$ eine Äquivalenzrelation auf G.

Beweis. Reflexivität: Sei $a \in G$. Dann ist $a^{-1}a = e \in H$. Also $a \sim_H a$.
Symmetrie: Gelte $a \sim_H b$, also $a^{-1}b \in H$. Dann ist auch $b^{-1}a = (a^{-1}b)^{-1} \in H$ und damit $b \sim_H a$.
Transitivität. Gelte $a \sim_H b$ und $b \sim_H c$, sprich $a^{-1}b, b^{-1}c \in H$. Dann folgt $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$ und somit $a \sim_H c$. □

Definition 5.3.6. Sei H eine Untergruppe von G. Bezeichne die Äquivalenzklasse von a bezüglich $\sim_H$ mit aH und schreibe $G/H := G/\sim_H$ für die Menge der Äquivalenzklassen.

Lemma 5.3.7. *Sei H eine Untergruppe von G. Sei $a \in G$. Betrachte die Abbildung*

$$l_a : G \to G, \ g \mapsto ag.$$

Es gilt:

(1) l_a ist bijektiv.
(2) $l_a(H) = aH$.

Beweis.

(1) Betrachte die Abbildung $l_{a^{-1}}$. Es gilt $(l_{a^{-1}} \circ l_a)(g) = a^{-1}(ag) = g$ für jedes $g \in G$. Also ist $l_{a^{-1}} \circ l_a = \mathrm{id}_G$. Genauso sieht man $l_a \circ l_{a^{-1}} = \mathrm{id}_G$. Damit ist l_a bijektiv (und es gilt $(l_a)^{-1} = l_{a^{-1}}$).
(2) Es gilt zunächst

$$l_a(H) = \{g \in G \mid \exists\, h \in H : \ g = \underbrace{l_a(h)}_{=ah}\}.$$

Nun zeigen wir $l_a(H) = aH$.
Zu „$\subseteq$“: Sei $g \in l_a(H)$. Also $g = ah$ für ein $h \in H$. Damit ist $a^{-1}g = a^{-1}(ah) = h \in H$ und deshalb $a \sim_H g$. Daher ist $g \in aH$.
Zu „$\supseteq$“: Sei $g \in aH$. Das bedeutet $a \sim_H g$, sprich $a^{-1}g \in H$. Dann ist

$$l_a(H) \ni l_a(a^{-1}g) = a(a^{-1}g) = g.$$

□

Satz 5.3.8 (Lagrange)**.** *Sei G eine endliche Gruppe und H eine Untergruppe von G. Dann ist* $\mathrm{ord}(H)$ *ein Teiler von* $\mathrm{ord}(G)$.

Beweis. Sei $N := \operatorname{ord}(G)$ und $n := \operatorname{ord}(H)$. Für jedes $a \in G$ gilt nach Lemma 5.3.7 $|aH| = |H| = n$. Nun wenden wir Lemma 5.3.5 an. Da $\sim_H$ eine Äquivalenzrelation ist, folgt

$$G = \bigcup_{aH \in G/H} aH$$

und diese Vereinigung ist disjunkt – das heißt $aH \cap a'H = \emptyset$ für alle $a \not\sim_H a'$. Daraus folgt

$$N = \operatorname{ord}(G) = \sum_{aH \in G/H} \underbrace{|aH|}_{n} = n \cdot |G/H|.$$

Somit ist $n = \operatorname{ord}(H)$ ein Teiler von $N = \operatorname{ord}(G)$. □

5.4. **Zyklische Gruppen.**

Lemma 5.4.1. *Sei G eine Gruppe. Sei $g \in G$. Dann ist die Teilmenge*

$$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$$

eine Untergruppe von G.

Beweis. (U.1) $e = g^0 \in \langle g \rangle$
(U.2) Seien $b = g^n, c = g^m \in \langle g \rangle$, dann auch $bc = g^{n+m} \in \langle g \rangle$.
(U.3) Sei $b = g^n \in \langle g \rangle$. Dann ist $b^{-1} = g^{-n} \in \langle g \rangle$. □

Definition 5.4.2. Man nennt $\langle g \rangle$ die von g *erzeugte Untergruppe* von G.

Definition 5.4.3. Eine Gruppe G heißt *zyklisch*, wenn es ein $g \in G$ mit $G = \langle g \rangle$ gibt. Ein solches $g \in G$ heißt ein *Erzeuger* von G.

Bemerkung 5.4.4. Zyklische Gruppen sind abelsch.

Beispiel 5.4.5. (1) Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch; ein Erzeuger ist 1.
(2) Sei $m \in \mathbb{N}$. Die Gruppe $(\mathbb{Z}/m\mathbb{Z}, +)$ ist ebenfalls zyklisch; ein Erzeuger ist $1 + m\mathbb{Z}$.

Satz 5.4.6 (Klassifikation der zyklischen Gruppen)**.** *Sei G eine zyklische Gruppe. Sei $g \in G$ ein Erzeuger.*

(1) Ist G unendlich, so ist G isomorph zu $(\mathbb{Z}, +)$.
(2) Ist G endlich, so ist G isomorph zu $(\mathbb{Z}/d\mathbb{Z}, +)$ und es gilt $d = \operatorname{ord}(g) = \operatorname{ord}(G)$.

Beweis. Die Abbildung $\psi : \mathbb{Z} \to G$ definiert durch

$$\psi(n) := g^n$$

ist surjektiv, da g ein Erzeuger von G ist. Außerdem ist $\psi : (\mathbb{Z}, +) \to (G, \cdot)$ ein Gruppenhomomorphismus, denn für $n, m \in \mathbb{Z}$ gilt

$$\psi(n + m) = g^{n+m} = g^n g^m = \psi(n)\psi(m).$$

Für dessen Kern gilt

$$\ker(\psi) = \{n \in \mathbb{Z} \mid \psi(n) = e\} = \{n \in \mathbb{Z} \mid g^n = e\} = \operatorname{Ann}(g).$$

Da $\operatorname{Ann}(g)$ ein Ideal von $\mathbb{Z}$ ist, existiert ein (eindeutig bestimmtes) $d \in \mathbb{N}_0$ mit $\operatorname{Ann}(g) = d\mathbb{Z}$. Nun betrachte die Abbildung $\overline{\psi} : \mathbb{Z}/d\mathbb{Z} \to G$ definiert durch

$$\overline{\psi}(n + d\mathbb{Z}) = g^n.$$

Diese Abbildung ist wohldefiniert. Dazu seien $n, m \in \mathbb{Z}$ mit $n \equiv m \pmod{d}$. Dann ist $n - m \in d\mathbb{Z} = \mathrm{Ann}(g)$, also gilt

$$g^n = g^{m+(n-m)} = g^m g^{n-m} = g^m.$$

Ferner ist $\overline{\psi} : (\mathbb{Z}/d\mathbb{Z}, +) \to (G, \cdot)$ ein Gruppenhomomorphismus, denn für $n + d\mathbb{Z}, m + d\mathbb{Z} \in \mathbb{Z}/d\mathbb{Z}$ gilt

$$\begin{aligned}\overline{\psi}((n + d\mathbb{Z}) + (m + d\mathbb{Z})) &= \overline{\psi}(n + m + d\mathbb{Z}) \\ &= \psi(n + m) \\ &= \psi(n) \cdot \psi(m) \\ &= \overline{\psi}(n + d\mathbb{Z}) \cdot \overline{\psi}(m + d\mathbb{Z}).\end{aligned}$$

Wir zeigen schließlich, dass $\overline{\psi}$ bijektiv ist. Die Surjektivität von $\overline{\psi}$ folgt sofort aus der Surjektivität von ψ. Zur Injektivität. Sei $n + d\mathbb{Z} \in \mathbb{Z}/d\mathbb{Z}$ mit $\overline{\psi}(n + d\mathbb{Z}) = e$. Dann ist $\psi(n) = e$, also $n \in \ker(\psi) = d\mathbb{Z}$ und damit $n + d\mathbb{Z} = 0 + d\mathbb{Z}$.

(1) Ist G unendlich, so ist $d = 0$ (denn sonst wäre G isomorph zur endlichen Gruppe $(\mathbb{Z}/d\mathbb{Z}, +)$). Aber $(\mathbb{Z}/0\mathbb{Z}, +) = (\mathbb{Z}, +)$.
(2) Sei G endlich. Dann ist $d = \mathrm{ord}(g)$ nach Lemma 5.2.6. Ferner ist $d = \mathrm{ord}(\mathbb{Z}/d\mathbb{Z}) = \mathrm{ord}(G)$, denn die beiden Gruppen sind isomorph. □

Korollar 5.4.7. *Sei G eine endliche Gruppe.*

(1) Sei $g \in G$. Dann gilt $\mathrm{ord}(g) \mid \mathrm{ord}(G)$ und deshalb $g^{\mathrm{ord}(G)} = e$.
(2) Genau dann ist G zyklisch, wenn es ein $g \in G$ mit $\mathrm{ord}(g) = \mathrm{ord}(G)$ gibt. Jedes solche g ist ein Erzeuger von G.

Beweis.

(1) Betrachte die (endliche) zyklische Untergruppe $H := \langle g \rangle$. Dann ist $\mathrm{ord}(H) = \mathrm{ord}(g)$ nach Satz 5.4.6. Der Satz von Lagrange sagt uns $\mathrm{ord}(H)$ teilt $\mathrm{ord}(G)$. Da $\mathrm{ord}(g)$ ein Teiler von $\mathrm{ord}(G)$ folgt $g^{\mathrm{ord}(G)} = e$ aus Korollar 5.2.7.
(2) Zu „$\Rightarrow$“: Ist G zyklisch, so gilt für einen Erzeuger g bereits $\mathrm{ord}(g) = \mathrm{ord}(\langle g \rangle) = \mathrm{ord}(G)$.
Zu „$\Leftarrow$“: Sei $g \in G$ mit $\mathrm{ord}(g) = \mathrm{ord}(G)$. Sei $H := \langle g \rangle$. Dann ist H zyklisch und damit $\mathrm{ord}(H) = \mathrm{ord}(g) = \mathrm{ord}(G)$. Weil $H \subseteq G$ und G endlich ist, folgt $H = G$. □

Beispiel 5.4.8. Betrachte die Einheitengruppen $(\mathbb{Z}/7\mathbb{Z})^\times$ und $(\mathbb{Z}/8\mathbb{Z})^\times$.

(1) Die Gruppe $(\mathbb{Z}/7\mathbb{Z})^\times$ ist zyklisch, denn $\mathrm{ord}(3 + 7\mathbb{Z}) = 6 = \varphi(7) = \mathrm{ord}((\mathbb{Z}/7\mathbb{Z})^\times)$ (vergleiche Beispiel 5.2.4).
(2) Die Gruppe $(\mathbb{Z}/8\mathbb{Z})^\times$ ist nicht zyklisch. Das liegt daran, dass $\mathrm{ord}(g) \in \{1, 2\}$ ist für alle $g \in (\mathbb{Z}/8\mathbb{Z})^\times$, aber $\mathrm{ord}((\mathbb{Z}/8\mathbb{Z})^\times) = \varphi(8) = 4$ (vergleiche Beispiel 5.3.3).

5.5. **Der Satz von Euler.**

Satz 5.5.1 (Euler)**.** *Seien $a \in \mathbb{Z}$ und $m \in \mathbb{N}$ mit $\mathrm{ggT}(a, m) = 1$. Dann ist*

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

Beweis. Da $\mathrm{ggT}(a,m) = 1$, ist $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$. Es gilt per Definition $\varphi(m) = \mathrm{ord}((\mathbb{Z}/m\mathbb{Z})^\times)$. Aus Korollar 5.4.7 folgt deshalb $(a + m\mathbb{Z})^{\varphi(m)} = 1 + m\mathbb{Z}$, oder anders ausgedrückt $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Bemerkung 5.5.2. Hieraus kann man sofort den kleinen Satz von Fermat (Satz 3.3.2) folgern.

5.6. **Ordnungen in Einheitengruppen von Restklassenringen.**

Definition 5.6.1. Sei $m \in \mathbb{N}$ und sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,m) = 1$ (also $a+m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$). Definiere

$$\mathrm{ord}_m(a) := \mathrm{ord}_{(\mathbb{Z}/m\mathbb{Z})^\times}(a + m\mathbb{Z}).$$

Lemma 5.6.2. *Sei $m \in \mathbb{N}$ und sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,m) = 1$. Dann gilt $\mathrm{ord}_m(a) \mid \varphi(m)$.*

Beweis. Nach dem Satz von Euler ist $a^{\varphi(m)} \equiv 1 \pmod{m}$. Nach Lemma 5.2.7 folgt $\mathrm{ord}_a(m)$ teilt $\varphi(m)$. □

Lemma 5.6.3. *Seien $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$ und $a \in \mathbb{Z}$, so dass $\mathrm{ggT}(a,mn) = 1$. Dann sind auch $\mathrm{ggT}(a,m) = \mathrm{ggT}(a,n) = 1$ und es gilt*

$$\mathrm{ord}_{mn}(a) = \mathrm{kgV}(\mathrm{ord}_m(a), \mathrm{ord}_n(a)).$$

Beweis. Seien $r := \mathrm{ord}_m(a)$, $s := \mathrm{ord}_n(a)$, $t := \mathrm{ord}_{mn}(a)$ und $v := \mathrm{kgV}(r,s)$. Es ist $t = v$ zu zeigen.
Wegen $a^t \equiv 1 \pmod{mn}$ gilt erst recht $a^t \equiv 1 \pmod{m}$ und $a^t \equiv 1 \pmod{n}$. Damit ist t ein gemeinsames Vielfaches von r und s und deshalb $v = \mathrm{kgV}(r,s) \mid t$.
Um $t \mid v$ zu zeigen, reicht es $a^v \equiv 1 \pmod{mn}$ zu verifizieren. Es gilt $a^v \equiv 1 \pmod{m}$ und $a^v \equiv 1 \pmod{n}$, da v ein Vielfaches sowohl von r als auch von s ist. Also ist a^v eine Lösung der simultanen Kongruenz

$$x \equiv 1 \pmod{m}$$
$$x \equiv 1 \pmod{n}.$$

Eine weitere Lösung dieser simultanen Kongruenz ist aber $x = 1$. Nach dem Chinesischen Restsatz (Satz 4.4.4) ist die Lösungsmenge aber eine Kongruenzklasse modulo $\mathrm{kgV}(m,n)$. Da m, n teilerfremd sind, ist $\mathrm{kgV}(m,n) = mn$. Somit folgt

$$a^v \equiv 1 \pmod{mn}.$$

□

Satz 5.6.4. *Sei $m \in \mathbb{N}$ und sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,m) = 1$. Seien $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen und $n_1, \ldots, n_r \in \mathbb{N}$, so dass $m = \prod_{i=1}^r p_i^{n_i}$ gilt. Dann ist*

$$\mathrm{ord}_m(a) = \mathrm{kgV}(\mathrm{ord}_{p_1^{n_1}}(a), \ldots, \mathrm{ord}_{p_r^{n_r}}(a)).$$

Beweis. Induktion nach r. Für $r = 1$ ist nichts zu zeigen. Ist $r > 1$, so definieren wir $m' := p_2^{n_2} \ldots p_r^{n_r}$ und nehmen an, es gelte

$$\mathrm{ord}_{m'}(a) = \mathrm{kgV}(\mathrm{ord}_{p_2^{n_2}}(a), \ldots, \mathrm{ord}_{p_r^{n_r}}(a)).$$

Da $m = p_1^{n_1} \cdot m'$ und $\mathrm{ggT}(p_1^{n_1}, m') = 1$, können wir Lemma 5.6.3 anwenden. Wir erhalten

$$\begin{aligned}\mathrm{ord}_m(a) &= \mathrm{kgV}(\mathrm{ord}_{p_1^{n_1}}(a), \mathrm{ord}_{m'}(a)) \\ &= \mathrm{kgV}(\mathrm{ord}_{p_1^{n_1}}(a), \mathrm{kgV}(\mathrm{ord}_{p_2^{n_2}}(a), \ldots, \mathrm{ord}_{p_r^{n_r}}(a))) \\ &= \mathrm{kgV}(\mathrm{ord}_{p_1^{n_1}}(a), \ldots, \mathrm{ord}_{p_r^{n_r}}(a)).\end{aligned}$$

□

Bemerkung 5.6.5. Der Satz reduziert die Berechnungen von Ordnungen $\mathrm{ord}_m(a)$ auf die Berechnung von $\mathrm{ord}_{p^n}(a)$, wobei p eine Primzahl ist. Ferner gilt

$$\begin{aligned}&\mathrm{ord}_{p^n}(a) \mid \varphi(p^n) = p^{n-1}(p-1) \\ &\mathrm{ord}_{p^i}(a) \mid \mathrm{ord}_{p^n}(a) \quad (i = 1, \ldots, n-1)\end{aligned}$$

Also kommen für $\mathrm{ord}_{p^n}(a)$ nur die Teiler von $\varphi(p^n)$ infrage, die auch Vielfache von $\mathrm{ord}_{p^{n-1}}(a)$ sind.

Beispiel 5.6.6. Sei $m = 1000$ und $a = 7$. Es gilt $\mathrm{ggT}(7, 1000) = 1$. Berechne $\mathrm{ord}_{1000}(7)$.

- Es gilt $1000 = 8 \cdot 125 = 2^3 \cdot 5^3$.
- Bestimme $\mathrm{ord}_8(7)$. Es gilt $\varphi(8) = 4$. Berechne $7^2 = 49 \equiv 1 \pmod 8$. Deshalb ist $\mathrm{ord}_8(7) = 2$.
- Bestimme $\mathrm{ord}_{125}(7)$. Wir haben $\varphi(125) = 25 \cdot 4 = 100$. Für die Ordnung kommen also nur Teiler von 100 infrage.
  - Zunächst bestimmen wir $\mathrm{ord}_5(7) = \mathrm{ord}_5(2)$. Es ist $\varphi(5) = 4$. Es gilt $2^2 = 4 \not\equiv 1 \pmod 5$. Also ist $\mathrm{ord}_5(7) = 4$.
  - Nun berechnen wir $\mathrm{ord}_{25}(7)$. Da $\varphi(25) = 20$ und $\mathrm{ord}_5(7) = 4$ sind, folgt $\mathrm{ord}_{25}(7) \in \{4, 20\}$. Wir berechnen
    $$7^4 = (49)^2 \equiv (-1)^2 = 1 \pmod{25}$$
    also ist $\mathrm{ord}_{25}(7) = 4$.
  - Schließlich zu $\mathrm{ord}_{125}(7)$. Wegen $\varphi(125) = 100$ und $\mathrm{ord}_{25}(7) = 4$, folgt $\mathrm{ord}_{125}(7) \in \{4, 20, 100\}$. Berechne
    $$7^4 = (49)^2 = 2401 \equiv -99 \pmod{125}$$
    also ist $\mathrm{ord}_{125}(7) \neq 4$. Nun ist
    $$\begin{aligned}7^{20} &= (-99)^5 \\ &= -99 \cdot (99^2)^2 \\ &= -99 \cdot (9801)^2 \\ &\equiv -99 \cdot (51)^2 && \pmod{125} \\ &= -99 \cdot 2601 \\ &\equiv -99 \cdot 101 && \pmod{125} \\ &= -9999 \\ &\equiv 1 && \pmod{125}\end{aligned}$$
    Also ist $\mathrm{ord}_{125}(7) = 20$.
- Wir bekommen $\mathrm{ord}_{1000}(7) = \mathrm{kgV}(2, 20) = 20$.

5.7. **Mersenne-Primzahlen.**

Lemma 5.7.1. *Seien $a, n \in \mathbb{N} \setminus \{1\}$. Falls $a^n - 1$ eine Primzahl ist, so ist $a = 2$ und n eine Primzahl.*

Beweis. Angenommen $a^n - 1$ ist eine Primzahl. Da $a - 1$ ein Teiler von $a^n - 1$ ist, ist $a - 1 = 1$ oder $a - 1 = a^n - 1$. Letzteres ist ausgeschlossen, da $a, n \geq 2$. Also ist $a = 2$. Angenommen n wäre keine Primzahl, so gälte $n = rs$ für $r, s \in \{2, \ldots, n-1\}$. Aber $a^r - 1$ ist ein Teiler von $a^n - 1 = (a^r)^s - 1$. Ein Widerspruch. □

Definition 5.7.2. Sei p eine Primzahl. Die Zahl $M_p := 2^p - 1$ heißt die p-te *Mersenne-Zahl*. Falls M_p eine Primzahl ist, so heißt M_p eine *Mersenne-Primzahl*.

Lemma 5.7.3. *Seien p, q Primzahlen. Falls q die Mersenne-Zahl M_p teilt, gilt $q \equiv 1$ (mod p).*

Beweis. Natürlich ist $q \neq 2$. Da $2^p \equiv 1 \pmod{q}$, folgt $\mathrm{ord}_q(2)$ teilt p. Da p prim ist, gilt $\mathrm{ord}_q(2) = p$. Andererseits ist $\mathrm{ord}_q(2)$ ein Teiler von $\varphi(q) = q - 1$ nach dem Satz von Euler. Somit gilt $p \mid (q-1)$, oder anders ausgedrückt $q \equiv 1 \pmod{p}$. □

Bemerkung 5.7.4. Um zu testen, ob eine Mersenne-Zahl M_p prim ist, reicht es für alle Primzahlen $q < \sqrt{M_p}$ mit $q \equiv 1 \pmod{p}$ zu testen, ob $q \mid M_p$ gilt.

Beispiel 5.7.5.

(1) Sei $p = 11$. Dann ist $M_{11} = 2^{11} - 1 = 2047$. Es gilt $\sqrt{2047} < 50$. Nun bestimme alle $np + 1 < 50$:
$$12, 23, 34, 45.$$
Davon ist nur 23 eine Primzahl. Man rechnet nach, dass $2047 = 23 \cdot 89$. Also ist M_{11} keine Primzahl.

(2) Sei $p = 13$. Dann ist $M_{13} = 2^{13} - 1 = 8191$. Es gilt $\sqrt{8191} < 91$. Bestimme alle $np + 1 < 91$:
$$14, 27, 40, 53, 66, 79.$$
Davon Primzahlen: $53, 79$. Beide teilen nicht 8191. Also ist M_{13} eine Primzahl.

Bemerkung 5.7.6. Mit mehr Theorie kann man einen effektiveren Primzahltest (als den oben geschilderten) für Mersenne-Zahlen herleiten, den sog. Lucas–Lehmer-Test. Damit wurden bis heute (Stand Juni 2021) 51 Mersenne-Primzahlen bestimmt. Es ist weder bekannt, ob es unendlich viele Mersenne-Primzahlen gibt, noch ob es unendlich viele Mersenne-Zahlen gibt, die nicht prim sind. Für mehr Informationen, siehe https://primes.utm.edu/mersenne/index.html.

5.8. **Periodenlänge von Dezimalbrüchen.**

Lemma 5.8.1. *Sei $x \in [0, 1)$ eine reelle Zahl.*

(1) Es existiert eine eindeutig bestimmte Folge $(r_n)_{n \in \mathbb{N}}$ von Zahlen $r_n \in \{0, \ldots, 9\}$, so dass
$$x = \sum_{n=1}^{\infty} r_n \frac{1}{10^n}$$
und so dass $r_n \neq 9$ für unendlich viele $n \in \mathbb{N}$.

(2) *Umgekehrt ist für jede Folge* $(r_n)_{n\in\mathbb{N}}$ *von Zahlen* $r_n \in \{0,\dots,9\}$ *mit* $r_n \neq 9$ *für unendlich viele* $n \in \mathbb{N}$ *die Reihe* $\sum_{n=1}^{\infty} r_n \frac{1}{10^n}$ *konvergent und ihr Reihenwert liegt in* $[0,1)$.

Beweis. Siehe Analysis. □

Definition 5.8.2. Man nennt die Darstellung aus Lemma 5.8.1 die *Dezimalbruchentwicklung* von x.

Beispiel 5.8.3. Die Dezimalbruchentwicklung von $\frac{1}{3}$ ist

$$\frac{1}{3} = \sum_{n=1}^{\infty} 3\frac{1}{10^n} = 0,3333\ldots = 0,\overline{3}$$

Definition 5.8.4. Sei $x \in [0,1)$. Sei $\sum_{n=1}^{\infty} r_n \frac{1}{10^n}$ die Dezimalbruchentwicklung von x.

(1) Man sagt, die Dezimalbruchentwicklung *bricht ab*, wenn es ein $n \in \mathbb{N}$ gibt, so dass $r_n = r_{n+1} = \ldots = 0$ gilt.

(2) Man sagt, die Dezimalbruchentwicklung *ist periodisch*, wenn es $v \in \mathbb{N}_0$ und $l \in \mathbb{N}$ so gibt, dass

$$r_{v+kl+i} = r_{v+i}$$

gilt für alle $i = 1,\dots,l$ und alle $k \in \mathbb{N}$. Man nennt v die *Länge der Vorperiode* und l die *Periodenlänge*.

Bemerkung 5.8.5. Wie gelangt man für eine rationale Zahl von der Darstellung als gekürzter Bruch zur Dezimalbruchentwicklung und umgekehrt?

(1) Sei $x = \frac{a}{b} \in [0,1)$, wobei $a, b \in \mathbb{N}$ teilerfremd seien. Dividiere $10a$ mit Rest durch b und erhalte

$$10a = r_1 b + a_1$$

mit $r_1 \in \{0,\dots,9\}$ und $a_1 < b$. Nun dividiere $10a_1$ mit Rest durch b und erhalte $10a_1 = r_2 b + a_2$. So fortfahrend erhalten wir alle Koeffizienten $r_1, r_2, r_3, \ldots$. Wiederhole das so lange, bis ein Divisionsrest a_n entsteht, der vorher bereits aufgetreten ist. (A priori ist nicht klar, warum das ein endliches Verfahren ist. Das wird in Satz 5.8.7 bewiesen.)

(2) Sei $x = \sum_{n=1}^{\infty} r_n \frac{1}{10^n} \in [0,1)$ eine periodische Dezimalbruchentwicklung mit Vorperiodenlänge v und Periodenlänge l. Also ist

$$x = 0, r_1 \ldots r_v \overline{r_{v+1} \ldots r_{v+l}}.$$

Bringe die Vorperiode und eine Periode vors Komma, also betrachte das 10^{v+l}-fache von x. Subtrahiere davon die das 10^v-fache von x (d.h. bringe die Vorperiode von x vors Komma). Subtrahieren wir diese Zahlen, so erhalten wir

$$10^{v+l}x - 10^v x = 10^v(10^l - 1)x =: n$$

Das ist eine natürliche Zahl, denn $10^{v+l}x$ und $10^v x$ haben die gleichen Nachkommastellen (siehe Satz 5.8.7 für einen formalen Beweis). Also ist

$$x = \frac{n}{10^v(10^l - 1)}.$$

Nun Kürzen.

Beispiel 5.8.6.

(1) Berechne die Dezimalbruchentwicklung von $x = \frac{5}{66}$.

$$\begin{array}{l} 5 \qquad\quad : 66 \quad = \quad 0,0\overline{75} \\ \hline 50 \\ \;\;0 \\ \hline \;\;500 \\ \;\;462 \\ \hline \;\;\;380 \\ \;\;\;330 \\ \hline \;\;\;\;500 \end{array}$$

(2) Berechne umgekehrt die Darstellung von $0,0\overline{75}$ als vollständig gekürzter Bruch:

$$0,0\overline{75} = \frac{75,\overline{75} - 0,\overline{75}}{1000 - 10} = \frac{75}{990} = \frac{5}{66}$$

Satz 5.8.7. *Sei $x \in [0,1)$.*

(1) Falls x irrational ist, so ist die Dezimalbruchentwicklung von x weder abbrechend noch periodisch.
(2) Falls $x \in \mathbb{Q}$ ist, so wähle $a, b \in \mathbb{N}$ teilerfremd mit $x = \frac{a}{b}$. Ferner schreibe $b = 2^r 5^s d$ mit $r, s \in \mathbb{N}_0$ und $d \in \mathbb{N}$, so dass $\mathrm{ggT}(d, 10) = 1$. Dann treten 2 Fälle auf:
  (a) Ist $d = 1$, so bricht die Dezimalbruchentwicklung ab.
  (b) Ist $d > 1$, so ist die Dezimalbruchentwicklung periodisch mit Vorperiodenlänge $v = \max\{r, s\}$ und Periodenlänge $l = \mathrm{ord}_d(10)$.

Beispiel 5.8.8. Betrachte die Dezimalzahl $x = 0,0\overline{75}$. Wir haben bereits gesehen, dass $0,0\overline{75} = \frac{5}{66}$. Da $66 = 2 \cdot 33$, ist $r = 1$, $s = 0$ und $d = 33 = 3 \cdot 11$. Berechne $\mathrm{ord}_{33}(10)$. Offensichtlich ist $10^2 = 100 \equiv 1 \pmod{33}$ (und $10 \not\equiv 1 \pmod{33}$). Also ist $\mathrm{ord}_{33}(10) = 2$. Wir erhalten $v = 1$ und $l = 2$, was mit der Dezimalbruchentwicklung von $\frac{5}{66}$ korreliert.

Beweis.

(1) Wenn die Dezimalbruchentwicklung von x abbricht, so ist x offensichtlich rational. Nun nehmen wir an, die Entwicklung von x sei periodisch, sagen wir mit Vorperiodenlänge v und Periodenlänge l, so wäre

$$x = \sum_{n=1}^{\infty} r_n \frac{1}{10^n} = \underbrace{\frac{10^{v-1} r_1 + \ldots + r_v}{10^v}}_{\in \mathbb{Q}} + \frac{1}{10^v} \sum_{n=v+1}^{\infty} r_n \frac{1}{10^n}.$$

Wir dürfen also ohne Einschränkung $v = 0$ annehmen. Dann gilt also $r_{kl+i} = r_i$ für alle $i = 1, \ldots, l$ und alle $k \in \mathbb{N}$. Wir berechnen

$$\begin{aligned}
x &= \sum_{n=1}^{\infty} r_n \frac{1}{10^n} \\
&= \frac{r_1}{10} + \frac{r_2}{100} + \ldots + \frac{r_l}{10^l} + \\
&\quad + \frac{r_{l+1}}{10^{l+1}} + \frac{r_{l+2}}{10^{l+2}} + \ldots + \frac{r_{2l}}{10^{2l}} + \\
&\quad \vdots \\
&\quad + \frac{r_{kl+1}}{10^{kl+1}} + \frac{r_{kl+2}}{10^{kl+2}} + \ldots + \frac{r_{(k+1)l}}{10^{(k+1)l}} + \\
&\quad \vdots \\
&= \overbrace{\frac{r_1}{10} + \frac{r_2}{100} + \ldots + \frac{r_l}{10^l}}^{=:y \in \mathbb{Q}} + \\
&\quad + \frac{1}{10^l}\left(\frac{r_1}{10} + \frac{r_2}{100} + \ldots + \frac{r_l}{10^l}\right) + \\
&\quad \vdots \\
&\quad + \frac{1}{10^{kl}}\left(\frac{r_1}{10} + \frac{r_2}{100} + \ldots + \frac{r_l}{10^l}\right) + \\
&\quad \vdots \\
&= y \cdot \sum_{k=0}^{\infty} \frac{1}{10^{kl}} \\
&= y \cdot \frac{1}{1 - \frac{1}{10^l}} \\
&= y \cdot \frac{10^l}{10^l - 1} \\
&= \frac{10^{l-1} r_1 + 10^{l-2} r_2 + \ldots + r_l}{10^l - 1}.
\end{aligned}$$

und das ist eine rationale Zahl.

(2) Wir erweitern $x = \frac{a}{b}$ mit $c := 2^{v-r} 5^{v-s}$. Dann ist

$$x = \frac{a}{2^r 5^s d} = \frac{ac}{10^v d}$$

und es gilt $\mathrm{ggT}(ac, d) = 1$.
Falls $d = 1$ ist, bricht die Dezimalbruchentwicklung ab.
Wir nehmen an, dass $d > 1$ ist. Wir dividieren ac durch d mit Rest und erhalten $ac = qd + r$ mit $r \in \{0, \ldots, d-1\}$. Es folgt

$$\frac{a}{b} = \frac{q}{10^v} + \frac{r}{10^v d}.$$

Sei $l := \mathrm{ord}_d(10)$. Es gilt also $d \mid (10^l - 1)$, folglich existiert $e \in \mathbb{N}$ mit $de = 10^l - 1$. Wir erweitern mit e und erhalten

$$\begin{aligned} \frac{a}{b} &= \frac{q}{10^v} + \frac{1}{10^v}\frac{re}{10^l - 1} \\ &= \frac{q}{10^v} + \frac{1}{10^l}\sum_{k=1}^{\infty}\frac{re}{10^{kl}} \end{aligned}$$

Da $re \leq de < 10^l$ bedeutet das, dass die Dezimalbruchentwicklung periodisch mit Periodenlänge l und Vorperiodenlänge v ist. Die Dezimalstellen von re (also die Koeffizienten der 10-adischen Entwicklung) geben genau die Periode an. $\square$

6. Quadratische Reste

Ziel. Sei p eine Primzahl. Ziel dieses Abschnitts ist die Lösung einer allgemeinen quadratischen Kongruenz der Form

$$(*) \qquad ax^2 + bx + c \equiv 0 \pmod{p}$$

wobei $a, b, c \in \mathbb{Z}$ mit $a \not\equiv 0 \pmod{p}$ seien.

6.1. Reduktion auf quadratische Reste.

Konventionen.

- In diesem Unterabschnitt sei p eine Primzahl und seien $a, b, c \in \mathbb{Z}$ mit $a \not\equiv 0 \pmod{p}$.
- Für eine ganze Zahl n schreibe $\overline{n} := n + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$. Für $n \in \mathbb{Z}$ und $a \in \mathbb{Z}$ mit $p \nmid a$ schreiben wir $\frac{\overline{n}}{\overline{a}} := \overline{a}^{-1}\overline{n}$.

Lemma 6.1.1. *Genau dann ist $n \in \mathbb{Z}$ eine Lösung der quadratischen Kongruenz (*), wenn $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$ eine Lösung der quadratischen Gleichung*

$$(\#) \qquad x^2 + \frac{\overline{b}}{\overline{a}}x + \frac{\overline{c}}{\overline{a}} = 0$$

über $\mathbb{Z}/p\mathbb{Z}$ ist.

Beweis. Beachte, dass wegen $a \not\equiv 0 \pmod{p}$ die Restklasse $\overline{a}$ eine Einheit von $\mathbb{Z}/p\mathbb{Z}$ ist. Damit gilt:

$$\begin{aligned} n \text{ ist eine Lösung von } (*) &\Leftrightarrow an^2 + bn + c \equiv 0 \pmod{p} \\ &\Leftrightarrow \overline{a}\,\overline{n}^2 + \overline{b}\overline{n} + \overline{c} = 0 \text{ in } \mathbb{Z}/p\mathbb{Z} \\ &\Leftrightarrow \overline{n}^2 + \frac{\overline{b}}{\overline{a}}\overline{n} + \frac{\overline{c}}{\overline{a}} = 0 \text{ in } \mathbb{Z}/p\mathbb{Z} \\ &\Leftrightarrow \overline{n} \text{ ist eine Lösung von } (\#). \end{aligned}$$

□

Bemerkung 6.1.2. Das obige Lemma reduziert die Lösung einer allgemeinen quadratischen Kongruenz modulo p auf die Lösung von quadratischen Gleichungen der Form

$$(\#\#) \qquad x^2 + \overline{u}x + \overline{v}$$

über $\mathbb{Z}/p\mathbb{Z}$. Auf diese Gleichung möchten wir quadratische Ergänzung anwenden. Jedoch involviert quadratische Ergänzung den Faktor $\frac{1}{2}$, was in $\mathbb{Z}/2\mathbb{Z}$ nicht existiert. Den Fall $p = 2$ müssen wir also gesondert behandeln.

Lemma 6.1.3. *Über $\mathbb{Z}/2\mathbb{Z}$ gibt es die folgenden 4 quadratischen Gleichungen der Form ##:*

(1) $x^2 = \overline{0}$; die einzige Lösung ist $\overline{0}$.
(2) $x^2 + \overline{1} = \overline{0}$; die einzige Lösung ist $\overline{1}$.
(3) $x^2 + x = \overline{0}$; sie hat die Lösungen $\overline{0}$ und $\overline{1}$.
(4) $x^2 + x + 1 = \overline{0}$; sie hat keine Lösungen.

Beweis. Nachprüfen. □

Lemma 6.1.4. *Sei $p \neq 2$ eine Primzahl. Seien $u, v \in \mathbb{Z}$. Sei $n \in \mathbb{Z}$. Genau dann ist $\overline{n}$ eine Lösung von (##), wenn $\overline{n}$ eine Lösung der quadratischen Gleichung*

$$(\#\#\#) \qquad \left(x + \frac{\overline{u}}{\overline{2}}\right)^2 = \frac{\overline{u}^2}{\overline{4}} - \overline{v}$$

über $\mathbb{Z}/p\mathbb{Z}$ ist.

Beweis. Sei $x \in \mathbb{Z}/p\mathbb{Z}$. Es gilt mit quadratischer Ergänzung über $\mathbb{Z}/p\mathbb{Z}$

$$x^2 + \overline{u}x + \overline{v} = x^2 + \overline{u}x + \frac{\overline{u}^2}{\overline{4}} - \left(\frac{\overline{u}^2}{\overline{4}} - \overline{v}\right) = \left(x + \frac{\overline{u}}{\overline{2}}\right)^2 - \left(\frac{\overline{u}^2}{\overline{4}} - \overline{v}\right)$$

und daraus folgt die Gleichheit der beiden Lösungsmengen. □

Bemerkung 6.1.5. Das vorige Lemma reduziert die Lösung einer quadratischen Gleichung über $\mathbb{Z}/p\mathbb{Z}$ für $p \in \mathbb{P} \setminus \{2\}$ von der Form (##) auf eine quadratische Gleichung der Form

$$(\#\#\#\#) \qquad x^2 = \overline{d}$$

wobei $d \in \mathbb{Z}$ ist.

Lemma 6.1.6. *Sei $p \neq 2$ eine Primzahl und $d \in \mathbb{Z}$. Sei $n \in \mathbb{Z}$. Genau dann ist $\overline{n}$ eine Lösung der Gleichung (####), wenn n eine Lösung der quadratischen Kongruenz*

$$(**) \qquad x^2 \equiv d \pmod{p}$$

ist.

Beweis. Gleicher Beweis wie bei Lemma 6.1.1. □

6.2. **Das Legendre-Symbol.**

Definition 6.2.1. Sei p eine Primzahl. Eine Zahl $d \in \mathbb{Z}$ heißt *quadratischer Rest* modulo p, wenn es ein $n \in \mathbb{Z}$ mit $n^2 \equiv d \pmod{p}$ gibt. Andernfalls heißt d ein *quadratischer Nichtrest.*

Definition 6.2.2. Sei p eine Primzahl. Eine Restklasse $d + p\mathbb{Z}$ heißt ein *Quadrat* in $\mathbb{Z}/p\mathbb{Z}$, wenn es ein $n + p\mathbb{Z}$ in $\mathbb{Z}/p\mathbb{Z}$ gibt, so dass $n^2 + p\mathbb{Z} = d + p\mathbb{Z}$. Ansonsten heißt $d + p\mathbb{Z}$ ein *Nicht-Quadrat.*

Definition 6.2.3. Sei p eine Primzahl und sei $d \in \mathbb{Z}$. Definiere

$$\left(\frac{d}{p}\right) := \begin{cases} 1 & d \not\equiv 0 \pmod{p} \text{ und } d \text{ ist quadratischer Rest modulo } p \\ -1 & d \text{ ist quadratischer Nichtrest modulo } p \\ 0 & d \equiv 0 \pmod{p} \end{cases}$$

Man nennt $\left(\frac{d}{p}\right)$ das *Legendre-Symbol* d nach p.

Bemerkung 6.2.4. Sei p eine Primzahl und sei $d \in \mathbb{Z}$. Folgende Aussagen sind äquivalent:

- d ist ein quadratischer Rest modulo p.
- Die quadratische Kongruenz $x^2 \equiv d \pmod{p}$ ist lösbar.
- $\left(\frac{d}{p}\right) \in \{0, 1\}$.
- $d + p\mathbb{Z}$ ist ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$.

Ferner gilt für $d' \in \mathbb{Z}$ mit $d \equiv d' \pmod{p}$:

(1) Genau dann ist d ein quadratischer Rest modulo p, wenn d' ein quadratischer Rest modulo p ist.
(2) $\left(\frac{d}{p}\right) = \left(\frac{d'}{p}\right)$.

Beispiel 6.2.5. Bestimme alle $d \in \{0, \ldots, 4\}$, die quadratische Reste modulo $p = 5$ sind. Es gilt

$$0^2 = 0 \qquad 1^2 = 1 \qquad 2^2 = 4 \qquad 3^2 \equiv 4 \qquad 4^2 \equiv 1$$

(jeweils mod 5). Also ist d genau dann ein quadratischer Rest modulo 5, wenn $d \equiv 0$, $d \equiv 1$, oder $d \equiv 4 \pmod{5}$ ist. Damit können wir auch die Legendre-Symbole nach 5 berechnen:

$$\left(\frac{0}{5}\right) = 0 \qquad \left(\frac{1}{5}\right) = 1 \qquad \left(\frac{2}{5}\right) = -1 \qquad \left(\frac{3}{5}\right) = -1 \qquad \left(\frac{4}{5}\right) = 1$$

Lemma 6.2.6. *Sei $p \neq 2$ eine Primzahl. Sei $d \in \mathbb{Z}$.*

(1) Genau dann ist d ein quadratischer Rest modulo p, wenn $d \equiv a \pmod{p}$ für ein $a \in \{0, 1, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\}$ ist.
(2) Es gibt in $\mathbb{Z}/p\mathbb{Z}$ genau $\frac{p+1}{2}$ Quadrate und $\frac{p-1}{2}$ Nicht-Quadrate.

Beweis.

(1) Zu „$\Leftarrow$“: Jede Quadratzahl ist ein quadratischer Rest modulo p.
Zu „$\Rightarrow$“: Sei d ein quadratischer Rest modulo p. Es gibt also ein $n \in \mathbb{Z}$ mit $n^2 \equiv d \pmod{p}$. Dann existiert auch ein $m \in \{0, \ldots, p-1\}$ mit $m^2 \equiv d \pmod{p}$. Ist $m > \frac{p-1}{2}$, so ist $1 \leq p - m \leq \frac{p-1}{2}$ und

$$(p-m)^2 = (m-p)^2 \equiv m^2 \equiv d \pmod{p}.$$

(2) Wir haben in (1) gezeigt, dass

$$\{\overline{d} \in \mathbb{Z}/p\mathbb{Z} \mid \overline{d} \text{ Quadrat in } \mathbb{Z}/p\mathbb{Z}\} = \{\overline{n}^2 \mid n \in \underbrace{\{0, 1, \ldots, \frac{p-1}{2}\}}_{\frac{p+1}{2} \text{ Elemente}}\}$$

Daher reicht es zu zeigen, dass $n^2 \not\equiv m^2 \pmod{p}$ für alle $n, m \in \{0, 1, \ldots, \frac{p-1}{2}\}$ mit $n \neq m$. Angenommen doch. Dann gilt

$$p \mid n^2 - m^2 = (n-m)(n+m)$$

und da $p \nmid n+m$ (denn $0 < n+m < p$) muss $p \mid n-m$ gelten. Da aber $|n-m| < p$ ist, muss $n - m = 0$ sein. □

Beispiel 6.2.7. Sei $p = 11$. Schreibe $\overline{n} := n + 11\mathbb{Z} \in \mathbb{Z}/11\mathbb{Z}$. Es gibt in $\mathbb{Z}/11\mathbb{Z}$ genau 6 Quadrate; sie sind

$$\overline{0},\ \overline{1},\ \overline{2}^2 = \overline{4},\ \overline{3}^2 = \overline{9},\ \overline{4}^2 = \overline{16} = \overline{5},\ \overline{5}^2 = \overline{25} = \overline{3}.$$

Die quadratischen Nicht-Reste sind demnach $\overline{2}, \overline{6}, \overline{7}, \overline{8}, \overline{10}$.

6.3. **Exkurs über Polynome über Körpern.**

Definition 6.3.1. Sei K ein Körper. Ein *Polynom* über K in der Unbestimmten X ist eine formales Symbol $f = \sum_{n=0}^{d} a_n X^n$, wobei $a_0, \ldots, a_d \in K$ seien. Mit $K[X]$ bezeichnen wir die Menge der Polynome in der Unbestimmten X.

Beispiel 6.3.2. Sei $K = \mathbb{Q}$ und betrachte das Polynom $f = 7X^3 + 4X + 1$. Dann sind also die Koeffizient $a_3 = 7$, $a_1 = 4$ und $a_0 = 1$.

Bemerkung 6.3.3. Seien $f = \sum_{n=0}^{d} a_n X^n$ und $g = \sum_{n=0}^{e} b_n X^n$ Polynome über K. Definiere

$$\begin{aligned} f + g &:= \sum_{n=0}^{\max\{d,e\}} (a_n + b_n) X^n \\ f \cdot g &:= \sum_{n=0}^{d} \sum_{m=0}^{e} a_n b_m X^{n+m} = \sum_{k=0}^{d+e} \Big(\sum_{n+m=k} a_n b_m \Big) X^k \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1 + a_2 b_0) X^2 + \ldots + a_d b_e X^{d+e} \end{aligned}$$

Dann sind $f+g$ und $f \cdot g$ wieder Polynome über K in der Unbestimmten X. Wir erhalten also Abbildungen

$$+, \cdot : K[X] \times K[X] \to K[X].$$

Beispiel 6.3.4. Bei der Addition und Multiplikation von Polynomen können wir so rechnen, als handele es sich bei X um eine Zahl (die wir nicht kennen).
Sei zum Beispiel $K = \mathbb{R}$ und $f = 3X^2 + 9$ (d.h. $d = 2$ und $a_0 = 9, a_1 = 0, a_2 = 3$), sowie $g = 7X + 1$ (also $e = 1$ und $b_0 = 1, b_1 = 7$); alle anderen a_n und b_m sind 0. Mit den Definitionen von $+$ und $\cdot$ berechnen wir

$$\begin{aligned} f + g &= a_0 + b_0 + (a_1 + b_1) X + (a_2 + b_2) X^2 \\ &= 10 + 7X + 3X^2 \\ f \cdot g &= a_0 b_0 + (a_0 b_1 + a_1 b_0) X + (a_1 b_1 + a_2 b_0) X^2 + a_2 b_1 X^3 \\ &= 9 + 63X + 3X^2 + 21X^3. \end{aligned}$$

Lemma 6.3.5. *Sei K ein Körper. Mit den Abbildungen $+$ und $\cdot$ ist $K[X]$ ein Ring.*

Beweis. Die Null von $K[X]$ ist $0 = 0 \cdot X^0$ und die Eins ist $1 = 1 \cdot X^0$. Wir müssen die Ringaxiome nachprüfen. Wir weisen exemplarisch eines der Distributivgesetze nach.

Seien $f = \sum_n a_n X^n$, $g = \sum_n b_n X^n$ und $h = \sum_n c_n X^n$ drei Polynome. Dann gilt

$$\begin{aligned} f \cdot (g+h) &= \Big(\sum_n a_n X^n\Big) \cdot \Big(\sum_m (b_m + c_m) X^n\Big) \\ &= \sum_k \Big(\sum_{n+m=k} a_n(b_m + c_m)\Big) X^k \\ &= \sum_k \Big(\sum_{n+m=k} (a_n b_m + a_n c_m)\Big) X^k \\ &= \sum_k \Big(\sum_{n+m=k} a_n b_m\Big) X^k + \sum_k \Big(\sum_{n+m=k} a_n c_m\Big) X^k \\ &= f \cdot g + f \cdot h. \end{aligned}$$

Dabei haben wir in der dritten Umformung das Distributivgesetz in K angewendet. Die restlichen Ringaxiome sind ähnlich einfach zu verifizieren. □

Definition 6.3.6. Sei $f = \sum_{n=0}^d a_n X^n \in K[X]$ und sei $b \in K$. Wir definieren

$$f(b) := \sum_{n=0}^d a_n b^n \in K$$

Man nennt $f(b)$ den *Wert* von f an b. Falls $f(b) = 0$ ist, so nennen wir b eine *Nullstelle* von f (in K).

Beispiel 6.3.7. Sei $f = X^2 + 1 \in \mathbb{R}[X]$. Dann ist $f(b) = b^2 + 1 > 0$ für alle $b \in \mathbb{R}$. Also hat das Polynom f keine Nullstelle in $\mathbb{R}$. Fassen wir allerdings f als ein Polynom in $\mathbb{C}[X]$ auf, so hat f Nullstellen in $\mathbb{C}$, nämlich i und $-i$.

Bemerkung 6.3.8.

(1) Sei $b \in K$. Dann ist die Abbildung $\varphi_b : K[X] \to K$ definiert durch $\varphi_b(f) := f(b)$ ein Ringhomomorphismus. (Der Beweis ist leicht; wir überlassen ihn als Übung, da wir die Aussage auch nicht weiter verwenden müssen.)

(2) Sei $f \in K[X]$ ein Polynom. Dann erhalten wir eine Funktion $\tilde{f} : K \to K$ definiert durch $\tilde{f}(b) := f(b)$. Wenn K ein endlicher Körper ist, kann es passieren, dass $\tilde{f}$ die Nullfunktion ist, obwohl f nicht das Nullpolynom ist. Betrachte zum Beispiel $K = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ und das Polynom

$$f = (X - \overline{0})(X - \overline{1}) \ldots (X - \overline{p-1}).$$

Das ist nicht das Nullpolynom, denn der Koeffizient von X^p ist $\overline{1}$. Allerdings ist jedes $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$ eine Nullstelle von f, denn

$$f(\overline{n}) = (\overline{n} - \overline{0}) \ldots (\underbrace{\overline{n} - \overline{n}}_{=\overline{0}}) \ldots (\overline{n} - \overline{p-1}) = 0.$$

Also ist $\tilde{f}$ die Nullfunktion.
Wenn wir über endlichen Körpern arbeiten wollen, ist es also wichtig zwischen Polynomen und polynomialen Funktionen zu unterscheiden.

Definition 6.3.9. Sei $f = \sum_{n=0}^{d} a_n X^n$ ein Polynom über eine Körper K in X. Gelte $f \neq 0$. Man nennt

$$k = \max\{n \in \{1, \ldots, d\} \mid a_n \neq 0\}$$

den *Grad* von f. Wir schreiben $\deg(f) := k$ für den Grad.
Formal definieren wir $\deg(0) := -\infty$.

Satz 6.3.10 (Division mit Rest im Polynomring über einem Körper)**.** *Sei K ein Körper. Sei $f \in K[X]$ ein Polynom mit $f \neq 0$. Dann gibt es für jedes $g \in K[X]$ eindeutig bestimmte $q \in K[X]$ und $r \in K[X]$ mit*

$$g = qf + r$$

und $\deg(r) < \deg(f)$.

Beweis. Zur Existenz: Sei $d := \deg(f)$ und $e := \deg(g)$. Wir Beweisen die Existenz per Induktion über e. Ist $e < d$, so ist nichts zu zeigen. Sei $e > d$ und wir nehmen an, die behauptete Existenzaussage gelte für alle Polynome $g' \in K[X]$ mit $\deg(g') < e$. Seien

$$f = a_d X^d + \text{Terme von Grad} < d$$
$$g = b_e X^e + \text{Terme von Grad} < e$$

Betrachte

$$g' := g - \underbrace{\frac{b_e}{a_d} X^{e-d}}_{=:q''} \cdot f$$

(beachte, dass $a_d \in K \setminus \{0\} = K^\times$ ist, also können wir durch a_d dividieren). Dann ist $\deg(g') < e$, also greift die Induktionsannahme. Wir finden $q' \in K[X]$ und $r \in K[X]$, so dass $\deg(r) < d$ und

$$g' = q'f + r.$$

Wir berechnen

$$g = g' + q''f = q'f + r + q''f = (q' + q'')f + r.$$

Zur Eindeutigkeit: Sei $g = q_1 f + r_1 = q_2 f + r_2$, wobei $\deg(r_1), \deg(r_2) < d$ sind. Dann folgt

$$(q_1 - q_2)f = r_2 - r_1.$$

Angenommen $q_1 \neq q_2$. Dann ist $\deg((q_1 - q_2)f) \geq \deg(f) = d$. Andererseits ist aber $\deg(r_2 - r_1) \leq \max\{\deg(r_1), \deg(r_2)\} < d$. Das ist ein Widerspruch. Also muss $q_1 = q_2$ gelten und damit auch $r_1 = r_2$. □

Beispiel 6.3.11. Die Polynome q und r aus dem obigen Satz bestimmt man durch Polynomdivision.

(1) Sei $K = \mathbb{R}$ und seien $g = X^3 + X^2 + X + 1 \in \mathbb{R}[X]$ und $f = X - 1 \in \mathbb{R}[X]$.

$$\begin{array}{rl}
(X^3 + X^2 + X + 1) & : (X - 1) \;=\; X^2 + 2X + 3 \\
-(X^3 - X^2) & \\
\hline
2X^2 + X + 1 & \\
-(2X^2 - 2X) & \\
\hline
3X + 1 & \\
-(3X - 3) & \\
\hline
4 &
\end{array}$$

Dann ist $q = X^2 + 2X + 3$ und $r = 4$.

(2) Sei $K = \mathbb{Z}/2\mathbb{Z}$ und $g = X^3 + X^2 + X + \overline{1} \in \mathbb{Z}/2\mathbb{Z}[X]$ und $f = X - \overline{1} \in (\mathbb{Z}/2\mathbb{Z})[X]$. Die gleiche Rechnung zeigt $q = X^2 + \overline{2}X + \overline{3} = X^2 + \overline{1}$ und $r = \overline{4} = \overline{0}$.

Korollar 6.3.12. *Sei $g \in K[X]$ ein Polynom über einem Körper K in X und sei $b \in K$. Genau dann ist b eine Nullstelle von g, wenn es ein Polynom $g \in K[X]$ so gibt, dass*

$$g = (X - b) \cdot q.$$

Beweis. Zu „$\Rightarrow$“: Sei b eine Nullstelle von g. Dividiere g mit Rest durch $f = X - b$. Wir erhalten $q \in K[X]$ und $r \in K[X]$ mit $g = (X - b)q + r$ und $\deg(r) < \deg(X - b) = 1$. Also ist $r = c \in K$. Dann ist

$$0 = g(b) = \underbrace{(b - b)q(b)}_{=0} + \underbrace{r(b)}_{=c} = c$$

und demnach $g = (X - b)q$.
Zu „$\Leftarrow$“: Ist klar. □

Korollar 6.3.13. *Sei $g \in K[X] \setminus \{0\}$ ein Polynom vom Grad d. Dann hat g höchstens d Nullstellen über K.*

Beweis. Per Induktion über d. Ist $d = 0$, so ist $g = a_0 \in K^\times$ ein konstantes Polynom, aber nicht das Nullpolynom. Dann hat g keine Nullstellen. Ist $d = 1$, so ist $g = a_1X + a_0$ mit $a_1 \in K^\times$. Die einzige Nullstelle von g ist $b = -a_0/a_1$. Sei nun $d > 1$. Falls g keine Nullstelle in K besitzt sind wir fertig. Andernfalls sei b eine Nullstelle von g. Nach Korollar 6.3.12 gibt es ein $q \in K[X]$ mit $g = (X - b) \cdot q$. Da q Grad $d - 1$ hat, greift die Induktionsannahme. Danach hat q höchstens $d - 1$ Nullstellen. Damit hat g höchstens d Nullstellen. □

6.4. **Das Euler-Kriterium.**

Satz 6.4.1 (Euler-Kriterium)**.** *Sei $p \neq 2$ eine Primzahl und sei $d \in \mathbb{Z}$. Dann gilt*

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

Beweis. Falls $p \mid d$, so sind beide Seiten kongruent zu 0 modulo p. Wir nehmen also $p \nmid d$ an. Dann gilt nach dem kleinen Satz von Fermat $d^{p-1} \equiv 1 \pmod{p}$, oder äquivalent

$$\overline{d}^{p-1} = \overline{1}$$

in $\mathbb{Z}/p\mathbb{Z}$. Betrachte das Polynom $f = X^{p-1} - \overline{1} \in (\mathbb{Z}/p\mathbb{Z})[X]$. Dann ist $\overline{d}$ eine Nullstelle von f in $\mathbb{Z}/p\mathbb{Z}$. Somit ist jedes $\overline{d} \in (\mathbb{Z}/p\mathbb{Z})^\times$ eine Nullstelle von f in $\mathbb{Z}/p\mathbb{Z}$. Der Grad von f ist aber $p - 1$, weshalb das auch die einzigen Nullstellen von f sind.
Nach dritter binomischer Formel können wir f faktorisieren als

$$f = (\underbrace{X^{\frac{p-1}{2}} - 1}_{=:g})(\underbrace{X^{\frac{p-1}{2}} + 1}_{=:h})$$

Nun unterscheide 2 Fälle:

Fall 1: Sei d ein quadratischer Rest modulo p. Dann ist $\overline{d}$ ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$. Also gibt es ein $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$, so dass $\overline{d} = \overline{a}^2$. Damit ist

$$\overline{d}^{\frac{p-1}{2}} = \overline{a}^{p-1} = 1$$

nach dem kleinen Satz von Fermat (beachte $\overline{a} \neq \overline{0}$, also $p \nmid a$). Das bedeutet $\overline{d}$ ist eine Nullstelle von g. Es gilt also

$$d \text{ quadratischer Rest modulo } p \text{ und } p \nmid d \Rightarrow d^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$d \text{ quadratischer Rest modulo } p \text{ und } p \nmid d \Rightarrow \left(\frac{d}{p}\right) = 1.$$

Die Behauptung gilt also in diesem Fall.
Allerdings gibt es genau $\frac{p-1}{2}$ von $\overline{0}$ verschiedene Quadrate in $\mathbb{Z}/p\mathbb{Z}$. Deshalb sind die einzigen Nullstellen von g in $\mathbb{Z}/p\mathbb{Z}$ die von $\overline{0}$ verschiedenen Quadrate in $\mathbb{Z}/p\mathbb{Z}$.
Fall 2: Sei d ein quadratischer Nicht-Rest modulo p. Dann ist $\overline{d}$ kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$. Wir haben bereits gezeigt, dass $\overline{d}$ keine Nullstelle von g sein kann. Aber $\overline{d}$ ist eine Nullstelle von $f = gh$. Demnach muss $\overline{d}$ eine Nullstelle von h sein. Somit gilt

$$d \text{ quadratischer Nicht-Rest modulo } p \Rightarrow d^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

$$d \text{ quadratischer Nicht-Rest modulo } p \Rightarrow \left(\frac{d}{p}\right) = -1.$$

Die Behauptung ist also auch in diesem Fall richtig. □

Korollar 6.4.2. *Sei $p \neq 2$ eine Primzahl. Dann gilt:*

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

(2) Für alle $a, b \in \mathbb{Z}$ ist $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Beweis.

(1) Es gilt nach dem Euler-Kriterium

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

Beide Seiten sind aber in $\{\pm 1\}$ enthalten. Da $1 \not\equiv -1 \pmod{p}$ gilt, sind beide Seiten sogar gleich. Das zeigt die erste behauptete Gleichung. Die zweite Gleichung ist sofort klar.

(2) Wir wenden das Euler-Kriterium zweimal an und erhalten

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

In diesem Fall sind beide Seiten in $\{0, \pm 1\}$. Diese drei Zahlen sind paarweise nicht kongruent modulo p, also sind die beiden Seiten der obigen Kongruenz gleich. □

Beispiel 6.4.3. Sei $p = 83$. Dann ist $p \equiv 3 \pmod{4}$.

(1) Es gilt $\left(\frac{-1}{83}\right) = -1$.

(2) Sei $d = 60 = 4 \cdot 15$. Dann ist $\left(\frac{60}{83}\right) = \left(\frac{4}{83}\right)\left(\frac{15}{83}\right) = \left(\frac{15}{83}\right)$, denn $\left(\frac{4}{83}\right) = 1$, da $4 = 2^2$ ein quadratischer Rest modulo 83 ist. Wir berechnen weiter $\left(\frac{15}{83}\right) = \left(\frac{3}{83}\right)\left(\frac{5}{83}\right)$. Um das weiter zu vereinfachen, brauchen wir mehr Theorie.

6.5. **Das quadratische Reziprozitätsgesetz.**

Lemma 6.5.1. *Für eine Primzahl $p \neq 2$ ist $p^2 - 1$ durch 8 teilbar und es gilt*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \ (mod\ 8) \\ -1 & p \equiv \pm 3 \ (mod\ 8) \end{cases}$$

Satz 6.5.2 (Quadratisches Reziprozitätsgesetz)**.** *Seien $p \neq q$ zwei Primzahlen mit $p, q \neq 2$. Dann gilt*

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

Bemerkung 6.5.3. Für den Beweis von Lemma 6.5.1 und des quadratischen Reziprozitätsgesetzes brauchen wir einiges an Vorbereitung. Zunächst ziehen wir eine Folgerung und berechnen als Anwendung einige Legendre-Symbole.

Korollar 6.5.4. *Seien $p \neq q$ zwei Primzahlen mit $p, q \neq 2$. Dann gilt*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{falls } p \equiv 1 \ (mod\ 4) \text{ oder } q \equiv 1 \ (mod\ 4) \\ -\left(\frac{q}{p}\right) & \text{falls } p \equiv 3 \equiv q \ (mod\ 4). \end{cases}$$

Beweis. Nach dem quadratischen Reziprozitätsgesetz ist

$$\begin{aligned} \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \\ &= \begin{cases} 1 & p \equiv 1 \pmod 4 \text{ oder } q \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \equiv q \pmod 4. \end{cases} \end{aligned}$$

□

Beispiel 6.5.5. Wir haben gesehen, dass $\left(\frac{60}{83}\right) = \left(\frac{3}{83}\right)\left(\frac{5}{83}\right)$. Da $3 \equiv 3 \equiv 83 \pmod 4$ ist nach Satz 6.5.2

$$\left(\frac{3}{83}\right) = -\left(\frac{83}{3}\right) = -\left(\frac{2}{3}\right) = 1$$

nach Division mit Rest und Lemma 6.5.1. Andererseits gilt

$$\left(\frac{5}{83}\right) = \left(\frac{83}{5}\right) = \left(\frac{3}{5}\right) = -1$$

letzteres folgt aus dem Euler-Kriterium. Insgesamt gilt also $\left(\frac{60}{83}\right) = -1$.

Beispiel 6.5.6. Seien $p = 67$ und $q = 139$. Beides sind Primzahlen mit $p \equiv 3 \equiv q \pmod 4$. Also gilt nach quadratischem Reziprozitätsgesetz

$$\left(\frac{67}{139}\right) = -\left(\frac{139}{67}\right)$$

Da $139 = 2 \cdot 67 + 5$ ist $\left(\frac{139}{67}\right) = \left(\frac{5}{67}\right)$. Es gilt $5 \equiv 1 \pmod 4$. Also ist wieder mit quadratischem Reziprozitätsgesetz

$$\left(\frac{5}{67}\right) = -\left(\frac{67}{5}\right) = -\left(\frac{2}{5}\right)$$

Da $5 \equiv -3 \pmod 8$, ist $\left(\frac{2}{5}\right) = -1$. Demnach ist unter Verwenndung von Lemma 6.5.1

$$\left(\frac{67}{139}\right) = 1.$$

Somit ist 67 ein quadratischer Rest modulo 139.

Algorithmus 6.5.7. Seien $p \neq 2$ eine Primzahl und $d \in \mathbb{Z}$. Der Algorithmus berechnet das Legendre-Symbol $\left(\frac{d}{p}\right)$ (und damit, ob d ein quadratischer Rest modulo p ist oder nicht).

(1) Dividiere d durch p mit Rest und erhalte $d = ap + r$ mit $r \in \{0, \dots, p-1\}$. Es gilt dann $\left(\frac{d}{p}\right) = \left(\frac{r}{p}\right)$.

(2) Falls $r \in \{0, 1, p-1\}$ ist, so bestimme $\left(\frac{r}{p}\right)$ direkt:
- Für $r = 0$ ist $\left(\frac{r}{p}\right) = 0$.
- Für $r = 1$ ist $\left(\frac{r}{p}\right) = 1$.
- Für $r = p-1$ ist $\left(\frac{r}{p}\right) = \left(\frac{-1}{p}\right)$. Benutze Korollar 6.4.2.

(3) Ansonsten zerlege r in Primfaktoren

$$r = q_1^{n_1} \dots q_l^{n_l} q_{l+1}^{n_{l+1}} \dots q_s^{n_s}$$

in paarweise verschiedene Primzahlen $q_1, \dots, q_s$ und $n_1, \dots, n_s \in \mathbb{N}$ mit $n_1, \dots, n_l$ ungerade und $n_{l+1}, \dots, n_s$ gerade. Nach Korollar 6.4.2 gilt

$$\left(\frac{r}{p}\right) = \left(\frac{q_1}{p}\right) \dots \left(\frac{q_l}{p}\right)$$

Berechne die einzelnen $\left(\frac{q_i}{p}\right)$.
- Falls $q_i = 2$, benutze Lemma 6.5.1.
- Falls $q_i \neq 2$, so ist nach dem quadratischen Reziprozitätsgesetz

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

Wende den Algorithmus auf $\left(\frac{p}{q_i}\right)$ an.

6.6. **Die Gaußschen Zahlen.**

Definition 6.6.1. Eine *Gaußsche Zahl* ist eine komplexe Zahl der Form $a + bi$ mit $a, b \in \mathbb{Z}$. Mit $\mathbb{Z}[i]$ bezeichnen wir die Menge der Gaußschen Zahlen, also

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Lemma 6.6.2.

(1) Die Summe und das Produkt von zwei Gaußschen Zahlen ist eine Gaußsche Zahl. Damit erhalten wir Abbildungen $+, \cdot : \mathbb{Z}[i] \times \mathbb{Z}[i] \to \mathbb{Z}[i]$.
(2) $0 = 0 + 0i$ *und* $1 = 1 + 0i$ *sind Gaußsche Zahlen.*
(3) Zusammen mit $+$ *und* $\cdot$ *wie in (1) ist* $\mathbb{Z}[i]$ *ein Ring.*

Beweis.

(1) Seien $z = a + bi$ und $z' = a' + b'i$ Gaußsche Zahlen. Dann sind

$$z + z' = (a + a') + (b + b')i \qquad zz' = (aa' - bb') + (ab' + a'b)i$$

ebenfalls Gaußsche Zahlen.
(2) Klar.
(3) Die Ringaxiome folgen aus den Ringaxiomen von $\mathbb{C}$; dabei beachten wir, dass $0, 1 \in \mathbb{Z}[i]$ ist und das negative einer Gaußschen Zahl wieder eine Gaußsche Zahl ist. □

Bemerkung 6.6.3. Wir identifizieren eine ganze Zahl $a \in \mathbb{Z}$ mit der Gaußschen Zahl $a + 0i$. Auf diese Weise können wir $\mathbb{Z}$ als Teilmenge von $\mathbb{Z}[i]$ ansehen.

Lemma 6.6.4.

(1) Seien $z, w \in \mathbb{Z}[i]$. *Falls* $zw = 0$, *so ist* $z = 0$ *oder* $w = 0$.
(2) $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Beweis.

(1) Sei $z \neq 0$. Da $\mathbb{C}$ ein Körper ist, existiert ein Inverses $z^{-1} \in \mathbb{C}$ (nicht notwendig in $\mathbb{Z}[i]$). Dann ist $0 = z^{-1}zw = w$.
(2) Zu „$\supseteq$“: Offensichtlich sind ± 1 und $\pm i$ Einheiten von $\mathbb{Z}[i]$.
Zu „$\subseteq$“: Sei $z = a + bi \in \mathbb{Z}[i]^\times$. Dann gibt es ein $w = c + di \in \mathbb{Z}[i]$ mit $zw = 1$. Betrachte das Quadrat des Betrags $|z|^2 = a^2 + b^2 \in \mathbb{N}_0$. Da

$$1 = |1|^2 = |z|^2|w|^2$$

gilt, muss $|z|^2 = 1$ sein. Damit $a^2 + b^2 = 1$ werden kann, muss entweder $a = \pm 1$ sein und $b = 0$, oder es muss $a = 0$ und $b = \pm 1$ gelten. Das sind genau die 4 Einheiten ± 1 und $\pm i$. □

Definition 6.6.5. Seien $x, y, z \in \mathbb{Z}[i]$. Wir schreiben $x \equiv y \pmod{z}$, wenn es ein $w \in \mathbb{Z}[i]$ gibt, so dass $zw = y - x$. In diesem Fall sagen wir x und y seien *kongruent* modulo z.

Bemerkung 6.6.6.

(1) Die Relation Kongruenz modulo z ist eine Äquivalenzrelation auf $\mathbb{Z}[i]$.
(2) Sind $x \equiv x' \pmod{z}$ und $y \equiv y' \pmod{z}$, so sind auch $x + x' \equiv y + y' \pmod{z}$ und $xx' \equiv yy' \pmod{z}$.

Lemma 6.6.7. *Sei* $m \in \mathbb{N}$ *und betrachte* m *als Gaußsche Zahl. Für Gaußsche Zahlen* $x = a + bi$ *und* $x' = a' + b'i$ *gilt genau dann* $x \equiv x' \pmod{m}$, *wenn* $a \equiv a' \pmod{m}$ *und* $b \equiv b' \pmod{m}$.

Beweis. Genau dann ist $x \equiv x' \pmod{m}$, wenn es ein $w = c + di \in \mathbb{Z}[i]$ gibt mit

$$(+) \qquad x - x' = wm.$$

Es gilt einerseits $x - x' = (a - a') + (b - b')i$ und andererseits $wm = cm + (dm)i$. Also ist $(+)$ äquivalent zu

$$\begin{aligned} a - a' &= cm \\ b - b' &= dm \end{aligned}$$

und das ist gleichbedeutend mit $a \equiv a' \pmod{m}$ und $b \equiv b' \pmod{m}$. $\square$

Beweis von Lemma 6.5.1. Beachte, dass sowohl $p - 1$ als auch $p + 1$ gerade sind und genau eine der beiden Zahlen durch 4 teilbar ist. Damit ist $p^2 - 1 = (p-1)(p+1)$ durch 8 teilbar.
Schreibe $p = 8k + r$ mit $r \in \{1, 3, 5, 7\}$. Es gilt $2 = -i(1+i)^2$ (denn $-i(1+i)^2 = -i(1 + 2i + i^2) = -i \cdot 2i = 2$). Also gilt nach dem Euler-Kriterium

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

Wir multiplizieren diese Gleichung mit $(1 + i)$ durch und erhalten

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

Mit der (ersten) binomischen Formel berechnen wir

$$(1+i)^p = 1 + \sum_{n=1}^{p-1} \binom{p}{n} i^n + i^p \equiv 1 + i^p \pmod{p}$$

denn für jedes $n \in \{1, \ldots, p\}$ ist $\binom{p}{n} = \frac{p!}{n!(p-n)!}$ durch p teilbar. Also folgern wir

$$\begin{aligned} (1+i)\left(\frac{2}{p}\right) &\equiv (-i)^{\frac{p-1}{2}}(1+i^p) \pmod{p} \\ &= (-i)^{\frac{8k+r-1}{2}}(1+i^{8k+r}) \\ &= (-i)^{4k}(-i)^{\frac{r-1}{2}}(1+i^{8k}i^r) \\ &= (-i)^{\frac{r-1}{2}}(1+i^r) \\ &= \begin{cases} 1+i & r=1 \\ (-i)(1-i) = -(1+i) & r=3 \\ (-i)^2(1+i^5) = -(1+i) & r=5 \\ (-i)^3(1+i^7) = 1+i & r=7. \end{cases} \end{aligned}$$

Beide Seiten der obigen Kongruenz sind von der Form $\pm(1+i)$. Da $1+i \not\equiv -(1+i) \pmod{p}$, muss die obige Kongruenz bereits eine Gleihheit sein. Nach Lemma 6.6.4(1) können wir $(1 + i)$ aus der obigen Gleichung kürzen und erhalten

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & r=1 \\ -1 & r=3 \\ -1 & r=5 \\ 1 & r=7. \end{cases}$$

Das zeigt die Gleichheit der linken und der rechten Seite der behaupteten Gleichung. Um zu zeigen, dass die rechte Seite der Gleichung mit der mittleren übereinstimmt, berechnen wir

$$\frac{p^2-1}{8} = \frac{64k^2 - 16kr + r^2 - 1}{8} = 8k^2 - 2kr + \frac{r^2-1}{8}$$

und deshalb gilt

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{r^2-1}{8}} = \begin{cases} 1 & r = 1 \\ -1 & r = 3 \\ -1 & r = 5 \\ 1 & r = 7. \end{cases}$$

□

6.7. **Der Beweis des quadratischen Reziprozitätsgesetzes.**

Lemma 6.7.1 (Eisenstein)**.** *Seien $p, q \neq 2$ Primzahlen mit $p \neq q$. Definiere*

$$S(p,q) := \sum_{n=0}^{\frac{p-1}{2}} \left\lfloor \frac{nq}{p} \right\rfloor .$$

Dann gilt die Identität

$$S(p,q) + S(q,p) = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Beweis. Betrachte die Funktion

$$\begin{aligned} f : \{1, \ldots, \frac{p-1}{2}\} \times \{1, \ldots, \frac{q-1}{2}\} &\to \mathbb{Z} \\ (n,m) &\mapsto nq - mp \end{aligned}$$

Die Funktion f ist injektiv. Um das zu sehen, seien $(n,m), (n',m') \in \{1, \ldots, \frac{p-1}{2}\} \times \{1, \ldots, \frac{q-1}{2}\}$, so dass $f(n,m) = f(n',m')$, das heißt

$$nq - mp = n'q - m'p$$

Daraus folgt $(n-n')q = (m-m')p$. Da p eine Primzahl ist, die nicht q teilt, folgt $p \mid n - n'$. Aber $-\frac{p-1}{2} \leq n - n' \leq \frac{p-1}{2}$, deshalb muss bereits $n - n' = 0$ gelten. Auf die gleiche Art sieht man $m = m'$.
Ein ähnliches Argument zeigt außerdem, dass 0 nicht im Bild von f liegt.
Nun untersuchen wir, für welche Paare (n,m) der Wert $f(n,m)$ positiv ist und für welche negativ. Wir sehen

$$\begin{aligned} f(n,m) > 0 &\Leftrightarrow nq > mp \\ &\Leftrightarrow m < \frac{nq}{p} \\ &\Leftrightarrow m \leq \left\lfloor \frac{nq}{p} \right\rfloor \end{aligned}$$

(beachte im letzten Schritt, dass wegen der Teilerfremdheit von p und q der Bruch $\frac{nq}{p}$ keine ganze Zahl sein kann). Damit ist

$$\left|\left\{(n,m) \in \{1,\dots,\frac{p-1}{2}\} \times \{1,\dots,\frac{q-1}{2}\} \mid f(n,m) > 0\right\}\right| = S(p,q).$$

Auf die gleiche Art sieht man

$$\left|\left\{(n,m) \in \{1,\dots,\frac{p-1}{2}\} \times \{1,\dots,\frac{q-1}{2}\} \mid f(n,m) < 0\right\}\right| = S(q,p).$$

Also folgt $S(p,q) + S(q,p) = \frac{p-1}{2} \cdot \frac{q-1}{2}$. □

Definition 6.7.2. Sei $a \in \mathbb{Z}$. Die eindeutig bestimmte Zahl

$$\rho_p(a) \in \left\{-\frac{p-1}{2}, \dots, 0, \dots, \frac{p-1}{2}\right\},$$

für die $\rho_p(a) \equiv a \pmod p$ gilt nennt man den *absolut kleinsten Rest* modulo p.

Beispiel 6.7.3. Es gilt $\rho_7(10) = 3$ und $\rho_4(11) = -3$.

Lemma 6.7.4 (Gauß)**.** *Sei $p \neq 2$ eine Primzahl und sei $a \in \mathbb{Z}$ mit $p \nmid a$. Dann gilt:*

(1) $\{|\rho_p(na)| \mid n = 1, \dots, \frac{p-1}{2}\} = \{1, \dots, \frac{p-1}{2}\}$

(2) Sei $\mu_p(a) := |\{n \in \{1, \dots, \frac{p-1}{2}\} \mid \rho_p(na) < 0\}|$. *Dann gilt*

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

Beweis.

(1) Es genügt zu zeigen, dass die Werte $|\rho_p(na)|$ paarweise verschieden sind wenn n die Menge $\{1, \dots, \frac{p-1}{2}\}$ durchläuft. Dazu seien $m, n \in \{1, \dots, \frac{p-1}{2}\}$. Angenommen es gilt $|\rho_p(na)| = |\rho_p(ma)|$. Dann gilt $\rho_p(na) = \pm\rho_p(ma)$ und damit

$$na \equiv \rho_p(na) \equiv \pm\rho_p(ma) \equiv \pm ma \pmod p.$$

Also ist $(n \mp m)a \equiv 0 \pmod p$. Da aber $-(p-1) \leq n \mp m \leq p-1$ gilt, folgt $n \mp m = 0$. Also ist $n = \pm m$. Beide sind aber positiv. Es folgt $n = m$.

(2) Für $n \in \{1, \dots, \frac{p-1}{2}\}$ sei

$$\varepsilon_n := \begin{cases} 1 & \text{falls } \rho_p(na) > 0 \\ -1 & \text{falls } \rho_p(na) < 0. \end{cases}$$

Dann gilt

$$\prod_{n=1}^{\frac{p-1}{2}} \varepsilon_n \cdot \rho_p(na) = \prod_{n=1}^{\frac{p-1}{2}} |\rho_p(na)| = \left(\frac{p-1}{2}\right)!$$

Es gilt aber auch $\varepsilon_1 \dots \varepsilon_{\frac{p-1}{2}} = (-1)^{\mu_p(a)}$. Also erhalten wir

$$\prod_{n=1}^{\frac{p-1}{2}} \rho_p(na) = (-1)^{\mu_p(a)} \left(\frac{p-1}{2}\right)!$$

Andererseits ist

$$\prod_{n=1}^{\frac{p-1}{2}} \rho_p(na) \equiv \prod_{n=1}^{\frac{p-1}{2}} na = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{a}{p}\right) \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Es folgt also

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

Da $\left(\frac{p-1}{2}\right)!$ nicht durch p teilbar ist, können wir diesen Faktor aus der Kongruenz kürzen und erhalten die Kongruenz $\left(\frac{a}{p}\right) \equiv (-1)^{\mu_p(a)}$. Beide Seiten sind in $\{\pm 1\}$ enthalten. Also folgt, dass sie gleich sind. □

Beweis des quadratischen Reziprozitätsgesetzes. Wir müssen zeigen, dass für zwei verschiedene Primzahlen $p, q \neq 2$ gilt

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

Sei $n \in \{1, \ldots, \frac{p-1}{2}\}$. Sei $r_n \in \{1, \ldots, p-1\}$ die eindeutig bestimmte Zahl, so dass

$$nq = p \left\lfloor \frac{nq}{p} \right\rfloor + r_i$$

(beachte, dass $r_n \neq 0$, denn nq ist nicht durch p teilbar). Wir unterscheiden 2 Fälle:
Fall 1: $r_n \leq \frac{p-1}{2}$. Dann ist $r_n = \rho_p(nq) > 0$.
Fall 2: $r_n > \frac{p-1}{2}$. Dann ist $\rho_p(nq) = r_n - p < 0$. Laut der Definition von $\mu_p(q)$ in Lemma 6.7.4 tritt dieser Fall genau $\mu_p(q)$ Mal auf.
Betrachte die Summe

$$\sum_{n=1}^{\frac{p-1}{2}} |\rho_p(nq)|.$$

Einerseits gilt mit Lemma 6.7.4(1)

$$\sum_{n=1}^{\frac{p-1}{2}} |\rho_p(nq)| = \sum_{n=1}^{\frac{p-1}{2}} n = \frac{\frac{p-1}{2} \cdot \left(\frac{p-1}{2} + 1\right)}{2} = \frac{p^2-1}{8}.$$

Andererseits folgern wir unter Verwendung von Lemma 6.7.4(2)

$$\begin{aligned}
\sum_{n=1}^{\frac{p-1}{2}} |\rho_p(nq)| &= \sum_{\substack{n \in \{1, \ldots, \frac{p-1}{2}\} \\ r_n \leq \frac{p-1}{2}}} |\rho_p(nq)| + \sum_{\substack{n \in \{1, \ldots, \frac{p-1}{2}\} \\ r_n > \frac{p-1}{2}}} |\rho_p(nq)| \\
&= \sum_{\substack{n \in \{1, \ldots, \frac{p-1}{2}\} \\ r_n \leq \frac{p-1}{2}}} r_n + \sum_{\substack{n \in \{1, \ldots, \frac{p-1}{2}\} \\ r_n > \frac{p-1}{2}}} (p - r_n)
\end{aligned}$$

Diese beiden Gleichungen zusammen ergeben

$$\text{(A)} \qquad \frac{p^2-1}{8} = \underbrace{\sum_{\substack{n\in\{1,\dots,\frac{p-1}{2}\}\\ r_n\le\frac{p-1}{2}}} r_n}_{=:R_1} - \underbrace{\sum_{\substack{n\in\{1,\dots,\frac{p-1}{2}\}\\ r_n>\frac{p-1}{2}}} r_n}_{=:R_2} + \mu_p(q)p.$$

Nun betrachten wir die Summe

$$\sum_{n=1}^{\frac{p-1}{2}} nq.$$

Einerseits ist wieder

$$\sum_{n=1}^{\frac{p-1}{2}} nq = q\sum_{n=1}^{\frac{p-1}{2}} = \frac{p^2-1}{8}q$$

Andererseits gilt

$$\sum_{n=1}^{\frac{p-1}{2}} nq = \sum_{n=1}^{\frac{p-1}{2}}(p\left\lfloor\frac{nq}{p}\right\rfloor + r_n) = p\sum_{n=1}^{\frac{p-1}{2}}\left\lfloor\frac{nq}{p}\right\rfloor + \sum_{n=1}^{\frac{p-1}{2}} r_n = pS(p,q) + R_1 + R_2.$$

also insgesamt

$$\text{(B)} \qquad \frac{p^2-1}{8}q = pS(p,q) + R_1 + R_2.$$

Wir subtrahieren Gleichung (A) von Gleichung (B) und erhalten

$$\text{(C)} \qquad \frac{(p^2-1)}{8}(q-1) = p(S(p,q) - \mu_p(q)) + 2R_2.$$

Die linke Seite von Gleichung (C) ist eine gerade ganze Zahl. Also muss $S(p,q) \equiv \mu_p(q) \pmod 2$ gelten. Daraus folgern wir

$$(-1)^{S(p,q)} = (-1)^{\mu_p(q)} = \left(\frac{q}{p}\right).$$

Für die letzte Gleichheit haben wir Lemma 6.7.4(2) verwendet. Die gleiche Überlegung mit vertauschten Rollen von p und q zeigt

$$(-1)^{S(q,p)} = \left(\frac{p}{q}\right).$$

Nun verwenden wir Lemma 6.7.1. Es zeigt

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Das beweist das quadratische Reziprozitätsgesetz. $\square$

6.8. **Lösungen von quadratischen Kongruenzen.**

Bemerkung 6.8.1. Mithilfe des Legendre-Symbols, das sich effektiv mit dem quadratischen Reziprozitätsgesetz ausrechnen lässt, können wir bestimmen, ob eine quadratische Kongruenz der Form $x^2 \equiv d \pmod{p}$ besitzt. Allerdings gibt die Methode keine Auskunft darüber, wie die Lösungen dieser Gleichung, im Falle der Lösbarkeit, aussehen.

Lemma 6.8.2. *Sei p eine Primzahl mit $p \equiv 3$ (mod 4) und sei $d \in \mathbb{Z}$ ein quadratischer Rest modulo p. Dann ist die Lösungmenge L der quadratischen Kongruenz $x^2 \equiv d$ (mod p) gegeben durch*

$$L = \{x \in \mathbb{Z} \mid x^2 \equiv d \ (mod\ p)\} = \{x \in \mathbb{Z} \mid x \equiv d^{\frac{p+1}{4}}\} \cup \{x \in \mathbb{Z} \mid x \equiv -d^{\frac{p+1}{4}}\}$$

Beweis. Sei $a := d^{\frac{p+1}{4}}$. Es genügt zu zeigen, dass $a^2 \equiv d \pmod{p}$ ist. Dann ist nämlich auch $(-a)^2 \equiv d \pmod{p}$ und somit sind $\pm\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ die (einzigen) beiden Lösungen der quadratischen Gleichung $x^2 = \overline{d}$ in $\mathbb{Z}/p\mathbb{Z}$. Wir berechnen also

$$a^2 = d^{\frac{p+1}{2}} = d \cdot d^{\frac{p-1}{2}} \equiv d\left(\frac{d}{p}\right) = d$$

nach dem Euler-Kriterium. Beachte, dass $\left(\frac{d}{p}\right) = 1$ ist, denn d ist als quadratischer Rest modulo p vorausgesetzt. □

Bemerkung 6.8.3. Dieses Verfahren funktioniert nur für Primzahlen $p \equiv 3 \pmod{4}$. Für Primzahlen $p \equiv 1 \pmod{4}$ gibt es den Tonelli–Shanks-Algorithmus, der eine Lösung (und damit alle Lösungen) der Kongruenz $x^2 \equiv d \pmod{p}$ bestimmt. Allerdings benötigt man dafür mehr Theorie, als wir zur Verfügung haben.

Algorithmus 6.8.4. Sei $p \equiv 3 \pmod{4}$ eine Primzahl. Seien $u, v \in \mathbb{Z}$. Der Algorithmus bestimmt die Lösungsmenge der quadratischen Kongruenz $x^2 + ux + v \equiv 0 \pmod{p}$.

(1) Bestimme ein $w \in \mathbb{Z}$ mit $w \equiv u \cdot \frac{p+1}{2} \pmod{p}$. Dann gilt $2w \equiv u \pmod{p}$.
(2) Bestimme ein $d \in \mathbb{Z}$ mit $d \equiv w^2 - v \pmod{p}$. Berechne das Legendre-Symbol $\left(\frac{d}{p}\right)$ mittels Algorithmus 6.5.7.
(3) Falls $\left(\frac{d}{p}\right) = -1$, so besitzt die Kongruenz keine Lösungen.
Falls $\left(\frac{d}{p}\right) \in \{0, 1\}$, so sind

$$x_1 = d^{\frac{p+1}{4}} - w \qquad\qquad x_2 = -d^{\frac{p+1}{4}} - w$$

Lösungen von $x^2 + ux + v \equiv 0 \pmod{p}$ und die Lösungsmenge der Kongruenz ist

$$L = \{x \in \mathbb{Z} \mid x \equiv x_1 \pmod{p}\} \cup \{x \in \mathbb{Z} \mid x \equiv x_2 \pmod{p}\}.$$

Satz 6.8.5. *Der Algorithmus berechnet die Lösungsmenge der Kongruenz $x^2+ux+v \equiv 0$ (mod p).*

Beweis. Genau dann ist n eine Lösung der Kongruenz, wenn $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$ eine Lösung der quadratischen Gleichung

$$\left(x + \frac{\overline{u}}{\overline{2}}\right)^2 = \frac{\overline{u}^2}{\overline{4}} - \overline{v}$$

in $\mathbb{Z}/p\mathbb{Z}$ ist. Da $2w \equiv u \pmod{p}$ gilt ist $\overline{w} = \frac{\overline{u}}{\overline{2}}$ und damit auch $\overline{d} = \overline{w}^2 - \overline{v} = \frac{\overline{u}^2}{\overline{4}} - \overline{v}$. Substituiere $y = x + w$ und betrachte die quadratische Kongruenz

$$y^2 \equiv d \pmod{p}.$$

Sie ist dann und nur dann lösbar, wenn $\left(\frac{d}{p}\right) \neq -1$; nach Lemma 6.8.2 sind die beiden Lösungen, bis auf Kongruenz modulo p, genau $y_{1,2} = \pm d^{\frac{p+1}{4}}$. So erhalten wir die beiden Lösungen $x_{1,2} = y_{1,2} - w$. □

Beispiel 6.8.6. Bestimme die Lösungsmenge von $x^2+2x+3 \equiv 0 \pmod{19}$. Offensichtlich ist $19 \equiv 3 \pmod{4}$.

(1) $w \equiv 2 \cdot \frac{20}{2} = 20 \equiv 1 \pmod{19}$.

(2) $d \equiv 1^2 - 3 = -2$. Es gilt $\left(\frac{-2}{19}\right) = \left(\frac{-1}{19}\right)\left(\frac{2}{19}\right) = (-1) \cdot (-1) = 1$.

(3) Wir rechnen aus $d^{\frac{p+1}{4}} = (-2)^5 = -32 \equiv 6 \pmod{19}$. Dann sind

$$x_1 = 6 - 1 = 5 \qquad\qquad x_2 = -6 - 1 = -7 \equiv 12$$

modulo 19 die Lösungen. Es gilt

$$L = (5 + 19\mathbb{Z}) \cup (12 + 19\mathbb{Z}).$$

Probe: $5^2 + 2 \cdot 5 + 3 = 38 \equiv 0 \pmod{19}$ und $12^2 + 2 \cdot 12 + 3 = 171 \equiv 0 \pmod{19}$.

7. Quadratsummen

Frage. Welche natürlichen Zahlen lassen sich als Summe von 2 Quadraten (in $\mathbb{N}_0$) darstellen? Welche als Summe von 3, 4, 5, etc.?

Beispiel.

$$\begin{aligned}
1 &= 1^2 + 0^2 \\
2 &= 1^2 + 1^2 \\
3 &= 1^2 + 1^2 + 1^2 \\
4 &= 2^2 + 0^2 \\
5 &= 2^2 + 1^2 \\
6 &= 2^2 + 1^2 + 1^2 \\
7 &= 2^2 + 1^2 + 1^2 + 1^2 \\
8 &= 2^2 + 2^2 \\
9 &= 3^2 + 0^2 \\
10 &= 3^2 + 1^1 \\
&\vdots
\end{aligned}$$

7.1. Summe von zwei Quadraten.

Lemma 7.1.1. *Sei p eine Primzahl. Genau dann ist p eine Summe von zwei Quadraten, wenn $p \not\equiv 3 \pmod 4$.*

Beweis. Zu „$\Rightarrow$“: Sei $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$. Modulo 4 sind 0 und 1 quadratische Reste und 2 und 3 quadratische Nichtreste. Also gilt $x^2, y^2 \equiv 0, 1 \pmod 4$ und damit $p = x^2 + y^2 \equiv 0, 1, 2 \pmod 4$.
Zu „$\Leftarrow$“: Sei $p \not\equiv 3 \pmod 4$. Dann ist $p \equiv 1$ oder $p \equiv 2 \pmod 4$. Im letzteren Fall ist $p = 2 = 1^2 + 1^2$. Also untersuchen wir den Fall $p \equiv 1 \pmod 4$. Dann gilt $\left(\frac{-1}{p}\right) = 1$ nach Korollar 6.4.2, also ist -1 ein quadratischer Rest modulo p. Damit existiert eine natürliche Zahl n mit $n^2 \equiv -1 \pmod p$. Nun betrachte die Abbildung

$$f : \{0, \ldots, \lfloor\sqrt{p}\rfloor\} \times \{0, \ldots, \lfloor\sqrt{p}\rfloor\} \to \mathbb{Z}/p\mathbb{Z}$$

definiert durch $f(x, y) = (nx - y) + p\mathbb{Z}$. Da der Definitionsbereich von f genau $(1 + \lfloor\sqrt{p}\rfloor)^2 > p$ Elemente hat, kann f nicht injektiv sein. Also gibt es $(x_1, y_1), (x_2, y_2) \in \{0, \ldots, \lfloor\sqrt{p}\rfloor\} \times \{0, \ldots, \lfloor\sqrt{p}\rfloor\}$ mit $(x_1, y_1) \neq (x_2, y_2)$, so dass

$$nx_1 - y_1 \equiv nx_2 - y_2 \pmod p.$$

Es folgt $n(x_1 - x_2) \equiv y_1 - y_2 \pmod p$. Definiere $x := x_1 - x_2$ und $y := y_1 - y_2$. Wir quadrieren die Kongruenz $nx \equiv y \pmod p$ und erhalten

$$y^2 \equiv n^2x^2 \equiv -x^2 \pmod p$$

oder anders ausgedrückt $x^2 + y^2 \equiv 0 \pmod p$. Nun waren $0 \leq x_i < \sqrt{p}$. Also auch $0 \leq |x|, |y| < \sqrt{p}$ und deshalb $0 \leq x^2, y^2 < p$. Da $(x_1, y_1) \neq (x_2, y_2)$ war, folgt, dass $|x|$

und $|y|$ nicht beide Null sein können. Also erhalten wir

$$0 < x^2 + y^2 < 2p.$$

Die einzige Zahl in $\{1, \ldots, 2p-1\}$, die durch p teilbar ist, ist aber p. Daher folgt $x^2+y^2 = p$. □

Lemma 7.1.2. *Genau dann lässt sich n als eine Summe von zwei Quadraten darstellen, wenn es eine Gaußsche Zahl $z \in \mathbb{Z}[i]$ gibt mit $n = |z|^2$.*

Beweis. Zu „$\Rightarrow$“: Ist $n = x^2 + y^2$, so gilt $n = |x + iy|^2$.
Zu „$\Leftarrow$“: Sei $n = |z|^2$ mit $z = x + iy \in \mathbb{Z}[i]$. Dann ist $n = x^2 + y^2$. □

Satz 7.1.3 (Zwei-Quadrate-Satz)**.** *Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{p\in\mathbb{P}} p^{m_p}$. Folgende Aussagen sind äquivalent:*

(1) n ist eine Summe von zwei Quadraten, d.h. es gibt $x, y \in \mathbb{N}_0$ mit $n = x^2 + y^2$.
(2) Für jede Primzahl $p \equiv 3 \pmod 4$ gilt $2 \mid m_p$.

Beweis. Zu „(1) $\Rightarrow$ (2)“: Sei $n = x^2 + y^2$. Sei $d := \mathrm{ggT}(x, y)$ und seien $\tilde{x} = x/d$, $\tilde{y} = y/d$. Dann ist $n = d^2(\tilde{x}^2+\tilde{y}^2)$ und $\mathrm{ggT}(\tilde{x}, \tilde{y}) = 1$. Betrachte die Primfaktorzerlegung $d = \prod_{p\in\mathbb{P}} p^{k_p}$ und $\tilde{n} := n/d^2$. Dann gelten

$$\tilde{n} = \tilde{x}^2 + \tilde{y}^2$$
$$\tilde{n} = \prod_{p\in\mathbb{P}} p^{m_p-2k_p}.$$

Wir zeigen, dass jeder Primfaktor $p \neq 2$ von $\tilde{n}$ die Kongruenz $p \equiv 1 \pmod 4$ erfüllt. Daraus folgt dann die Behauptung. Sei $p \neq 2$ ein Primfaktor von $\tilde{n}$. Dann gilt $p \nmid \tilde{x}$, denn sonst würde auch $p \mid \tilde{y}$ gelten und p wäre ein gemeinsamer Teiler von $\tilde{x}$ und $\tilde{y}$. Damit sind $\tilde{x}$ und p teilerfremd. Nach Bézouts Lemma finden wir $a, b \in \mathbb{Z}$ mit $ap + b\tilde{x} = 1$. Somit folgt $b\tilde{x} \equiv 1 \pmod p$. Damit

$$(b\tilde{y})^2 = b^2\tilde{n} - (b\tilde{x})^2 \equiv -(b\tilde{x})^2 \equiv -1 \pmod p.$$

und deshalb ist -1 ein quadratischer Rest modulo p. Es folgt $\left(\frac{-1}{p}\right) = 1$ und das ist äquivalent zu $p \equiv 1 \pmod 4$ mit Korollar 6.4.2.
Zu „(1) $\Rightarrow$ (2)“: Jeder Primfaktor p mit $p \not\equiv 3 \pmod 4$ ist eine Summe von zwei Quadraten; wir finden nach Lemma 7.1.2 also $z_p \in \mathbb{Z}[i]$ mit $p = |z_p|^2$. Da für $p \equiv 3 \pmod 4$ der Exponent $m_p = 2l_p$ gerade ist, ist $p^{m_p} = (p^2)^{l_p} = (|p|^2)^{l_p}$, wobei wir p als Gaussche Zahl auffassen. Damit ist

$$n = \left(\prod_{\substack{p\in\mathbb{P}\\ p\not\equiv 3 \pmod 4}} (|z_p|^2)^{m_p}\right) \cdot \left(\prod_{\substack{p\in\mathbb{P}\\ p\equiv 3 \pmod 4}} (|p|^2)^{l_p}\right) = |z|^2$$

wobei

$$\left(\prod_{\substack{p\in\mathbb{P}\\ p\not\equiv 3 \pmod 4}} z_p^{m_p}\right) \cdot \left(\prod_{\substack{p\in\mathbb{P}\\ p\equiv 3 \pmod 4}} p^{l_p}\right) \in \mathbb{Z}[i]$$

sei. □

Beispiel 7.1.4.

(1) $60 = 2^2 \cdot 3 \cdot 5$ ist keine Summe von 2 Quadraten, denn 3 hat als Primfaktor in 60 ungerade Vielfachheit.
Probe: Bilde für alle Quadrate n^2 zwischen 1 und $60/2 = 30$ die Differenz $60 - n^2$ und prüfe, ob sie eine Quadratzahl ist.

$$60 - 1^2 = 59$$
$$60 - 2^2 = 56$$
$$60 - 3^2 = 51$$
$$60 - 4^2 = 44$$
$$60 - 5^2 = 35$$

Alles keine Quadratzahlen.

(2) $180 = 2^2 \cdot 3^2 \cdot 5$ ist eine Summe von 2 Quadraten, denn der einzige Primfaktor mit ungerader Vielfachheit (5 mit Vielfachheit 1) erfüllt $5 \equiv 1$ modulo 4.
Um eine Darstellung als Quadratsumme konkret zu bestimmen, geht man wie im Beweis vom Zwei-Quadrate-Satz vor: es gilt $5 = 2^2 + 1^2 = |2 + i|^2$. Damit ist

$$180 = |2 \cdot 3 \cdot (2 + i)|^2 = |12 + 6i|^2 = 12^2 + 6^2$$

Probe: $12^2 + 6^2 = 144 + 36 = 180$.

7.2. **Summe von 4 Quadraten.**

Satz 7.2.1 (Vier-Quadrate-Satz von Lagrange)**.** *Jede natürliche Zahl lässt sich als Summe von 4 Quadraten darstellen.*

Lemma 7.2.2. *Es gibt einen nicht-kommutativen Ring $\mathbb{H}_\mathbb{Z}$ und eine Abbildung $|\cdot| : \mathbb{H}_\mathbb{Z} \to \mathbb{N}_0$, die folgende Eigenschaften erfüllen:*

(1) $|q \cdot q'| = |q| \cdot |q'|$ für alle $q, q' \in \mathbb{H}_\mathbb{Z}$.
(2) Genau dann ist n als Summe von vier Quadraten darstellbar, wenn es ein $q \in \mathbb{H}_\mathbb{Z}$ mit $n = |q|^2$ gibt.

Beweis. Siehe Abschnitt 7.3. □

Bemerkung 7.2.3. Um Satz 7.2.1 zu zeigen, geügt es nachzuweisen, dass sich jede Primzahl als Summe von 4 Quadraten schreiben lässt.

Beweis. Angenommen jede Primzahl ist als Summe von 4 Quadraten darstellbar. Dann gibt es nach Lemma 7.2.2 für jedes $p \in \mathbb{P}$ ein $q_p \in \mathbb{H}_\mathbb{Z}$, so dass $p = |q_p|^2$. Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung $p_1 \dots p_s$ (wobei $p_1, \dots, p_s$ nicht notwendig verschieden seien). Dann ist

$$n = p_1 \dots p_s = |q_{p_1}|^2 \dots |q_{p_2}|^2 = |q_{p_1} \dots q_{p_s}|^2$$

und damit ist n als Summe von 4 Quadraten darstellbar. □

Lemma 7.2.4. *Für jede Primzahl p gibt es eine Lösung der quadratischen Kongruenz in zwei Variablen*

$$x^2 + y^2 \equiv -1 \pmod{p}.$$

Beweis. Für $p = 2$ ist $-1 \equiv 1 \pmod 2$ und wir können $x = 1$ und $y = 0$ wählen.
Ist $p \equiv 1 \pmod 4$, so ist $\left(\frac{-1}{p}\right) = 1$, also ist -1 ein quadratischer Rest modulo p. Wir finden also ein $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \pmod p$ und können $y = 0$ wählen.
Sei $p \equiv 3 \pmod 4$. In diesem Fall ist -1 ein quadratischer Nichtrest modulo p. Sei n ein quadratischer Nichtrest. Dann ist

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

also ist $-n$ ein quadratischer Rest. Daher gibt es ein $y \in \mathbb{Z}$ mit $-n \equiv y^2 \pmod p$.
Nun zeigen wir, dass es ein $x \in \mathbb{Z}$ gibt, so dass $x^2 + 1$ ein quadratischer Nichtrest ist. Angenommen nicht. Dann wäre $1^2 + 1 = 2$ ein quadratischer Rest, also gibt es ein $x \in \mathbb{Z}$ mit $2 \equiv x^2 \pmod p$. Dann wäre aber auch $x^2 + 1 \equiv 2 + 1 = 3$ ein quadratischer Rest. So fortfahrend wären alle $n \in \mathbb{N}_0$ quadratische Reste modulo p. Das kann aber nicht sein.
Wir finden also ein $x \in \mathbb{Z}$, so dass $x^2 + 1$ ein quadratischer Nichtrest modulo p ist. Dann gibt es aber ein $y \in \mathbb{Z}$, so dass $x^2 + 1 \equiv -y^2 \pmod p$ ist. Dann gilt $x^2 + y^2 \equiv -1$. □

Beweis von Satz 7.2.1. Nach Bemerkung 7.2.3 genügt es zu zeigen, dass jede Primzahl eine Summe von 4 Quadraten ist. Nach Lemma 7.2.4 gibt es eine Lösung der Kongruenz

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod p$$

von der Gestalt $(x_0, x_1, x_2, x_3) = (x, y, 1, 0)$. Wir können statt x und y jeweils den absolut kleinsten Rest modulo p nehmen, also annehmen $|x|, |y| < p/2$. Dann gilt $x^2 + y^2 + 1 < p^2/2 + 1 < p^2$.
Es gibt also ein $1 \leq k < p$ und Zahlen $x_0, \ldots, x_3 \in \mathbb{Z}$, so dass

$$x_0^2 + \ldots + x_3^2 = kp.$$

Falls $k = 1$ ist, sind wir fertig. Falls $k \geq 2$ ist, müssen wir zeigen, dass es $z_0, \ldots, z_3 \in \mathbb{Z}$ und ein $1 \leq k' < k$ gibt, so dass

$$z_0^2 + \ldots + z_3^2 = k'p.$$

Ist k gerade, so müssen aus den Zahlen x_0, x_1, x_2, x_3 entweder keine Zahl, genau zwei Zahlen, oder alle 4 Zahlen gerade sein. Ohne Einschränkung seien sie so geordnet, dass x_0 und x_1, sowie x_2 und x_3 die gleiche Parität haben. Dann gilt

$$\left(\frac{x_0 - x_1}{2}\right)^2 + \left(\frac{a + x_1}{2}\right)^2 + \left(\frac{x_2 - x_3}{2}\right)^2 + \left(\frac{x_2 + x_3}{2}\right)^2 = \frac{k}{2}p.$$

Nun sei $k \geq 3$ ungerade. Wir finden Zahlen $y_0, \ldots, y_3$ mit $|y_i| < k/2$ für $i = 0, \ldots, 3$ und, so dass

$$y_0 \equiv -x_0 \pmod k$$
$$y_i \equiv x_i \pmod k$$

für $i = 1, 2, 3$. Dann gilt $y_0^2 + \ldots + y_3^2 \equiv x_0^2 + \ldots + x_3^2 \equiv 0 \pmod k$ und $y_0^2 + \ldots + y_3^2 < k^2$. Es gibt also ein $k' < k$ mit $y_0^2 + \ldots + y_3^2 = k'k$. Angenommen es gälte $k' = 0$. Dann wären $y_0 = \ldots = y_3 = 0$ und deshalb $x_i \equiv 0 \pmod k$ für $i = 0, \ldots, 3$. Damit gälte auch $x_i^2 \equiv 0 \pmod{k^2}$ und somit

$$kp = x_0^2 + \ldots + x_3^2 \equiv 0 \pmod{k^2}$$

Das würde $k \mid p$ implizieren. Aber nach Annahme ist $1 < k < p$ und p ist eine Primzahl. Also ein Widerspruch.
Nun gilt

$$k^2k'p = (x_0^2 + \ldots + x_3^2) \cdot (y_0^2 + \ldots + y_3^2) = w_0^2 + w_1^2 + w_2^2 + w_3^2$$

und durch explizites Berechnen der w_i sieht man, dass w_1, w_2 und w_3 alle durch k teilbar sind. Damit erhalten wir

$$k'p = \left(\frac{w_0}{k}\right)^2 + \ldots + \left(\frac{w_3}{k}\right)^2.$$

□

Beispiel 7.2.5. $87 = 9^2 + 2^2 + 1^2 + 1^2$.

7.3. **Quaternionen.**

Bemerkung 7.3.1. Auf dem $\mathbb{R}$-Vektorraum $\mathbb{H} := \mathbb{R}^4$ definieren wir die Struktur eines nicht-kommutativen Ringes. Seien

$$\begin{aligned} 1 &:= (1,0,0,0) \\ i &:= (0,1,0,0) \\ j &:= (0,0,1,0) \\ k &:= (0,0,0,1). \end{aligned}$$

Sei $+ : \mathbb{H} \times \mathbb{H} \to \mathbb{H}$ die Vektorraum-Addition auf $\mathbb{R}^4$. Sei $\cdot : \mathbb{H} \times \mathbb{H} \to \mathbb{H}$ die eindeutig bestimmte $\mathbb{R}$-bilineare Abbildung, die auf den Basiselementen folgende Werte annimmt (Zeile · Spalte in der folgenden Tabelle):

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Lemma 7.3.2. *Mit den oben erklärten Verknüpfungen $+$ und $\cdot$ ist $\mathbb{H}$ ein nicht-kommutativer Ring, also erfüllt die Axiome (R.1)–(R.4).*

Beweis. Zu $q = a + bi + cj + dk \in \mathbb{H}$ definiere die Matrix

$$S_q := \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} \in M_{4\times 4}(\mathbb{R}).$$

Man sieht, dass $S_{q+q'} = S_q + S'_q$ gilt. Ferner rechnet man nach, dass S_1, S_i, S_j und S_k sich genauso multiplizieren, wie in der Tabelle in Bemerkung 7.3.1. Da die Ringaxiome (R.1)–(R.4) in $M_{4\times 4}(\mathbb{R})$ gelten, folgern wir, dass sie auch in $\mathbb{H}$ gelten müssen. □

Definition 7.3.3. Der nicht-kommutative Ring $\mathbb{H}$ heißt der Ring der Quaternionen (oder auch Hamilton-Quaternionen; daher die Notation).

Beispiel 7.3.4. In $\mathbb{H}$ gilt

$$\begin{aligned}
&(1+2i+3j+4k)\cdot(1-i+j-k)\\
&=1\cdot(1-i+j-k)+2i\cdot(1-i+j-k)+3j\cdot(1-i+j-k)+4k\cdot(1-i+j-k)\\
&=1-i+j-k+2i-2i^2+2ij-2ik+3j-3ji+3j^2-3jk+4k-4ki+4kj-4k^2\\
&=1-i+j-k+2i-2\cdot(-1)+2k-2\cdot(-j)+3j-3\cdot(-k)+3\cdot(-1)-3i\\
&\quad+4k-4j+4\cdot(-i)-4\cdot(-1)\\
&=4-6i+2j+8k
\end{aligned}$$

Lemma 7.3.5. *Die Abbildung $\varphi:\mathbb{C}\to\mathbb{H}$ definiert durch $z=x+iy\mapsto x+iy$ ist ein injektiver Ringhomomorphismus. Wir fassen $\mathbb{C}$ auf diese Art als Teilmenge von $\mathbb{H}$ auf.*

Beweis. Seien $z=x+iy$ und $z'=x'+iy'$ komplexe Zahlen. Es gilt $z\cdot z'=(xx'-yy')+(xy'+x'y)i$. Fassen wir z und z' via φ als Quaternionen auf, so gilt $\varphi(z)\cdot\varphi(z')=(xx'-yy')+(xy'+x'y)i=\varphi(z\cdot z')$. Ferner gilt offensichtlich auch $\varphi(z+z')=\varphi(z)+\varphi(z')$ und $\varphi(1)=1$. □

Lemma 7.3.6. *Sei $q=a+bi+cj+dk\in\mathbb{H}$.*

(1) Wir definieren das Konjugierte *von q als*

$$\overline{q}:=a-bi-cj-dk.$$

Sei $q'\in\mathbb{H}$. Dann gilt $\overline{q\cdot q'}=\overline{q'}\cdot\overline{q}$ (beachte die Reihenfolge). Ferner gilt $\overline{\overline{q}}=q$.

(2) Es gilt

$$q\cdot\overline{q}=\overline{q}\cdot q=a^2+b^2+c^2+d^2\in\mathbb{R}_{\geq 0}.$$

Also ist $|q|:=\sqrt{q\cdot\overline{q}}\in\mathbb{R}_{\geq 0}$ wohldefiniert. Man nennt $|q|$ die Norm *von q.*

(3) Für $q\neq 0$ definieren wir

$$q^{-1}:=\frac{1}{|q|}\cdot q.$$

Dann gilt $q^{-1}\cdot q=q\cdot q^{-1}=1$. Also besitzt jedes $q\in\mathbb{H}\setminus\{0\}$ ein multiplikatives Inverses.

Beweis.

(1) Hier ist alles offensichtlich, bis auf die Identität $\overline{q\cdot q'}=\overline{q'}\cdot\overline{q}$. Da die Abbildung $\mathbb{H}\to\mathbb{H},\ q\mapsto\overline{q}$ eine $\mathbb{R}$-lineare Abbildung ist, reicht es die nachzuweisende Identität für die Basiselemente zu prüfen. So gilt beispielsweise

$$\overline{ij}=\overline{k}=-k \qquad\qquad \overline{j}\cdot\overline{i}=(-j)\cdot(-i)=ji=-k.$$

(2) Man rechnet nach, dass die Matrixprodukte $S_q\cdot S_{\overline{q}}$ und $S_{\overline{q}}\cdot S_q$ beide übereinstimmen mit der Matrix $(a^2+b^2+c^2+d^2)\cdot E_4$.

(3) Ist klar mit (2). □

Definition 7.3.7. Wir definieren $\mathbb{H}_{\mathbb{Z}}=\{a+bi+cj+dk\mid a,b,c,d\in\mathbb{Z}\}\subseteq\mathbb{H}$ und nennen die Elemente dieser Menge *ganzzahlige Quaternionen.*

Lemma 7.3.8.

(1) Für $q,q'\in\mathbb{H}_{\mathbb{Z}}$ gilt $q+q',q\cdot q'\in\mathbb{H}_{\mathbb{Z}}$.

(2) $\mathbb{H}_{\mathbb{Z}}$ ist ebenfalls ein nicht-kommutativer Ring.

(3) $|q| \in \mathbb{N}_0$ *für alle* $q \in \mathbb{H}_{\mathbb{Z}}$.

Beweis. Leicht. $\square$