1 Elementare Zahlentheorie

1.1 Primzahlen

Notation:
$\mathbb{N} = 1, 2, \ldots$
$\mathbb{N}_0 = 0, 1, 2, \ldots$

Definition 1.1. Eine **Primzahl** ist eine natürliche Zahl $p > 1$ die nur durch 1 und sich selbst teilbar ist.
M.a.W.: Primzahlen sind die positiven irreduziblen Elemente in $\mathbb{Z}$.

Division mit Rest ganzer Zahlen ist wohlbekannt, man erhält daher:

Lemma 1.2. *Die Funktion*

$$\nu : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}, \qquad a \longmapsto |a|,$$

ist eine euklidische Normfunktion. Insbesondere ist $\mathbb{Z}$ ein Hauptidealring und faktoriell.

Satz 1.3. *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen es gäbe nur endlich viele und sei P ihr Produkt. Dann ist $P + 1$ durch keine Primzahl teilbar. Widerspruch. □

Frage: Haben wir jetzt gezeigt, dass es in jedem faktoriellen Ring unendlich viele Primelemente gibt?

Antwort: Nein, $P + 1$ könnte eine Einheit sein!

Lemma 1.4. $\mathbb{Z}^\times = \{\pm 1\}$.

Zum Beweis brauchen wir, dass auf $\mathbb{Z}$ eine Anordnung existiert, d.h. die „$\leq$“-Relation mit ihren bekannten Eigenschaften (vgl. Algebra 1, 6.22).
Außerdem brauchen wir: Zu $a \in \mathbb{Z}$ gibt es keine ganze Zahl b mit $a < b < a + 1$.

Beweis von Lemma 1.4. Seien $a, b \in \mathbb{Z}$ mit $ab = 1$. Dann gilt $0 \neq a$, $0 \neq b$. Wäre $a > 1$, so gilt $b > 0$ (sonst $ab < 0$) also $b \geq 1$ und dann $ab > 1 \cdot b = b \geq 1 \Rightarrow 1 > 1$ Widerspruch.
Wäre $a < -1$, so gilt $b < 0$ (sonst $ab < 0$) also $b \leq -1$ und

$$-ab = a(-b) < (-1)(-b) = b \leq -1$$

also $-1 < -1$ Widerspruch. □

Erinnerung:

$$\sum_{n\in\mathbb{N}} \frac{1}{n} = \infty, \qquad \sum_{n\in\mathbb{N}} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Satz 1.5.

$$\sum_{p \text{ Primzahl}} \frac{1}{p} = \infty.$$

Bemerkung 1.6. Es gibt also „mehr“ Primzahlen als Quadratzahlen.

Beweis. Die Folge $\left(1+\frac{1}{n}\right)^n$ konvergiert von unten gegen e. Insbesondere gilt $\left(1+\frac{1}{p-1}\right)^{p-1} < e$, also $\log\left(1+\frac{1}{p-1}\right) < \frac{1}{p-1} = \frac{1}{p} + \frac{1}{p(p-1)}$. Wegen $\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p-1}$ gilt für jedes $N \in \mathbb{N}$:

$$\begin{aligned} \log \prod_{p\le N} \tfrac{1}{1-\frac{1}{p}} &= \sum_{p\le N} \log\left(1+\tfrac{1}{p-1}\right) \\ &< \sum_{p\le N} \tfrac{1}{p} + \sum_{p\le N} \tfrac{1}{p(p-1)}. \end{aligned}$$

Wir setzen: $p_+(1) = 0$ und für $n \ge 2$: $p_+(n) =$ größter Primteiler von n. Mithilfe der geometrischen Reihe $\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \dots$ erhalten wir

$$\begin{aligned} \prod_{p\le N} \tfrac{1}{1-\frac{1}{p}} = \prod_{p\le N} (1 + \tfrac{1}{p} + \tfrac{1}{p^2} + \dots) &= \sum_{p_+(n)\le N} \tfrac{1}{n} \\ \ge \sum_{n=1}^{N} \tfrac{1}{n} \ge \int_1^{N+1} \tfrac{dx}{x} &= \log(N+1). \end{aligned}$$

Zusammen:

$$\log\log(N+1) < \sum_{p\le N} \frac{1}{p} + \sum_{p\le N} \frac{1}{p(p-1)}.$$

Nun gilt:

$$\sum_{p\le N} \frac{1}{p(p-1)} \le \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \sum_{n=2}^{\infty} \frac{1}{n-1} - \frac{1}{n} = 1,$$

also

$$\log\log(N+1) - 1 < \sum_{p\le N} \frac{1}{p}.$$

□

Lemma 1.7. *In $\mathbb{N}$ gibt es beliebig große primzahlfreie Teilabschnitte.*

Beweis. Für jedes $n \in \mathbb{N}$ ist unter den n Zahlen

$$(n+1)!+2, (n+1)!+3, \dots, (n+1)!+n+1$$

keine Primzahl. □

Bemerkung 1.8. Sei $\pi(n) =$ Anzahl der Primzahlen $\le n$. Dann gilt

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\log(n)}} = 1.$$

1.2 Die Eulersche φ-Funktion

Definition 1.9. (Eulersche φ-Funktion). Für $n \in \mathbb{N}$ ist

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

Lemma 1.10. $(n,m) = 1 \Longrightarrow \varphi(nm) = \varphi(n)\varphi(m)$.

Beweis. Nach gilt $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, also
$(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$. □

Lemma 1.11. *Für $a \in \mathbb{Z}$, $n > 1$ bezeichne $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ die Restklasse von a* mod *n. Dann gilt*

$$\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \text{ggT}\,(a,n) = 1.$$

Beweis. Sei $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ und $b \in \mathbb{Z}$ so dass $\bar{a}\bar{b} = 1$. Dann gilt $ab = 1 + cn$, $c \in \mathbb{Z}$, also $\text{ggT}(a,n) \mid 1$.

Gilt $\text{ggT}(a,n) = 1$, so existieren $\alpha, \beta \in \mathbb{Z}$ mit $\alpha a + \beta n = 1$ (lineare Kombinierbarkeit des ggT in Hauptidealringen). Dann gilt $\bar{\alpha}\bar{a} = \bar{1}$, also $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

Korollar 1.12. *Sei p eine Primzahl. Dann gilt: $\varphi(p^k) = (p-1)p^{k-1}$.*

Beweis. Unter den p^k Restklassen $\overline{1}, \overline{2}, \ldots, \overline{p^k}$ sind genau die p^{k-1} Restklassen: $\overline{p}, \overline{2p}, \ldots, \overline{p^{k-1}p}$ nicht prim. Also $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$. □

Korollar 1.13. *Für $n = \prod_{i=1}^{r} p_i^{e_i}$ gilt $\varphi(n) = \prod_{i=1}^{r} (p-1)p^{e_i-1}$.*

Bemerkung 1.14. Die Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ (hier: $\zeta_n = e^{2\pi i/n}$) ist vom Grad $\varphi(n)$ mit Galoisgruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ (siehe Algebra 1, 4.47).

Satz 1.15. *Für jede natürliche Zahl m gilt: $\sum_{d|m} \varphi(d) = m$.*

Beweis. Induktion über die Anzahl der verschiedenen Primteiler von m.
$m = 1$ (0 Primteiler). Die Aussage ist trivial (bzw. formal).
Induktionsschritt: $m = np^e$, p Primzahl $n, e \in \mathbb{N}$, $p \nmid n$. Jeder Teiler von m hat eine eindeutige Darstellung der Form dp^i mit $d \mid n$ und $0 \le i \le e$. Wir erhalten

$$\begin{aligned}
\sum_{d|m} \varphi(d) &= \sum_{d|n} \varphi(d) + \sum_{d|n} \varphi(dp) + \cdots + \sum_{d|n} \varphi(dp^e) \\
&= n + n\varphi(p) + \cdots + n\varphi(p^e) \\
&= n(1 + (p-1)p^0 + \cdots + (p-1)p^{e-1}) \\
&= np^e = m.
\end{aligned}$$

□

Bemerkung 1.16. Das Minimalpolynom $\Phi_m(X)$ von ζ_m über $\mathbb{Q}$ heißt das *m-te Kreisteilungspolynom*. Da jede m-te Einheitswurzel primitive d-te Einheitswurzel für genau einen Teiler d von m ist, gilt

$$X^m - 1 = \prod_{d|m} \Phi_d(X)$$

(siehe Algebra 1, §4.5). Grade auswerten liefert einen alternativen Beweis von Satz 1.15.

Satz 1.17 (Kleiner Fermatscher Satz). *Für $(a, m) = 1$ gilt*

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

Beweis. Es gilt $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ und somit gilt $\mathrm{ord}(a) \mid \#(\mathbb{Z}/m\mathbb{Z})^\times = \varphi(m)$. Also folgt $\bar{a}^{\varphi(m)} = \bar{1}$ in $\mathbb{Z}/m\mathbb{Z}$. □

Korollar 1.18. *$a \in \mathbb{Z}$, p Primzahl $\Rightarrow a^p \equiv a \mod p$.*

Beweis. $(a, p) = 1 \Rightarrow a^{p-1} = a^{\varphi(p)} \equiv 1 \mod p \Rightarrow a^p \equiv a$. Ansonsten gilt $p \mid a$ und daher $a^p \equiv 0 \equiv a \mod p$ □

Definition 1.19. $a \in \mathbb{Z}$ heißt **primitive Wurzel** modulo einer Primzahl p, wenn die Restklassen $\bar{a}, \bar{a}^2, \ldots, \bar{a}^{p-1} = 1$ alle Restklassen $\neq 0 \mod p$ durchlaufen.

Satz 1.20 (Gauß). *Es existieren primitive Wurzeln modulo p.*

Beweis. $\mathbb{Z}/p\mathbb{Z}$ ist ein endlicher Körper. Daher ist $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch (Algebra 1, 3.103). Wähle $a \in \mathbb{Z}$ so dass $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ ein Erzeuger ist. □

2 Das Quadratische Reziprozitätsgesetz

Das Quadratische Reziprozitätsgesetz (QRG) wurde von Euler vermutet und zuerst von Gauss bewiesen. Es ist einer der wichtigsten Sätze der klassischen Zahlentheorie. Es setzt die Frage, ob eine Primzahl p quadratischer Rest modulo einer Primzahl q ist, in Beziehung zu der „reziproken“ Frage, ob q quadratischer Rest modulo p ist. Ein solcher Zusammenhang ist erstaunlich und tiefliegend, da eine Aussage über Reste modulo q mit einer über Reste modulo p verknüpft wird. Das Quadratische Reziprozitätsgesetz ist von *globaler* Natur, d.h. nicht durch Rechnen mit Restklassen modulo einer festen Zahl zu verstehen. Ein tieferes Verständnis des QRG erhält man erst im Rahmen seiner modernen Verallgemeinerung, der *Klassenkörpertheorie*.

2.1 Quadratische Reste modulo p

Im Folgenden bezeichne p stets eine von 2 verschiedene Primzahl.

Definition 2.1. Eine ganze Zahl a (bzw. ihre Restklasse modulo p) heißt **quadratischer Rest** modulo p, wenn $p \nmid a$ und $\bar{a} = \bar{b}^2 \in \mathbb{Z}/p\mathbb{Z}$ für ein $b \in \mathbb{Z}$. Wenn $p \nmid a$ und a kein quadratischer Rest ist, dann heißt a **quadratischer Nichtrest**.

Definition 2.2. Für $a \in \mathbb{Z}$ ist das **Legendre-Symbol** $\left(\frac{a}{p}\right)$ folgendermaßen definiert:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{wenn } a \text{ quadratischer Rest } \bmod p, \\ 0, & \text{wenn } p \mid a, \\ -1, & \text{wenn } a \text{ quadratischer Nichtrest } \bmod p. \end{cases}$$

Aus $a \equiv b \bmod p$ folgt offenbar $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Wir benutzen daher auch die Notation $\left(\frac{\bar{a}}{p}\right)$, d.h. wir fassen das Legendre-Symbol als Funktion auf den Restklassen modulo p auf. Wir sagen, eine ganze Zahl g sei primitive Wurzel modulo p, wenn ihre Restklasse $\bar{g} \in \mathbb{Z}/p\mathbb{Z}$ eine primitive Wurzel ist.

Lemma 2.3. *Sei g eine primitive Wurzel modulo p. Dann gilt für $r \in \mathbb{N}$*

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

Beweis. Zu zeigen ist: g^r ist quadratischer Rest $\iff 2|r$.
($\Longrightarrow$): Sei $\bar{g}^r = \bar{h}^2$. Dann ist $\bar{h} = \bar{g}^n$ für ein n. Also ist $\bar{g}^r = \bar{g}^{2n}$. Es gilt somit $p - 1 = \mathrm{ord}(\bar{g}) \mid (r - 2n)$ und folglich ist r gerade.
($\Longleftarrow$): Ist r gerade, so gilt $\bar{g}^r = (\bar{g}^{r/2})^2$. □

Korollar 2.4. *In $\mathbb{Z}/p\mathbb{Z}$ gibt es genau $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste.*

Beweis. Die Werte g^r, $r = 1, \ldots, p-1$, durchlaufen genau die primen Restklassen modulo p. Nach Lemma 2.3 sind die quadratischen Reste genau die Werte mit geradem Exponenten und die quadratischen Nichtreste genau die Werte mit ungeradem Exponenten. □

Nun zeigen wir die Multiplikativität des Legendre-Symbols.

Satz 2.5.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Beweis. Es gilt die Implikation $p|ab \Longrightarrow p|a$ oder $p|b$. Daher ist die linke Seite der Gleichung genau dann gleich Null, wenn es die rechte ist. Sei g eine primitive Wurzel modulo p. Sind a und b nicht durch p teilbar, so existieren r, s mit $\bar{a} = \bar{g}^r$, $\bar{b} = \bar{g}^s$, und es gilt

$$\left(\frac{ab}{p}\right) = \left(\frac{g^{r+s}}{p}\right) = (-1)^{r+s}$$

$$= (-1)^r(-1)^s = \left(\frac{g^r}{p}\right)\left(\frac{g^s}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Korollar 2.6. *Das Produkt zweier quadratischer Nichtreste ist ein quadratischer Rest.*

Beweis. Sind a und b quadratische Nichtreste, so gilt $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)(-1) = 1$. Daher ist ab quadratischer Rest. □

Mit Hilfe des Legendre-Symbols können wir das Lösungsverhalten quadratischer Gleichungen modulo p angeben.

Satz 2.7. *Die quadratische Gleichung $X^2 + aX + b = 0$ hat modulo p*

- *genau zwei verschiedene Lösungen,* *wenn* $\left(\frac{a^2-4b}{p}\right) = +1$,
- *genau eine Lösung,* *wenn* $\left(\frac{a^2-4b}{p}\right) = 0$,
- *keine Lösung,* *wenn* $\left(\frac{a^2-4b}{p}\right) = -1$.

Beweis. Da p als ungerade vorausgesetzt ist, können wir Restklassen modulo p durch 2 teilen. Die gegebene Gleichung ist äquivalent zu

$$\left(X + \frac{a}{2}\right)^2 - \frac{a^2}{4} + b \equiv 0 \mod p$$

bzw. zu

$$(2X + a)^2 \equiv a^2 - 4b \mod p.$$

Hieraus folgt die Behauptung. □

Wegen $p > 2$ sind die Restklassen modulo p der Zahlen -1, 0 und 1 paarweise verschieden. Daher ist das Legendre-Symbol bereits durch seine Restklasse modulo p eindeutig bestimmt. Diese berechnet sich wie folgt.

Satz 2.8 (Euler)**.** *Für $a \in \mathbb{Z}$ gilt*

$$\overline{\left(\frac{a}{p}\right)} = \bar{a}^{\frac{p-1}{2}} \qquad \text{in } \mathbb{Z}/p\mathbb{Z}.$$

Beweis. Ist a durch p teilbar, so sind beide Seiten gleich Null. Also können wir $p \nmid a$ annehmen. Wegen $(\bar{a}^{\frac{p-1}{2}})^2 = \bar{a}^{p-1} = \bar{1}$ nimmt $\bar{a}^{\frac{p-1}{2}}$ nur die Werte $+\bar{1}, -\bar{1}$ an, und wir müssen zeigen: $\left(\frac{a}{p}\right) = 1 \iff \bar{a}^{\frac{p-1}{2}} = \bar{1}$.

($\Longrightarrow$): Ist $\left(\frac{a}{p}\right) = 1$, so ist $\bar{a} = \bar{b}^2$ für ein b. Also ist $\bar{a}^{\frac{p-1}{2}} = \bar{b}^{p-1} = \bar{1}$.

($\Longleftarrow$): Sei g eine primitive Wurzel und $\bar{a} = \bar{g}^r$. Dann gilt $\bar{g}^{r\frac{p-1}{2}} = \bar{1}$, also $(p-1) \mid r\frac{p-1}{2}$, weshalb r gerade ist. Dann ist $\left(\frac{a}{p}\right) = (-1)^r = 1$. □

2.2 Das Quadratische Reziprozitätsgesetz

Theorem 2.9 (Quadratisches Reziprozitätsgesetz)**.** *Es seien $p, q > 2$ Primzahlen. Dann gilt*

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

Mit anderen Worten: Ist eine der beiden Primzahlen p und q kongruent 1 modulo 4, so gilt $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Im verbleibenden Fall gilt $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Bevor wir das QRG beweisen, formulieren wir noch seine zwei sogenannten Ergänzungssätze. Mit Hilfe des QRG und seiner Ergänzungssätze kann man dann die Legendre-Symbole $\left(\frac{a}{p}\right)$ bequem ausrechnen.

Theorem 2.10 (1. Ergänzungssatz zum QRG)**.**

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

Mit anderen Worten: -1 ist genau dann quadratischer Rest modulo einer Primzahl p, wenn p kongruent 1 modulo 4 ist.

Theorem 2.11 (2. Ergänzungssatz zum QRG)**.**

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

Mit anderen Worten: 2 ist genau dann quadratischer Rest modulo einer Primzahl p, wenn p kongruent ± 1 modulo 8 ist.

Zum Beweis des QRG benötigen wir das sogenannte Gauß-Lemma. Sei

$$H = \left\{\bar{1}, \bar{2}, \ldots, \overline{\frac{p-1}{2}}\right\}.$$

Dann hat jedes Element aus $(\mathbb{Z}/p\mathbb{Z})^\times$ die Gestalt $\pm\bar{h}$ mit $\bar{h} \in H$. Sei nun $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ ein fixiertes Element. Dann erhalten wir Gleichungen der folgenden Form

$$\begin{array}{rcll}
\bar{a}\cdot\bar{1} & = & \varepsilon_1\cdot\bar{h}_1, & \bar{h}_1 \in H, \varepsilon_1 \in \{+1,-1\} \\
\bar{a}\cdot\bar{2} & = & \varepsilon_2\cdot\bar{h}_2, & \bar{h}_2 \in H, \varepsilon_2 \in \{+1,-1\} \\
\vdots & & \vdots & \vdots \\
\bar{a}\cdot\overline{\frac{p-1}{2}} & = & \varepsilon_{\frac{p-1}{2}}\cdot\bar{h}_{\frac{p-1}{2}}, & \bar{h}_{\frac{p-1}{2}} \in H, \varepsilon_{\frac{p-1}{2}} \in \{+1,-1\}.
\end{array}$$

Lemma 2.12 (Gauß-Lemma). $$\left(\frac{a}{p}\right) = \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i.$$

Beweis. Zunächst zeigen wir, dass die $\bar{h}_i$ paarweise verschieden sind. Wäre nämlich $\bar{h}_i = \bar{h}_j$, so schließt man $\bar{a}^2\bar{i}^2 = \bar{a}^2\bar{j}^2$, also $\bar{i}^2 = \bar{j}^2$, also $\bar{i} = \pm\bar{j}$. Wegen $\bar{i}, \bar{j} \in H$ folgt $i = j$. Also taucht jedes Element aus H genau einmal als $\bar{h}_i$ auf, und wir erhalten

$$\bar{a}^{\frac{p-1}{2}} \cdot \prod_{i=1}^{\frac{p-1}{2}} \bar{i} = \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i \cdot \prod_{i=1}^{\frac{p-1}{2}} \bar{h}_i = \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i \cdot \prod_{i=1}^{\frac{p-1}{2}} \bar{i}\ .$$

Teilen wir beide Seiten durch $\prod_{i=1}^{\frac{p-1}{2}} \bar{i}$ und wenden Satz 2.8 an, erhalten wir

$$\overline{\left(\frac{a}{p}\right)} = \bar{a}^{\frac{p-1}{2}} = \overline{\left(\prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i\right)} \quad \text{in } \mathbb{Z}/p\mathbb{Z},$$

was wegen $p \geq 3$ die Behauptung zeigt. □

Beweis des QRG und seiner Ergänzungssätze. 1. Schritt: Satz 2.8 für $a = -1$ impliziert die Behauptung des 1. Ergänzungssatzes.

2. Schritt: Wir schreiben für $1 \leq i \leq \frac{p-1}{2}$

$$a \cdot i = \varepsilon_i \cdot h_i + e_i \cdot p$$

mit $1 \leq h_i \leq \frac{p-1}{2}$, $\varepsilon_i \in \{\pm 1\}$ und $e_i \in \mathbb{Z}$. Ist $\varepsilon_i = +1$, so gilt $2ai = 2h_i + 2e_ip$ und daher

$$\frac{2ai}{p} = \frac{2h_i}{p} + 2e_i.$$

Folglich gilt

$$\left[\frac{2ai}{p}\right] = 2e_i,$$

und $\left[\frac{2ai}{p}\right]$ ist in diesem Fall eine gerade ganze Zahl. Ist $\varepsilon_i = -1$, so gilt $2ai = p - 2h_i + (2e_i - 1)p$, und daher

$$\frac{2ai}{p} = \frac{p - 2h_i}{p} + 2e_i - 1.$$

Folglich gilt

$$\left[\frac{2ai}{p}\right] = 2e_i - 1,$$

und $\left[\frac{2ai}{p}\right]$ ist in diesem Fall eine ungerade ganze Zahl. Zusammen erhalten wir die Gleichung

$$\varepsilon_i = (-1)^{\left[\frac{2ai}{p}\right]}.$$

3. Schritt: Nach dem Gauß-Lemma (2.12) und Schritt 2 gilt

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1}\left[\frac{2ai}{p}\right]},$$

wobei $p_1 = \frac{p-1}{2}$ ist.

4. Schritt: Sei a ungerade. Dann gilt

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right).$$

Beachtet man nun $\left(\frac{4}{p}\right) = 1$, so folgt unter Verwendung der wohlbekannten Formel für die Summe der ersten n natürlichen Zahlen aus Schritt 3 die Formel

$$\begin{aligned}\left(\frac{2a}{p}\right) &= (-1)^{\sum_{i=1}^{p_1}\left[\frac{(a+p)i}{p}\right]} \\ &= (-1)^{\sum_{i=1}^{p_1} i + \sum_{i=1}^{p_1}\left[\frac{ai}{p}\right]} \\ &= (-1)^{\frac{p^2-1}{8}+\sum_{i=1}^{p_1}\left[\frac{ai}{p}\right]}.\end{aligned}$$

Setzt man in dieser Gleichung $a = 1$, so erhält man die Aussage des 2. Ergänzungssatzes.

5. Schritt: Aus der Multiplikativität des Legendre-Symbols, dem 2. Ergänzungssatz und der letzten Gleichung in Schritt 4 erhält man für ungerades a die Gleichung

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1}\left[\frac{ai}{p}\right]}.$$

6. Schritt: Von nun an sei $a = q$ eine von p verschiedene Primzahl größer als 2 und $q_1 = \frac{q-1}{2}$. Wir setzen

$$\begin{aligned}S_1 &= \#\left\{(i,j) \mid 1 \le i \le p_1, 1 \le j \le q_1, qi > pj\right\} \\ S_2 &= \#\left\{(i,j) \mid 1 \le i \le p_1, 1 \le j \le q_1, qi < pj\right\}.\end{aligned}$$

Weil stets $qi \neq pj$ ist, gilt

$$S_1 + S_2 = p_1 q_1.$$

Für ein fest gewähltes i ist $qi > pj$ äquivalent zu $j \le \left[\frac{qi}{p}\right]$. Also gilt

$$S_1 = \sum_{i=1}^{p_1}\left[\frac{qi}{p}\right].$$

Analog erhält man

$$S_2 = \sum_{j=1}^{q_1} \left[\frac{pj}{q}\right].$$

Zusammen mit Schritt 5 zeigt dies

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\sum_{i=1}^{p_1}\left[\frac{qi}{p}\right]+\sum_{j=1}^{q_1}\left[\frac{pj}{q}\right])} = (-1)^{(S_1+S_2)} = (-1)^{p_1 q_1},$$

und der Beweis des QRG ist erbracht. □

Mit Hilfe dieser Sätze ist das Legendre-Symbol $\left(\frac{a}{p}\right)$ schnell ausgerechnet. Zum Beispiel:

$$\left(\frac{17}{19}\right) = \left(\frac{19}{17}\right) = \left(\frac{2}{17}\right) = +1$$

$$\left(\frac{21}{23}\right) = \left(\frac{3}{23}\right)\left(\frac{7}{23}\right) = (-1)\left(\frac{23}{3}\right)(-1)\left(\frac{23}{7}\right) =$$

$$\left(\frac{2}{3}\right)\left(\frac{2}{7}\right) = (-1)(+1) = -1.$$

2.3 Primzahlen mit vorgegebener Restklasse

Satz 2.13. (i) *Es gibt unendlich viele Primzahlen kongruent* -1 *modulo* 3.

(ii) *Es gibt unendlich viele Primzahlen kongruent* -1 *modulo* 4.

Beweis. (i) Angenommen es gäbe nur endlich viele. Sei P ihr Produkt. Dann ist die Zahl $3P - 1$ durch keine Primzahl kongruent -1 modulo 3 und auch nicht durch 3 teilbar. Daher ist sie Produkt von Primzahlen kongruent 1 modulo 3; sie selbst ist aber kongruent -1 modulo 3. Widerspruch. (ii) Angenommen es gäbe nur endlich viele. Sei P ihr Produkt. Dann ist die Zahl $4P - 1$ durch keine Primzahl kongruent -1 modulo 4 und auch nicht durch 2 teilbar. Daher ist die Produkt von Primzahlen kongruent 1 modulo 4; sie selbst ist aber kongruent -1 modulo 4. Widerspruch. □

Der Beweis von 2.13 war elementar. Um entsprechende Aussagen auch für die $+1$-Restklassen zu bekommen, wenden wir das Quadratische Reziprozitätsgesetz an. Wir beginnen mit einem Lemma.

Lemma 2.14. *Für beliebiges* $a \in \mathbb{Z}$ *hat die Zahl* $n = 4a^2 + 1$ *nur Primteiler kongruent* 1 *modulo* 4.

Beweis. Zunächst ist n stets positiv und ungerade. Ist p ein Primteiler von n, so ist -1 quadratischer Rest modulo p. Nach dem ersten Ergänzungssatz zum QRG folgt $p \equiv 1 \bmod 4$. □

Satz 2.15. *Es gibt unendlich viele Primzahlen kongruent* 1 *modulo* 4.

Beweis. Angenommen es gäbe nur endlich viele. Sei P ihr Produkt. Dann ist die Zahl $4P^2+1$ durch keine Primzahl kongruent 1 modulo 4 teilbar. Nach dem obigen Lemma hat sie aber nur solche Primteiler. Widerspruch. □

Dieses Vorgehen kann verallgemeinert werden.

Satz 2.16. *Zu jeder ganzen Zahl $a \neq 0$ existieren unendlich viele Primzahlen p, so dass a quadratischer Rest modulo p ist.*

Beweis. Wir nehmen an, dass es nur endlich viele (ungerade) Primzahlen $p_1, \ldots, p_n$ mit $\left(\frac{a}{p_i}\right) = 1$ gäbe. Wir wählen eine ganze Zahl A prim zu a. Ist a ungerade, so wählen wir A gerade und umgekehrt. Ferner sei A so groß gewählt, dass die ganze Zahl

$$N = (p_1 \cdots p_n A)^2 - a$$

größer als 1 ist. Entsprechend unseren Wahlen ist N ungerade, durch keines der p_i teilbar und es gilt $(N, a) = 1$. Sei q ein Primteiler von N. Dann ist a quadratischer Rest modulo q. Widerspruch. □

Satz 2.17. *Es gibt unendlich viele Primzahlen kongruent* 1 *modulo* 3.

Beweis. Nach dem letzten Satz gibt es unendlich viele Primzahlen p mit $\left(\frac{-3}{p}\right) = 1$. Daher folgt alles aus dem nächsten Lemma. □

Lemma 2.18. *Eine ungerade Primzahl p ist genau dann $\equiv 1 \bmod 3$, wenn*

$$\left(\frac{-3}{p}\right) = 1.$$

Beweis. Zunächst ist $\left(\frac{-3}{3}\right) = 0$, so dass wir $p > 3$ annehmen können. Dann gilt

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Nun ist aber $\left(\frac{p}{3}\right) = +1 \Longleftrightarrow p \equiv 1 \bmod 3$. □