MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Quadratische Kongruenzen und das quadratische Reziprozitätsgesetz“

verfasst von / submitted by

Rebecca Eigner BEd

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Education (MEd)

Wien, 2023 / Vienna 2023

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 199 510 520 02
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Lehramt Sek (AB) Lehrverbund Unterrichtsfach Geographie und wirtschaftliche Bildung Lehrverbund Unterrichtsfach Mathematik Lehrverbund
Betreut von / Supervisor:	ao. Univ.-Prof. Mag. Dr. Christoph Baxa

Abriss

Das quadratische Reziprozitätsgesetz ist eine zentrale Erkenntnis der Zahlentheorie und heute der am häufigsten bewiesene Satz der Mathematik. In der vorliegenden Masterarbeit werden aufbauend alle Konzepte, Definition und Sätze erarbeitet, die zur Formulierung des quadratischen Reziprozitätsgesetzes notwendig sind. Im Zuge dessen werden insbesondere quadratische Kongruenzen sowie quadratische Reste und das Legendre-Symbol näher betrachtet. Weiters werden unter Zuhilfenahme des Lemmas von Gauß zwei ausgewählte Beweise der Aussage angeführt und anhand mehrerer Beispiele Anwendungen des Reziprozitätsgesetzes demonstriert.

Abstract

The quadratic reciprocity law is a central result of number theory and is currently the most frequently proven theorem in mathematics. This master's thesis presents a step-by-step approach to all the concepts, definitions, and theorems necessary for formulating the quadratic reciprocity law. In this context quadratic congruences, quadratic residues, and the Legendre symbol are examined in detail. Furthermore, using Gauss's lemma, two selected proofs of the statement are presented and several examples demonstrate the applications of the reciprocity law.

Inhaltsverzeichnis

1 Einleitung

Das Hauptinteresse der vorliegenden Masterarbeit liegt in der Behandlung von quadratischen Resten und dem quadratischen Reziprozitätsgesetz sowie dessen Beweise. Die Auseinandersetzung mit diesen Themen ermöglicht es, eine Entscheidung über die Lösbarkeit von quadratischen Kongruenzgleichungen der Form $a \cdot x^2 + b \cdot x + c \equiv 0 \pmod{m}$ $(a, b, c, m \in \mathbb{Z})$ zu treffen und diese anschließend unter Zuhilfenahme von anderen zahlentheoretischen Hilfsmitteln wie dem chinesischen Restsatz zu lösen. Eine zentrale Rolle spielen dabei das Legendre-Symbol, das Lemma von Gauß und die beiden Ergänzungssätze des Reziprozitätsgesetzes, welche allesamt schrittweise erarbeitet und schlussendlich für die Beweise des quadratischen Reziprozitätsgesetzes herangezogen werden. Insgesamt werden in der vorliegenden Masterarbeit daher Inhalte bearbeitet, die über die in österreichischen Schulen vermittelte Zahlentheorie weit hinausgehen. Als Zielgruppe können daher Studierende des Lehramts für Mathematik genannt werden, die sich weiterführend mit zahlentheoretischen Inhalten beschäftigen möchten.

Das Thema der quadratischen Reste und insbesondere des quadratischen Reziprozitätsgesetzes wurde aufgrund von mehreren Aspekten zur Behandlung ausgewählt. Einerseits ist das Reziprozitätsgesetz aus historischer Sicht besonders interessant, da es bereits 1783 entdeckt wurde, jedoch erst Jahre später von Gauß erstmals bewiesen werden konnte, bevor das Gesetz über die Jahre hinweg zum am häufigsten bewiesenen Satz der Mathematik wurde und damit heute sogar den Satz von Pythagoras in der Anzahl an bekannten Beweisen übertrifft. Andererseits ist die Aussage des quadratischen Reziprozitätsgesetzes eine der zentralsten Erkenntnisse der Zahlentheorie und auch die Eigenschaft von quadratischen Resten ist aus Sicht der Mathematik sehr besonders, denn nicht jede Zahl tritt bei der Division einer Quadratzahl durch eine Primzahl als Rest auf.

Da die Behandlung des quadratischen Reziprozitätsgesetzes ein gewisses mathematisches Vorwissen voraussetzt, werden im ersten Teil der Arbeit grundlegende Konzepte, Definitionen und Sätze, einschließlich der Begriffe “Teilbarkeit” und “Kongruenz” eingeführt. Anschließend daran findet eine detailreiche Auseinandersetzung mit quadratischen Kongruenzen, quadratischen Resten und dem Legendre-Symbol statt, wobei die allgemeine Form der quadratischen Kongruenzgleichung $a \cdot x^2 + b \cdot x + c \equiv 0 \pmod{m}$ $(a, b, c, m \in \mathbb{Z})$ zu Beginn auf die deutlich kürzere Form $x^2 \equiv a \pmod{p}$ mit $a \in \mathbb{Z}, p \in \mathbb{P}$ reduziert wird. Den Hauptinhalt dieses Abschnittes stellen das Lemma von Gauß und die beiden Ergänzungssätze dar. Im dritten Teil der Masterarbeit wird schlussendlich das quadratische Reziprozitätsgesetz für das Legendresche Restsymbol eingeführt

und dessen Anwendung bei der Bestimmung des Wertes des Legendre-Symbols anhand einiger Beispiele demonstriert. Da die Wiedergabe der über 200 existierenden Beweise des Reziprozitätsgesetzes im Zuge einer Masterarbeit unmöglich ist, wurden zwei besonders eindrucksvolle Beweise, die jeweils auf den Erkenntnissen des Lemmas von Gauß basieren, zur Behandlung ausgewählt. Das letzte Kapitel der Arbeit stellt einen kurzen thematischen Exkurs dar und beschäftigt sich mit dem Jacobischen Restsymbol sowie den entsprechenden Sätzen über quadratische Reste, mit deren Hilfe die Bestimmung des Legendre-Symbols und somit die Entscheidung über die Lösbarkeit von quadratischen Kongruenzgleichungen deutlich verkürzt werden kann.
Insgesamt bietet die Masterarbeit daher einen umfassenden Überblick über quadratische Kongruenzen und das quadratische Reziprozitätsgesetz sowie deren Anwendungen bei der Lösung verschiedener Fragestellungen.

Bemerkung. In der vorliegenden Masterarbeit wird folgende Definition für die Menge der natürlichen Zahlen herangezogen:

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

Soll die Zahl 0 von dieser Menge explizit ausgeschlossen werden, wird daher der Ausdruck $\mathbb{N} \setminus \{0\}$ verwendet.

2 Teilbarkeit

Die vorliegende Masterarbeit hat den Anspruch, Schritt für Schritt das gesamte Vorwissen zu erarbeiten, das für die Formulierung des quadratischen Reziprozitätsgesetzes notwendig ist. Da die in diesem Kapitel angeführten Sätze und Beweise über die Teilbarkeit von ganzen Zahlen für gewöhnlich den Einstieg in die Zahlentheorie darstellen, können sie in einer Vielzahl an Quellen vorgefunden werden. Ein Beispiel dafür ist unter anderem das Werk von Bundschuh (2008). [9]

Definition. Es seien $m, n \in \mathbb{Z}$. Die Zahl n heißt teilbar durch m, wenn es ein $d \in \mathbb{Z}$ gibt, sodass $n = d \cdot m$. Man sagt auch n ist ein Vielfaches von m.
Formal schreibt man $m \mid n$, wenn m ein Teiler von n ist. Ist m kein Teiler von n (existiert also kein $d \in \mathbb{Z}$, sodass $n = d \cdot m$) schreibt man $m \nmid n$.

Beispiel. $4 \mid 32$, denn $32 = 8 \cdot 4$

Lemma 2.1 (Eigenschaften der Teilbarkeit)**.** *Es seien l, m und $n \in \mathbb{Z}$. Dann gelten folgende Eigenschaften:*

i) $1 \mid n$ *und* $n \mid n$

ii) $n \mid 0$ *und* $0 \mid n \Rightarrow n = 0$

iii) $m \mid n \Rightarrow (-m) \mid n$ *und* $m \mid (-n)$

iv) $m \mid n$ *und* $n \neq 0 \Rightarrow |m| \leq |n|$

v) $n \mid 1 \Leftrightarrow n \in \{1, -1\}$

vi) $m \mid n$ *und* $n \mid m \Rightarrow n = m$ *oder* $n = -m$

vii) $l \mid m$ *und* $m \mid n \Rightarrow l \mid n$ *(Transitivität)*

viii) $m \mid n \Rightarrow l \cdot m \mid l \cdot n \ \ \forall l \in \mathbb{Z}$

ix) $l \cdot m \mid l \cdot n$ *mit* $l \neq 0 \Rightarrow m \mid n$

x) $m_j \mid n_j$ *mit* $j = 1, 2, ..., r \Rightarrow m_1 \cdot m_2 \cdot ... \cdot m_r \mid n_1 \cdot n_2 \cdot ... \cdot n_r$

xi) $m \mid n_j$ *mit* $j = 1, 2, ..., r \Rightarrow m \mid (l_1 \cdot n_1 + l_2 \cdot n_2 + ... + l_r \cdot n_r) \ \ \forall l_j \in \mathbb{Z}$

Beweis. i) Es gilt $n = 1 \cdot n \ \ \forall n \in \mathbb{Z}$.
ii) Es gilt $0 = 0 \cdot n \Rightarrow n \mid 0 \ \ \forall n \in \mathbb{Z}$.
Per Definition der Teilbarkeit bedeutet $0 \mid n$, dass $\exists\ d \in \mathbb{Z}$ sodass $n = 0 \cdot d = 0$.
iii) Es gilt $m \mid n \Rightarrow \exists\ d \in \mathbb{Z} : n = m \cdot d$. Das bedeutet zum einen $n = (-m) \cdot (-d)$ und daher $(-m) \mid n$ und zum anderen $(-n) = m \cdot (-d)$ und daher $m \mid (-n)$.
iv) Aus $m \mid n$ und $n \neq 0$ folgt $m = \frac{n}{d}$ für ein $d \in \mathbb{Z} \backslash \{0\}$ und daher $|m| = \frac{|n|}{|d|} \leq |n|$.
v) Aus $n \mid 1$ folgt $|n| \leq 1$ (iv) und daher $n \in \{-1, 0, 1\}$. Da $1 = 0 \cdot d$ unmöglich ist, ist $n \in \{-1, 1\}$. Umgekehrt folgt aus $1 = (\pm 1)^2$, dass $\pm 1 \mid 1$.
vi) Aus $m \mid n$ und $n \mid m$ folgt: $\exists\ d_1, d_2 \in \mathbb{Z}$ sodass $n = d_1 \cdot m$ und $m = d_2 \cdot n$. Daher ist $n = d_1 \cdot d_2 \cdot n$. Für $n = 0$ ist auch $m = 0$ und somit $m = n$. Für $n \neq 0$ folgt $d_1 \cdot d_2 = 1$ also $d_1 \mid 1$ und $d_2 \mid 1$. Nach v) gilt daher $d_1 = \pm 1$ und $d_2 = \pm 1$. Daraus folgt schließlich $m = \pm n$.
vii) Aus $l \mid m$ und $m \mid n$ folgt: $\exists\ d_1, d_2 \in \mathbb{Z}$ sodass $m = l \cdot d_1$ und $n = m \cdot d_2$. Es folgt also $n = (l \cdot d_1) \cdot d_2 \Leftrightarrow n = l \cdot (d_1 \cdot d_2)$ und daher $l \mid n$.
viii) Aus $n = m \cdot d$ folgt $l \cdot n = l \cdot (m \cdot d) = (l \cdot m) \cdot d \ \ \forall l \in \mathbb{Z}$. Daraus folgt schließlich $l \cdot m \mid l \cdot n$.
ix) Aus $l \cdot m \mid l \cdot n$ folgt $l \cdot n = d \cdot l \cdot m$. Da $l \neq 0$ gilt, folgt $n = d \cdot m$ und somit $m \mid n$.
x) Aus $m_j \mid n_j$ mit $j = 1, 2, ..., r$ folgt: $\exists\ d_j \in \mathbb{Z}$, sodass $n_j = d_j \cdot m_j$ für $j = 1, 2, \ldots, r$. Daraus ergibt sich

$$n_1 \cdot n_2 \cdot ... \cdot n_r = (d_1 \cdot m_1) \cdot (d_2 \cdot m_2) \cdot ... \cdot (d_r \cdot m_r) = (d_1 \cdot d_2 \cdot ... \cdot d_r) \cdot (m_1 \cdot m_2 \cdot ... \cdot m_r)$$

woraus $m_1 \cdot m_2 \cdot ... \cdot m_r \mid n_1 \cdot n_2 \cdot \ldots \cdot n_r$ folgt.
xi) Aus $m \mid n_j$ mit $j = 1, 2, \ldots, r$ folgt: $\exists\ d_j \in \mathbb{Z}$, sodass $n_j = d_j \cdot m$ für

$j = 1, 2, \ldots, r$. Es gilt also

$$\begin{aligned} l_1 \cdot n_1 + l_2 \cdot n_2 + \ldots + l_r \cdot n_r &= l_1 \cdot d_1 \cdot m + l_2 \cdot d_2 \cdot m + \ldots + l_r \cdot d_r \cdot m \\ &= m \cdot (l_1 \cdot d_1 + l_2 \cdot d_2 + \ldots + l_r \cdot d_r) \end{aligned}$$

woraus $m \mid (l_1 \cdot n_1 + l_2 \cdot n_2 + \ldots + l_r \cdot n_r)$ folgt. □

Bemerkung. 1) Aus i) und iii) folgt, dass jede Zahl $n \in \mathbb{Z}$ die trivialen Teiler ± 1 und $\pm n$ besitzt. Gilt $m \mid n$ und ist m kein Element der Menge $\{-1, 1, -n, n\}$, so wird m echter Teiler von n genannt.

2) Aus $|m| \leq |n|$ iv) und somit $-|n| \leq m \leq |n|$ folgt, dass jede Zahl $n \in \mathbb{Z}$, $n \neq 0$ nur endlich viele Teiler besitzt.

Satz 2.1 (Division mit Rest)**.** *Es seien $m, n \in \mathbb{Z}$, $m > 0$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $0 \leq r < m$, sodass $n = q \cdot m + r$.*

Beweis. Zunächst wird die Existenz bewiesen:
Es sei $q \in \mathbb{Z}$ derart, dass $q \leq \frac{n}{m} < q + 1$. Daraus folgt $q \cdot m \leq n < q \cdot m + m$ und $0 \leq n - q \cdot m < m$. Setzt man nun $r = n - q \cdot m$, so sind $n = q \cdot m + r$ und $0 \leq r < m$ erfüllt.
Nun muss noch die Eindeutigkeit überprüft werden:
Angenommen $n = q \cdot m + r = q' \cdot m + r'$ mit $0 \leq r, r' < m$. Dann folgt $(q - q') \cdot m = r' - r$ und daher $q - q' = \frac{r'-r}{m}$. Aus $-m < r' - r < m$ folgt $-1 < \frac{r'-r}{m} < 1$. Da $\frac{r'-r}{m} \in \mathbb{Z}$, muss $\frac{r'-r}{m} = 0$ gelten. Somit folgt $r' - r = 0$ und daher gilt $r' = r$ und $q' = q$. □

2.1 Größter gemeinsamer Teiler

Definition. Es seien $n_1, n_2, ..., n_r \in \mathbb{Z}$. Falls $m \mid n_j$ für $j = 1, 2, ..., r$ heißt m gemeinsamer Teiler von $n_1, n_2, ..., n_r$.

Beispiel. 4 ist gemeinsamer Teiler von 16 und 44, denn $4 \mid 16$ und $4 \mid 44$.

Definition. Es seien $n_1, n_2, ..., n_r \in \mathbb{Z}$ nicht alle gleich 0. Der größte gemeinsame Teiler der Zahlen n_j mit $j = 1, 2, ..., r$ ist durch

$$\max\{m \in \mathbb{N} \setminus \{0\} : m \mid n_1, m \mid n_2, ..., m \mid n_r\} =: \mathrm{ggT}(n_1, n_2, ..., n_r)$$

bestimmt.

Beispiel. $\mathrm{ggT}(18, 24) = \max\{1, 2, 3, 6\} = 6$

Bemerkung. Die im Beispiel angeführte Methode zur Bestimmung des größten gemeinsamen Teilers ist nur für kleine Zahlen sinnvoll. Um den größten gemeinsamen Teiler von großen Zahlen zu finden, wird der Euklidische Algorithmus angewendet.

Satz 2.2 (Euklidischer Algorithmus)**.** *Es seien* $a, b \in \mathbb{N} \setminus \{0\}$ *gegeben, wobei o. B. d. A.* $b \leq a$ *gelten soll. Zur Bestimmung des* $\mathrm{ggT}(a, b)$ *werden die Reste bei wiederholter Division mit Rest bestimmt.*

$$\begin{aligned} a &= b \cdot q_0 + r_1, 0 \leq r_1 < b \\ b &= r_1 \cdot q_1 + r_2, 0 \leq r_2 < r_1 \\ r_1 &= r_2 \cdot q_2 + r_3, 0 \leq r_3 < r_2 \\ &\vdots \\ r_{j-1} &= r_j \cdot q_j + r_{j+1}, 0 \leq r_{j+1} < r_j \end{aligned}$$

Setze nun $b =: r_0$*. Wegen* $b = r_0 > r_1 > r_2 > \ldots > r_j > r_{r+1} > \ldots \geq 0$ *gibt es ein* $n \in \mathbb{N}$*, sodass* $r_{n+1} = 0$*. Dann gilt* $r_n = \mathrm{ggT}(a, b)$*.*

Beweis. Es wird zuerst gezeigt, dass r_n ein gemeinsamer Teiler der Zahlen a und b ist.
Aus $r_{n-1} = r_n \cdot q_n$ folgt $r_n \mid r_{n-1}$. Aus $r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n$ und Lemma 2.1 xi) folgt $r_n \mid r_{n-2}$.
Es sei bereits gezeigt, dass $r_n \mid r_{j+1}$ und $r_n \mid r_j$. Da $r_{j-1} = r_j \cdot q_j + r_{j+1}$, gilt nach Lemma 2.1 xi) $r_n \mid r_{j-1}$. Für $j = 1$ ergibt sich $r_n \mid r_0$, also $r_n \mid b$ und somit schließlich auch $r_n \mid a$, weil $a = b \cdot q_0 + r_1$. Daher ist r_n ein gemeinsamer Teiler von a und b.
Es bleibt nun zu zeigen,dass r_n der größte gemeinsame Teiler der Zahlen a und b ist.
Es sei $d > 0$ ein beliebiger gemeinsamer Teiler von a und b. Da $r_1 = a - b \cdot q_0$, gilt nach Lemma 2.1 xi) auch $d \mid r_1$. Es sei bereits gezeigt, dass $d \mid r_1, r_2 \ldots, r_j$. Da $r_{j+1} = r_{j-1} - r_j \cdot q_j$ gilt nach Lemma 2.1 xi) auch $d \mid r_{j+1}$. Für $j = n - 1$ ergibt sich $d \mid r_n$ und wegen Lemma 2.1 iv) gilt $d \leq r_n$. □

Beispiel. Gegeben sind die beiden natürlichen Zahlen 124 und 86. Mithilfe des Euklidischen Algorithmus kann der größte gemeinsame Teiler der Zahlen wie

folgt bestimmt werde:

$$\begin{aligned} 124 &= 86 \cdot 1 + 38 \\ 86 &= 38 \cdot 2 + 10 \\ 38 &= 10 \cdot 3 + 8 \\ 10 &= 8 \cdot 1 + 2 \\ 8 &= 2 \cdot 4 \end{aligned}$$

Daraus folgt, dass $\mathrm{ggT}(124, 86) = 2$.

Einige weiter wichtige Eigenschaften des größten gemeinsamen Teilers werden im folgenden Abschnitt kurz erläutert. Da einige Erkenntnisse sofort aus der Definition des größten gemeinsamen Teilers und den Eigenschaften der Teilbarkeit folgen, werden an dieser Stelle einige Sätze ohne Beweis angeführt.

Satz 2.3. *Es seien $n_1, n_2, ..., n_r \in \mathbb{Z}$ nicht alle gleich 0. Dann gilt:*

i) $\mathrm{ggT}(n_1, n_2, ..., n_r) = \mathrm{ggT}(|n_1|, |n_2|, ..., |n_r|)$

ii) Die Reihenfolge der n_j, $j = 1, 2, ..., r$ ist für die Bestimmung des ggT *nicht relevant.*

iii) Ist $r \geq 2$ und $n_r = 0$, dann ist $\mathrm{ggT}(n_1, n_2, ..., n_r) = \mathrm{ggT}(n_1, n_2, ..., n_{r-1})$. *Das bedeutet, dass für die Berechnung des* $\mathrm{ggT}(n_1, n_2, ..., n_r)$ *alle $n_j = 0$, $j = 1, 2, ..., r$ weggelassen werden können.*

iv) Ist $r \geq 2$ und $n_{r-1} = n_r$, dann ist $\mathrm{ggT}(n_1, n_2, ..., n_r) = \mathrm{ggT}(n_1, n_2, ..., n_{r-1})$. *Das bedeutet, dass bei der Berechnung des* $\mathrm{ggT}(n_1, n_2, ..., n_r)$ *mehrfach vorkommende Zahlen nur einmal beachtet werden müssen.*

v) Es seien $x_1, x_2, ..., x_{r-1} \in \mathbb{Z}$, dann ist

$$\mathrm{ggT}(n_1, n_2, ..., n_r) = \mathrm{ggT}\left(n_1, n_2, ..., n_{r-1}, n_r + \sum_{i=1}^{r-1} x_i \cdot n_i\right).$$

Beweis. Ohne Beweis. Die Aussagen folgen aus den Rechenregeln der Teilbarkeit. □

Satz 2.4. *Es seien $n_1, n_2, \ldots, n_r \in \mathbb{Z}$ nicht alle gleich 0. Dann gibt es $x_j \in \mathbb{Z}$, $j = 1, 2, \ldots, r$, sodass $d = \mathrm{ggT}(n_1, n_2, \ldots, n_r) = \sum_{j=1}^{r} x_j \cdot n_j$.*
Dh.: Der größte gemeinsame Teiler der Zahlen $n_1, n_2, \ldots, n_r$ lässt sich als Linearkombination der n_j darstellen.

Um sich von der Gültigkeit des Satzes zu überzeugen, wird der Satz zuerst allgemeiner formuliert und anschließend bewiesen:

Satz 2.5. *Es seien $n_1, n_2, \ldots, n_r \in \mathbb{Z}$ nicht alle gleich 0. Dann gilt:*

$$\mathrm{ggT}(n_1, n_2, \ldots, n_r) = \min\left(\left\{\sum_{j=1}^{r} x_j \cdot n_j \middle| x_j \in \mathbb{Z}\right\} \cap \mathbb{N} \setminus \{0\}\right)$$

Beweis. Es sei $d = \mathrm{ggT}(n_1, n_2, \ldots, n_r)$ und die Menge L sei folgendermaßen definiert:

$$L = \left\{\sum_{j=1}^{r} x_j \cdot n_j \middle| x_j \in \mathbb{Z}, \sum_{j=1}^{r} x_j \cdot n_j > 0\right\} \subseteq \mathbb{N} \setminus \{0\}$$

Die Menge L ist nicht leer, da $\sum_{j=1}^{r} n_j^2$ auf jeden Fall größer als Null ist und somit in L liegt. Aufgrund des Wohlordnungsaxioms der natürlichen Zahlen besitzt die Menge L dann auch ein kleinstes Element. Sei $d' := \min(L)$. Es bleibt zu zeigen, dass $d' = d$.
Zunächst wird bewiesen, dass $d \leq d'$ ist: Weil d' ein Element der Menge L ist, gilt $d' = \sum_{j=1}^{r} y_j \cdot n_j$ mit $y_j \in \mathbb{Z}$. Zusätzlich gilt laut Voraussetzung $d \mid n_j$. Nach Lemma 2.1 xi) folgt daraus $d \mid d'$ und wegen Lemma 2.1 iv) gilt dann $0 < d \leq d'$.
Um die Behauptung vollständig zu beweisen, bleibt nun noch zu zeigen, dass $d' \leq d$ gilt: Laut Satz 2.1 ist $n_j = q_j \cdot d' + r_j$ mit $0 \leq r_j < d'$ für $j = 1, 2, \ldots, r$. Es folgt

$$\begin{aligned} d' > r_j &= n_j - q_j \cdot d' \\ &= n_j - q_j \cdot \sum_{k=1}^{r} y_k \cdot n_k \\ &= (1 - q_j \cdot y_j) \cdot n_j + \sum_{k=1, k\neq j}^{r} (-q_j \cdot y_k) \cdot n_k \end{aligned}$$

Falls $r_{j_0} > 0$ für ein j_0, ist r_{j_0} ein Element von L, da sich die Zahl r_{j_0} als Linearkombination der n_j, $j = 1, 2, \ldots, r$ schreiben lässt und es gilt $0 < r_{j_0} < d'$. Dies ist ein Widerspruch zur Annahme, dass d' das kleinste Element der Menge L ist. Daher ist $r_j = 0$ für alle $j = 1, 2, \ldots, r$ und es gilt $n_j = q_j \cdot d'$. Es folgt $d' \mid n_j$ und somit ist d' ein gemeinsamer Teiler der Zahlen $n_1, n_2, \ldots, n_r$. Da d ihr größter gemeinsamer Teiler ist, folgt $d' \leq d$.
Insgesamt erhält man aus $d \leq d'$ und $d' \leq d$ schließlich die Aussage des Satzes. □

Beispiel. Gesucht sind $x, y \in \mathbb{Z}$ sodass $\mathrm{ggT}(35, 125) = x \cdot 35 + y \cdot 125$. Dazu wird

zuerst der Euklidische Algorithmus durchgeführt:

$$\begin{aligned} 125 &= 3 \cdot 35 + 20 \\ 35 &= 1 \cdot 20 + 15 \\ 20 &= 1 \cdot 15 + 5 \\ 15 &= 3 \cdot 5 + 0 \end{aligned}$$

Somit wurde gezeigt, dass $\text{ggT}(35, 125) = 5$. Um ein Paar möglicher Werte für x und y zu finden, wird der Euklidische Algorithmus im nächsten Schritt noch einmal rückwärts durchgeführt:

$$\begin{aligned} 5 &= 20 - 1 \cdot 15 \\ 5 &= 20 - 1 \cdot (35 - 1 \cdot 20) \\ 5 &= 2 \cdot 20 - 35 \\ 5 &= 2 \cdot (125 - 3 \cdot 35) - 35 \\ 5 &= 2 \cdot 125 - 7 \cdot 35 \end{aligned}$$

Daraus folgt $x = -7$ und $y = 2$ und $5 = \text{ggT}(35, 125) = -7 \cdot 35 + 2 \cdot 125$.

Satz 2.6. *Es seien $n_1, n_2, \ldots, n_r \in \mathbb{Z}$, nicht alle gleich 0. Dann ist*

$$\text{ggT}(l \cdot n_1, l \cdot n_2, \ldots, l \cdot n_r) = |l| \cdot \text{ggT}(n_1, n_2, ..., n_r) \; \forall l \in \mathbb{Z} \setminus \{0\}$$

Beweis. Ohne Beweis. □

Korollar 2.2. *Sind $n_1, n_2, \ldots, n_r \in \mathbb{Z}$ nicht alle gleich 0 und $d = \text{ggT}(n_1, n_2, \ldots, n_r)$. Dann ist:* $\text{ggT}(\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_r}{d}) = 1$

Beweis. Es gilt $d \mid n_i$ für $1 \leq i \leq r$. Daher sind $\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_r}{d} \in \mathbb{Z}$ ebenfalls nicht alle gleich 0. Mithilfe von Satz 2.6 folgt aus

$$d = \text{ggT}(n_1, n_2, \ldots, n_r) = \text{ggT}\left(d \cdot \frac{n_1}{d}, d \cdot \frac{n_2}{d}, \ldots, d \cdot \frac{n_r}{d}\right) = d \cdot \text{ggT}\left(\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_r}{d}\right)$$

wegen $d \neq 0$ sofort $\text{ggT}(\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_r}{d}) = 1$. □

Satz 2.7. *Es seien m, n_1, $n_2 \in \mathbb{Z}$ und $m \neq 0$. Aus $m \mid n_1 \cdot n_2$ und $\text{ggT}(m, n_1) = 1$ folgt $m \mid n_2$.*

Beweis. Laut Satz 2.4 gibt es $x_1, x_2 \in \mathbb{Z}$ sodass gilt:

$$\begin{aligned} & x_1 \cdot m + x_2 \cdot n_1 = 1 && \mid \cdot n_2 \\ & x_1 \cdot \underbrace{m \cdot n_2}_{m \mid (m \cdot n_2)} + x_2 \cdot \underbrace{n_1 \cdot n_2}_{m \mid (n_1 \cdot n_2)} = n_2 \end{aligned}$$

Die Aussage folgt sofort aus Lemma 2.1 xi). □

Definition. Es seien $n_1, n_2, \ldots, n_r \in \mathbb{Z}$ nicht alle gleich 0.
Die Zahlen $n_1, n_2, \ldots, n_r$ heißen relativ prim oder teilerfremd, wenn

$$\text{ggT}(n_1, n_2, \ldots, n_r) = 1.$$

2.2 Primzahlen

Nicht nur bei der Auseinandersetzung mit der Teilbarkeit von ganzen Zahlen sondern auch bei der Formulierung und den Beweisen des quadratischen Reziprozitätsgesetzes spielen die Primzahlen eine wichtige Rolle. Daher werden im nächsten Abschnitt die grundlegenden Eigenschaften von Primzahlen thematisiert. Die Ausführung orientiert sich dabei erneut am Werk von Bundschuh [9] sowie am Skriptum von Fulmek [7].

Definition. Es sei $p \in \mathbb{N}$, $p > 1$. Die Zahl p heißt Primzahl, wenn p nur die trivialen Teiler ± 1 und $\pm p$ besitzt.
Die Menge aller Primzahlen wird mit $\mathbb{P}$ bezeichnet:

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots\}$$

Bemerkung. Aus der Definition von Primzahlen folgt sofort, dass zwei verschiedene Primzahlen p_1 und p_2 stets teilerfremd sind. Es gilt daher: $\text{ggT}(p_1, p_2) = 1$.

Lemma 2.3. *Es sei $p \in \mathbb{P}$. Weiters sei $n \in \mathbb{Z}$. Dann sind äquivalent:*

i) $p \nmid n$

ii) $\text{ggT}(p, n) = 1$

Beweis. i) $\Rightarrow$ ii)Angenommen $\text{ggT}(p, n) = d > 1$. Dann gilt: $d \mid p$ und $d \mid n$. Da $p \in \mathbb{P}$ ist also $d = p$ und somit folgt $p \mid n \Rightarrow$ Widerspruch zur Annahme $p \nmid n$.
ii)$\Rightarrow$ i) Angenommen $p \mid n$. Dann gilt $\text{ggT}(p, n) = p > 1 \Rightarrow$ Widerspruch zur Annahme $\text{ggT}(p, n) = 1$. □

Satz 2.8. *Es sei $p \in \mathbb{N}$, $p > 1$. Dann sind äquivalent:*

i) p ist eine Primzahl

ii) Falls $p \mid a \cdot b$ mit $a, b \in \mathbb{Z}$, gilt entweder $p \mid a$ oder $p \mid b$.

iii) Falls $p = x \cdot y$ mit $x, y \in \mathbb{Z}$, gilt entweder $x = \pm 1$ oder $y = \pm 1$

Beweis. i) $\Rightarrow$ ii) Gilt $p \mid a$, so ist die Behauptung erfüllt. Gilt $p \nmid a$, so folgt aus Lemma 2.3 $\text{ggT}(p, a) = 1$ woraus wegen Satz 2.7 sofort $p \mid b$ folgt.

ii) $\Rightarrow$ iii) Gilt $p = x \cdot y$, dann gilt trivialerweise auch $p \mid x \cdot y$. Nach Voraussetzung gilt dann $p \mid x$ oder $p \mid y$. Angenommen es gilt $p \mid x$. Aus $p = x \cdot y$ folgt auch $x \mid p$ und daher $p = |x|$ (Lemma 2.1). Damit folgt $p = |p| = |x \cdot y| = |x| \cdot |y| = p \cdot |y|$ und somit gilt $|y| = 1$. Gilt $p \mid y$, so folgt völlig analog $|x| = 1$.
iii) $\Rightarrow$ i) Es sei n ein Teiler von p. Dann gibt es ein $m \in \mathbb{Z}$ sodass $p = m \cdot n$. Nach Voraussetzung folgt somit, dass entweder $n = \pm 1$ oder $m = \pm 1$, woraus $n = \pm p$ folgt. Daher ist $n \in \{-p, -1, 1, p\}$ und p besitzt nur die trivialen Teiler. Per Definition ist p somit eine Primzahl. □

Lemma 2.4. *Es sei $p \in \mathbb{P}$. Weiters seien $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.*
Falls $p \mid a_1 \cdot a_2 \cdot \ldots \cdot a_n$, dann gibt es ein $j \in \{1, 2, \ldots, n\}$ sodass $p \mid a_j$.

Beweis. Die Behauptung folgt aus Satz 2.8 ii) und Induktion. □

Satz 2.9 (Fundamentalsatz der Arithmetik)**.** *Jede natürliche Zahl $n > 1$ lässt sich als Produkt von Primzahlen schreiben. Die Darstellung der Zahl n als Produkt von Primzahlen wird Primfaktorzerlegung von n genannt und ist bis auf die Reihenfolge der Faktoren eindeutig. Dh:*

$$n = \prod_{j=1}^{\infty} {p_j}^{\alpha_j}$$

für gewisse, eindeutig bestimmte $\alpha_j \in \mathbb{N}$, wobei $\alpha_j = 0$ für alle,bis auf endlich viele j.

Beispiel. $60 = 2^2 \cdot 3 \cdot 5$

Beweis. Die Existenz der Primfaktorzerlegung wird mittels Induktion gezeigt:
$n = 2 \in \mathbb{P}$. Es sei nun $n > 2$. Es sei bereits gezeigt, dass sich jedes $k = 2, 3, \ldots, n-1$ als Produkt von Primzahlen schreiben lässt. Zu zeigen bleibt demnach, dass n sich ebenfalls als Produkt von Primzahlen schreiben lässt.
Ist n eine Primzahl, so ist nichts zu zeigen, da n als Produkt mit einem Faktor aufgefasst werden kann. Ist n keine Primzahl, so existiert ein $d \in \mathbb{N}$, $1 < d < n$ sodass $d \mid n$ und $n = d \cdot m$. Dann gilt auch $1 < m < n$ und nach Induktionsannahme sind d und m jeweils Produkte von Primzahlen. Folglich ist auch n ein Produkt von Primzahlen.
Es bleibt noch die Eindeutigkeit der Primfaktorzerlegung zu zeigen:
Angenommen es gibt zwei Primfaktorzerlegungen einer natürlichen Zahl ≥ 2, die sich nicht nur durch die Reihenfolge der Primfaktoren unterscheiden. Dann existiert eine kleinste Zahl $n \in \mathbb{N}$, die zwei wesentlich verschiedene Primfaktorzerlegungen besitzt. Dh: $n = p_1 \cdot p_2 \ldots p_r = q_1 \cdot q_2 \ldots q_s$ wobei $p_j, q_j \in \mathbb{P}$ und $p_j \neq q_k$ $\forall j, k$, denn sonst könnte man kürzen und erhielte eine kleinere Zahl mit nicht eindeutiger Primfaktorzerlegung. Da $p_1 \mid n$ folgt, dass $p_1 \mid (q_1 \cdot q_2 \ldots q_s)$. Nach

Lemma 2.4 gibt es ein $k \in \{1, 2, \ldots, s\}$ sodass $p_1 \mid q_k$. Da $p_1 > 1$, muss $p_1 = q_k$ gelten. Daraus folgt ein Widerspruch zur Annahme $p_1 \neq q_1, q_2, \ldots, q_s$. □

Neben den eben thematisierten Aussagen über Primzahlen, gibt es natürlich eine Vielzahl an weiteren Aussagen über die Menge der Primzahlen [3], die einer näheren Betrachtung würdig sind. Doch da diese Aussagen für das quadratische Reziprozitätsgesetz nicht ausschlaggebend sind, werden sie an dieser Stelle nicht weiter ausgeführt.

2.3 Kleinstes gemeinsames Vielfaches

Betrachtet man eine Menge von mehreren natürlichen Zahlen, so ist man häufig nicht nur daran interessiert ihren größten gemeinsamen Teiler zu finden, sondern möchte zusätzlich auch das kleinste gemeinsame Vielfache der Zahlen angeben. Daher und aufgrund der Bedeutung der folgenden Aussagen für weitere Heranführung an das Reziprozitätsgesetz wird im folgenden Abschnitt kurz das kleinste gemeinsame Vielfache von natürlichen Zahlen thematisiert.

Definition. Es seien $n_1, n_2, \ldots, n_r \in \mathbb{Z}$. Eine Zahl $m \in \mathbb{Z}$ heißt gemeinsames Vielfaches von $n_1, n_2, \ldots, n_r$, wenn gilt: $n_1 \mid m$, $n_2 \mid m$, …, $n_r \mid m$.

Definition. Es seien $n_1, n_2, \ldots, n_r \in \mathbb{Z} \setminus \{0\}$. Das kleinste gemeinsame Vielfache der Zahlen $n_1, n_2, \ldots, n_r$ ist definiert durch

$$\mathrm{kgV}(n_1, n_2, \ldots, n_r) := \min\{m \in \mathbb{N} \setminus \{0\} : n_1 \mid m, n_2 \mid m, \ldots, n_r \mid m\}$$

Beispiel.

$$\begin{aligned}\mathrm{kgV}(5, 15, 25) &= \min(\{5, 10, \ldots, 75, \ldots\} \cap \{15, 30, \ldots, 75 \ldots\} \cap \{25, 50, 75, \ldots\}) \\ &= 75\end{aligned}$$

Satz 2.10. *Es seien $n_1, n_2, \ldots, n_k \in \mathbb{Z} \setminus \{0\}$. Dann sind äquivalent:*

i) m ist ein gemeinsames Vielfaches von $n_1, n_2, \ldots, n_k$

ii) $\mathrm{kgV}(n_1, n_2, \ldots, n_k) \mid m$

Beweis. Es sei $v := \mathrm{kgV}(n_1, n_2, \ldots, n_k)$.
i)⇒ ii) Aus der Division mit Rest ergibt sich $m = q \cdot v + r$ für $q, r \in \mathbb{Z}$ mit $0 \leq r < v$. Da $n_i \mid m$ und $n_i \mid v$ folgt aus Lemma 2.1, dass $n_i \mid r$ für alle $i = 1, 2, \ldots, k$. Somit ist r ein gemeinsames Vielfaches von $n_1, n_2, \ldots, n_k$. Da aber $r < v$ ist und v das kleinste gemeinsame Vielfache von $n_1, n_2, \ldots, n_k$ ist, folgt $r = 0$. Daher ist $m = q \cdot v$ und $v \mid m$.
ii) Aus $n_i \mid v$ und $v \mid m$ folgt wegen Lemma 2.1 vii) sofort $n_i \mid m$. □

3 Kongruenzen

Im Kapitel 2 wurden bislang lediglich Aussagen über die Teilbarkeit einer Zahl $n \in \mathbb{Z}$ durch eine andere Zahl $m \in \mathbb{Z}$ getroffen. Formuliert man die Erkenntnisse der Teilbarkeit für die Division mit Rest so wurde bis hierher demnach nur unterschieden, ob die Division von n durch m den Rest 0 oder einen Rest ungleich 0 liefert. Im folgenden Abschnitt wird diese Sichtweise nun erweitert, indem Zahlen, die bei Division durch m denselben Rest liefern, zu Restklassen zusammengefasst werden. Sind zwei Zahlen n_1 und n_2 Elemente derselben Restklasse, so nennt man sie kongruent. Die Ausarbeitung zum Thema Kongruenz basiert dabei auf mehreren Quellen der Fachliteratur.[10], [9], [7], [3]

Satz 3.1. *Es seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$, $m \geq 2$. Dann sind äquivalent:*

i) a und b haben bei Division durch m denselben Rest.

ii) $m \mid (a - b)$

iii) Es gibt ein $k \in \mathbb{Z}$, derart dass $a = b + k \cdot m$.

Beweis. i) $\Rightarrow$ ii) Es seien $q_1, q_2, r \in \mathbb{Z}$, sodass $a = q_1 \cdot m + r$ und $b = q_2 \cdot m + r$ mit $0 \leq r < m$. Dann ist $a - b = (q_1 \cdot m + r) - (q_2 \cdot m + r) = (q_1 - q_2) \cdot m$ und daher gilt $m \mid (a - b)$.
ii) $\Rightarrow$ iii) Da $m \mid (a - b)$ gibt es laut Definition der Teilbarkeit ein $k \in \mathbb{Z}$ mit $a - b = k \cdot m$ woraus sofort $a = b + k \cdot m$ folgt.
iii) $\Rightarrow$ i) Die Division von b durch m mit Rest liefert $b = q \cdot m + r$ für $q, r \in \mathbb{Z}$ und $0 \leq r < m$. Damit folgt nun

$$a = b + k \cdot m = q \cdot m + r + k \cdot m = (q + k) \cdot m + r$$

Die Division von a durch m liefert daher ebenfalls den Rest r. □

Definition. Es seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$, $m \geq 2$. Erfüllen a, b und m eine und somit alle Bedingungen aus Satz 3.1, so bezeichnet man a und b als kongruent modulo m und schreibt dafür $a \equiv b \pmod{m}$ (kurz: $a \equiv b\,(m)$). Die Zahl m wird hierbei Modul genannt.
Erfüllen a, b und m die Bedingungen des Satzes nicht, so bezeichnet man a und b als inkongruent modulo m und schreibt dafür $a \not\equiv b \pmod{m}$ (kurz: $a \not\equiv b\,(m)$).

Beispiel. $7 \equiv 39 \pmod{8}$, weil 7 und 39 haben bei der Division durch die Zahl 8 beide Rest 7, beziehungsweise gilt $8 \mid (7 - 39)$ und ebenso gilt $7 = 39 + (-4) \cdot 8$.

Satz 3.2. *Es sei $m \in \mathbb{N}$, $m \geq 2$. Kongruent modulo m zu sein ist eine Äquivalenzrelation. Das heißt $\equiv$ ist reflexiv, symmetrisch und transitiv.*

Beweis. Reflexivität: $a \equiv a \pmod{m}$
Symmetrie: $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
Transitivität: $a \equiv b \pmod{m}$ und $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$
Es ist offensichtlich, dass alle drei Aussagen erfüllt sind. □

Lemma 3.1 (Rechenregeln für Kongruenzen)**.** *Es seien* $a, b, c, d, k, n \in \mathbb{Z}$, $n \neq 0$ *und* $m \in \mathbb{N}$, $m \geq 2$. *Weiters sei* $a \equiv b \pmod{m}$ *und* $c \equiv d \pmod{m}$. *Dann gelten folgende Aussagen:*

i) $a + c \equiv b + d \pmod{m}$

ii) $a \cdot c \equiv b \cdot d \pmod{m}$

iii) Aus $n \mid m$ *folgt* $a \equiv b \pmod{|n|}$ *für* $|n| \geq 2$.

iv) $n \cdot a \equiv n \cdot b \pmod{|n| \cdot m}$

v) $n \cdot a \equiv n \cdot b \pmod{m} \iff a \equiv b \left(\mathrm{mod}\, \frac{m}{\mathrm{ggT}(m,n)}\right)$

vi) Falls $a \equiv b \pmod{m}$ *und* $a \equiv b \pmod{n}$, *dann* $a \equiv b \pmod{\mathrm{kgV}(m,n)}$

vii) $a + k \equiv b + k \pmod{m}$

viii) $a \cdot k \equiv b \cdot k \pmod{m}$

ix) $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, …, $a_k \equiv b_k \pmod{m}$
$\Rightarrow a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k \pmod{m}$

x) $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, … $a_k \equiv b_k \pmod{m}$
$\Rightarrow a_1 \cdot a_2 \cdot \ldots \cdot a_k \equiv b_1 \cdot b_2 \cdot \ldots \cdot b_k \pmod{m}$

xi) $a^k \equiv b^k \pmod{m}$ *für* $k \in \mathbb{N} \setminus \{0\}$

xii) Ist p *ein Polynom mit Koeffizienten aus* $\mathbb{Z}$, *so gilt* $p(a) \equiv p(b) \pmod{m}$.

xiii) Aus $k \cdot a \equiv k \cdot b \pmod{m}$ *und* $\mathrm{ggT}(k, m) = 1$ *folgt* $a \equiv b \pmod{m}$.

Beweis. i) Es gilt $m \mid (a - b)$ und $m \mid (c - d)$. Daraus folgt aufgrund von Lemma 2.1 xi)

$$m \mid (a - b) + (c - d) \iff m \mid (a + c) - (b + d) \iff a + c \equiv b + d \pmod{m}$$

ii) Es gilt $m \mid (a - b)$ und $m \mid (c - d)$. Daraus folgt

$$m \mid (a - b) \cdot c + b \cdot (c - d) \iff m \mid a \cdot c - b \cdot d \iff a \cdot c \equiv b \cdot d \pmod{m}.$$

iii) Aus $n \mid m$ folgt $|n|\big|m$ (Lemma 2.1 iii)). Es gilt also $|n|\big|m$ und $m \mid (a-b)$, weil $a \equiv b \pmod{m}$. Aus der Transitivität der Teilbarkeit folgt

$$|n|\big|(a-b) \Longleftrightarrow a \equiv b \pmod{|n|}$$

iv) Es gilt $m \mid (a-b)$, das bedeutet $\exists k \in \mathbb{Z}$ mit $a-b = k \cdot m$. Daraus folgt

$$\begin{aligned} n \cdot a - n \cdot b = n \cdot k \cdot m &\Longrightarrow n \cdot m \mid (n \cdot a - n \cdot b) \\ &\Longleftrightarrow |n| \cdot m \big| (n \cdot a - n \cdot b) \\ &\Longleftrightarrow n \cdot a \equiv n \cdot b \pmod{|n| \cdot m} \end{aligned}$$

v) Es sei $\mathrm{ggT}(n,m) := d$.
Es wird zunächst die Implikation $n \cdot a \equiv n \cdot b \pmod{m} \Longrightarrow a \equiv b \left(\mathrm{mod}\, \frac{m}{\mathrm{ggT}(m,n)}\right)$ überprüft: Es gilt $m \mid (n \cdot a - n \cdot b)$. Das bedeutet $\exists k \in \mathbb{Z}$ sodass $n \cdot (a-b) = k \cdot m$. Es folgt $\frac{n}{d} \cdot (a-b) = k \cdot \frac{m}{d}$, wobei $\frac{n}{d}, \frac{m}{d} \in \mathbb{Z}$ sind. Daraus folgt $\frac{m}{d} \mid \frac{n}{d} \cdot (a-b)$ und weil nach Korollar 2.2 $\mathrm{ggT}(\frac{m}{d}, \frac{n}{d}) = 1$ gilt, folgt aus Satz 2.7 schließlich $\frac{m}{d} \mid (a-b) \Longleftrightarrow a \equiv b \left(\mathrm{mod}\, \frac{m}{\mathrm{ggT}(m,n)}\right)$.
Nun wird noch die zweite Implikation gezeigt: Laut Annahme gilt $\frac{m}{d} \mid (a-b)$. Daraus folgt, dass ein $k \in \mathbb{Z}$ existiert, sodass $a - b = k \cdot \frac{m}{d}$. Daraus ergibt sich $n \cdot a - n \cdot b = k \cdot \frac{m}{d} \cdot n$ wobei $k \cdot \frac{n}{d} \in \mathbb{Z}$ ist. Somit erhält man $m \mid (n \cdot a - n \cdot b)$ und damit die Aussage.
vi) Es gilt $m \mid (a-b)$ und $n \mid (a-b)$. Aus der Definition des gemeinsamen Vielfachen folgt, dass $a-b$ ein gemeinsames Vielfaches von m und n ist. Da das kleinste gemeinsame Vielfache zweier Zahlen alle gemeinsamen Vielfachen der beiden Zahlen teilt, gilt auch $\mathrm{kgV}(m,n) \mid (a-b)$ was äquivalent zu
$a \equiv b \pmod{\mathrm{kgV}(m,n)}$ ist.
vii) Die Aussage ist ein Spezialfall von i).
viii) Die Aussage ist ein Spezialfall von ii).
ix) Beweis durch Induktion: Für $k = 1$ ist nichts zu zeigen und $k = 2$ wurde in i) bereits gezeigt. Es sei also $k \geq 2$ und $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, …, $a_k \equiv b_k \pmod{m}$, $a_{k+1} \equiv b_{k+1} \pmod{m}$. Nach Induktionsvoraussetzung gilt $a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k \pmod{m}$. Wendet man i) auf diese Kongruenz und die Kongruenz $a_{k+1} \equiv b_{k+1} \pmod{m}$ an, erhält man die Aussage.
x) Der Beweis kann mittels Induktion völlig analog zum Beweis von ix) geführt werden:
Nach Induktionsvoraussetzung gilt $a_1 \cdot a_2 \cdot \ldots \cdot a_k \equiv b_1 \cdot b_2 \cdot \ldots \cdot b_k \pmod{m}$. Wendet man ii) auf diese Kongruenz und die Kongruenz $a_{k+1} \equiv b_{k+1} \pmod{m}$ an, erhält man die Aussage.
xi) Die Aussage ist ein Spezialfall von x).

xii) Es sei

$$p(x) = c_n \cdot x^n + c_{n-1} \cdot x^{n-1} + \ldots + c_1 \cdot x + c_0$$

ein Polynom mit $c_0, c_1, \ldots, c_l \in \mathbb{Z}$.
Laut xi) gilt

$$a^2 \equiv b^2 \pmod{m}, a^3 \equiv b^3 \pmod{m}, \ldots, a^n \equiv b^n \pmod{m}$$

Laut viii) gilt

$$c_1 \cdot a \equiv c_1 \cdot b \pmod{m}, c_2 \cdot a^2 \equiv c_2 \cdot b^2 \pmod{m}, \ldots, c_n \cdot a^n \equiv c_n \cdot b^n \pmod{m}$$

Nach Anwendung von ix) folgt schließlich die Aussage.
xiii) Die Aussage ist ein Spezialfall von v). □

3.1 Lineare Kongruenzen

Definition. Es seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$, $m \geq 2$.
Die Gleichung $a \cdot x \equiv b \pmod{m}$ wird als lineare Kongruenz beziehungsweise lineare Kongruenzgleichung bezeichnet.

Bemerkung. Beim Lösen der linearen Kongruenzgleichung $a \cdot x \equiv b \pmod{m}$ sucht man alle modulo m inkongruenten Lösungen.

Satz 3.3. *Es seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$, $m \geq 2$. Die lineare Kongruenz $a \cdot x \equiv b \pmod{m}$ ist genau dann lösbar, wenn $\mathrm{ggT}(a, m) \mid b$. In diesem Fall gibt es genau $\mathrm{ggT}(a, m)$ verschiedene inkongruente Lösungen modulo m.*
Insbesondere gilt: $\mathrm{ggT}(a, m) = 1 \iff a \cdot x \equiv b \pmod{m}$ besitzt eine eindeutige Lösung modulo m.

Beweis. Es sei $d := \mathrm{ggT}(a, m)$.
$\Longrightarrow$ Die Kongruenz $a \cdot x \equiv b \pmod{m}$ sei lösbar. Dann gibt es ein $k \in \mathbb{Z}$ sodass gilt:

$$a \cdot x \equiv b \pmod{m} \iff m \mid (a \cdot x - b) \iff a \cdot x - b = k \cdot m \iff a \cdot x - k \cdot m = b$$

Wegen $d \mid a$ und $d \mid m$ folgt mithilfe von Lemma 2.1 xi) auch $d \mid b$.
$\Longleftarrow$ Da sich $\mathrm{ggT}(a, m)$ nach Satz 2.4 als Linearkombination schreiben lässt, existieren ganze Zahlen x' und k', sodass $d = x' \cdot a + k' \cdot m$. Laut Annahme existiert weiters ein $l \in \mathbb{Z}$, sodass $b = d \cdot l$. Daraus ergibt sich: $b = d \cdot l = x' \cdot l \cdot a + k' \cdot l \cdot m$ woraus wiederum $b \equiv x' \cdot l \cdot a \pmod{m}$ folgt. Setzt man nun $x = x' \cdot l$, so ist x eine Lösung von $a \cdot x \equiv b \pmod{m}$.
Abschließend bleibt zu zeigen, dass die Anzahl der modulo m inkongruenten Lösungen genau d beträgt.

Dazu wird die Behauptung aufgestellt, dass, wenn x_0 eine Lösung der linearen Kongruenz $a \cdot x \equiv b \pmod{m}$ ist (wobei $m = d \cdot c \iff c = \frac{m}{d} \in \mathbb{N} \setminus \{0\}$) alle modulo m inkongruenten Lösungen durch

$$\underbrace{x_0 + 0 \cdot c}_{x_0},\ \underbrace{x_0 + 1 \cdot c}_{x_1},\ \ldots,\ \underbrace{x_0 + (d-1) \cdot c}_{x_{d-1}}.$$

gefunden sind. Um das zu überprüfen, überzeugen wir uns zuerst davon, dass $x_0, x_1, \ldots, x_{d-1}$ tatsächlich Lösungen der Kongruenz sind:
Es sei $i \in \mathbb{Z}$. Dann gilt:

$$a \cdot (x_0 + i \cdot c) = a \cdot x_0 + i \cdot a \cdot c = a \cdot x_0 + i \cdot \frac{a}{d} \cdot m \equiv a \cdot x_0 \equiv b \pmod{m}$$

Aus $x_0 + i \cdot c \equiv x_0 + j \cdot c \pmod{m}$ folgt zusätzlich

$$m \mid (i-j) \cdot c \iff d \cdot c \mid (i-j) \cdot c \overset{\text{Teilbarkeitsr.}}{\implies} d \mid (i-j)$$

und für $0 \leq i, j \leq d-1$ gilt $d \mid (i-j)$ nur im Fall $i = j$. Damit ist gezeigt, dass die Lösungen paarweise inkongruent sind.
Sei nun $y \in \mathbb{Z}$ eine beliebige Lösung der linearen Kongruenz. Dann gilt für $r, q \in \mathbb{Z}$ und $j \in \{0, \ldots, d-1\}$:

$$\begin{aligned}
a \cdot y \equiv a \cdot x_0 \equiv b \pmod{m} &\overset{\text{Kürzungsr.}}{\iff} y \equiv x_0 \left(\operatorname{mod} \frac{m}{\operatorname{ggT}(m,a)} \right) \\
&\iff y \equiv x_0 \left(\operatorname{mod} \frac{m}{d} \right) \\
&\iff y = x_0 + r \cdot \frac{m}{d} \\
&\iff y = x_0 + (q \cdot d + j) \cdot \frac{m}{d} \\
&\iff y = x_0 + q \cdot m + j \cdot \frac{m}{d} \\
&\iff y \equiv x_0 + c \cdot j = x_j \pmod{m}
\end{aligned}$$

Dh. jede beliebige Lösung ist kongruent zu einer der Lösungen $x_0, x_1, \ldots, x_{d-1}$, wodurch beweisen ist, dass es $d = \operatorname{ggT}(a, m)$ verschiedene modulo m inkongruente Lösungen gibt. □

Beispiel. i) $8 \cdot x \equiv 4 \pmod{16}$
Der $\operatorname{ggT}(8, 16)$ ist 8, aber $8 \nmid 4$. Daraus folgt sofort, dass die lineare Kongruenz nicht lösbar ist.
ii) $8 \cdot x \equiv 4 \pmod{15}$
Der $\operatorname{ggT}(8, 15)$ ist 1 und $1 \mid 4$. Daraus folgt, dass die lineare Kongruenz lösbar ist

und genau eine Lösung besitzt. Um die Lösung zu finden, wird der Euklidische Algorithmus zuerst vorwärts und dann rückwärts ausgeführt:

$$\begin{aligned} 15 &= 8 \cdot 1 + 7 \\ 8 &= 7 \cdot 1 + 1 \\ 7 &= 1 \cdot 7 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 8 - 7 \cdot 1 \\ 1 &= 8 - (15 - 8 \cdot 1) \cdot 1 \\ 1 &= 2 \cdot 8 - 15 \end{aligned}$$

Damit wurde die Linearkombination des $\mathrm{ggT}(8, 15)$ gefunden:

$$\mathrm{ggT}(8, 15) = 1 = 2 \cdot 8 + (-1) \cdot 15$$

Daraus ergibt sich schließlich:

$$\begin{aligned} 2 \cdot 8 + (-1) \cdot 15 &= 1 && \mid \cdot 4 \\ 8 \cdot 8 + (-4) \cdot 15 &= 4 \\ 8 \cdot 8 &\equiv 4 \pmod{15} \Longrightarrow x_0 = 8 \end{aligned}$$

Probe: $64 \equiv 4 \pmod{15}$, weil $15 \mid (64 - 4)$.

Dieses Beispiel demonstriert bereits, wie die Lösung einer linearen Kongruenzgleichung gefunden werden kann, sofern sie existiert. Da eines der Ziele der vorliegenden Arbeit jedoch die Lösung von quadratischen Kongruenzgleichungen ist, wird es jedoch nötig sein, auch Systeme von mehreren linearen Kongruenzen zu lösen. Dazu wird der chinesische Restsatz herangezogen.

Definition. Es seien $m_1, m_2, \ldots, m_k \in \mathbb{N} \setminus \{0, 1\}$ und $c_1, c_2, \ldots, c_k \in \mathbb{Z}$.
Das System $x \equiv c_j \pmod{m_j}$ für $j = 1, 2, \ldots, k$ heißt simultane Kongruenz.

Beispiel. Die Kongruenzen $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$ und $x \equiv 2 \pmod 7$ bilden eine simultane Kongruenz. Beim Lösen dieser simultanen Kongruenz wird daher eine Zahl x gesucht, die bei der Division durch 3 den Rest 2 hat, bei der Division durch 5 den Rest 3 hat und bei der Division durch 7 den Rest 2 hat und somit alle Kongruenzen der simultanen Kongruenz erfüllt.

Satz 3.4 (Chinesischer Restsatz)**.** *Es seien $m_1, m_2, \ldots, m_k \in \mathbb{N} \setminus \{0, 1\}$ paarweise teilerfremd.*
Dann besitzt die simultane Kongruenz $x \equiv c_j \pmod{m_j}$ eine Lösung, die modulo

$m_1 \cdot m_2 \cdot \ldots \cdot m_k$ *eindeutig ist.*

Beweis. Es sei $M := m_1 \cdot m_2 \cdot \ldots \cdot m_k$.
Weiters sei $M_j = \frac{M}{m_j} = m_1 \cdot \ldots \cdot m_{j-1} \cdot m_{j-1} \cdot \ldots \cdot m_k$.
Es gilt $\text{ggT}(m_j, M_j) = 1 \; \forall j = 1, 2, \ldots, k$, denn angenommen $\text{ggT}(m_j, M_j) > 1$, dann existiert ein $p \in \mathbb{P}$, sodass

$$p \mid m_j \text{ und } p \mid M_j \iff p \mid m_1 \cdot \ldots \cdot m_{j-1} \cdot m_{j-1} \cdot \ldots \cdot m_k$$

Aus Lemma 2.4. folgt daher $p \mid m_i$ für ein $i \neq j$. Dann ist aber $\text{ggT}(m_j, m_i) \geq p$ und dies ist ein Widerspruch zur Annahme, dass $m_1, m_2, \ldots, m_k$ paarweise teilerfremd sind.
Laut Satz 2.4 existieren daher $x_j, y_j \in \mathbb{Z}$, sodass $x_j \cdot m_j + y_j \cdot M_j = 1$ für alle $j = 1, 2, \ldots, k$ gilt. Dann gilt

$$y_j \cdot M_j \equiv 1 \pmod{m_j} \quad \text{und} \quad y_j \cdot M_j \equiv 0 \pmod{m_i} \text{ für } i \neq j$$

wobei die zweite Kongruenz gilt, da m_i für $i \neq j$ sicher im Produkt M_j enthalten ist.
Setzt man nun $x = \sum_{i=1}^{k} c_i \cdot y_i \cdot M_i$, dann ist x eine Lösung der simultanen Kongruenz, weil

$$\begin{aligned} x &= c_j \cdot \underbrace{y_j \cdot M_j}_{\equiv 1 \pmod{m_j}} + \sum_{i=1, i\neq j}^{k} c_i \cdot \underbrace{y_i \cdot M_i}_{\equiv 0 \pmod{m_j}} \\ &\equiv c_j \cdot 1 + \sum_{i=1, i\neq j}^{k} c_i \cdot 0 \equiv c_j \pmod{m_j} \end{aligned}$$

Es bleibt zu zeigen, dass die Lösung eindeutig ist.
Angenommen $x \equiv c_j \pmod{m_j}$ und $y \equiv c_j \pmod{m_j}$. Dann ist $x \equiv y \pmod{m_j}$ und es gilt $m_j \mid (x - y) \; \forall j = 1, 2, \ldots, k$. Demnach ist $x - y$ ein gemeinsames Vielfaches der m_j. Wegen $\text{kgV}(m_1, m_2, \ldots, m_k) = m_1 \cdot m_2 \cdot \ldots \cdot m_k$ folgt daher $m_1 \cdot m_2 \cdot \ldots \cdot m_k \mid (x - y)$ und daher $x \equiv y \pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_k}$. Die Lösung ist daher modulo $m_1 \cdot m_2 \cdot \ldots \cdot m_k$ eindeutig. □

Der Beweis des chinesischen Restsatzes ist konstruktiv, dh. die Schritte des Beweises können auch zur Lösung konkreter Beispiele herangezogen werden und führen stets zur Lösung der simultanen Kongruenz. Im folgenden Beispiel wird jedoch eine schnellere Lösungsmethode demonstriert.

Beispiel. Die simultane Kongruenz $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$ und $x \equiv 2 \pmod{7}$ soll gelöst werden. Laut chinesischem Restsatz ist das System der linearen Kongruenzen lösbar, da $3, 5$ und 7 teilerfremd sind.

$x \equiv 2 \pmod 3$ ist äquivalent $x = 2 + 3 \cdot t$ für $t \in \mathbb{Z}$. Diese Erkenntnis wird nun in die zweite Kongruenz des Systems eingesetzt:

$$\begin{aligned}
& x \equiv 3 \pmod 5 \\
\iff\ & 2 + 3 \cdot t \equiv 3 \pmod 5 && \mid -2 \\
\iff\ & 3 \cdot t \equiv 1 \pmod 5 && \mid \cdot 2 \\
\iff\ & 6 \cdot t \equiv 2 \pmod 5 \\
\iff\ & t \equiv 2 \pmod 5
\end{aligned}$$

Das bedeutet $t = 2 + 5 \cdot v$.
Daraus folgt nun $x = 2 + 3 \cdot t = 2 + 3 \cdot (2 + 5 \cdot v) = 8 + 15 \cdot v$. Nun wird erneut eingesetzt:

$$\begin{aligned}
& x \equiv 2 \pmod 7 \\
\iff\ & 8 + 15 \cdot v \equiv 2 \pmod 7 \\
\iff\ & 1 + v \equiv 2 \pmod 7 && \mid -1 \\
\iff\ & v \equiv 1 \pmod 7
\end{aligned}$$

Das bedeutet $v = 1 + 7 \cdot w$. Es folgt schlussendlich

$$x = 8 + 15 \cdot v = 8 + 15 \cdot (1 + 7 \cdot w) = 23 + 105 \cdot w$$

was äquivalent zu $x \equiv 23 \pmod{105}$ ist.

Bemerkung. Der Chinesische Restsatz kann auch verwendet werden um lineare Kongruenzgleichungen modulo großer Zahlen zu lösen. Denn wie im späteren Verlauf der Arbeit für $n = 2$ gezeigt wird (Satz 4.1), gilt:

$x^n \equiv a \pmod m$ ist lösbar $\iff x^n \equiv a \pmod{p_i^{\alpha_i}}$ ist lösbar für $1 \leq i \leq k$.
Diese Erkenntnis kann verwendet werden um die Kongruenz modulo einer großen Zahl mittels Primfaktorzerlegung in ein System von simultanen Kongruenzen mit deutlich kleineren Moduli zu zerlegen. Anschließend kann das System von linearen Kongruenzen mithilfe des chinesischen Restsatzes wie im oben angeführten Beispiel gelöst werden.

Beispiel. Die Kongruenzgleichung $883 \cdot x \equiv -103 \pmod{2275}$ kann gelöst werden, in dem der Chinesische Restsatz auf die Kongruenzen $883 \cdot x \equiv -103 \pmod{25}$, $883 \cdot x \equiv -103 \pmod 7$ und $883 \cdot x \equiv -103 \pmod{13}$ angewendet wird. Dazu

werden die Kongruenzen zuerst vereinfacht:

$$\begin{aligned} 883 \cdot x \equiv -103 \pmod{25} &\Longrightarrow \quad 8 \cdot x \equiv -3 \pmod{25} && \mid \cdot 3 \\ &\iff \quad 24 \cdot x \equiv -9 \pmod{25} \\ &\iff \quad (-1) \cdot x \equiv -9 \pmod{25} \\ &\iff \quad x \equiv 9 \pmod{25} \end{aligned}$$

$$883 \cdot x \equiv -103 \pmod{7} \iff x \equiv -5 \pmod{7}$$

$$\begin{aligned} 883 \cdot x \equiv -103 \pmod{13} &\iff \quad 12 \cdot x \equiv 1 \pmod{13} \\ &\iff \quad (-1) \cdot x \equiv 1 \pmod{13} \\ &\iff \quad x \equiv -1 \pmod{13} \end{aligned}$$

Die Kongruenzen haben jetzt die Form $x \equiv a \pmod{m}$ für $a \in \mathbb{Z}, m \in \mathbb{N}$. Daher kann die simultane Kongruenz in ihrer vereinfachten Darstellung nun mithilfe des chinesischen Restsatzes (wie im vorherigen Beispiel) gelöst werden.

3.2 Restklassen

Die vorhergehende Kapitel haben bereits einige Erkenntnisse über Kongruenzen sowie lineare Kongruenzgleichungen geliefert. Für die weitere Auseinandersetzung wird es zudem wichtig sein, einen genaueren Blick auf die Äquivalenzrelation der Kongruenz und die dabei entstehenden Restklassen zu werfen.

Definition. Es sei $m \in \mathbb{N}, m \geq 2$. Die Äquivalenzklassen der Äquivalenzrelation der Kongruenz modulo m werden Restklassen modulo m genannt.

Satz 3.5. *Es sei $a \in \mathbb{Z}$ und $m \in \mathbb{N}, m \geq 2$.*

i) Die Restklasse von a modulo m wird mit $\overline{a}$ bezeichnet und enthält alle ganzen Zahlen, die bei der Division durch m denselben Rest wie a liefern. Formal bedeutet dies:
$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$ bzw. $\overline{a} = \{x \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : x = q \cdot m + a\}$ bzw. $\overline{a} = a + m \cdot \mathbb{Z}$

ii) Die Anzahl der Äquivalenzklassen (=Restklassen), in die $\mathbb{Z}$ durch die Kongruenz modulo m zerfällt, beträgt genau m.

Beweis. i) Die Aussage folgt sofort aus der Definition der Kongruenz modulo m und der Definition der Restklassen.

ii) Wird $a \in \mathbb{Z}$ durch m dividiert, gibt es genau m mögliche Reste: $0, 1, \ldots, m-1$. Jeder dieser möglichen Reste ist Repräsentant einer eigenen Restklasse. Insgesamt gibt es daher m disjunkte Restklassen. □

Beispiel. Betrachtet man die Kongruenz modulo 4, so zerfällt $\mathbb{Z}$ in die vier Restklassen $\overline{0}, \overline{1}, \overline{2}, \overline{3}$. Diese Restklassen bestehen jeweils aus allen Zahlen, die bei der Division durch 4 den Rest 0 bzw. 1 bzw. 2 oder 3 haben.

$$\overline{0} = \{0 + 4 \cdot k | k \in \mathbb{Z}\} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$\overline{1} = \{1 + 4 \cdot k | k \in \mathbb{Z}\} = \{\ldots, -7, -3, 1, 5, 9 \ldots\}$$
$$\overline{2} = \{2 + 4 \cdot k | k \in \mathbb{Z}\} = \{\ldots, -6, -2, 2, 6, 10 \ldots\}$$
$$\overline{3} = \{3 + 4 \cdot k | k \in \mathbb{Z}\} = \{\ldots, -5, -1, 3, 7, 11 \ldots\}$$

Bemerkung. Ist eine Menge gegeben, die von jeder der Äquivalenzklassen einer Äquivalenzrelation genau ein Element enthält, so spricht man von einem vollständigen Repräsentantensystem. Die Menge $\{0, 1, \ldots, m-1\}$ stellt demnach ein vollständiges Repräsentantensystem der Äquivalenzklassen (=Restklassen) der Kongruenz modulo m dar, denn die Repräsentanten verkörpern alle möglichen Reste, die bei der Division durch m entstehen können. Die Mengendarstellung des Restsystems modulo m ist jedoch nicht eindeutig, da beispielsweise auch die Menge $\{m, m+1, \ldots, m+m-1\}$ aus jeder Restklasse einen Repräsentanten enthält und somit ein vollständiges Repräsentantensystem bildet.

Definition. Die Addition und die Multiplikation von Restklassen sind folgendermaßen definiert:
Addition: $\overline{a} + \overline{b} = \overline{a+b}$ bzw. $(a + m \cdot \mathbb{Z}) + (b + m \cdot \mathbb{Z}) = (a + b) + m \cdot \mathbb{Z}$
Multiplikation: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ bzw. $(a + m \cdot \mathbb{Z}) \cdot (b + m \cdot \mathbb{Z}) = a \cdot b + m \cdot \mathbb{Z}$

Definition (Restklassenring)**.** Es sei $m \in \mathbb{N}, m \geq 2$. Die Restklassen, die durch die Kongruenz modulo m entstehen, bilden zusammen mit diesen beiden Verknüpfungen den Restklassenring modulo m. Der Restklassenring wird kurz mit $\mathbb{Z}_m$ bezeichnet.
Es gilt: $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ wobei $\overline{a} = \{a + m \cdot z | z \in \mathbb{Z}\}$ für $0 \leq a \leq m-1$.

Satz 3.6. $(\mathbb{Z}_m, +, \cdot)$ *ist ein kommutativer Ring mit Eins. Daher gelten folgende Eigenschaften:*

- $(\mathbb{Z}_m, +)$ *ist eine abelsche Gruppe*
- $(\mathbb{Z}_m, \cdot)$ *ist eine Halbgruppe*
- *die Distributivgesetze sind gültig*

- $(\mathbb{Z}_m, \cdot)$ *besitzt das Einselement* $\overline{1}$

Beweis. Die Gültigkeit des Assoziativgesetzes und des Kommutativgesetzes sowie die Existenz des neutralen Elements $\overline{0}$ (Nullelement) und die Existenz der inversen Elemente für $(\mathbb{Z}_m, +)$ folgen sofort aus den Rechenregeln für $\mathbb{Z}$. Ebenso kann auch die Assoziativität der multiplikativen Verknüpfung sofort aus den Rechenregeln der ganzen Zahlen gefolgert werden.
Es werden daher lediglich beispielhaft die Distributivgesetze sowie die Existenz eines Einselements der multiplikativen Verknüpfung gezeigt.
Distributivgesetz:

$$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b+c} = \overline{a \cdot (b+c)} = \overline{a \cdot b + a \cdot c} = \overline{a \cdot b} + \overline{a \cdot c} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$$

Analog kann $(\overline{a} + \overline{b}) \cdot \overline{c} = \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c}$ gezeigt werden.
Einselement von $(\mathbb{Z}_m, \cdot)$: $\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}$ □

Bemerkung. Da $(\mathbb{Z}_m, \cdot)$ eine Halbgruppe ist, muss ein $\overline{a} \in \mathbb{Z}_m$ für die Verknüpfung $\cdot$ nicht invertierbar sein. Existiert zwei Restklassen $\overline{a}, \overline{b} \in \mathbb{Z}_m$ mit $\overline{a} \cdot \overline{b} = \overline{1}$, so ist dies also eine besondere Eigenschaft.

Definition. Es sei $m \in \mathbb{N}, m \geq 2$. Eine Restklasse $\overline{a} \in \mathbb{Z}_m$ heißt Einheit oder invertierbar, wenn es eine Restklasse $\overline{b} \in \mathbb{Z}_m$ gibt, sodass $\overline{a} \cdot \overline{b} = \overline{1}$ in $\mathbb{Z}_m$. Die Menge der Einheiten von $\mathbb{Z}_m$ wird mit $\mathbb{Z}_m^*$ bezeichnet.

Beispiel. Ausgangspunkt ist der Restklassenring $\mathbb{Z}_6^*$. Zunächst wird eine Tabelle angefertigt, die Informationen über die Ergebnisse der Multiplikation von Restklassen liefert.

$\cdot$	$\overline{\mathbf{0}}$	$\overline{\mathbf{1}}$	$\overline{\mathbf{2}}$	$\overline{\mathbf{3}}$	$\overline{\mathbf{4}}$	$\overline{\mathbf{5}}$
$\overline{\mathbf{0}}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{\mathbf{1}}$	$\overline{0}$	$\overline{\mathbf{1}}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{\mathbf{2}}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{\mathbf{3}}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{\mathbf{4}}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{\mathbf{5}}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{\mathbf{1}}$

Daraus folgt, dass $\mathbb{Z}_6^* = \{\overline{1}, \overline{5}\}$, weil $\overline{1} \cdot \overline{1} = \overline{1}$ und $\overline{5} \cdot \overline{5} = \overline{1}$.

Lemma 3.2. $(\mathbb{Z}_m^*, \cdot)$ *ist eine abelsche Gruppe mit Einselement* $\overline{1}$.

Beweis. Seien $\overline{a}, \overline{b} \in \mathbb{Z}_m^*$. Es wird zunächst gezeigt, dass $\overline{a} \cdot \overline{b} \in \mathbb{Z}_m^*$:
Da $\overline{a}$ und $\overline{b}$ invertierbar sind, existieren $\overline{c}$ und $\overline{d} \in \mathbb{Z}_m$, sodass $\overline{a} \cdot \overline{c} = \overline{1}$ und $\overline{b} \cdot \overline{d} = \overline{1}$. Daher folgt:

$$(\overline{a} \cdot \overline{c}) \cdot \overline{b} \cdot \overline{d} = (\overline{a} \cdot \overline{b}) \cdot \overline{c} \cdot \overline{d} = \overline{1} \cdot \overline{1} = \overline{1}$$

Demnach ist $\overline{a} \cdot \overline{b} \in \mathbb{Z}_m^*$.
Weiters gilt: $\overline{a} \in \mathbb{Z}_m^* \iff \overline{a} \cdot \overline{b} = \overline{1} \iff \overline{b} \in \mathbb{Z}_m^*$. Damit ist gezeigt, dass zum einen die multiplikative Verknüpfung von zwei Einheiten wieder einen Einheit bildet und zum anderen das Inverse einer Einheit wieder eine Einheit ist. □

Satz 3.7. $\overline{a} \in \mathbb{Z}_m^* \iff \mathrm{ggT}(a, m) = 1$

Beweis. $\Longrightarrow$ Es sei $\overline{a}$ eine Einheit in $\mathbb{Z}_m$. Dann gibt es eine Restklasse $\overline{x} \in \mathbb{Z}_m$, sodass $\overline{a} \cdot \overline{x} = \overline{1} \iff \overline{a \cdot x} = \overline{1}$. Dies ist äquivalent zu $a \cdot x \equiv 1 \pmod{m}$. Daher gilt $a \cdot x = 1 + y \cdot m, \iff a \cdot x - y \cdot m = 1$ für $y \in \mathbb{Z}$. Aus Lemma 2.1 folgt somit die Aussage.
$\Longleftarrow$ Es sei $\mathrm{ggT}(a, m) = 1$. Dann existieren $x, y \in \mathbb{Z}$ sodass $a \cdot x + m \cdot y = 1$. Man erhält daher $a \cdot x \equiv 1 \pmod{m}$. Schreibt man dieses Zusammenhang mithilfe von Restklassen an, so erhält man $\overline{a} \cdot \overline{x} = \overline{a \cdot x} = \overline{1}$. Somit ist $\overline{a}$ Einheit in $\mathbb{Z}_m$ mit Inversen $\overline{x}$. □

Bemerkung. $\mathbb{Z}_m^*$ ist die prime Restklassengruppe von $\mathbb{Z}_m$ und enthält daher die zu m teilerfremden Elemente der Menge $\{\overline{1}, \overline{2}, \ldots, \overline{m-1}\}$.

Bevor sich der weitere Abschnitt des Kapitels vorrangig mit der Eulerschen φ-Funktion und daraus resultierenden Sätzen beschäftigt, wird an dieser Stelle der Satz von Wilson formuliert und bewiesen.[2] Der Satz von Wilson ist ein Primzahlentest und wird später in den Beweise der Sätze über quadratische Reste eine wichtige Rolle spielen.

Satz 3.8 (Satz von Wilson)**.** *Sei $p \in \mathbb{N}$, $p > 1$. Dann gilt:*
p ist eine Primzahl $\iff (p-1)! \equiv -1 \pmod{p}$

Beispiel. Für $p = 7$ gilt:

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = \overbrace{1}^{\equiv 1\,(7)} \cdot \underbrace{2 \cdot 4}_{=8 \equiv 1\,(7)} \overbrace{3 \cdot 5}^{=15 \equiv 1\,(7)} \cdot \underbrace{6}_{\equiv -1\,(7)} \equiv -1 \pmod{7}$$

Beweis. $\Longrightarrow$ Es sei $p \in \mathbb{P}$. Für $p = 2$ und $p = 3$ ist die Aussage offensichtlich erfüllt. Es sei daher $p \geq 5$. Es werden nun die Elemente des Restklassensystems $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ betrachtet. Da p eine Primzahl ist, sind alle Elemente von $\mathbb{Z}_p$ außer $\overline{0}$ auch Element von $\mathbb{Z}_p^*$. Man betrachtet nun Paare von Restklassen $\overline{a}, \overline{b} \in \mathbb{Z}_p^*$ mit $a \cdot b \equiv 1 \pmod{p}$. Dazu überlegt man zuerst, für welche $\overline{a} \in \mathbb{Z}_p^*$ $\overline{a} \cdot \overline{a} = \overline{1} \iff a^2 \equiv 1 \pmod{p} \iff p \mid (a^2 - 1)$ gilt, denn dann wurden bereits alle selbstinversen Elemente der Menge $\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ gefunden.
Es gilt: $p \mid (a^2 - 1) \iff p \mid (a-1) \cdot (a+1)$ und nach Satz 2.8 ii) folgt, entweder $p \mid (a-1) \iff a \equiv 1 \pmod{p}$ oder $p \mid (a+1) \iff a \equiv -1 \equiv p-1 \pmod{p}$. Daher sind nur die beiden Restklassen $\overline{1}$ und $\overline{p-1}$ selbstinvers.
Die restlichen Restklassen der Menge $\{\overline{2}, \ldots, \overline{p-2}\}$ bilden also $\frac{p-3}{2}$ Paare, für

die $\overline{a} \cdot \overline{b} = \overline{1} \Longleftrightarrow a \cdot b \equiv 1 \pmod{m}$ gilt, wobei $\overline{a} \neq \overline{b}$ und $\overline{a}, \overline{b} \in \{\overline{2}, \ldots, \overline{p-2}\}$. Ordnet man die $p-3$ Reste der Menge $\{\overline{2}, \ldots, \overline{p-2}\}$ also so in Paaren an, dass deren Produkt immer kongruent 1 modulo p ist, erhält man:

$$\begin{aligned} & 2 \cdot 3 \cdot \ldots \cdot (p-3) \cdot (p-2) \equiv 1 \,(\mathrm{mod}\, p) & \\ \Longleftrightarrow \quad & (p-2)! \equiv 1 \,(\mathrm{mod}\, p) & \mid \cdot(p-1) \\ \Longleftrightarrow \quad & (p-1)! \equiv 1 \cdot (p-1) \equiv -1 \,(\mathrm{mod}\, p) & \end{aligned}$$

$\Longleftarrow$ Um die andere Implikation zu zeigen, wird nun angenommen, dass $p \geq 2$ keine Primzahl ist. Dann gibt es $a, b \in \mathbb{N}$, $1 < a, b < p$ sodass $p = a \cdot b$. Gilt $a \neq b$, dann enthält das Produkt $(p-1)!$ sowohl a als auch b als Faktoren und es folgt:

$$(p-1)! = a \cdot b \cdot \ldots = p \cdot \ldots \equiv 0 \pmod{p}$$

Gilt jedoch $a = b$, kann ein Trick verwendet werden, um $(p-1)! \not\equiv -1 \pmod{p}$ zu zeigen [8]:

$$p = a \cdot a \Longleftrightarrow -p = a \cdot (-a) \equiv a \cdot (p-a) \pmod{p}$$

Für $a \neq p-a$ kann analog zum Fall $a \neq b$ argumentiert werden, denn das Produkt $(p-1)!$ enthält sowohl a als auch $p-a$ als Faktoren. Es bleibt also nur noch der Fall $p = a \cdot a = a^2$ und $a = p - a \Longleftrightarrow p = 2 \cdot a$ zu klären. Die einzige Zahl, die $p = a^2 = 2 \cdot a$ erfüllt ist jedoch 4, sodass nun leicht nachgerechnet werden kann.

$$(4-1)! = 3! = 1 \cdot 2 \cdot 3 = 6 \equiv 2 \pmod{4}$$

Ist p keine Primzahl, dann ist demnach $(p-1)! \not\equiv -1 \pmod{p}$. □

Definition (Eulersche φ-Funktion)**.** Die Abbildung $\varphi : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N} \setminus \{0\}$, bei der $\varphi(m)$ die Anzahl der zu m teilerfremden natürlichen Zahlen kleiner als m angibt, heißt Eulersche φ-Funktion.
Formal: $\varphi(m) = |\{k \in \mathbb{N} : 0 \leq k \leq m-1, \mathrm{ggT}(k, m) = 1\}|$. Für $m \geq 2$ ist $\varphi(m) = |\mathbb{Z}_m^*|$ und $\varphi(1) = 1$.

Definition. Es sei $m \in \mathbb{N}, m \geq 2$. Dann heißt $\varphi(m) = |\mathbb{Z}_m^*|$ Ordnung von $\mathbb{Z}_m^*$.

Lemma 3.3. *Es sei $p \in \mathbb{P}$ und $\alpha \in \mathbb{N} \setminus \{0\}$. Dann gilt:*

i) $\varphi(p) = p - 1$

ii) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \cdot (1 - \frac{1}{p})$.

Beweis. i) Die Primzahl p besitzt in $\mathbb{N}$ nur die trivialen Teiler 1 und p. Für alle

$p-1$ Zahlen $a < p \in \mathbb{N} \setminus \{0\}$ ist daher $\text{ggT}(a,p) = 1$ und es folgt:

$$\varphi(p) = |\mathbb{Z}_p^*| = |\{a \in \mathbb{N} : 1 \leq a \leq p-1, \text{ggT}(a,p) = 1\}| = p-1$$

ii) Von den p^α Zahlen $1, 2, \ldots, p^\alpha$ sind genau die Vielfachen von p nicht teilerfremd zu p^α. Das bedeutet die Zahlen $\underbrace{1 \cdot p, 2 \cdot p, \ldots, (p^{\alpha-1}-1) \cdot p, p^{\alpha-1} \cdot p}_{p^{\alpha-1}}$ haben mit p^α den größten gemeinsamen Teiler p. Daraus folgt:

$$\varphi(p^\alpha) = |\{k \in \mathbb{N} : 1 \leq k \leq p^{\alpha-1}, \text{ggT}(k, p^{\alpha-1}) = 1\}| = p^\alpha - p^{\alpha-1} = p^\alpha \cdot \left(1 - \frac{1}{p}\right)$$

□

Korollar 3.4. *Es sein $m, n \in \mathbb{N} \setminus \{0\}$ und $\text{ggT}(m,n) = 1$.*
Dann gilt $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$. Mithilfe der Primfaktorzerlegung von natürlichen Zahlen folgt daraus:
Sei $m \in \mathbb{N}$ mit der Primfaktorzerlegung $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, dann gilt:

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) \\ &= \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}) \\ &= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdot \ldots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1})\end{aligned}$$

Beweis. Ohne Beweis. □

Korollar 3.5 (Satz von Euler)**.** *Es seien $m, a \in \mathbb{Z}$, $m \geq 2$ mit $\text{ggT}(a,m) = 1$, dh. $\overline{a} \in \mathbb{Z}_m^*$. Dann gilt: $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

Es gibt eine Vielzahl an verschiedenen Möglichkeiten den Satz von Euler zu beweisen. In der Fachliteratur sind häufig Beweise vorzufinden, die sich auf die Erkenntnisse der Gruppentheorie oder den Binomialkoeffizienten beziehen. Da diese Art von Beweisen jedoch mit einem hohen Aufwand an mathematischer Vorarbeit verbunden ist, wird in dieser Arbeit der elementarere Beweis von Ivory und Dirichlet angeführt.[10]

Beweis. Zur Vereinfachung der Darstellungen sei $n := \varphi(m)$.
Dann existieren n verschiedene Zahlen $x_1, x_2, \ldots, x_n$, die teilerfremd zu m sind und aus der Menge $\{1, 2, \ldots, m-1\}$ stammen. Nun werden ihre Produkte mit $a \in \mathbb{Z}$ gebildet: $x_1 \cdot a, x_2 \cdot a, \ldots, x_n \cdot a$
Führt man nun die Division mit Rest durch m durch, erhält man folgende n Gleichungen:

$$x_j \cdot a = q_j \cdot m + r_j \quad \text{mit } 0 \leq r_j < m, \quad j = 1, 2, \ldots, n$$

Dabei gilt $\text{ggT}(x_j, m) = 1 \; \forall j = 1, 2, \ldots, n$, da die x_j laut Voraussetzung teilerfremd zu m sind und laut Annahme gilt auch $\text{ggT}(a, m) = 1$. Daraus ergibt sich:

$$\text{ggT}(r_j, m) = 1 \quad \forall j = 1, 2, \ldots, n$$

Nun wird die Behauptung, dass alle Reste $r_1, r_2, \ldots, r_n$ paarweise verschieden sind, überprüft:
Aus $r_k = r_l$ folgt $(x_k - x_l) \cdot a = (q_k - q_l) \cdot m \equiv 0 \pmod{m}$. Und damit ergibt sich wegen $\text{ggT}(a, m) = 1$ und der Kürzungsregel für Kongruenzen (Lemma 3.1) $x_k - x_l \equiv 0 \pmod{m}$.
Weil $1 \leq x_k < m$ und $1 \leq x_l < m$ gilt auch $|x_k - x_l| < m$. Daraus folgt gemeinsam mit $x_k - x_l \equiv 0 \pmod{m} \iff m \mid (x_k - x_l)$, dass $x_k = x_l$ und somit $k = l$, da $x_1, x_2, \ldots, x_n$ paarweise verschieden sind und nur bei $k = l$ Gleichheit gelten kann.
Somit ergibt sich:

$$x_1 \cdot a \equiv r_1 \pmod{m}, x_2 \cdot a \equiv r_2 \pmod{m}, \ldots, x_n \cdot a \equiv r_n \pmod{m} \quad (3.1)$$

wobei eben gezeigt wurde, dass die Mengen $\{x_1, x_2, \ldots, x_n\}$ und $\{r_1, r_2, \ldots, r_n\}$ übereinstimmen, da sie jeweils alle zu m teilerfremden Zahlen kleiner als m enthalten.
Im letzten Schritt des Beweises setzt man nun $c := \prod_{j=1}^{n} x_j = \prod_{j=1}^{n} r_j$. Multipliziert man alle Kongruenzen aus 3.1 miteinander erhält man unter Anwendung der Rechenregeln für Kongruenzen (Lemma 3.1) $c \cdot a^n \equiv c \pmod{m}$. Da $\text{ggT}(x_j, m) = 1 \; \forall j = 1, 2, \ldots, n$ und somit auch $\text{ggT}(c, m) = 1$ gilt, liefert die Kürzungsregel für Kongruenzen schließlich die zu beweisende Aussage:

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

□

Der kleine Satz von Fermat stellt einen Sonderfall des Satzes von Euler dar und kann wiefolgt formuliert werden.

Korollar 3.6 (Kleiner Satz von Fermat)**.** *Es sei $p \in \mathbb{P}$ und $a \in \mathbb{Z}$, sodass $p \nmid a$. Dann gilt: $a^{p-1} \equiv 1 \pmod{p}$ beziehungsweise $a^p \equiv a \pmod{p}$ für jedes $a \in \mathbb{Z}$.*

Beweis. Es wurde bereits gezeigt, dass $\varphi(p) = p - 1$. Daher folgt die Aussage sofort durch das Einsetzen dieser Tatsache in die Kongruenz des Satzes von Euler. □

Der Satz von Euler und der kleine Satz von Fermat sind hilfreich, um

Berechnungen mit Kongruenzen durchzuführen. Ein konkretes Anwendungsfeld wird anhand des folgenden Beispiels demonstriert.

Beispiel. Es soll 2^{10000} modulo 67 berechnet werden.
Da die Zahl 67 eine Primzahl ist, gilt: $2^{66} \equiv 1 \pmod{67}$. Nun kann der Exponent durch Division mit Rest geeignet zerlegt werden:

$$\begin{aligned} 10000 &= 151 \cdot 66 + 34 \\ \Longrightarrow 2^{10000} &= (2^{66})^{151} \cdot 2^{34} \\ \Longleftrightarrow 2^{10000} &\equiv 2^{34} \pmod{67} \end{aligned}$$

Nun wird die Rechte Seite der Kongruenzgleichung noch weiter zerlegt:

$$\begin{aligned} 2^{34} &= (2^6)^5 \cdot 2^4 \equiv (-3)^5 \cdot 16 \pmod{67} \\ 2^{34} &\equiv (-3) \cdot (-3)^4 \cdot 16 \pmod{67} \\ 2^{34} &\equiv (-3) \cdot 81 \cdot 16 \pmod{67} \\ 2^{34} &\equiv (-3) \cdot 14 \cdot 16 \pmod{67} \\ 2^{34} &\equiv (-42) \cdot 16 \pmod{67} \\ 2^{34} &\equiv 25 \cdot 16 \pmod{67} \\ 2^{34} &\equiv 400 = 6 \cdot 67 - 2 \pmod{67} \\ 2^{34} &\equiv -2 \pmod{67} \end{aligned}$$

Somit ergibt sich schließlich $2^{10000} \equiv -2 \pmod{67}$.

4 Quadratische Kongruenzen

Die bisherige Auseinandersetzung mit Kongruenzen und Kongruenzgleichungen hat sich ausschließlich mit linearen Kongruenzen befasst. Da die Ziele dieser Arbeit jedoch die Formulierung des quadratischen Reziprozitätsgesetzes sowie die Erläuterung von dessen Beweisen sind, ist die Betrachtung von quadratischen Kongruenzen unumgänglich. Aufgrund dessen werden im nächsten Kapitel die quadratischen Kongruenzen $a \cdot x^2 + b \cdot x + c \equiv 0 \pmod{m}$ für $a, m \in \mathbb{N} \setminus \{0\}, b, c, x \in \mathbb{Z}, m \geq 2$ näher beleuchtet. Die Ausarbeitung orientiert sich dabei vorrangig den Werken von Remmert und Ullrich [10], Pieper [6], Fulemk [7] und Schüler [2].

4.1 Quadratische Kongruenz mod p

Das erste Ziel ist es, quadratische Kongruenzgleichungen der allgemeinen Form $a \cdot x^2 + b \cdot x + c \equiv 0 \pmod{m}$ für $a, m \in \mathbb{N} \setminus \{0\}, b, c, x \in \mathbb{Z}, m \geq 2$ bezüglich ihrer

Lösbarkeit zu untersuchen. Dazu wird das Problem durch wenige Schritte zuerst auf eine einfacher Form zurückgeführt. Die Darlegung dieser Schritte basiert dabei auf den Texten von Remmert und Ullrich (2008) und dem Vorlesungsskript der VO Zahlentheorie von Markus Fulmek (Sommersemester 2019). [10], [7]

$$\begin{aligned}
& a \cdot x^2 + b \cdot x + c \equiv 0 \pmod{m} \\
\iff\ & m \mid (a \cdot x^2 + b \cdot x + c) \\
\iff\ & 4 \cdot a \cdot m \mid (4 \cdot a^2 \cdot x^2 + 4 \cdot a \cdot b \cdot x + 4 \cdot a \cdot c) \\
\iff\ & 4 \cdot a \cdot m \mid ((2 \cdot a \cdot x + b)^2 + 4 \cdot a \cdot c - b^2) \\
\iff\ & (2 \cdot a \cdot x + b)^2 \equiv b^2 - 4 \cdot a \cdot c \pmod{4 \cdot a \cdot m}
\end{aligned}$$

Die Kongruenzgleichung $a \cdot x^2 + b \cdot x + c \equiv 0 \pmod{m}$ ist also genau dann lösbar, wenn das Gleichungssystem

$$\begin{aligned}
y^2 &\equiv b^2 - 4 \cdot a \cdot c \pmod{4 \cdot a \cdot m} \\
y &\equiv 2 \cdot a \cdot x + b \pmod{4 \cdot a \cdot m}
\end{aligned}$$

lösbar ist. Da es sich bei der zweiten Gleichung dieses Gleichungssystems um eine lineare Kongruenz handelt, kann durch die Anwendung des Satzes 3.3 leicht festgestellt werden, ob die lineare Kongruenzgleichung lösbar ist. Weitaus komplexer ist jedoch die Entscheidung über die Lösbarkeit der ersten Gleichung des Gleichungssystem, denn diese ist vom Typ $x^2 \equiv a \pmod{m}$ für $m \in \mathbb{N}$, $m \geq 2$. Es handelt sich bei dieser Kongruenzgleichung also um eine quadratische Kongruenz.
Um die Entscheidung über die Lösbarkeit einer quadratischen Kongruenz der Form $x^2 \equiv a \pmod{m}$ weiter zu vereinfachen, wird die Kongruenz modulo einer beliebigen natürlichen Zahl m nun schrittweise auf eine Kongruenz modulo $p \in \mathbb{P}$ zurückgeführt:

- Im ersten Schritt wird die Kongruenz modulo einer natürlichen Zahl m auf eine Kongruenz modulo einer Primzahlpotenz zurückgeführt.

  Satz 4.1. *Es sei $m \in \mathbb{N}$ mit $m \geq 2$ mit der Primfaktorzerlegung*

  $$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

  Dann gilt $x^2 \equiv a \pmod{m}$ ist lösbar $\iff$ $x^2 \equiv a \pmod{p_i^{\alpha_i}}$ ist lösbar für $1 \leq i \leq k$.

Beweis. Zunächst wird der Modul m näher betrachtet. Laut dem Fundamentalsatz der Arithmetik (2.9) besitzt m eine Primfaktorzerlegung:

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

$\Longrightarrow$ Laut Voraussetzung gilt $p_i^{\alpha_i} \mid m \ \forall i$ und $m \mid (x^2 - a)$. Daraus folgt wegen der Teilbarkeitsregeln (2.1) $p_i^{\alpha_i} \mid (x^2 - a) \ \forall i$, was äquivalent zu $x^2 \equiv a \pmod{p_i^{\alpha_i}}$ ist.
$\Longleftarrow$ Diese Implikation der Aussage folgt durch Induktion:
Es gilt $\mathrm{ggT}(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_{l-1}^{\alpha_{l-1}}, p_l^{\alpha_l}) = 1$.
Es sei weiters bereits gezeigt, dass $x^2 \equiv a \pmod{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_{l-1}^{\alpha_{l-1}}}$. Dann gilt wegen $\mathrm{ggT}(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_{l-1}^{\alpha_{l-1}}, p_l^{\alpha_l}) = 1$:

$$\mathrm{kgV}(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_{l-1}^{\alpha_{l-1}}, p_l^{\alpha_l}) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_{l-1}^{\alpha_{l-1}} \cdot p_l^{\alpha_l}$$

Aufgrund der Rechenregeln für Kongruenzen (Lemma 3.1 vi)) folgt damit sofort $x^2 \equiv a \pmod{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_{l-1}^{\alpha_{l-1}} \cdot p_l^{\alpha_l}}$.
Für $l = k$ folgt dann $x^2 \equiv a \pmod{m}$. □

Es ist daher ausreichend quadratische Kongruenzgleichungen der Form $x^2 \equiv a \pmod{p^\alpha}$ für $p \in \mathbb{P}$ und $\alpha \in \mathbb{N} \setminus \{0\}$ zu betrachten.

- Zusätzlich kann eine weitere Spezifizierung vorgenommen werden. Denn wie nun verdeutlicht wird, genügt es Kongruenzen der Form $x^2 \equiv a \pmod{p^\alpha}$ für $p \in \mathbb{P}, \alpha \in \mathbb{N} \setminus \{0\}$ zu betrachten, für die zusätzlich $\mathrm{ggT}(p, a) = 1$ gilt.

  Satz 4.2. *Es sei $p \in \mathbb{P}, \alpha \in \mathbb{N} \setminus \{0\}$ und $a = p^\beta \cdot b$ mit $\beta \in \mathbb{N} \setminus \{0\}$, dh. $\mathrm{ggT}(p, a) \neq 1$. Weiters sei $\mathrm{ggT}(p, b) = 1$. Dann gilt:*

  i) Für $\beta \geq \alpha$ ist $x^2 \equiv p^\beta \cdot b \pmod{p^\alpha}$ lösbar.

  ii) Für $\beta < \alpha$ ist $x^2 \equiv p^\beta \cdot b \pmod{p^\alpha}$ genau dann lösbar, wenn $2 \mid \beta$ und die Kongruenz $y^2 \equiv b \pmod{p^{\alpha-\beta}}$ lösbar ist.

  Beweis. i) Aus $\beta \geq \alpha$ folgt, dass p^β ein Vielfaches von p^α ist was wiederum bedeutet, dass $p^\beta \cdot b \equiv 0 \pmod{p^\alpha}$.
  Nun werden die beiden Implikationen der zweiten Aussage ii) bewiesen:
  $\Longrightarrow$ Es sei $x_0 \in \mathbb{Z}$ eine Lösung der Kongruenz $x^2 \equiv p^\beta \cdot b \pmod{p^\alpha}$. Das Quadrat von x_0 kann als $x_0^2 = p^\gamma \cdot y_0^2$ mit $\gamma \in \mathbb{N}$ und $\mathrm{ggT}(p, y_0^2) = 1$ geschrieben werden und offenbar gilt dann $2 \mid \gamma$.
  Wegen $p^\beta \mid p^\alpha$ und $p^\alpha \mid (x_0^2 - p^\beta \cdot b)$ folgt aus Lemma 2.1 xi)

  $$p^\beta \mid x_0^2 \Longleftrightarrow p^\beta \mid p^\gamma \cdot y_0^2$$

und somit $\gamma \geq \beta$, weil $p \nmid y_0^2$ und sonst die Teilbarkeit nicht gilt.
Mit einem indirekten Beweis wird nun gezeigt, dass nicht $\gamma > \beta$ gelten kann:
Angenommen es gilt $p^{\beta+1} \mid p^\alpha$ (weil $\beta + 1 \leq \alpha$) und zusätzlich

$$p^\alpha \mid (x_0^2 - p^\beta \cdot b) \iff p^\alpha \mid (p^\gamma \cdot y_0^2 - p^\beta \cdot b) \iff p^\alpha \mid p^\beta \cdot (p^{\gamma-\beta} \cdot y_0^2 - b)$$

Mit den Teilbarkeitsregeln vii) und ix) folgt sofort

$$p^{\beta+1} \mid p^\beta \cdot (p^{\gamma-\beta} \cdot y_0^2 - b) \iff p^\beta \cdot p \mid p^\beta \cdot (p^{\gamma-\beta} \cdot y_0^2 - b) \iff p \mid (p^{\gamma-\beta} \cdot y_0^2 - b)$$

woraus wiederum $p \mid b$ folgt. Dies stellt einen Widerspruch zur Annahme $\mathrm{ggT}(p, b) = 1$ dar.
Also gilt $\gamma = \beta$ und daher folgt aus der eben gewonnen Erkenntnis $2 \mid \gamma$ nun auch $2 \mid \beta$ und ebenso gilt $p^\alpha \mid (x_0^2 - p^\beta \cdot b) \iff p^\alpha \mid p^\beta \cdot y_0^2 - p^\beta \cdot b$ was wiederum gleichbedeutend zu $p^{\alpha-\beta} \mid (y_0^2 - b)$ ist. Formuliert man diese nun als Kongruenz, so erhält man die Aussage.
$\Longleftarrow$ Es sei $\beta = 2 \cdot \delta$.
Weiters sei $y_0 \in \mathbb{Z}$ eine Lösung der Kongruenz $y^2 \equiv b \pmod{p^{\alpha-\beta}}$. Die Aussage kann durch mehrere Umformungen gezeigt werden:

$$\begin{aligned}
& y_0^2 \equiv b \pmod{p^{\alpha-\beta}} \\
\iff\ & p^{\alpha-\beta} \mid (y_0^2 - b) && \mid \cdot p^\beta \\
\iff\ & p^\alpha \mid (y_0^2 \cdot p^\beta - b \cdot p^\beta) \\
\iff\ & y_0^2 \cdot p^\beta \equiv b \cdot p^\beta \pmod{p^\alpha} \\
\iff\ & y_0^2 \cdot p^\beta \equiv a \pmod{p^\alpha} \\
\iff\ & y_0^2 \cdot p^{2\cdot\delta} \equiv a \pmod{p^\alpha} \\
\iff\ & (y_0 \cdot p^\delta)^2 \equiv a \pmod{p^\alpha}
\end{aligned}$$

□

Um eine Aussage über die Lösbarkeit von allgemeinen quadratischen Kongruenzen treffen zu können, ist es also ausreichend, die Kongruenzen der Gestalt $x^2 \equiv a \pmod{p^\alpha}$ für $p \in \mathbb{P}, \alpha \in \mathbb{N} \setminus \{0\}$ und $\mathrm{ggT}(a, p) = 1$ zu untersuchen.

- Ist die Kongruenz $x^2 \equiv a \pmod{p^\alpha}$ lösbar, dann ist offensichtlich auch $x^2 \equiv a \pmod{p}$ lösbar, denn es gilt $p \mid p^\alpha$ und $p^\alpha \mid (x^2 - a)$ und wegen Lemma 2.1 folgt daraus $p \mid (x^2 - a) \iff x^2 \equiv a \pmod{p}$.
  Für $p > 2$ und $\mathrm{ggT}(p, a) = 1$ gilt aber auch die Umkehrung dieser Aussage:

Satz 4.3. *Es sei $p \in \mathbb{P}, p > 2$ und $\alpha \in \mathbb{N} \setminus \{0\}$. Dann gilt:*
$x^2 \equiv a \pmod{p^\alpha}$ ist lösbar $\Longrightarrow$ $x^2 \equiv a \pmod{p^{\alpha+1}}$ ist lösbar.

Beweis. Es sei x_0 eine Lösung der Kongruenz $x^2 \equiv a \pmod{p^\alpha}$. Dann ist auch $x_0 + t \cdot p^\alpha \ \forall t \in \mathbb{Z}$ eine Lösung dieser Kongruenz. Es gilt:

$$\begin{aligned}(x_0 + t \cdot p^\alpha)^2 - a &= x_0^2 + 2 \cdot x_0 \cdot t \cdot p^\alpha + t^2 \cdot p^{2\cdot\alpha} - a \\ &\equiv (x_0^2 - a) + 2 \cdot x_0 \cdot t \cdot p^\alpha \pmod{p^{\alpha+1}} \\ &\equiv p^\alpha \cdot \Big(\underbrace{\frac{x_0^2 - a}{p^\alpha}}_{\in\mathbb{Z}} + 2 \cdot x_0 \cdot t \Big) \pmod{p^{\alpha+1}}\end{aligned}$$

wobei die erste Kongruenz gilt da $2 \cdot \alpha \geq \alpha + 1 \Longrightarrow p^{2\cdot\alpha} \equiv 0 \pmod{p^{\alpha+1}}$. Um die Gültigkeit der zu beweisenden Aussage $(x_0^2 + t \cdot p^\alpha)^2 \equiv a \pmod{p^{\alpha+1}}$ zu zeigen, muss bewiesen werden, dass ein t gefunden werden kann, sodass $p \mid (\frac{x_0^2 - a}{p^\alpha} + 2 \cdot x_0 \cdot t)$, denn dann ist $\frac{x_0^2 - a}{p^\alpha} + 2 \cdot x_0 \cdot t = k \cdot p$ und es folgt $(x_0^2 + t \cdot p^\alpha)^2 - a \equiv 0 \pmod{p^{\alpha+1}}$.
Um dieses t zu finden, muss die lineare Kongruenzgleichung

$$2 \cdot x_0 \cdot t \equiv \frac{a - x_0^2}{p^\alpha} \pmod{p}$$

gelöst werden.
Da aus $p \nmid a$ sofort $p \nmid x_0$ folgt und zusätzlich $p \neq 2$ gilt, ist $\mathrm{ggT}(2 \cdot x_0, p) = 1$ und nach Satz 3.3 ist die lineare Kongruenz mit Sicherheit nach t lösbar. □

Somit konnte gezeigt werden, dass es für $p > 2$ ausreichend ist, Kongruenzen der Form $x^2 \equiv a \pmod{p}$ mit $\mathrm{ggT}(p, a) = 1$ zu betrachten, um eine Aussage über die Lösbarkeit der Kongruenz treffen zu können.
Insgesamt konnten Kongruenzgleichungen der Form

$$a \cdot x^2 + b \cdot x + c \equiv 0 \pmod{m}$$

somit in drei Schritten auf die deutlich vereinfachte Form $x^2 \equiv a \pmod{p}$, $p \in \mathbb{P}$, $p > 2$ und $\mathrm{ggT}(p, a) = 1$ reduziert werden. Daher werden in der weiterführenden Behandlung von quadratischen Kongruenzen und ihrer Lösbarkeit ausschließlich Kongruenzgleichungen der reduzierten Form behandelt.

4.2 Der Fall p=2

Nachdem nun bereits mehrere Aussagen über die Lösbarkeit von quadratischen Kongruenzen modulo einer beliebigen Zahl größer 2 getroffen wurden, ist es an der Zeit sich auch genauer mit dem Fall $p = 2$ auseinanderzusetzen.
Die einzige gerade Primzahl $p = 2$ stellt einen Sonderfall dar, da sich quadratische Kongruenzen der Form $x^2 \equiv a \pmod{2^\alpha}$ durch die gerade beschriebene Vorgehensweise nicht auf den Fall $x^2 \equiv a \pmod 2$ reduzieren lassen. Die Lösbarkeit von quadratischen Kongruenzen modulo 2^α wird daher vorweg an dieser Stelle separat betrachtet.

Satz 4.4. *Es sei $a \in \mathbb{Z}$, sodass $2 \nmid a$. Dann gilt:*

i) Die Kongruenz $x^2 \equiv a \pmod 2$ ist lösbar (dh. $\overline{x}^2 = \overline{a}$ in $\mathbb{Z}_2$)

ii) Die Kongruenz $x^2 \equiv a \pmod 4$ ist lösbar $\iff a \equiv 1 \pmod 4$

iii) Für $\alpha \in \mathbb{N}$, $\alpha \geq 3$ ist die Kongruenz $x^2 \equiv a \pmod{2^\alpha}$ lösbar $\iff a \equiv 1 \pmod 8$

Beweis. Für die ersten beiden Aussagen ist aufgrund der wenigen Restklassen das simple Überprüfen der Tatsachen ausreichend:
i) Aus $2 \nmid a$ folgt für jede Lösung x_0 der Kongruenz $2 \nmid x_0$. In $\mathbb{Z}_2$ ist $\overline{1}$ die einzige Restklasse $\overline{a}$ mit $2 \nmid a$ und es gilt $\overline{1}^2 = \overline{1}$ in $\mathbb{Z}_2$.
ii) Wieder gilt aufgrund von $2 \nmid a$ für jede Lösung x_0 der Kongruenz auch $2 \nmid x_0$. In $\mathbb{Z}_4$ gibt es nur zwei Restklassen $\overline{a}$ mit $2 \nmid a$, nämlich $\overline{1}$ und $\overline{3}$. Es gilt $\overline{1}^2 = \overline{3}^2 = \overline{1}$ in $\mathbb{Z}_4$ und daraus folgt $\overline{a} = \overline{1} \iff a \equiv 1 \pmod 4$.
iii) Um die dritte Aussage zu beweisen, wird zunächst die quadratische Kongruenz $x^2 \equiv a \pmod 8$, dh. der Fall $\alpha = 3$, betrachtet. Dazu wird die Aussage erneut durch simples Nachrechnen überprüft:
Die Repräsentanten der Restklassen $\overline{1}, \overline{3}, \overline{5}$ und $\overline{7}$ erfüllen die Voraussetzung der Teilerfremdheit mit 2 und kommen daher für die Restklasse $\overline{a}$ von a in Frage. Es gilt $\overline{1}^2 = \overline{3}^2 = \overline{5}^2 = \overline{7}^2 = \overline{1}$ in $\mathbb{Z}_8$ und daraus folgt $\overline{a} = \overline{1}$, was äquivalent zu $a \equiv 1 \pmod 8$ ist.
Für $\alpha > 3$ ist das reine Überprüfen der Aussage nicht mehr sinnvoll, weshalb die Aussage für $\alpha > 3$ nun allgemein beweisen wird.
$\Longrightarrow$ Aus $x_0^2 \equiv a \pmod{2^\alpha}$ für $\alpha > 3$ folgt, dass $x_0^2 \equiv a \pmod 8$ (siehe Schritt drei der Vereinfachung der quadratischen Kongruenz). Durch die gerade eben angestellten Überlegungen für den Fall $\alpha = 3$ ist die erste Implikation damit bereits vollständig bewiesen.
$\Longleftarrow$ Sei $x_0^2 \equiv a \pmod{2^k}$, $k \geq 3$. Dann ist auch $x_0 + 2^{k-1} \cdot t$ mit $t \in \mathbb{Z}$ eine Lösung von $x_0^2 \equiv a \pmod{2^k}$, denn es gilt:

$$(x_0 + 2^{k-1} \cdot t)^2 = x_0^2 + 2 \cdot 2^{k-1} \cdot x_0 \cdot t + 2^{2 \cdot k-2} \cdot t^2 \equiv x_0^2 \equiv a \pmod{2^k}$$

Im nächsten Schritt wird nun ähnlich wie im Beweis von Satz 4.3 gezeigt, dass für passendes $t \in \mathbb{Z}$ sogar $(x_0 - 2^{k-1} \cdot t)^2 \equiv a \pmod{2^{k+1}}$ gilt, denn damit ergibt sich durch Induktion die zu zeigende Behauptung.

$$\begin{aligned}(x_0 - 2^{k-1} \cdot t)^2 - a =& x_0^2 + 2 \cdot 2^{k-1} \cdot x_0 \cdot t + 2^{2 \cdot k-2} \cdot t^2 - a \\ \equiv& x_0^2 - a + 2^k \cdot x_0 \cdot t \pmod{2^{k+1}} \\ \equiv& 2^k \cdot \Big(\underbrace{\frac{x_0^2 - a}{2^k}}_{\in \mathbb{Z}} + x_0 \cdot t \Big) \pmod{2^{k+1}}\end{aligned}$$

Um die Gültigkeit der zu beweisenden Aussage $(x_0 - 2^{k-1} \cdot t)^2 \equiv a \pmod{2^{k+1}}$ zu zeigen, muss bewiesen werden, dass ein $t \in \mathbb{Z}$ gefunden werden kann, sodass $2 \mid (\frac{x_0^2 - a}{2^k} + x_0 \cdot t)$, denn dann ist $\frac{x_0^2 - a}{2^k} + x_0 \cdot t = 2 \cdot n$ und es folgt

$$(x_0 - 2^{k-1} \cdot t)^2 - a \equiv 0 \pmod{2^{k+1}}$$

Um dieses t zu finden, muss die lineare Kongruenzgleichung $x_0 \cdot t \equiv \frac{a - x_0^2}{2^k} \pmod 2$ gelöst werden. Da wegen $\text{ggT}(2, a) = 1$ sofort auch $\text{ggT}(2, x_0) = 1$ gilt, hat die lineare Kongruenz $x_0 \cdot t \equiv \frac{a - x_0^2}{2^k} \pmod 2$ aufgrund von Satz 3.3 mit Sicherheit eine Lösung t_0. Für diese Lösung gilt $(x_0 - 2^{k-1} \cdot t_0)^2 - a \equiv 0 \pmod{2^{k+1}}$ und somit $(x_0 - 2^{k-1} \cdot t_0)^2 \equiv a \pmod{2^{k+1}}$. □

4.3 Quadratische Reste

Nachdem die allgemeine Form der quadratischen Kongruenzgleichung $a \cdot x^2 + b \cdot x + c \equiv 0 \pmod m$ mit $a, m \in \mathbb{N}, b, c, x \in \mathbb{Z}, m \geq 2$ nun auf die deutlich verkürzte Form $x^2 \equiv a \pmod p$ mit $\text{ggT}(a, p) = 1$ zurückgeführt werden konnte und auch der Sonderfall $p = 2$ bereits behandelt wurde, können nun Aussagen zur Lösung von Kongruenzen dieser Art mit $p > 2$ formuliert und überprüft werden.

Definition (Quadratische Reste)**.** Es sei $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $\text{ggT}(a, p) = 1$.
Die Zahl a heißt quadratischer Rest (= QR) modulo p, wenn ein $x \in \mathbb{Z}$ existiert, sodass die quadratische Gleichung $x^2 \equiv a \pmod p$ lösbar ist.
Die Zahl a heißt quadratischer Nichtrest (= QNR) modulo p, wenn keine Zahl $x \in \mathbb{Z}$ existiert, sodass die Kongruenz $x^2 \equiv a \pmod p$ lösbar ist.

Betrachtet man also eine Kongruenz modulo einer Primzahl p, so kann man je nachdem ob "gewöhnliche" ganze Zahlen oder Quadratzahlen betrachtet werden, ein maßgeblicher Unterschied feststellt werden:
Angenommen es ist eine der Zahlen $0, 1, \ldots, p - 1$ gegeben.

- Dann kann immer eine ganze Zahl a gefunden werden, die bei der Division

durch p die gegebene Zahl als Rest ergibt. Denn ist beispielsweise $p = 7$ und die gegebene Zahl ist 5, dann gibt es unendlich viele Zahlen, die bei Division durch 7 den Rest 5 haben: $5, 12, 19, \ldots$.

- Betrachtet man weiterhin die Kongruenz modulo p, so erkennt man einerseits, dass sich unter den Zahlen $0, 1, \ldots, p-1$ sehr wohl Zahlen befinden, die als Reste der Division von Quadratzahlen durch p auftreten.
  Es sei beispielsweise die Zahl 4 gegeben und $p = 7$. Es gilt $5^2 = 3 \cdot 7 + 4$. Die Zahl 4 ist also ein quadratischer Rest modulo 7, da sie als Rest der Division einer Quadratzahl durch 7 auftritt. Im Gegensatz dazu kann jedoch auch der Fall eintreten, dass keine Quadratzahl existiert, die bei der Division durch p die gegebene Zahl als Rest ergibt. Es sei beispielsweise die Zahl 5 gegeben und $p = 7$. Dann existiert keine Quadratzahl, deren Rest bei der Division durch 7 die Zahl 5 ist.

Anhand dieser Beispiele wird also deutlich, dass es sich um eine besondere Eigenschaft handelt, wenn eine Zahl als Rest bei der Division einer Quadratzahl durch eine Primzahl auftritt, dh. wenn die Zahl quadratischer Rest modulo einer Primzahl ist. [6]

Bemerkung.

i) Man kann die Definition für quadratische Reste und Nichtreste auch für allgemeine Moduli aus $\mathbb{N}$ formulieren [10], doch wie in Abschnitt 4.1 verdeutlicht wurde, ist dies nicht notwendig.

ii) Verwendet man die Schreibweise des Restklassenrings $\mathbb{Z}_p^*$ ist die Definition der quadratischen Reste gleichbedeutend mit $\overline{x}^2 = \overline{a} \Longrightarrow a$ ist QR modulo p.

iii) Die Zahl 0 ist kein quadratischer Rest, obwohl die quadratische Kongruenzgleichung $x^2 \equiv 0 \pmod{p}$ trivialerweise lösbar ist.

Beispiel. Um alle quadratischen Reste modulo p zu finden, werden häufig Tabellen verwendet. Wird das Beispiel von vorhin genauer betrachtet und daher $p = 7$ gewählt, ergibt sich folgende Tabelle:

$\mathbf{x}$	$\overline{\mathbf{0}}$	$\overline{\mathbf{1}}$	$\overline{\mathbf{2}}$	$\overline{\mathbf{3}}$	$\overline{\mathbf{4}}$	$\overline{\mathbf{5}}$	$\overline{\mathbf{6}}$
$\mathbf{x^2}$	0	1	4	9	16	25	36
$\mathbf{x^2} \pmod{\mathbf{7}}$	0	1	4	2	2	4	1

Alle Zahlen, die modulo 7 ein quadratischer Rest sind und somit bei der Division von Quadratzahlen durch 7 als Rest auftreten, können nun aus der untersten Zeile der Tabelle abgelesen werden. Es gilt also:

QR modulo 7: 1, 2, 4

QNR modulo 7: 3, 5, 6

Lemma 4.1. *Es sei $p \in \mathbb{P}, p > 2$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,p) = 1$.*
Ist a ein quadratischer Rest modulo p, so besitzt die quadratische Kongruenzgleichung $x^2 \equiv a \pmod{p}$ genau zwei modulo p inkongruente Lösungen.

Beweis. Es sei $x_0 \in \mathbb{Z}$ eine Lösung von $x^2 \equiv a \pmod{p}$. Weiters sei $x_1 \in \mathbb{Z}$ eine weiter beliebige Lösung der Kongruenz. Dann gilt:

$$x_0^2 \equiv x_1^2 \pmod{p} \iff p \mid (x_0^2 - x_1^2) \iff p \mid (x_0 - x_1) \cdot (x_0 + x_1)$$

Aufgrund von Satz 2.8 gilt daher entweder $p \mid (x_0 - x_1)$ oder $p \mid (x_0 + x_1)$ was gleichbedeutend zu $x_0 \equiv x_1 \pmod{p}$ beziehungsweise $x_0 \equiv -x_1 \pmod{p}$ ist. Es gibt also nur die beiden Lösungen $\pm x_0$. Da $p \neq 2$ sind diese Lösungen inkongruent.
(Bem.: Fü $p = 2$ sind diese Lösungen nicht inkongruent, da $1 \equiv -1 \pmod{2}$ gilt.) □

Lemma 4.2. *Es sei $p \in \mathbb{P}, p > 2$.*
Dann gibt es genau $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste.

Beweis. Da $p \in \mathbb{P}$ gilt $|\mathbb{Z}_p^*| = p - 1$ beziehungsweise $\varphi(p) = p - 1$. Es wird nun gezeigt, dass von den $p - 1$ primen Restklassen modulo p genau die $\frac{p-1}{2}$ Restklassen $\overline{1}^2, \overline{2}^2, \ldots, \overline{\frac{p-1}{2}}^2$ quadratische Reste sind:
Trivialerweise sind die Restklassen $\overline{1}^2, \overline{2}^2, \ldots, \overline{\frac{p-1}{2}}^2$ quadratische Reste. Es bleibt jedoch zu zeigen, dass diese quadratischen Reste alle verschieden sind:
Es seien k, l aus der Menge $\{1, 2, \ldots, \frac{p-1}{2}\}$. Angenommen $k^2 \equiv l^2 \pmod{p}$. Dann gilt:

$$p \mid (k^2 - l^2) \iff p \mid (k - l) \cdot (k + l)$$

und daraus folgt wegen Satz 2.8 entweder $k \equiv l \pmod{p} \iff p \mid (k - p)$ oder $k \equiv -l \pmod{p} \iff p \mid (k + p)$. Da k und l jedoch beide aus der Menge $\{1, 2, \ldots, \frac{p-1}{2}\}$ sind, gilt jedoch $2 \leq k + l \leq p - 1$ woraus sofort $p \nmid (k + l)$ folgt. Daher muss laut Satz 2.8 $p \mid (k - l)$ gelten und es folgt $k = l$, weil $p \mid (k - l)$ nur für $k - l = 0$ gelten kann. Somit wurde gezeigt, dass die $\frac{p-1}{2}$ Restklassen $\overline{1}^2, \overline{2}^2, \ldots, \overline{\frac{p-1}{2}}^2$ der quadratischen Reste modulo p alle verschieden sind.
Betrachtet man nun die übrigen primen Restklassen modulo p, so erkennt man

folgendes:

$$\begin{aligned}
\overline{\frac{p+1}{2}} &= \overline{p - \frac{p-1}{2}} = -\overline{\frac{p-1}{2}} \\
\overline{\frac{p+3}{2}} &= \overline{p - \frac{p-3}{2}} = -\overline{\frac{p-3}{2}} \\
&\vdots \\
\overline{\frac{p+p-2}{2}} &= \overline{p-1} = \overline{-1}
\end{aligned}$$

Wenn diese Restklassen nun quadriert werden, ergeben sich keine neuen quadratischen Reste modulo p.

□

4.3.1 Legendre-Symbol

Im Zusammenhang mit quadratischen Resten wird in der Fachliteratur zur Erleichterung der Schreibweise häufig das Legendre-Symbol verwendet.

Definition (Legendre-Symbol)**.** Es sei $p \in \mathbb{P}, p > 2$ und $a \in \mathbb{Z}$. Das Legendre-Symbol $\left(\frac{a}{p}\right)$ ist definiert durch:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ falls } p \mid a \\ 1 \text{ falls } a \text{ ein QR modulo } p \text{ ist.} \\ -1 \text{ falls } a \text{ ein QNR modulo } p \text{ ist.} \end{cases}$$

Bemerkung. i) Das Legendre-Symbol ist nach dem französischen Mathematiker Adrien-Marie Legendre benannt und ausschließlich für Kongruenzen modulo einer Primzahl definiert. Eine Erweiterung für ungerade natürliche Zahlen wurde von Carl Gustav Jacob Jacobi entwickelt und trägt daher den Namen Jacobi-Symbol. Das Jacobi-Symbol wird jedoch erst im späteren Verlauf der Arbeit genauer betrachtet.

ii) Ist $a \equiv b \pmod{p}$, dann gilt $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ da $x^2 \equiv a \equiv b \pmod{p}$.

Um den Wert des Legendre-Symbols zu berechnen und somit eine Aussage über die Lösbarkeit der quadratischen Kongruenz $x^2 \equiv a \pmod{p}$ treffen zu können, werden nun einige wichtige Sätze formuliert und bewiesen, die schlussendliche auch zur Formulierung des quadratischen Reziprozitätsgestzes führen.

Satz 4.5 (Eulersches Kriterium)**.** *Es sei $p \in \mathbb{P}, p > 2$ und $a \in \mathbb{Z}$.*
Dann gilt: $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$
Beziehungsweise anders formuliert: a ist QR modulo $p \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

Beweis. Fall 1: Gilt $p \mid a$, dann ist $a \equiv 0 \pmod{p}$. Daraus folgt sofort $a^{\frac{p-1}{2}} \equiv 0 = \left(\frac{a}{p}\right) \pmod{p}$.
Fall 2: Es wird nun der Fall, dass $p \nmid a$ und a ein QNR modulo p ist, betrachtet. Die Kongruenzgleichung $x^2 \equiv a \pmod{p}$ ist daher laut Voraussetzung nicht lösbar. Da $p \nmid a$ gilt, ist a ein Element der Einheitengruppe $\mathbb{Z}_p^*$.
Weiters existiert per Definition der Einheitengruppe für jedes x, das ein Element des primen Restsystems $S := \{1, 2, \ldots, p-1\}$ modulo p ist, genau ein $y \in S$ sodass $x \cdot y \equiv a \pmod{p}$ gilt, wobei $y \in S$ dabei der Repräsentant der Restklasse $\overline{x}^{-1} \cdot \overline{a} \in \mathbb{Z}_p^*$ ist.
Wenn nun a ein QNR ist, gilt stets $x \neq y$, denn sonst wäre $x^2 \equiv a \pmod{p}$ lösbar. Das prime Restsystem S zerfällt also in $\frac{p-1}{2}$ verschiedene zweielementige Teilmengen:

$$S = \bigcup_{i=1}^{\frac{p-1}{2}} \{x_i; y_i\} \qquad \text{mit } x_i \neq y_i \text{ und } x_i \cdot y_i \equiv a \pmod{p}$$

Es gilt weiters:

$$(p-1)! = \prod_{j=1}^{p-1} j = \prod_{i=1}^{\frac{p-1}{2}} x_i \cdot y_i \equiv a^{\frac{p-1}{2}} \pmod{p}$$

und durch Anwendung des Satzes von Wilson folgt

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

Fall 3: Zuletzt wird der Fall, dass $p \nmid a$ und a ein QR modulo p ist, untersucht. Wie im Fall 2 wird erneut die Kongruenz $x \cdot y \equiv a \pmod{p}$ für $x, y \in S$ betrachtet. Da die Kongruenzgleichung $x^2 \equiv a \pmod{p}$ nun lösbar ist und laut Lemma 3.3 die beiden Lösungen x_0 und $-x_0 \equiv p - x_0 \pmod{p}$ besitzt, gilt in der Kongruenz $x \cdot y \equiv a \pmod{p}$ genau zweimal $x = y$.
Das prime Restsystem S zerfällt nun also in $\frac{p-3}{2}$ zweielementige Teilmengen und zwei einelementige Teilmengen:

$$S = \{x_0\} \cup \{p - x_0\} \cup \bigcup_{i=1}^{\frac{p-3}{2}} \{x_i; y_i\} \text{ und } x_i \cdot y_i \equiv a \pmod{p}$$

Es gilt weiters:

$$(p-1)! = \prod_{j=1}^{p-1} j = x_0 \cdot (p - x_0) \cdot \prod_{i=1}^{\frac{p-3}{2}} x_i \cdot y_i \equiv \overbrace{(x_0 \cdot p - x_0^2)}^{\equiv -a \pmod p} \cdot \prod_{i=1}^{\frac{p-3}{2}} x_i \cdot y_i$$
$$\equiv -a \cdot a^{\frac{p-3}{2}} = -a^{\frac{p-1}{2}} \pmod p$$

und mit dem Satz von Wilson gilt $-1 \equiv (p-1)! \equiv -a^{\frac{p-1}{2}} \pmod p$. Dies ist gleichbedeutend mit $a^{\frac{p-1}{2}} \equiv 1 = \left(\frac{a}{p}\right) \pmod p$. □

Mithilfe des Eulerschen Kriteriums können nun einige weitere Eigenschaften des Legendre-Symbols gezeigt werden.

Korollar 4.3. *Es sei $p \in \mathbb{P}$, $p > 2$. Weiters seien $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ und $c \in \mathbb{Z}, p \nmid c$. Dann gilt:*

i) $\left(\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_n}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_1}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right)$

ii) $\left(\frac{a \cdot c^2}{p}\right) = \left(\frac{a}{p}\right)$

Beweis. i) Das Produkt $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ ist ein Element der ganzen Zahlen und aus dem Eulerschen Kriterium folgt daher

$$\left(\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_n}{p}\right) \equiv (a_1 \cdot a_2 \cdot \ldots \cdot a_n)^{\frac{p-1}{2}}$$
$$= a_1^{\frac{p-1}{2}} \cdot a_2^{\frac{p-1}{2}} \cdot \ldots \cdot a_n^{\frac{p-1}{2}}$$
$$\equiv \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_1}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right) \pmod p$$

ii) Es gilt $\left(\frac{c}{p}\right) \cdot \left(\frac{c}{p}\right) = 1 \; \forall c \in \mathbb{Z}$ mit $p \nmid c$, denn entweder $\left(\frac{c}{p}\right) = 1$ oder $\left(\frac{c}{p}\right) = -1$. Aus i) folgt somit

$$\left(\frac{a \cdot c^2}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{c^2}{p}\right) = \left(\frac{a}{p}\right) \cdot 1 = \left(\frac{a}{p}\right)$$

□

Korollar 4.4. *Es seien $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}, p > 2$ sodass $p \nmid a$ und $p \nmid b$. Dann gilt:*

i) Sind a und b quadratische Reste modulo p, dann ist auch $a \cdot b$ ein quadratischer Rest modulo p.

ii) Sind a und b quadratische Nichtreste modulo p, dann ist $a \cdot b$ ein quadratischer Rest modulo p.

Beweis. Die Aussage folgt sofort aus Korollar 4.3 □

Eine weitere Aussage über das Legendre Symbol, die ebenfalls aus dem Eulerschen Kriterium resultiert, wird in der Literatur erster Ergänzungssatz genannt. Gemeinsam mit dem Lemma von Gauß und dem zweiten Ergänzungssatz bildet dieses Korollar die letzte zu überwindende Hürde, um schlussendlich das quadratische Reziprozitätsgesetz formulieren und beweisen zu können.

Korollar 4.5 (Erster Ergänzungssatz)**.** *Es sei $p \in \mathbb{P}, p > 2$.*
Dann gilt: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
Dies kann auch folgendermaßen geschrieben werden:

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

Beweis. Laut dem Eulerschen Kriterium gilt $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$. Da sowohl die rechte als auch die linke Seite der Kongruenz jeweils nur die Werte -1 oder 1 annehmen können, gilt demnach entweder $-1 \equiv 1 \pmod p$ oder $1 \equiv 1 \pmod p \iff -1 \equiv -1 \pmod p$. Der Fall $-1 \equiv 1 \pmod p$ wurde dabei jedoch bereits im Vorhinein ausgeschlossen, da $p > 2$ gilt und dieser Fall nur bei $p = 2$ eintritt. Daher gilt folgt für alle $p > 2$ aus $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$ sofort $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
Es existiert jeweils ein $k \in \mathbb{Z}$, sodass gilt:

$$(-1)^{\frac{p-1}{2}} = 1 \iff \frac{p-1}{2} = 2 \cdot k \iff p = 4k + 1 \iff p \equiv 1 \pmod 4$$

Umgekehrt gilt:

$$(-1)^{\frac{p-1}{2}} = -1 \iff \frac{p-1}{2} = 2 \cdot k + 1 \iff p = 4k + 3 \iff p \equiv 3 \pmod 4$$

□

Im nächsten Schritt wird nun das Lemma von Gauß, auch Gaußsches Lemma genannt, näher betrachtet. Die Behandlung dieses Lemmas ist für die Auseinandersetzung mit dem quadratischen Reziprozitätsgesetz unumgänglich, da es den Ausgangspunkt einer Vielzahl an Beweisen des Reziprozitätsgesetzes darstellt. [10] Für die Formulierung des Gaußschen Lemmas, wird das vollständige Restsystem $\{0, 1, 2, \ldots, p-1\}$ modulo p nun auf eine andere Art und Weise dargestellt:

$$S = \left\{ -\frac{p-1}{2}, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{p-1}{2} \right\}$$

Die Elemente dieses vollständigen Systems von Resten modulo p werden Minimalreste modulo p genannt. Ist nun a eine zu p teilerfremde Zahl, so hat a mit

Sicherheit nicht 0 als Minimalrest.
Bildet man die $\frac{p-1}{2}$ Zahlen $1 \cdot a, 2 \cdot a, \ldots, \frac{p-1}{2} \cdot a$, so kann festgestellt werden, dass jede dieser Zahlen teilerfremd zu p ist und daher zu genau einer der Zahlen aus $S \setminus \{0\}$ kongruent ist.
Für $j = 1, 2, \ldots, \frac{p-1}{2}$ sei n_j der Repräsentant der entsprechenden Restklasse $\overline{a \cdot j}$ aus dem Restsystem der Minimalreste modulo p. Formal bedeutet dies: $-\frac{p-1}{2} \leq n_j \leq \frac{p-1}{2} = -\frac{p-1}{2} + p - 1$. Wie anhand des folgenden Beispiels leicht sichtbar wird, sind gewisse Minimalreste n_j negativ.

Beispiel. Es sei $p = 7$ und $a = 5$. Dann ist $\frac{p-1}{2} = 3$ und somit $j = 1, 2, 3$

$\mathbf{a \cdot j}$	$\mathbf{5 \cdot 1}$	$\mathbf{5 \cdot 2}$	$\mathbf{5 \cdot 3}$
Reste	5	10	15
$\mathbf{n_j}$	-2	3	1

Außerdem ist jede der Zahlen $1 \cdot a, 2 \cdot a, \ldots, \frac{p-1}{2} \cdot a$ zu einer anderen Zahl aus $n_j \in S \setminus \{0\}$ kongruent. Denn wäre $a \cdot x \equiv a \cdot x' \pmod{p}$ für zwei verschiedene Zahlen x und x' aus $\{1, 2, \ldots, \frac{p-1}{2}\}$, wobei o.B.d.A $x > x'$ gilt, so würde sofort die Kongruenz $a \cdot (x - x') \equiv 0 \pmod{p}$ folgen. Dies ist aber nicht möglich, da sowohl $p \nmid a$ als auch $p \nmid (x - x')$ gilt.
Mithilfe dieser Überlegungen kann das Lemma von Gauß nun formal betrachtet und seine Gültigkeit bewiesen werden:

Satz 4.6 (Lemma von Gauß)**.** *Es sei $p \in \mathbb{P}, p > 2$ und $a \in \mathbb{Z}$ mit $p \nmid a$.*
Weiters sei $M = \{a \cdot 1, a \cdot 2, \ldots, a \cdot \frac{p-1}{2}\}$.
Dann ist $\left(\frac{a}{p}\right) = (-1)^{\gamma_p(a)}$, wobei $\gamma_p(a)$ die Anzahl der Elemente aus M mit negativen Minimalrest modulo p ist.

Beispiel. Im obigen Beispiel gilt also $\gamma_7(5) = 1 \Longrightarrow \left(\frac{5}{7}\right) = (-1)^1 = -1$. Daraus kann nun der Schluss gezogen werden, dass 5 ein quadratischer Nichtrest modulo 7 ist und somit die Kongruenz $x^2 \equiv 5 \pmod{7}$ nicht lösbar ist.

Beweis. Mithilfe der Überlegungen von vorhin kann das Lemma von Gauß schnell gezeigt werden.
Es sei $j = 1, 2, \ldots, \frac{p-1}{2}$. Dann gilt:

$$a \cdot j \equiv e_j \cdot r_j \pmod{p} \tag{4.1}$$

wobei r_j eine der Zahlen $1, 2, \ldots, \frac{p-1}{2}$ aus S^+ ist und $e_j \in \{-1, 1\}$ ist. Dabei ist $e_j = -1$, wenn der Minimalrest von $a \cdot j$ modulo p negativ ist, und $e_j = 1$, wenn der Minimalrest von $a \cdot j$ modulo p positiv ist. Die Produkte $e_j \cdot r_j$ bilden somit die Minimalreste n_j modulo p, die wie oben bereits gezeigt wurde, alle verschieden voneinander sind und aus der Menge $S \setminus \{0\} = \{-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}\}$

stammen .
Der wesentliche Schritt liegt nun darin zu zeigen dass die Zahlen $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ mit den Zahlen $1, 2, \ldots, \frac{p-1}{2} \in S^+$ übereinstimmen und sich lediglich in der Reihenfolge unterscheiden. Diese Tatsache kann aber sofort eingesehen werden, denn weil a und p teilerfremd sind $(p \nmid a)$ bilden neben den Zahlen

$$1, -1, 2, -2, \ldots, \frac{p-1}{2}, -\frac{p-1}{2} \tag{4.2}$$

auch die $p-1$ Zahlen

$$a \cdot 1, a \cdot (-1), a \cdot 2, a \cdot (-2), \ldots, a \cdot \frac{p-1}{2}, a \cdot \Big(-\frac{p-1}{2}\Big)$$

ein primes Restsystem modulo p. Laut 4.1 können die Minimalreste dieser Zahlen folgendermaßen angegeben werden:

$$e_1 \cdot r_1, -e_1 \cdot r_1, e_2 \cdot r_2, -e_2 \cdot r_2, \ldots, e_{\frac{p-1}{2}} \cdot r_{\frac{p-1}{2}}, -e_{\frac{p-1}{2}} \cdot r_{\frac{p-1}{2}}$$

Diese Zahlen sind (bis auf die Reihenfolge) ident zu 4.2. Die positiven unter ihnen, dh. $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ müssen also die Zahlen $1, 2, \ldots, \frac{p-1}{2}$ sein.
Hieraus folgt, dass gilt:

$$r_1 \cdot r_2 \cdot \ldots \cdot r_{\frac{p-1}{2}} = \Big(\frac{p-1}{2}\Big)!$$

Damit kann nun die Aussage gezeigt werden, indem die Kongruenzen aus 4.1 miteinander multipliziert werden und anschließend geeignet gekürzt wird:

$$\begin{aligned}
\Big(\frac{p-1}{2}\Big)! \cdot a^{\frac{p-1}{2}} &\equiv (e_1 \cdot e_2 \cdot \ldots \cdot e_{\frac{p-1}{2}}) \cdot (r_1 \cdot r_2 \cdot \ldots \cdot r_{\frac{p-1}{2}}) \pmod p \\
\Big(\frac{p-1}{2}\Big)! \cdot a^{\frac{p-1}{2}} &\equiv (e_1 \cdot e_2 \cdot \ldots \cdot e_{\frac{p-1}{2}}) \cdot \Big(\frac{p-1}{2}\Big)! \pmod p \\
a^{\frac{p-1}{2}} &\equiv e_1 \cdot e_2 \cdot \ldots \cdot e_{\frac{p-1}{2}} \pmod p \\
a^{\frac{p-1}{2}} &\equiv (-1)^{\gamma_p(a)} \pmod p
\end{aligned}$$

Nach Anwendung des Eulerschen Kriteriums erhaltet man schlussendlich

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

und da das Legendre-Symbol nur die Werte ± 1 annehmen kann, gilt schließlich $\left(\frac{a}{p}\right) = (-1)^{\gamma_p(a)}$ □

Korollar 4.6 (Zweiter Ergänzungssatz)**.** *Es sei $p \in \mathbb{P}, p > 2$.*

Dann gilt: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
Diese Aussage ist äquivalent zu :

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

Beweis. Laut dem gerade bewiesenen Lemma von Gauß muss zur Berechnung des Legendre-Symbols $\left(\frac{2}{p}\right)$ die Anzahl der Elemente der Menge

$$\left\{1 \cdot 2, 2 \cdot 2, \ldots \cdot \frac{p-1}{2} \cdot 2\right\} = \{2, 4, \ldots, p-1\}$$

bestimmt werden, die größer als $\frac{p-1}{2}$ sind, denn all diese Elemente besitzen einen negativen absolut kleinsten Rest bei Division durch p und die Anzahl dieser Elemente entspricht genau $\gamma_p(2)$. Anders formuliert bedeutet das, dass ein $m \in \mathbb{Z}$ gefunden werden muss, sodass $2 \cdot m \leq \frac{p-1}{2} < 2 \cdot (m+1)$ gilt, denn dann folgt $\gamma_p(2) = \frac{p-1}{2} - m$.
Im folgenden werden daher für alle möglichen Fälle m und $\gamma_p(2)$ berechnet:

- $p = 8 \cdot k + 1$: Dann ist $\frac{p-1}{2} = 4 \cdot k$, $m = 2 \cdot k$ und es folgt $\gamma_p(2) = 2 \cdot k$ und daher $\left(\frac{2}{p}\right) = (-1)^{2 \cdot k} = 1$
- $p = 8 \cdot k + 3$: Dann ist $\frac{p-1}{2} = 4 \cdot k + 1$, $m = 2 \cdot k$ und es folgt $\gamma_p(2) = 2k + 1$ und daher $\left(\frac{2}{p}\right) = (-1)^{2 \cdot k + 1} = -1$
- $p = 8 \cdot k + 5$: Dann ist $\frac{p-1}{2} = 4 \cdot k + 2$, $m = 2 \cdot k + 1$ und es folgt $\gamma_p(2) = 2k + 1$ und daher $\left(\frac{2}{p}\right) = (-1)^{2 \cdot k + 1} = -1$
- $p = 8 \cdot k + 7$: Dann ist $\frac{p-1}{2} = 4 \cdot k + 3$, $m = 2 \cdot k + 1$ und es folgt $\gamma_p(2) = 2k + 2$ und daher $\left(\frac{2}{p}\right) = (-1)^{2 \cdot k + 2} = 1$

Daher gilt $\left(\frac{2}{p}\right) = 1$ genau dann, wenn $p \equiv \pm 1 \pmod 8$ und $\left(\frac{2}{p}\right) = -1$, wenn $p \equiv \pm 3 \pmod 8$. □

Mit dem Beweis des zweiten Ergänzungssatzes ist die Darlegung des notwendigen mathematischen Vorwissens für das quadratische Reziprozitätsgesetz abgeschlossen, sodass in den folgenden Abschnitten der Ausarbeitung nun eine genauere Auseinandersetzung mit dem quadratischen Reziprozitätsgesetz und seinen Beweisen möglich ist.

5 Quadratisches Reziprozitätsgesetz

Die bisher formulierten und bewiesenen Sätze, Lemmata und Korollare ermöglichen zwar bereits die Berechnung des Legendre-Symbols, doch ist die Bestimmung des Wertes $\left(\frac{a}{p}\right)$ mit diesen mathematischen Hilfsmitteln insbesondere für große Primzahlen sehr zeitaufwendig und ineffizient. Durch das von Euler entdeckte quadratische Reziprozitätsgesetz, welches im folgenden Abschnitt der Arbeit thematisiert wird, ist es nun jedoch möglich, das Legendre-Symbol auch für große Primzahlen schnell zu berechnen. Das Reziprozitätsgesetz stellt das Hauptergebnis der vorliegenden Masterarbeit dar und wird aufgrund dessen im folgenden Abschnitt detailreich behandelt. Die Beschäftigung mit dem quadratischen Reziprozitätsgesetz erfolgt dabei in mehreren Schritten: Zuallererst wird ein kurzer historischer Überblick über die Geschichte des Reziprozitätsgesetzes gegeben, bevor die Aussage anschließend formuliert wird. Daran anschließend wird die Nützlichkeit des Satzes bei der Berechnung des Legendre-Symbols anhand von einigen Beispielen verdeutlicht, bevor schlussendlich zwei Beweise des Satzes angeführt werden.

5.1 Geschichte des quadratischen Reziprozitätsgesetzes

Bevor eine mathematische Auseinandersetzung mit dem quadratischen Reziprozitätsgesetzes stattfindet, wird in diesem Kapitel ein kurzer Einblick in die Geschichte des Reziprozitätsgesetzes gegeben.
Das quadratische Reziprozitätsgesetz wurde im Jahr 1783 von Leonhard Euler entdeckt, doch es gelang ihm nicht, die Aussage des Gesetzes auch zu beweisen. Auch Adrien-Marie Legendre, der dem quadratischen Reziprozitätsgesetz seinen Namen gab, scheiterte am Beweis der Aussage. Der erste vollständige Beweis wurde erst einige Zeit später im Jahr 1801 publiziert und stammt von Carl Friedrich Gauß. Bemerkenswert dabei ist, dass Gauß zum Zeitpunkt seiner Auseinandersetzung mit dem quadratischen Reziprozitätsgesetz, das er zu dieser Zeit Fundamentaltheorem nannte, nicht mit den Arbeiten von Euler und Legendre vertraut war. Stattdessen entdeckte er das Gesetz durch empirisches Arbeiten mit Zahlentabellen und Induktion. Des Weiteren gab sich Gauß nicht damit zufrieden, einen bisher unbewiesenen Satz auf eine Art zu beweisen, sondern erarbeitet insgesamt acht verschiedene Beweise die auf unterschiedlichen mathematischen Grundkenntnissen basieren. Während sein erster Beweis, der heute als einer der mühsameren Beweise angesehen wird, direkt aus den Erkenntnissen der Begriffsbildung der quadratischen Reste abgeleitet werden kann, basieren die anderen von Gauß angeführten Beweise auf mathematischen Hilfsmitteln wie den quadratischen Formen, der Kreisteilung, höheren Kongruenzen, der Gaußschen Summe oder kubischen und biquadratischen Resten.[6]

Doch nicht nur die bisher genannten Mathematiker beschäftigten sich mit dem Reziprozitätsgesetz. Heute ist das quadratische Reziprozitätsgesetz zur Verwunderung vieler das am häufigsten bewiesene mathematische Theorem und übertrifft somit in der Anzahl an bekannten Beweisen nicht nur den Fundamentalsatz der Algebra sondern auch den weitaus bekannteren Satz des Pythagoras. Vor zwanzig Jahren existierten bereits 196 Beweise des quadratischen Reziprozitätsgesetzes, die sich mehr oder weniger stark voneinander unterscheiden und auch in ihrer Länge und Komplexität höchst unterschiedlich sind. Zusätzlich gibt es auch mehrere Bücher, die sich einzig und alleine mit der Masse an Beweisen des Reziprozitätsgesetzes auseinandersetzen (z.B Pieper 1978 und Lemmermeyer 2000). [5], [6], [4] Diese Menge an Beweisen stammt neben Gauß von einer Vielzahl an bekannten Mathematikern, darunter auch Cauchy, Dedekind und Hilbert. Ferdinand Gotthold Eisenstein lieferte sogar fünf verschiedenen Beweise der Aussage. [6]

5.2 Formulierung und Anwendungen des quadratischen Reziprozitätsgesetzes

Das quadratische Reziprozitätsgesetz wird herangezogen, um zu bestimmen, ob einen Zahl $a \in \mathbb{Z}$ ein quadratischer Rest modulo eines gegebenen $m \in \mathbb{N}$ ist, und dadurch die Lösbarkeit der quadratische Kongruenz $x^2 \equiv a \pmod{m}$ zu überprüfen. Zusätzlich kann mithilfe des quadratischen Reziprozitätsgesetzes umgekehrt auch die Frage beantwortet werden, modulo welcher Zahlen $m \in \mathbb{N}$ eine vorgegebenen Zahl $a \in \mathbb{Z}$ ein quadratischer Rest ist. Durch die Erkenntnisse aus Abschnitt 4.1 kann die Lösung dieser Fragestellungen auf die Bestimmung des Legendre-Symbols zurückgeführt. Obwohl mit dem Eulerschen Kriterium und dem Lemma von Gauß bereits zwei Möglichkeiten zur Berechnung des Legendre-Symbols angeführt wurden, stellt das im folgenden dargelegte quadratische Reziprozitätsgesetz eine weitaus effizientere Möglichkeit dar. Aufgrund dessen bildet das quadratische Reziprozitätsgesetz das Hauptergebnis der vorliegenden Arbeit. [10]

5.2.1 Formulierung des quadratischen Reziprozitätsgesetzes

Satz 5.1 (Quadratisches Reziprozitätsgesetz)**.** *Es seien $p, q \in \mathbb{P} \setminus \{2\}$ mit $p \neq q$. Dann gilt:* $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$
Dies ist gleichbedeutend mit:

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, *wenn* $p \equiv 1 \pmod{4}$ *oder* $q \equiv 1 \pmod{4}$
- $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, *wenn* $p \equiv q \equiv 3 \pmod{4}$

Bemerkung. Der untere Teil der Aussage kann auch wie folgt formuliert werden:

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, wenn p, q nicht beide die Form $4 \cdot k + 3$ haben
- $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, wenn p, q beide die Form $4 \cdot k + 3$ haben

5.2.2 Anwendungen des quadratischen Reziprozitätsgesetzes

Bevor der Fokus auf die verschiedenen Beweise des quadratischen Reziprozitätsgesetzes gelegt wird, werden in diesem Unterkapitel einige Beispiele angeführt, die die Anwendung des Satzes bei der Bestimmung des Legendre-Symbols demonstrieren und die damit einhergehenden Erleichterungen bei der Berechnung des Legendre-Symbols gut verdeutlichen. Die Ausarbeitung der Beispiele 1-4 orientiert sich dabei am Werk von Remmert und Ullrich [10].

Beispiel (1). Im ersten Beispiel wird überprüft, ob die Zahl 3 ein quadratischer Rest oder Nichtrest modulo 29 ist. Laut dem quadratischen Reziprozitätsgesetz (Satz 5.1) gilt:

$$\left(\frac{3}{29}\right) \cdot \left(\frac{29}{3}\right) = (-1)^{\frac{3-1}{2}\frac{29-1}{2}} = 1 \Longrightarrow \left(\frac{3}{29}\right) = \left(\frac{29}{3}\right)$$

Weiters gilt $\left(\frac{29}{3}\right) = \left(\frac{2}{3}\right)$, da $29 \equiv 2 \pmod 3$. Mithilfe des zweiten Ergänzungssatzes (Korollar 4.6) folgt:

$$\left(\frac{29}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1.$$

Daraus folgt schlussendlich $\left(\frac{3}{29}\right) = -1$, was bedeutet, dass 3 quadratischer Nichtrest modulo 29 ist.

Beispiel (2). Im zweiten Beispiel soll überprüft werden, ob 35 ein quadratischer Rest modulo 281 ist. Im Gegensatz zum ersten Beispiel handelt es sich bei 281 bereits um eine eher größere Primzahl, an deren Beispiel gut erkennbar ist, dass das Eulersche Kriterium und das Lemma von Gauß für große Zahlen nicht effizient sind, um das Legendre-Symbol zu bestimmen. Denn für die Berechnung des Legendre-Symbols mittels Eulerschen Kriterium muss herausgefunden werden, in welcher Restklasse von 281 die Zahl 35^{140} liegt und für die Berechnung mittels Lemma von Gauß muss das Vorzeichen der absolut kleinsten Reste bei Division durch 281 von 140 Produkten bestimmt werden. Da beide diese Möglichkeiten zwar prinzipiell durchführbar, jedoch in ihrer Umsetzung sehr zeitaufwendig sind, wird als weitaus effizientere Methode das quadratische Reziprozitätsgesetz herangezogen:
Zuerst wird die Zahl 35 in ihre Primfaktoren zerlegt: $35 = 5 \cdot 7$. Wegen Korollar

4.3 gilt:

$$\left(\frac{35}{281}\right) = \left(\frac{5 \cdot 7}{281}\right) = \left(\frac{5}{281}\right) \cdot \left(\frac{7}{281}\right)$$

Da $5 \equiv 1 \pmod 4$ gilt nach Satz 5.1 $\left(\frac{5}{281}\right) = \left(\frac{281}{5}\right)$.
Analog folgt aus $281 \equiv 1 \pmod 4$, dass $\left(\frac{7}{281}\right) = \left(\frac{281}{7}\right)$. Aus den Eigenschaften des Legendre-Symbols ergibt sich weiters:

$$281 \equiv 1 \pmod 5 \Longrightarrow \left(\frac{281}{5}\right) = \left(\frac{1}{5}\right) = 1$$
$$281 \equiv 1 \pmod 7 \Longrightarrow \left(\frac{281}{7}\right) = \left(\frac{1}{7}\right) = 1$$

Insgesamt ergibt sich also $\left(\frac{35}{281}\right) = 1 \cdot 1 = 1$. Somit ist 35 quadratischer Rest modulo 281 und die quadratische Kongruenz $x^2 \equiv 35 \pmod{281}$ ist lösbar.

Beispiel (3). Es soll nun überprüft werden, ob -198 ein quadratischer Rest modulo 71 ist. Im ersten Schritt wird die Zahl -198 wieder in ein Produkt von Primzahlen zerlegt: $-198 = (-1) \cdot 2 \cdot 3^2 \cdot 11$.

Demnach gilt:

$$\left(\frac{-198}{71}\right) = \left(\frac{-1}{71}\right) \cdot \left(\frac{2}{71}\right) \cdot \left(\frac{3^2}{71}\right) \cdot \left(\frac{11}{71}\right)$$

Im nächsten Schritt wird nun der Wert jedes Legendre-Symbols einzeln betrachtet:

- Aus dem ersten Ergänzungssatz folgt:

$$\left(\frac{-1}{71}\right) = (-1)^{\frac{71-1}{2}} = (-1)^{35} = -1$$

- Aus dem zweiten Ergänzungssatz folgt:

$$\left(\frac{2}{71}\right) = (-1)^{\frac{71^2-1}{8}} = (-1)^{\frac{(71-1)\cdot(71+1)}{8}} = (-1)^{\frac{70\cdot 72}{8}} = 1$$

- $\left(\frac{3^2}{71}\right) = 1$, da die Kongruenzgleichung $x^2 \equiv 3^2 \pmod{71}$ offensichtlich lösbar ist.

- Wegen $11 \equiv 3 \pmod 4$, $71 \equiv 3 \pmod 4$ und $5 \equiv 1 \pmod 4$ gilt laut dem Reziprozitätsgesetzes:

$$\left(\frac{11}{71}\right) = -\left(\frac{71}{11}\right) = -\left(\frac{5}{11}\right) = -\left(\frac{11}{5}\right) = -\left(\frac{1}{5}\right) = -1$$

Insgesamt ergibt sich demnach:

$$\left(\frac{-198}{71}\right) = \left(\frac{-1}{71}\right) \cdot \left(\frac{2}{71}\right) \cdot \left(\frac{3^2}{71}\right) \cdot \left(\frac{11}{71}\right) = (-1) \cdot 1 \cdot 1 \cdot (-1) = 1$$

Die Zahl -198 ist daher ein quadratischer Rest modulo 71.

Beispiel (4). In den bisher angeführten Beispielen sollte bis jetzt stets überprüft werden, ob eine bestimmte Zahl $a \in \mathbb{Z}$ ein quadratischer Rest modulo einer vorgegeben Zahl $m \in \mathbb{N}$ ist. Das quadratische Reziprozitätsgesetz findet jedoch auch bei der umgekehrten Fragestellung Anwendung. Um diese zu verdeutlichen sollen im folgenden Beispiel alle Primzahlen bestimmt werden, modulo derer 10 ein quadratischer Rest ist. Gesucht ist daher die Menge aller $p \in \mathbb{P}$ mit $\left(\frac{10}{p}\right) = 1$. Die Fälle $p = 2$ und $p = 5$ werden dabei vorweg genommen, denn es gilt:

$$\left(\frac{10}{2}\right) = \left(\frac{10}{5}\right) = 0 \neq 1,$$

da in diesen Fällen $p \mid 10$ gilt.
Für $p \notin \{2, 5\}$ gilt:

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{5}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{p}{5}\right) \qquad \forall p \in \mathbb{P} \setminus \{2, 5\}$$

Aus dem zweiten Ergänzungssatz folgt nun:

a) $\left(\frac{2}{p}\right) = 1$ für alle $p \in \mathbb{P}$ mit $p \equiv 1 \pmod 8$ oder $p \equiv 7 \pmod 8$

b) $\left(\frac{2}{p}\right) = -1$ für alle $p \in \mathbb{P}$ mit $p \equiv 3 \pmod 8$ oder $p \equiv 5 \pmod 8$

Zusätzlich folgt aus der Anwendung des Eulerschen Kriteriums, der Ergänzungssätze und des Reziprozitätsgesetzes:

a') $\left(\frac{p}{5}\right) = 1$ für alle $p \in \mathbb{P}$ mit $p \equiv 1 \pmod 5$ oder $p \equiv 4 \pmod 5$

b') $\left(\frac{p}{5}\right) = -1$ für alle $p \in \mathbb{P}$ mit $p \equiv 2 \pmod 5$ oder $p \equiv 3 \pmod 5$

Das zu betrachtende Produkt $\left(\frac{2}{p}\right) \cdot \left(\frac{p}{5}\right)$ ist also genau dann 1, wenn entweder a) und a') oder b) und b') erfüllt sind. Damit die Zahl 10 ein quadratischer Rest modulo p ist, sind für p daher insgesamt acht verschiedene Kongruenzpaare möglich:

- $p \equiv 1 \pmod 8$ und $p \equiv 1 \pmod 5$
- $p \equiv 7 \pmod 8$ und $p \equiv 1 \pmod 5$
- $p \equiv 1 \pmod 8$ und $p \equiv 4 \pmod 5$

- $p \equiv 7 \pmod 8$ und $p \equiv 4 \pmod 5$
- $p \equiv 3 \pmod 8$ und $p \equiv 2 \pmod 5$
- $p \equiv 3 \pmod 8$ und $p \equiv 3 \pmod 5$
- $p \equiv 5 \pmod 8$ und $p \equiv 2 \pmod 5$
- $p \equiv 5 \pmod 8$ und $p \equiv 3 \pmod 5$

Mithilfe des Chinesischen Restsatzes können die eindeutigen Lösungen modulo $40 = 8 \cdot 5$ dieser Kongruenzpaare bestimmt werden. Dadurch ergeben sich folgende acht Lösungen:

$$1, 9, 31, 39, 27, 3, 37, 13$$

Damit kann nun der Schluss gezogen werden, dass die Zahl 10 genau dann ein quadratischer Rest modulo $p \in \mathbb{P}$ ist, wenn p eine der folgenden Kongruenzen erfüllt:

$$\begin{aligned} p &\equiv 1 \pmod{40}, & p &\equiv 3 \pmod{40} \\ p &\equiv 9 \pmod{40}, & p &\equiv 13 \pmod{40} \\ p &\equiv 27 \pmod{40}, & p &\equiv 31 \pmod{40} \\ p &\equiv 37 \pmod{40}, & p &\equiv 39 \pmod{40} \end{aligned}$$

Erfüllt die Primzahl p keine dieser Kongruenzen, so ist 10 modulo p ein quadratischer Nichtrest.

Beispiel (5). In den Beispielen 1-3 wurde stets die Lösbarkeit von quadratischen Kongruenzgleichungen der Form $x^2 \equiv a \pmod p$ für $a \in \mathbb{Z}, p \in \mathbb{P}, p > 2$ untersucht. Im folgenden Beispiel soll nun festgestellt werden, ob die quadratische Kongruenzgleichung $4x^2 + 5x + 19 \equiv 0 \pmod{105}$ der allgemeinen Form lösbar ist. Weiters soll im Fall, dass die Kongruenzgleichung lösbar ist, die Lösung mittels chinesischem Restsatz bestimmt werden.
Erneut wird dazu zuerst die Zahl 105 in Primfaktoren zerlegt: $105 = 3 \cdot 5 \cdot 7$.
Laut Satz 4.1 kann für die Entscheidung über die Lösbarkeit der Kongruenz modulo 105 auch die simultane Kongruenz

$$\begin{aligned} 4x^2 + 5x + 19 &\equiv 0 \pmod 3 \\ 4x^2 + 5x + 19 &\equiv 0 \pmod 5 \\ 4x^2 + 5x + 19 &\equiv 0 \pmod 7 \end{aligned}$$

betrachtet werden. Im nächsten Schritt werden diese drei Kongruenzgleichungen nun jeweils so bearbeitet, dass zum einen sichtbar wird, dass die Kongruenzen lösbar sind und zum anderen dadurch gleichzeitig ein System von linearen Kongruenzen entsteht:

- $$\begin{aligned} & 4x^2 + 5x + 19 \equiv 0 \pmod 3 \\ \iff\ & x^2 + 2x + 1 \equiv 0 \pmod 3 \\ \iff\ & (x+1)^2 \equiv 0 \pmod 3 \\ \iff\ & x + 1 \equiv 0 \pmod 3 \\ \iff\ & x \equiv -1 \pmod 3 \end{aligned}$$

- $$\begin{aligned} & 4x^2 + 5x + 19 \equiv 0 \pmod 5 \\ \iff\ & 4x^2 + 4 \equiv 0 \pmod 5 \\ \iff\ & 4x^2 \equiv -4 \pmod 5 \\ \iff\ & x^2 \equiv -1 \pmod 5 \end{aligned}$$

  Aus dem ersten Ergänzungssatz folgt $\left(\frac{-1}{5}\right) \equiv (-1)^{\frac{5-1}{2}} = 1$, weshalb $x^2 \equiv -1 \pmod 5$ mit Sicherheit lösbar ist. Es gilt:

  $$x^2 \equiv -1 \equiv 4 \pmod 5 \iff x \equiv \pm 2 \pmod 5$$

- $$\begin{aligned} & 4x^2 + 5x + 19 \equiv 0 \pmod 7 \\ \iff\ & 4x^2 + 5x + 5 \equiv 0 \pmod 7 && \mid +4 \\ \iff\ & 4x^2 + 5x + 9 \equiv 4 \pmod 7 \\ \iff\ & (2 \cdot x + 3)^2 \equiv 4 \pmod 7 \\ \iff\ & 2 \cdot x + 3 \equiv \pm 2 \pmod 7 \end{aligned}$$

  Dh. es gilt entweder $2 \cdot x \equiv -1 \pmod 7$ oder $2 \cdot x \equiv -5 \equiv 2 \pmod 7$. Daraus folgt nun:

  $$\begin{aligned} & 2 \cdot x \equiv -1 \pmod 7 && \mid \cdot 4 \\ \iff\ & 8 \cdot x \equiv -4 \pmod 7 \\ \iff\ & x \equiv -4 \equiv 3 \pmod 7 \end{aligned}$$

und

$$\begin{aligned} & 2 \cdot x \equiv 2 \pmod 7 && \mid \cdot 4 \\ \iff\ & 8 \cdot x \equiv 8 \pmod 7 \\ \iff\ & x \equiv 1 \pmod 7 \end{aligned}$$

Um die Lösungen der quadratischen Kongruenzgleichung zu finden, müssen nun die Lösung aller Kombinationen der erhaltenen linearen Kongruenzen mithilfe des chinesischen Restsatzes ermittelt werden. Dabei ist es hilfreich, die möglichen Kombinationen in einer Tabelle darzustellen:

Lösungen	1	2	3	4	
$x \equiv$	-1	-1	-1	-1	mod 3
$x \equiv$	2	-2	2	-2	mod 5
$x \equiv$	1	1	3	3	mod 7

Jede Spalte bildet eine simultane Kongruenz, die durch die Anwendung des chinesischen Restsatzes gelöst werden kann. Um die Aufgabe vollständig zu lösen und alle vier Lösungen der quadratischen Kongruenzgleichung zu erhalten, muss der chinesische Restsatz daher viermal ausgeführt werden. Da die Lösungen der simultanen Kongruenzen analog gefunden werden können, wird das Lösungsverfahren nur für den ersten Fall (=erste Spalte) demonstriert:

Es gilt $x \equiv -1 \pmod 3 \iff x = -1 + 3 \cdot t$ für $t \in \mathbb{Z}$. Durch Einsetzen in die zweite lineare Kongruenz folgt:

$$\begin{aligned} & x = -1 + 3 \cdot t \equiv 2 \pmod 5 \\ \iff\ & 3 \cdot t \equiv 3 \pmod 5 \\ \iff\ & t \equiv 1 \pmod 5 \end{aligned}$$

Daraus folgt $t = 1 + 5 \cdot u$ und somit gilt $x = -1 + 3 \cdot (1 + 5 \cdot u) = 2 + 15 \cdot u$. Dies wird nun in die dritte Kongruenz eingesetzt:

$$\begin{aligned} & x = 2 + 15 \cdot u \equiv 1 \pmod 7 \\ \iff\ & 15 \cdot u \equiv -1 \pmod 7 \\ \iff\ & u \equiv -1 \pmod 7 \end{aligned}$$

Also ist $u = -1 + 7 \cdot v$ und es folgt $x = 2 + 15 \cdot (-1 + 7 \cdot v) = -13 + 105 \cdot v$. Nach dem chinesischen Restsatz ist daher mit $x \equiv -13 \pmod{105}$ die modulo 105 eindeutige Lösung der simultanen Kongruenz gefunden.
Das bedeutet, alle $x \equiv -13 \pmod{105}$ erfüllen die ursprünglich gegebene qua-

dratische Kongruenzgleichung $4x^2 + 5x + 19 \equiv 0 \pmod{105}$ und sind somit eine Lösung der quadratischen Kongurenz.
Probe: $4 \cdot (-13)^2 + 5 \cdot (-13) + 19 \equiv 46 - 65 + 19 \equiv 0 \bmod (105)$

Die oben angeführten Beispiele haben verdeutlicht, dass das quadratische Reziprozitätsgesetz ein wichtiges mathematisches Hilfsmittel ist, wenn quadratische Kongruenzen gelöst werden sollen, da durch dessen Anwendung sowie die Anwendung der beiden Ergänzungssätze eine simple Vorgehensweise zur Bestimmung des Legendre-Symbols $\left(\frac{a}{p}\right)$ festgelegt ist. Im ersten Schritt wird dabei zunächst die Primfaktorzerlegung der Zahl a gebildet, sodass das Legendre-Symbol $\left(\frac{a}{p}\right)$ mithilfe der Produktregel (Korollar 4.3) in mehrere Faktoren zerlegt wird. Die Faktoren sind nach diesem Schritt von der Form $\left(\frac{q}{p}\right)$, $\left(\frac{-1}{p}\right)$ oder $\left(\frac{2}{p}\right)$, wobei die Werte für $\left(\frac{-1}{p}\right)$ und $\left(\frac{2}{p}\right)$ mithilfe der Ergänzungssätze schnell ermittelt werden können. Zusätzlich verwendet man die Tatsache, dass das Legendre-Symbol für alle Faktoren $\left(\frac{q}{p}\right)$ gleich 1 ist, wenn q eine Primzahlpotenz mit geradem Exponenten ist. Für die Bestimmung der Werte der Faktoren von der Form $\left(\frac{q}{p}\right)$, wobei q nun eine Primzahlpotenz mit ungeradem Exponenten ist, wird schließlich das Reziprozitätsgesetz angewendet, sodass nach endlich vielen Schritten schlussendlich nur noch Faktoren mit "Zähler" 1, -1 oder 2 übrig bleiben, die leicht berechnet werden können.[10]

5.3 Beweise des quadratischen Reziprozitätsgesetzes

Nachdem das quadratische Reziprozitätsgesetz in den letzten Abschnitten der vorliegenden Arbeit bereits als Theorem formuliert wurde und anhand von mehreren Beispielen auch seine Anwendung verdeutlicht wurde, ist es nun an der Zeit den Fokus auf den Beweis dieser mathematischen Aussage zu legen. Da die Formulierung des quadratischen Reziprozitätsgesetzes schon einige Seiten zurück liegt, wird es an dieser Stelle noch einmal angeführt, sodass klar ist, was in den nächsten Ausführungen gezeigt werden soll:

Satz 5.2 (Quadratisches Reziprozitätsgesetz)**.** *Es seien $p, q \in \mathbb{P} \setminus \{2\}$ mit $p \neq q$. Dann gilt: $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$*
Dies ist gleichbedeutend mit:

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, *wenn* $p \equiv 1 \pmod 4$ *oder* $q \equiv 1 \pmod 4$
- $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, *wenn* $p \equiv q \equiv 3 \pmod 4$

Wie bereits erwähnt existiert jedoch nicht "der eine Beweis" des quadratischen Reziprozitätsgesetzes, sondern es herrscht eine Koexistenz einer Vielzahl

an Beweisen, die auf unterschiedlichen Beweisideen und mathematischen Grundgerüsten basieren. Da die Wiedergabe aller bisher bekannten Beweise des Reziprozitätsgesetzes den Rahmen einer Masterarbeit bei weitem sprengen würde, werden im Folgenden nur zwei ausgewählte Beweise behandelt. Beweise, die an dieser Stelle nicht erwähnt werden, jedoch deshalb nicht weniger interessant beziehungsweise eindrucksvoll sind, können beispielsweise in den Werken von Pieper (1978, [6]) und Lemmermeyer (2000, [4]) nachgelesen werden.

5.3.1 Beweis 1: Gitterpunkte

Der erste Beweis der Tatsache $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ basiert auf dem im Jahr 1844 veröffentlichten Beweis des Mathematikers Ferdinand Gotthold Eisenstein, der ihn seinerzeit unter dem Namen "geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste" veröffentlichte. Ein Kernelement dieses Beweises ist dabei das Lemma von Gauß (Satz 4.6). Heute zählt dieser Beweis zu den am weitesten verbreitetsten Beweisen des quadratischen Reziprozitätsgesetzes und kann daher (in leicht abgeänderter Form) in einer Vielzahl an Publikationen, die sich mit quadratischen Kongruenzgleichungen auseinandersetzen, vorgefunden werden. Die nun folgende Darlegung des Beweises orientiert sich dabei an der Beweisführung von Remmert und Ullrich [10] sowie der von Hölzle [1].

Beweis. Das Lemma von Gauß besagt:

- $\left(\frac{p}{q}\right) = (-1)^{\gamma_q(p)}$ und
- $\left(\frac{q}{p}\right) = (-1)^{\gamma_p(q)}$

und daher ist $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\gamma_q(p)+\gamma_p(q)}$, wobei $\gamma_q(p)$ und $\gamma_p(q)$ die Anzahl der negativen absolut kleinsten Reste modulo q bzw. p ist. Dh.$\gamma_q(p)$ bzw. $\gamma_p(q)$ gibt die Anzahl der Elemente der Menge

$$\left\{1 \cdot p, 2 \cdot p, \ldots, \frac{q-1}{2} \cdot p\right\} \quad bzw. \quad \left\{1 \cdot q, 2 \cdot q, \ldots, \frac{p-1}{2} \cdot q\right\}$$

an, deren absolut kleinster Rest bei Division durch q bzw. p negativ ist.
Wendet man das Lemma von Gauß auf die Formulierung des quadratischen Reziprozitätsgesetzes an, so muss für den Beweis des Reziprozitätsgesetzes die Gleichheit

$$(-1)^{\gamma_q(p)+\gamma_p(q)} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

gezeigt werden. Diese Gleichheit ist genau dann erfüllt, wenn gilt:

$$\frac{1}{2} \cdot (p-1) \cdot \frac{1}{2} \cdot (q-1) = \gamma_q(p) + \gamma_p(q) + 2 \cdot \delta \text{ mit } \delta \in \mathbb{Z} \tag{5.1}$$

Um die Gültigkeit der Gleichung 5.1 zu zeigen, werden zuerst die Zahlen $\gamma_q(p)$ und $\gamma_p(q)$ genauer betrachtet und auf eine andere Art und Weise beschrieben: Es sei $S^+ = \{1, 2, \ldots, \frac{p-1}{2}\}$. Per Definition ist $\gamma_p(q)$ die Anzahl derjenigen Zahlen $q \cdot s$ mit $s \in S^+$, die einen negativen absolut kleinsten Rest bei Division durch p aufweisen. Formal betrachtet, sind dies genau diejenigen Zahlen $q \cdot s$ mit $s \in S^+$, für die es ein $t \in \mathbb{Z}$ gibt, sodass gilt:

$$-\frac{1}{2} \cdot p < q \cdot s - p \cdot t < 0$$

In dieser Ungleichungskette ist die Zahl t, sofern sie überhaupt existiert, eindeutig durch s bestimmt. Es gilt stets $t > 0$ und wegen $s < \frac{1}{2} \cdot p$ gilt weiters:

$$\begin{aligned}
& -\frac{1}{2} \cdot p < q \cdot s - p \cdot t && | + p \cdot t \\
\iff \quad & -\frac{1}{2} \cdot p + p \cdot t < q \cdot s && | + \frac{1}{2} \cdot p \\
\iff \quad & p \cdot t < q \cdot s + \frac{1}{2} \cdot p \\
\implies \quad & p \cdot t < q \cdot (\frac{1}{2} \cdot p) + \frac{1}{2} \cdot p \\
\iff \quad & p \cdot t < \frac{1}{2} \cdot p \cdot (q+1) \\
\iff \quad & t < \frac{1}{2}(q+1) \\
\iff \quad & t \leq \frac{1}{2}(q-1)
\end{aligned}$$

Die Zahl t ist also, sofern sie existiert, ein Element der Menge $1, 2, \ldots, \frac{q-1}{2}$. Damit folgt nun:
Die Zahl $\gamma_p(q)$ ist genau die Anzahl der Paare (s, t) natürlicher Zahlen, für die gilt:

a)
$$1 \leq s \leq \frac{1}{2} \cdot (p-1),\ 1 \leq t \leq \frac{1}{2} \cdot (q-1),\ -\frac{1}{2} \cdot p < q \cdot s - p \cdot t < 0$$

Analog erhält man, dass die Zahl $\gamma_q(p)$ genau die Anzahl der Paare (u, v) natürlicher Zahlen ist, für die gilt:

$$1 \leq u \leq \frac{1}{2} \cdot (q-1),\ 1 \leq v \leq \frac{1}{2} \cdot (p-1),\ -\frac{1}{2} \cdot q < p \cdot u - q \cdot v < 0$$

Ersetzt man v durch s und u durch t und formt die letzte Ungleichung entsprechend um, erhält man:

b)
$$1 \leq t \leq \frac{1}{2} \cdot (q-1),\ 1 \leq s \leq \frac{1}{2} \cdot (p-1),\ 0 < q \cdot s - p \cdot t < \frac{1}{2} \cdot q$$

Verbindet man diese Erkenntnisse, so ergibt sich:
Die Zahl $\gamma_q(p) + \gamma_p(q)$ ist genau die Anzahl der Paare (s,t) natürlicher Zahlen, für die gilt:

c)

$$1 \leq s \leq \frac{1}{2} \cdot (p-1),\ 1 \leq t \leq \frac{1}{2} \cdot (q-1),\ -\frac{1}{2} \cdot p < q \cdot s - p \cdot t < \frac{1}{2} \cdot q$$

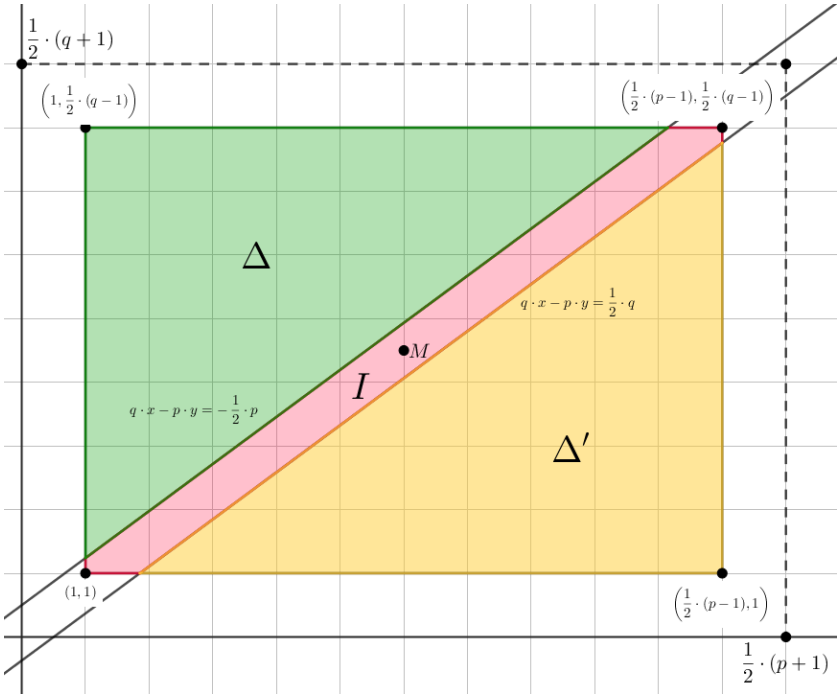
Es ist dabei offensichtlich, dass die $\gamma_p(q)$ Paare, die a) erfüllen, und die $\gamma_q(p)$ Paare, die b) erfüllen, jeweils auch die Ungleichungen aus c) erfüllen. Da die Menge der Zahlenpaare, die a) erfüllen, disjunkt zur Menge der Zahlenpaare, die b) erfüllen, ist (siehe Ungleichungskette) kann gefolgert werden, dass die Anzahl der Paare, die c) erfüllen, mindestens $\gamma_q(p) + \gamma_p(q)$ ist. Außer diesen $\gamma_q(p) + \gamma_p(q)$ Paaren kann es aber kein weiteres Paar (s', t') geben, das c) erfüllt, denn dann müsste $q \cdot s' - p \cdot t' = 0$ gelten. Dann gilt jedoch:

$$\begin{aligned}
& q \cdot s' - p \cdot t' = 0 && \\
\Longleftrightarrow & q \cdot s' = p \cdot t' && \mid : q \\
\Longleftrightarrow & s' = \frac{p \cdot t'}{q} && \mid : t' \\
\Longleftrightarrow & \frac{s'}{t'} = \frac{p}{q} && \text{mit } 1 \leq t' \leq \frac{1}{2} \cdot (q-1)
\end{aligned}$$

Das ist jedoch nicht möglich, da der Bruch $\frac{p}{q}$ bereits reduziert ist, da $p, q \in \mathbb{P}$ und daher nicht mit kleineren Zahlen t' und s' dargestellt werden kann. Daraus folgt also, dass c) von genau $\gamma_q(p) + \gamma_p(q)$ Paaren (s,t) erfüllt wird.
Deutet man die Ungleichungen aus c) nun geometrisch, so beschreiben die $\gamma_q(p) + \gamma_p(q)$ Paare, die c) genügen, genau die Anzahl der Gitterpunkte mit ganzzahligen Koordinaten in der reellen $x-y$-Ebene, die sowohl im abgeschlossenen Rechteck R mit den Eckpunkten $(1,1), (\frac{1}{2} \cdot (p-1), 1), (\frac{1}{2} \cdot (p-1), \frac{1}{2} \cdot (q-1))$ und $(1, \frac{1}{2} \cdot (q-1))$ als auch im Inneren des Streifens, der von den beiden parallelen Geraden $q \cdot x - p \cdot y = -\frac{1}{2} \cdot p$ und $q \cdot x - p \cdot y = \frac{1}{2} \cdot q$ gebildet wird, liegen. Die dadurch entstehende Menge wird mit I bezeichnet und es gilt:
Die Anzahl der Gitterpunkte mit ganzzahligen Koordinaten (s,t) im Rechteck R ist genau $\frac{1}{2} \cdot (p-1) \cdot \frac{1}{2} \cdot (q-1)$, da $1 \leq s \leq \frac{1}{2} \cdot (p-1)$ und $1 \leq t \leq \frac{1}{2} \cdot (q-1)$ gilt. Weiters kann festgestellt werden, dass R die Vereinigung der Menge I mit den beiden abgeschlossenen Dreiecksflächen Δ und Δ' ist. Das bedeutet $R = I \cup \Delta \cup \Delta'$, wobei diese drei Mengen paarweise disjunkt sind. Wird die Anzahl der Gitterpunkte in Δ bzw. Δ' nun mit δ bzw. δ' bezeichnet, so ergibt

sich:

$$\frac{1}{2} \cdot (p-1) \cdot \frac{1}{2} \cdot (q-1) = \gamma_p(q) + \gamma_q(p) + \delta + \delta'$$



Um zu zeigen, dass in den beiden Dreiecksflächen gleich viele Gitterpunkte liegen und somit die Gleichung 5.1 gilt, muss nun also noch gezeigt werden, dass $\delta = \delta'$ gilt. Anschaulich ist sofort erkennbar, dass diese Tatsache gilt, da die beiden Flächen Δ und Δ' symmetrisch zum Mittelpunkt M des Rechtecks R liegen, der die Koordinaten $\left(\frac{\frac{p+1}{2}}{2}), \frac{\frac{q+1}{2}}{2}\right) = \left(\frac{p+1}{4}, \frac{q+1}{4}\right)$ hat. Dies wird umso besser sichtbar, wenn man anstelle des Rechtecks R das in jeder Koordinatenrichtung um 1 vergrößerte Rechteck $R' = \{(x,y) \in \mathbb{R}^2 : 0 \leq x \leq \frac{1}{2} \cdot (p+1), 0 \leq y \leq \frac{1}{2} \cdot (q+1)\}$ betrachtet.
Um sich auch rechnerisch von der Tatsache $\Delta = \Delta'$ bzw. $\delta = \delta'$ zu überzeugen, betrachtet man nun die Abbildung σ mit:

$$\sigma : \mathbb{R}^2 \longrightarrow \mathbb{R}^2,\ (x,y) \longmapsto \left(\frac{1}{2} \cdot (p+1) - x, \frac{1}{2} \cdot (q+1) - y\right)$$

Durch diese bijektive Abbildungsforschrift mit $\sigma^{-1} = \sigma$ ist die Spiegelung am Mittelpunkt M des Rechtecks beschrieben. Nun muss noch gezeigt werden, jeder Punkt $(x,y) \in \Delta$ durch σ auf einen Punkt $(x',y') \in \Delta'$ abgebildet wird:
Die Gitterpunkte (x,y) aus Δ erfüllen folgende Eigenschaften:

$$1 \leq x \leq \frac{1}{2} \cdot (p-1),\ 1 \leq y \leq \frac{1}{2} \cdot (q-1),\ q \cdot x - p \cdot y \leq -\frac{1}{2} \cdot p$$

Die Anwendung von σ liefert zusätzlich

$$x' = \frac{1}{2} \cdot (p+1) - x,\ y' = \frac{1}{2} \cdot (q+1) - y$$

und

$$\begin{aligned} & q \cdot x' - p \cdot y' \\ =& \frac{1}{2} \cdot q \cdot p + \frac{1}{2} \cdot q - q \cdot x - \frac{1}{2} \cdot q \cdot p - \frac{1}{2} \cdot p + p \cdot y \\ =& \frac{1}{2} \cdot q - \frac{1}{2} \cdot p - (q \cdot x - p \cdot y) \end{aligned}$$

und daher erhält man für die Eigenschaften von x', y' und $q \cdot x' - p \cdot y'$ durch das Einsetzen der Bedingungen für x, y und $q \cdot x - p \cdot y$ in die Abbildungsvorschrift von σ folgende Ungleichungen:

$$1 \leq x' \leq \frac{1}{2} \cdot (p-1),\ 1 \leq y' \leq \frac{1}{2} \cdot (q-1),\ q \cdot x' - p \cdot y' \geq \frac{1}{2} \cdot q$$

Somit ist liegen die Gitterpunkte (x', y') in Δ' und die Tatsache $\sigma(\Delta) \subset \Delta'$ ist gezeigt. Analog kann $\sigma(\Delta') \subset \Delta$ gezeigt werden. Aufgrund von $\sigma^{-1} = \sigma$ folgt hieraus sofort $\Delta' \subset \sigma(\Delta)$, sodass man insgesamt folgendes erhält:

$$\sigma(\Delta) = \Delta' \text{ und } \sigma(\Delta') = \Delta$$

Die Spiegelung σ bildet Δ daher tatsächlich bijektiv auf Δ' ab (bzw. Δ' auf Δ). Da p und q ungerade sind, werden Gitterpunkte stets auf Gitterpunkte abgebildet. Insbesondere werden daher die δ Gitterpunkte von Δ bijektiv auf die δ' Gitterpunkte von Δ' abgebildet. Daher gilt $\delta = \delta'$ wodurch die Gleichung 5.1 schlussendlich bewiesen ist. [10] □

5.3.2 Beweis 2: Lemma von Gauß

Die Beweisidee eines weiteren Beweises des quadratischen Reziprozitätsgesetzes stammt von Carl Friedrich Gauß und stellt somit einen der acht von Gauß publizierten Beweise des Gesetzes dar. Inhaltlich bezieht sich der Beweis ebenfalls auf die Erkenntnisse des Lemmas von Gauß (Satz 4.6), weshalb dieses sowie zwei daraus resultierende Hilfssätze in der folgenden Auseinandersetzung zunächst noch einmal näher betrachtet werden, bevor aus den dadurch gewonnen Erkenntnissen schließlich der Beweis des Reziprozitätsgesetzes folgt. Die Darlegung dieser Schritte basiert dabei am Werk von Pieper (1978) [6].

Wie im Kapitel 4.1 bereits beschrieben wurde, liefert das Lemma von Gauß eine Möglichkeit um für ein vorgegebenes $p \in \mathbb{P}$ zu entscheiden, welche primen

Restklassen a modulo p quadratische Reste bzw. Nichtreste modulo p sind. Das Lemma kann überdies jedoch auch herangezogen werden um herauszufinden, von welchen Primzahlen $p > 2$ eine vorgegebene Zahl a mit $p \nmid a$ quadratischer Rest ist. Die folgenden Beispiele werden zeigen, wie diese Fragestellung für verschiedene $a \in \mathbb{N} \setminus \{0\}$ konkret gelöst werden kann.

Beispiel (1). Es sei $a = 2$. Um zu bestimmen, für welche Primzahlen $p > 2$ die Zahl 2 ein quadratischer Rest ist, genügt es laut dem Lemma von Gauß (Satz 4.6) die Anzahl der negativen Minimalreste der Zahlen $1 \cdot 2, 2 \cdot 2, \ldots, \frac{p-1}{2} \cdot 2 = 2, 4, \ldots, p-1$ modulo p zu bestimmen. Offenbar haben unter diesen Zahlen genau die Zahlen $> \frac{1}{2} \cdot p$ einen negativen Minimalrest. Es ist daher ausreichend zu überprüfen, welche Zahlen der Form $2 \cdot k$ die Ungleichungskette $\frac{1}{2} \cdot p < 2 \cdot k < p$ erfüllen. Zur Vereinfachung der folgenden Überlegungen wird die Ungleichungskette umgeformt:

$$\frac{1}{2} \cdot p < 2 \cdot k < p \Longleftrightarrow \frac{1}{4} \cdot p < k < \frac{1}{2} \cdot p$$

Da jede Primzahl $p > 2$ als $p = 8 \cdot m + r$ mit $r = 1, 3, 5, 7$ geschrieben werden kann, ist dies äquivalent zu

$$2 \cdot m + \frac{1}{4} \cdot r < k < 4 \cdot m + \frac{1}{2} \cdot r$$

Im nächsten Schritt muss nun die Anzahl der natürlichen Zahlen k bestimmt werden, die diese Ungleichung erfüllen, wobei es ausreichend ist zu bestimmen, ob diese Anzahl gerade oder ungerade ist (denn damit ist bereits das Vorzeichen von $\gamma_p(2)$ und somit $\left(\frac{2}{p}\right)$ festgelegt). Dabei ist es trivial, dass zwischen $\frac{1}{4} \cdot r$ und $\frac{1}{2} \cdot r$ genau gleich viele ganze Zahlen liegen, wie zwischen $4 \cdot m + \frac{1}{4} \cdot r < k < 4 \cdot m + \frac{1}{2} \cdot r$. Weiters ist klar, dass zwischen $2 \cdot m + \frac{1}{4} \cdot r$ und $4 \cdot m + \frac{1}{4} \cdot r$ genau $2 \cdot m$ natürliche Zahlen liegen. Daher gilt: Ist die Anzahl der Zahlen k , die zwischen $\frac{1}{4} \cdot r$ und $\frac{1}{2} \cdot r$ liege gerade (ungerade), so ist auch die Anzahl der Zahlen k zwischen $2 \cdot m + \frac{1}{4} \cdot r$ und $4 \cdot m + \frac{1}{2} \cdot r$ gerade (ungerade). Folglich ist es ausreichend die Ungleichung $\frac{1}{4} \cdot r < k < \frac{1}{2} \cdot r$ näher zu betrachten, um eine Entscheidung über die Anzahl der negativen Minimalreste zu treffen:

- $r = 1$: Im Intervall $\frac{1}{4} < k < \frac{1}{2}$ liegt keine natürliche Zahl $\Longrightarrow$ Anzahl ist gerade
- $r = 3$: Im Intervall $\frac{3}{4} < k < \frac{3}{2}$ liegt eine natürliche Zahl $\Longrightarrow$ Anzahl ist ungerade
- $r = 5$: Im Intervall $\frac{5}{4} < k < \frac{5}{2}$ liegt eine natürliche Zahl $\Longrightarrow$ Anzahl ist ungerade

- $r = 7$: Im Intervall $\frac{7}{4} < k < \frac{7}{2}$ liegen zwei natürliche Zahlen $\Longrightarrow$ Anzahl ist gerade

Mithilfe des Lemmas von Gauß folgt somit dass

- 2 ist ein quadratischer Rest für $p \equiv 1 \pmod 8$ und $p \equiv 7 \pmod 8$
- 2 ist ein quadratischer Nichtrest für $p \equiv 3 \pmod 8$ und $p \equiv 5 \pmod 8$

Die dadurch gezeigte Eigenschaft für $a = 2$ entspricht dem zweiten Ergänzungssatz der in Abschnitt 4.3.1 bereits auf eine ähnliche Art und Weise bewiesen wurde.

Beispiel (2). Es sei nun $a = 3$. Um die Primzahlen p zu finden, für die 3 ein quadratischer Rest ist, wird analog zu Beispiel 1 die Anzahl der negativen Minimalreste der Zahlen $3, 6, \ldots, 3 \cdot \frac{p-1}{2}$ $(< \frac{3}{2} \cdot p)$ modulo p bestimmt. Offenbar haben unter diesen Zahlen genau die Zahlen $> \frac{p}{2}$ und $< p$ einen negativen Minimalrest. Es muss daher überprüft werden, wie viele Zahlen der Form $3 \cdot k$ die Ungleichung $\frac{1}{2} \cdot p < 3 \cdot k < p$ bzw. $\frac{1}{6} \cdot p < k < \frac{1}{3} \cdot p$ erfüllen.
Da jede Primzahl $p > 3$ als $p = 12 \cdot m + r$ mit $r = 1, 5, 7, 11$ geschrieben werden kann, ist dies äquivalent zu

$$2 \cdot m + \frac{1}{6} \cdot r < k < 4 \cdot m + \frac{1}{3} \cdot r$$

Aufgrund der Überlegungen von Beispiel 1, ist es ausreichend die Ungleichung $\frac{1}{6} \cdot r < k < \frac{1}{3} \cdot r$ näher zu betrachten, um die Anzahl der Zahlen k mit negativem Minimalrest zu bestimmen:

- $r = 1$: Im Intervall $\frac{1}{6} < k < \frac{1}{3}$ liegt keine natürliche Zahl $\Longrightarrow$ Anzahl ist gerade
- $r = 5$: Im Intervall $\frac{5}{6} < k < \frac{5}{3}$ liegt eine natürliche Zahl $\Longrightarrow$ Anzahl ist ungerade
- $r = 7$: Im Intervall $\frac{7}{6} < k < \frac{7}{3}$ liegt eine natürliche Zahl $\Longrightarrow$ Anzahl ist ungerade
- $r = 11$: Im Intervall $\frac{11}{6} < k < \frac{11}{3}$ liegen zwei natürliche Zahlen $\Longrightarrow$ Anzahl ist gerade

Mithilfe des Lemmas von Gauß folgt somit dass

- 3 ist ein quadratischer Rest für $p \equiv 1 \pmod{12}$ und $p \equiv 11 \pmod{12}$
- 3 ist ein quadratischer Nichtrest für $p \equiv 5 \pmod{12}$ und $p \equiv 7 \pmod{12}$

Beispiel (3). Zuletzt sei $a = 5$. Wie zuvor ist es das Ziel, die Anzahl der negativen Minimalreste der Zahlen $5, 10, \ldots, 5 \cdot \frac{p-1}{2} (< \frac{5}{2} \cdot p)$ modulo p zu bestimmen. Wie bereits in den vorhergehenden Abschnitten der Arbeit thematisiert wurde, entspricht jede dieser Zahlen eine der Restklassen $-\frac{p-1}{2}, \ldots -1, 1, \ldots, \frac{p-1}{2}$. Daran kann nun erkannt werden, dass genau die Zahlen $> \frac{p}{2}$ und $< p$ sowie die Zahlen $> \frac{3}{2} \cdot p$ und $< 2 \cdot p$ einen negativen Minimalrest modulo p besitzen. Es muss daher überprüft werden, wie viele Zahlen der Form $5 \cdot k$ die Ungleichungen $\frac{1}{2} \cdot p < 5 \cdot k < p$ und $\frac{3}{2} \cdot p < 5 \cdot k < 2 \cdot p$ bzw. $\frac{1}{10} \cdot p < k < \frac{1}{5} \cdot p$ und $\frac{3}{10} \cdot p < k < \frac{2}{5} \cdot p$ erfüllen.
Da jede Primzahl $p \in \mathbb{P} \setminus \{2, 5\}$ als $p = 20 \cdot m + r$ mit $r = 1, 3, 7, 9, 11, 13, 17, 19$ geschrieben werden kann, ist dies äquivalent zu

$$2 \cdot m + \frac{1}{10} \cdot r < k < 4 \cdot m + \frac{1}{5} \cdot r$$

und

$$6 \cdot m + \frac{3}{10} \cdot r < k < 8 \cdot m + \frac{2}{5} \cdot r$$

Aufgrund der Überlegungen von vorhin, ist es wieder ausreichend die Ungleichungen $\frac{1}{10} \cdot r < k < \frac{1}{5} \cdot r$ und $\frac{3}{10} \cdot r < k < \frac{2}{5} \cdot r$ zu betrachten, um die Anzahl der Zahlen k mit negativem Minimalrest zu bestimmen.

r	Intervall	Anzahl der k	Intervall	Anzahl der k	Gesamtanzahl
1	$\frac{1}{10} < k < \frac{1}{5}$	0	$\frac{3}{10} < k < \frac{2}{5}$	0	0
3	$\frac{3}{10} < k < \frac{3}{5}$	0	$\frac{9}{10} < k < \frac{6}{5}$	1	1
7	$\frac{7}{10} < k < \frac{7}{5}$	1	$\frac{21}{10} < k < \frac{14}{5}$	0	1
9	$\frac{9}{10} < k < \frac{9}{5}$	1	$\frac{27}{10} < k < \frac{18}{5}$	1	2
11	$\frac{11}{10} < k < \frac{11}{5}$	1	$\frac{33}{10} < k < \frac{22}{5}$	1	2
13	$\frac{13}{10} < k < \frac{13}{5}$	1	$\frac{39}{10} < k < \frac{26}{5}$	2	3
17	$\frac{17}{10} < k < \frac{17}{5}$	2	$\frac{51}{10} < k < \frac{34}{5}$	1	3
19	$\frac{19}{10} < k < \frac{19}{5}$	2	$\frac{57}{10} < k < \frac{38}{5}$	2	4

Mithilfe des Lemmas von Gauß folgt somit dass

- 5 ist ein quadratischer Rest für $p \equiv 1 \pmod{20}$, $p \equiv 9 \pmod{20}$, $p \equiv 11 \pmod{20}$ und $p \equiv 19 \pmod{20}$
- 5 ist ein quadratischer Nichtrest für $p \equiv 3 \pmod{20}$, $p \equiv 7 \pmod{20}$, $p \equiv 13 \pmod{20}$ und $p \equiv 17 \pmod{20}$

Anhand dieser drei Beispiele ist erkennbar, dass:

- die Entscheidung ob 2 ein quadratischer Rest modulo einer Primzahl p ist, vom Rest r_2 abhängt, der entsteht wenn p durch $p = 8 \cdot m + r_2$ dargestellt wird.
- die Entscheidung ob 3 ein quadratischer Rest modulo einer Primzahl p ist, vom Rest r_3 abhängt, der entsteht wenn p durch $p = 12 \cdot m + r_3$ dargestellt wird.
- die Entscheidung ob 5 ein quadratischer Rest modulo einer Primzahl p ist, vom Rest r_5 abhängt, der entsteht wenn p durch $p = 20 \cdot m + r_2$ dargestellt wird.

Diese Argumentation kann klarerweise auch für andere Zahlen $a \in \mathbb{N} \setminus \{0\}$ analog geführt werden. Insgesamt ergibt sich aus diesen Erkenntnissen der erste Hilfssatz, der später im Beweis des Reziprozitätsgesetzes zur Anwendung kommen wird.

Satz 5.3 (Hilfssatz 1)**.** *Es sei $p \in \mathbb{P}, p > 2$ und $a \in \mathbb{N} \setminus \{0\}$ mit $p \nmid a$.*
Ob a ein quadratischer Rest modulo p ist, ist von der Restklasse von p modulo $4 \cdot a$ abhängig.

Des Weiteren wird anhand der angeführten Beispiele auch sichtbar, dass

- Die Zahl $a = 2$ hat für $p \equiv r_2 \pmod 8$ und $p' \equiv 8 - r_2 \pmod 8$ dasselbe quadratische Restverhalten:
  Für $p \equiv 1 \pmod 8$ und $p' \equiv 8 - 1 \pmod 8$ ist 2 jeweils quadratischer Rest.
  Für $p \equiv 3 \pmod 8$ und $p' \equiv 8 - 3 \pmod 8$ ist 2 jeweils quadratischer Nichtrest.
- Die Zahl $a = 3$ hat für $p \equiv r_3 \pmod{12}$ und $p' \equiv 12 - r_3 \pmod{12}$ dasselbe quadratische Restverhalten:
  Für $p \equiv 1 \pmod{12}$ und $p' \equiv 12 - 1 \pmod{12}$ ist 3 jeweils quadratischer Rest.
  Für $p \equiv 5 \pmod{12}$ und $p' \equiv 12 - 5 \pmod{12}$ ist 3 jeweils quadratischer Nichtrest.
- Die Zahl $a = 5$ hat für $p \equiv r_5 \pmod{20}$ und $p' \equiv 20 - r_5 \pmod{20}$ dasselbe quadratische Restverhalten:
  Für $p \equiv 1 \pmod{20}$ und $p' \equiv 20 - 1 \pmod{20}$ ist 5 jeweils quadratischer Rest.
  Für $p \equiv 9 \pmod{20}$ und $p' \equiv 20 - 9 \pmod{20}$ ist 2 jeweils quadratischer Rest.
  Für $p \equiv 3 \pmod{20}$ und $p' \equiv 20 - 3 \pmod{20}$ ist 5 jeweils quadratischer Nichtrest.

Für $p \equiv 7 \pmod{20}$ und $p' \equiv 20 - 7 \pmod{20}$ ist 5 jeweils quadratischer Nichtrest.

Auch diese Aussage kann für andere Zahlen $a \in \mathbb{N} \setminus \{0\}$ analog formuliert werden. Durch eine Verallgemeinerung ergibt sich daraus dann schließlich Hilfssatz 2.

Satz 5.4 (Hilfssatz 2)**.** *Es seien $p, p' \in \mathbb{P}$ mit $p, p' > 2$ und $a \in \mathbb{N} \setminus \{0\}$ mit $p \nmid a$ und $p' \nmid a$.*
Gilt $p \equiv r \pmod{4 \cdot a}$ und $p' \equiv 4 \cdot a - r \equiv -r \pmod{4 \cdot a}$, dann hat a für p und p' dasselbe quadratische Restverhalten. Formal bedeutet das: $\left(\frac{a}{p}\right) = \left(\frac{a}{p'}\right)$

Bevor das quadratische Reziprozitätsgesetz basierend auf den beiden Hilfssätzen bewiesen werden kann, muss zuerst überprüft werden, dass diese Sätze tatsächlich für beliebige $a \in \mathbb{N} \setminus \{0\}$ gültig sind.

Beweis der Hilfssätze . Um die beiden Aussagen zu beweisen, werden die Vielfachen $a \cdot k$ mit $k = 1, 2, \ldots, \frac{p-1}{2}$ von a betrachtet. Ziel ist es, die Anzahl der negativen Minimalreste modulo p der Zahlen $a \cdot k$ zu bestimmen. Jede Zahl $a \cdot k$ ist dabei, wie in Abschnitt 4.1 gezeigt wurde, kongruent zu einer der Zahlen $-\frac{p-1}{2}, \ldots -1, 1, \ldots, \frac{p-1}{2}$. Daraus ergibt sich, dass alle Zahlen $a \cdot k$, die eine der folgenden Eigenschaften erfüllen, einen negativen Minimalrest aufweisen.

- $\frac{1}{2} \cdot p < a \cdot k < p$
- $\frac{3}{2} \cdot p < a \cdot k < 2 \cdot p$
- $\frac{5}{2} \cdot p < a \cdot k < 3 \cdot p$
  $\vdots$
- $(b - \frac{1}{2}) \cdot p < a \cdot k < b \cdot p$, wobei $b = \frac{1}{2} \cdot a$ falls a gerade ist und $b = \frac{1}{2} \cdot (a-1)$, falls a ungerade ist

Somit ist die Anzahl der Zahlen k gesucht, für die

- $\frac{p}{2a} < k < \frac{p}{a}$ oder
- $\frac{3 \cdot p}{2 \cdot a} \cdot p < k < \frac{2 \cdot p}{a}$ oder
  $\vdots$
- $\frac{(2 \cdot b - 1) \cdot p}{2 \cdot a} < k < \frac{b \cdot p}{a}$

gilt. Da $p \equiv r \pmod{4 \cdot a}$ gilt, kann man in diesen Ungleichungen $p = 4 \cdot a \cdot m + r$ setzen, wobei $0 < r < 4 \cdot a$ gilt. Daraus entstehen die folgenden zu untersuchenden Ungleichungen:

- $2 \cdot m + \frac{r}{2 \cdot a} < k < 4 \cdot m + \frac{r}{a}$
- $6 \cdot m + \frac{3 \cdot r}{2 \cdot a} < k < 8 \cdot m + \frac{2 \cdot r}{a}$
  $\vdots$
- $2 \cdot (2 \cdot b - 1) \cdot m + \frac{(2 \cdot b - 1) \cdot r}{2 \cdot a} < k < 4 \cdot b \cdot m + \frac{b \cdot r}{a}$

Da es wie auch in den weiter oben angeführten Beispielen für die Entscheidung ob a ein quadratischer Rest modulo p ist lediglich darauf ankommt, ob die Anzahl der Zahlen k, die diese Intervalle jeweils erfüllen, gerade oder ungerade ist, ist es ausreichend die Ungleichungen

- $\frac{r}{2 \cdot a} < k < \frac{r}{a}$
- $\frac{3 \cdot r}{2 \cdot a} < k < \frac{2 \cdot r}{a}$
  $\vdots$
- $\frac{(2 \cdot b - 1) \cdot r}{2 \cdot a} < k < \frac{b \cdot r}{a}$

einzeln zu untersuchen. Wenn die Gesamtanzahl m der natürlichen Zahlen, die in den Intervallen liegen, gerade ist, dann ist a ein quadratischer Rest modulo p. Ist die Gesamtanzahl m der natürlichen Zahlen, die in diesen Intervallen liegen, ungerade, dann ist a ein quadratischer Nichtrest modulo p. Ob die Gesamtanzahl m der Zahlen in den Intervallen gerade oder ungerade ist, hängt laut den oben angeführten Ungleichungen nun aber einzig und alleine von r, also der Restklasse von p modulo $4 \cdot a$ ab. Daher liefern alle Primzahlen p, die in derselben Restklasse modulo $4 \cdot a$ liegen, die selbe Anzahl von Zahlen, die in den Intervallen liegen. Somit ist Hilfssatz 1 (5.3) bewiesen.
Um die Aussage des zweiten Hilfssatzes zu überprüfen, wird r (mit $0 < r < 4 \cdot a$) in den Ungleichungen nun jeweils durch $4 \cdot a - r$ mit $0 < 4 \cdot a - r < 4 \cdot a$ ersetzt. Dadurch entstehen folgende Ungleichungen:

- $2 - \frac{r}{2 \cdot a} < k < 4 - \frac{r}{a}$
- $6 - \frac{3 \cdot r}{2 \cdot a} < k < 8 - \frac{2 \cdot r}{a}$
  $\vdots$
- $4 \cdot b - 2 - \frac{(2 \cdot b - 1) \cdot r}{2 \cdot a} < k < 4 \cdot b - \frac{b \cdot r}{a}$

Die Gesamtanzahl der Zahlen, die in diesen neuen Intervallen liegen, sei nun m'. Um die Aussage aus Hilfssatz 2 (5.4) zu beweisen, muss nun gezeigt werden, dass $m \equiv m' \pmod 2$ gilt, denn dann sind m und m' entweder beide gerade oder beide ungerade. Dazu werden nun immer zwei einander entsprechende Ungleichungen aus den eben angeführten Systemen an Ungleichungen betrachtet:

Es bezeichne m_1 die Anzahl der ganzen Zahlen k im Intervall $\frac{r}{2\cdot a} < k < \frac{r}{a}$ und m_1' sei die Anzahl der ganzen Zahlen im Intervall $2 - \frac{r}{2\cdot a} < k < 4 - \frac{r}{a}$. Betrachtet man das Intervall $2 - \frac{r}{2\cdot a} < k < 4 - \frac{r}{a}$ genauer, so lässt sich erkennen, dass das Intervall genauso viele ganze Zahlen enthält, wie das Intervall

$$4 - \left(4 - \frac{r}{a}\right) = \frac{r}{a} < k < 4 - \left(2 - \frac{r}{2 \cdot a}\right) = 2 + \frac{r}{2a}$$

da es sich graphisch gesehen lediglich um eine Verschiebung des Intervalls auf der Zahlengerade handelt. Verbindet man nun das Intervall $\frac{r}{2\cdot a} < k < \frac{r}{a}$ mit dem Intervall $\frac{r}{a} < k < 2 + \frac{r}{2a}$, erhält man insgesamt das Intervall $\frac{r}{2\cdot a} < k < 2 + \frac{r}{2a}$ und ein Intervall der Länge 2, das daher exakt zwei ganze Zahlen enthält. Folglich ist $m_1 + m_1' = 2$.
Analog bezeichne nun m_2 die Anzahl der ganzen Zahlen k im Intervall $\frac{3\cdot r}{2\cdot a} < k < \frac{2\cdot r}{a}$ und m_2' sei die Anzahl der ganzen Zahlen im Intervall $6 - \frac{3\cdot r}{2\cdot a} < k < 8 - \frac{2\cdot r}{a}$. Betrachtet man das Intervall $6 - \frac{3\cdot r}{2\cdot a} < k < 8 - \frac{2\cdot r}{a}$ nun genauer, so kann festgestellt werden, dass es gleich viele ganze Zahlen enthält wie das Intervall

$$8 - \left(8 - \frac{2 \cdot r}{a}\right) = \frac{2 \cdot r}{a} < k < 8 - \left(6 - \frac{3 \cdot r}{2 \cdot a}\right) = 2 - \frac{3 \cdot r}{2 \cdot a}$$

da es sich erneut lediglich um eine Verschiebung des Intervalls auf der Zahlengerade handelt. Verbindet man nun die Intervalle $\frac{3\cdot r}{2\cdot a} < k < \frac{2\cdot r}{a}$ und $\frac{2\cdot r}{a} < k < 2 - \frac{3\cdot r}{2\cdot a}$ erhält man erneut ein Intervall der Länge 2. Daher gilt auch $m_2 + m_2' = 2$.
Man verfahre analog weiter so, bis man schließlich bei m_b und m_b' angelangt, wobei m_b die Anzahl der Zahlen k im Intervall $\frac{(2\cdot b-1)\cdot r}{2\cdot a} < k < \frac{b\cdot r}{a}$ und m_b' die Anzahl der Zahlen k im Intervall $4 \cdot b - 2 - \frac{(2\cdot b-1)\cdot r}{2\cdot a} < k < 4 \cdot b - \frac{b\cdot r}{a}$ bezeichne. Betrachtet man wieder das zweite dieser Intervalle genauer, lässt sich erkennen, dass das Intervall gleich viele ganze Zahlen enthält, wie das Intervall

$$\begin{aligned} & 4 \cdot b - \left(4 \cdot b - \frac{b \cdot r}{a}\right) < k < 4 \cdot b - \left(4 \cdot b - 2 - \frac{(2 \cdot b - 1) \cdot r}{2 \cdot a}\right) \\ \iff \quad & \frac{b \cdot r}{a} < k < 2 + \frac{(2 \cdot b - 1) \cdot r}{2 \cdot a} \end{aligned}$$

Werden die beiden Intervalle $\frac{(2\cdot b-1)\cdot r}{2\cdot a} < k < \frac{b\cdot r}{a}$ und $\frac{b\cdot r}{a} < k < 2 + \frac{(2\cdot b-1)\cdot r}{2\cdot a}$ aneinandergereiht entsteht erneut ein Intervall der Länge 2, sodass offensichtlich auch $m_b + m_b' = 2$ gilt.
Insgesamt ist daher $m + m' = m_1 + m_2 + \ldots + m_b + m_1' + m_2' + \ldots + m_b'$ eine gerade Zahl und daher sind die Gesamtanzahlen der ganzen Zahlen mit negativen Minimalresten für $p \equiv r \pmod{4 \cdot a}$ und $p' \equiv 4 \cdot a - r \pmod{4 \cdot a}$ entweder beide gerade oder beide ungerade, was bedeutet, dass a bezüglich p und p' dasselbe quadratische Restverhalten aufweist. Somit ist auch Hilfssatz 2 bewiesen. [6] $\square$

Da die Gültigkeit der beiden Hilfssätz nun gezeigt wurde, kann nun ein vergleichsmäßig kurzer Beweis des quadratischen Reziprozitätsgesetzes, der diese Sätze in seiner Argumentationslinie enthält, dargelegt werden.

Beweis. Das Ziel ist es, zu zeigen, dass für zwei Primzahlen p und q mit $p \neq q, p > q$ stets folgendes gilt:

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, wenn $p \equiv 1 \pmod 4$ oder $q \equiv 1 \pmod 4$
- $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, wenn $p \equiv q \equiv 3 \pmod 4$

Im folgenden Beweis wird zwischen zwei unterschiedlichen Fällen unterschieden, wobei die Fallunterscheidungen auf den Restklassen der Zahlen p und q modulo 4 basieren:
Fall 1: Es sein p und q Elemente derselben Restklasse modulo 4, dh. entweder beide kongruent 1 modulo 4 oder beide kongruent 3 modulo 4. Dies ist gleichbedeutend mit

$$p \equiv q \pmod 4 \iff 4 \mid (p-q) \iff p - q = 4 \cdot a$$

für eine Zahl $a \in \mathbb{N} \setminus \{0\}$ Dann folgt mithilfe der Anwendung der Rechenregeln für das Legendre-Symbol:

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

und

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

Da $p \equiv q \pmod{4 \cdot a}$ gilt, und p und q somit in derselben Restklasse modulo $4 \cdot a$ liegen, folgt aus Hilfssatz 1 (Satz 5.3) zusätzlich $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.
Damit folgt nun:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = \left(\frac{a}{q}\right) \cdot \left(\frac{-1}{p}\right) \cdot \left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{wenn } p \equiv q \equiv 1 \pmod 4 \\ -1 & \text{wenn } p \equiv q \equiv -1 \pmod 4 \end{cases}$$

wobei im letzten Schritt der erste Ergänzungssatz (Korollar 4.5) verwendet wurde. Aufgrund dessen ist also $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, wenn $p \equiv q \equiv 1 \pmod 4$ ist und $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, wenn $p \equiv q \equiv 3 \equiv -1 \pmod 4$ ist.
Fall 2: Es sei nun $p \not\equiv q \pmod 4$, das heißt eine Primzahl ist kongruent 1 und

eine Primzahl ist kongruent 3 modulo 4. Dies ist gleichbedeutend mit

$$p \equiv -q \pmod 4 \iff 4 \mid (p+q) \iff p+q = 4 \cdot a$$

für eine Zahl $a \in \mathbb{N} \setminus \{0\}$. Dann folgt mithilfe der Anwendung der Rechenregeln für das Legendre-Symbol:

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

und

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

Da wegen $p \equiv -q \pmod{4 \cdot a}$ aus $p \equiv r \pmod{4 \cdot a}$ sofort $q \equiv 4 \cdot a - r \equiv -r \pmod{4 \cdot a}$ folgt, gilt nach Hilfssatz 2 (Satz 5.4) zusätzlich $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Damit folgt nun:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = \left(\frac{a}{q}\right) \cdot \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) \cdot \left(\frac{a}{q}\right) = 1$$

Das bedeutet $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, wenn eine Primzahl kongruent 1 modulo 4 ist und die andere Primzahl kongruent 3 modulo 4 ist. Damit ist das quadratische Reziprozitätsgesetz bewiesen. □

6 Jacobi-Symbol

Im abschließenden Kapitel der vorliegenden Masterarbeit soll nun ein kleiner Exkurs gewagt werden. Dazu wird das Legendre-Symbol auf das Jacobi-Symbol erweitert und das quadratische Reziprozitätsgesetz auch für das Jacobische Restsymbol formuliert und beweisen. Die Ausarbeitung orientiert sich dabei am Werk von Remmert und Ullrich (2008) [10].
Die Auseinandersetzung mit dem Jacobischen Restsymbol erweist sich als überaus sinnvoll, da das Restsymbol $\left(\frac{a}{p}\right)$ mit den bisherigen Erkenntnissen nur dann berechnet werden kann, wenn die Zahl a in ihre Primfaktoren zerlegt wird und anschließend das Reziprozitätsgesetz sowie die Ergänzungssätze auf jeden Faktor einzeln angewendet werden. Durch die Erweiterung auf das Jacobi-Symbol $\left(\frac{a}{b}\right)$, wobei b nun nicht nur eine Primzahl sondern auch eine beliebige ungerade Zahl > 1 sein darf, und die Formulierung des Reziprozitätsgesetzes für dieses Restsymbol, ist die Primfaktorzerlegung von a nicht mehr notwendig. Das Verwenden des Jacobischen Restsymbols und seiner Rechenregeln führt also dazu, dass mithilfe von deutlich kürzeren Rechnungen entschieden werden kann, ob a ein quadratischer Rest modulo b ist.

6.1 Erweiterung auf das Jacobi-Symbol

Definition. Es seien $a, b \in \mathbb{Z} \setminus \{0\}$ mit $b \geq 3$, $2 \nmid b$ und $\text{ggT}(a, b) = 1$. Weiters sei die Primfaktorzerlegung von b gegeben durch:

$$b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

Dann ist das Jacobische Restymbol $\left(\frac{a}{b}\right)$ definiert durch:

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \left(\frac{a}{p_2}\right)^{\alpha_2} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{\alpha_k}$$

Bemerkung. Das Jacobi-Symbol nimmt für $\text{ggT}(a, b) = 1$ nur die Werte 1 und -1 an. Dabei gilt:

- Ist $\left(\frac{a}{b}\right) = -1$, dann ist a ein quadratischer Nichtrest modulo b, denn dann ist $\left(\frac{a}{p_l}\right) = -1$ für zumindest einen Index l und somit ist a ein quadratischer Nichtrest modulo p_l und wegen $p_l \mid b$ bzw. Satz 4.1 folgt sofort, dass a auch ein quadratischer Nichtrest modulo b ist.
- Ist $\left(\frac{a}{b}\right) = 1$, dann ist a nun nicht automatisch ein quadratischer Rest modulo b, denn im Produkt $\left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \left(\frac{a}{p_2}\right)^{\alpha_2} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{\alpha_k} = \left(\frac{a}{b}\right)$ hat möglicherweise eine gerade Anzahl von Faktoren den Wert -1.
- Ist b eine Primzahl, so stimmt das Jacobi-Symbol per Definition mit dem Legendre-Symbol überein.

Lemma 6.1 (Rechenregeln für das Jacobi-Symbol)**.** *Es seien $a, a', b, b', c \in \mathbb{Z} \setminus \{0\}$ mit $b \geq 3$, $b' \geq 3$, $2 \nmid b$ und $2 \nmid b'$. Dann gelten folgende Rechenregeln für das Jacobi-Symbol:*

i) $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$, *wenn* $a \equiv a' \pmod{b}$ *und* $\text{ggT}(a, b) = \text{ggT}(a', b) = 1$

ii) $\left(\frac{a \cdot a'}{b}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a'}{b}\right)$, *wenn* $\text{ggT}(a \cdot a', b) = 1$

iii) $\left(\frac{a}{b \cdot b'}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a}{b'}\right)$, *wenn* $\text{ggT}(a, b \cdot b') = 1$

iv) $\left(\frac{a \cdot c^2}{b}\right) = \left(\frac{a}{b}\right)$, *wenn* $\text{ggT}(a \cdot c, b) = 1$

v $\left(\frac{a}{b \cdot c^2}\right) = \left(\frac{a}{b}\right)$, *wenn* $\text{ggT}(a, b \cdot c) = 1$

Beweis. Die Rechenregeln für das Jacobische Restsymbol folgen direkt aus seiner Definition und den Rechenregeln für das Legendre-Symbol. □

Nachdem das Jacobische Restsymbol sowie seine grundlegenden Eigenschaften dargelegt wurden, widmet sich die Auseinandersetzung nun den beiden Ergänzungssätzen und dem quadratischen Reziprozitätsgesetz für das Jacobi-Symbol.

Bevor die Sätze formuliert und beweisen werden, wird zuerst jedoch ein Hilfssatz, der sich als äußerst nützlich erweisen wird, herangezogen.

Satz 6.1 (Hilfssatz)**.** *Für ungerade Zahlen $v, w \in \mathbb{Z}$ gilt:*

i) $\frac{v-1}{2} + \frac{w-1}{2} \equiv \frac{v \cdot w - 1}{2} \pmod 2$

ii) $\frac{v^2-1}{8} + \frac{w^2-1}{8} \equiv \frac{(v \cdot w)^2 - 1}{8} \pmod 8$

Beweis. i) Es sei $v = 2 \cdot k + 1$ und $w = 2 \cdot l + 1$ mit $k, l \in \mathbb{Z}$. Dann ist $v \cdot w - 1 = 4 \cdot k \cdot l + 2 \cdot k + 2 \cdot l$ und es gilt:

$$\frac{v \cdot w - 1}{2} = 2 \cdot k \cdot l + k + l \equiv k + l = \frac{v-1}{2} + \frac{w-1}{2} \pmod 2$$

Damit ist die erste Aussage des Hilfssatzes bereits bewiesen.
ii) Um die zweite Aussage des Hilfssatzes zu beweisen, muss man sich zuerst davon überzeugen, dass stets $v^2 - 1 \equiv 0 \pmod 8$ und $w^2 - 1 \equiv 0 \pmod 8$ gilt. Es ist

$$v^2 = (2 \cdot k + 1)^2 = 4 \cdot k^2 + 4 \cdot k + 1 \iff v^2 - 1 = 4 \cdot k \cdot (k+1)$$

und da das Produkt $k \cdot (k+1)$ mit Sicherheit gerade ist, gilt $2 \mid k \cdot (k+1)$ und aus den Rechenregeln der Teilbarkeit (Satz 2.1 viii)) folgt:

$$4 \cdot 2 \mid 4 \cdot k \cdot (k+1) \iff 8 \mid (v^2 - 1) \iff v^2 - 1 \equiv 0 \pmod 8$$

Analog folgt aus $w^2 - 1 = 4 \cdot l \cdot (l+1)$ und $2 \mid l \cdot (l+1)$ auch

$$4 \cdot 2 \mid 4 \cdot l \cdot (l+1) \iff 8 \mid (w^2 - 1) \iff w^2 - 1 \equiv 0 \pmod 8$$

Aus den Rechenregeln für Kongruenzen (Lemma 3.1 iv)) folgt außerdem, dass statt

$$\frac{v^2-1}{8} + \frac{w^2-1}{8} \equiv \frac{(v \cdot w)^2 - 1}{8} \pmod 8$$

nur die Aussage

$$v^2 - 1 + w^2 - 1 \equiv (v \cdot w)^2 - 1 \pmod{64}$$

gezeigt werden muss. Aus $v^2 - 1 \equiv 0 \pmod 8 \iff v^2 - 1 = 8 \cdot m$ für $m \in \mathbb{Z}$ und $w^2 - 1 \equiv 0 \pmod 8 \iff w^2 - 1 = 8 \cdot n$ für $n \in \mathbb{Z}$ folgt nun sofort

$$\begin{aligned} 8 \cdot m \cdot 8 \cdot n = 64 \cdot m \cdot n =& (v^2 - 1) \cdot (w^2 - 1) \equiv 0 \pmod{64} \\ \iff\ & v^2 \cdot w^2 - v^2 - w^2 + 1 \equiv 0 \pmod{64} \\ \iff\ & v^2 - 1 + w^2 - 1 \equiv (v \cdot w)^2 - 1 \pmod{64} \end{aligned}$$

□

In der Beweisführung der Ergänzungssätze und des Reziprozitätsgesetzes werden die Aussagen durch Induktion nun jeweils auf die entsprechenden Sätze für das Legendre-Symbol zurückgeführt.

Satz 6.2 (Erster Ergänzungssatz)**.** *Für jede ungerade Zahl $b > 2$ gilt:*

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

Beweis. Da $b > 2$ eine ganze Zahl ist, lässt sich b als Produkt von Primzahlen schreiben. Es sei daher $b = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ mit $p_1, p_2, \ldots, p_n \in \mathbb{P}$. Die Aussage des ersten Ergänzungssatzes für das Jacobi-Symbol kann nun mittels Induktion nach n gezeigt werden:
Für $n = 1$ entspricht die Aussage dem ersten Ergänzungssatz des Legendre-Symbols.
Es sei nun $n > 1$. Weiters sei die Behauptung für alle ganzen Zahlen b' mit $n - 1$ Primfaktoren bereits bewiesen. Setzt man nun $b' = p_2 \cdot \ldots \cdot p_n$ so ist $b = p_1 \cdot b'$ und aufgrund der Induktionsvoraussetzung und der Rechenregeln für das Jacobi-Symbol (Satz 6.1 iii)) sowie dem ersten Ergänzungssatzes des Legendre-Symbols folgt:

$$\left(\frac{-1}{b}\right) = \left(\frac{-1}{p_1}\right) \cdot \left(\frac{-1}{b'}\right) = (-1)^{\frac{p_1-1}{2}} \cdot (-1)^{\frac{b'-1}{2}} = (-1)^{\frac{p_1-1}{2}+\frac{b'-1}{2}}$$

Da p_1 und b' ungerade sind, ergibt sich aus dem Hilfssatz sofort

$$\frac{p_1 - 1}{2} + \frac{b' - 1}{2} \equiv \frac{p_1 \cdot b' - 1}{2} = \frac{b-1}{2} \pmod 2$$

und damit die zu beweisende Behauptung. □

Satz 6.3 (Zweiter Ergänzungssatz)**.** *Für jede ungerade Zahl $b > 2$ gilt:*

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

Beweis. Erneut sei $b = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ mit $p_1, p_2, \ldots, p_n \in \mathbb{P}$. Die Aussage kann nun analog zum ersten Ergänzungssatz mittels Induktion nach n gezeigt werden: für $n = 1$ entspricht die Aussage dem zweiten Ergänzungssatz des Legendre-Symbols.
Es sei nun $n > 1$. Weiters sei die Behauptung für alle ganzen Zahlen b' mit $n - 1$ Primfaktoren bereits bewiesen. Setzt man nun wieder $b' = p_2 \cdot \ldots p_n$ so ist $b = p_1 \cdot b'$ und aufgrund der Induktionsvoraussetzung und der Rechenregeln

für das Jacobi-Symbol (Satz 6.1 iii)) sowie dem zweiten Ergänzungssatzes des Legendre-Symbols folgt:

$$\left(\frac{2}{b}\right) = \left(\frac{2}{p_1}\right) \cdot \left(\frac{2}{b'}\right) = (-1)^{\frac{p_1^2-1}{8}} \cdot (-1)^{\frac{b'^2-1}{8}} = (-1)^{\frac{p_1^2-1}{8}+\frac{b'^2-1}{8}}$$

Da p_1 und b' ungerade sind, ergibt sich aus dem Hilfssatz sofort

$$\frac{p_1^2-1}{8} + \frac{b'^2-1}{8} \equiv \frac{(p_1 \cdot b')^2-1}{8} = \frac{b^2-1}{8} \pmod 8$$

und damit die zu beweisende Aussage. □

Da das quadratische Reziprozitätsgesetz für das Legendre-Symbol, die Hauptaussage der vorliegenden Masterarbeit darstellt, wird die Aussage an dieser Stelle nun auch für das Jacobische Restsymbol formuliert.

Satz 6.4. *Es seine $a, b \in \mathbb{N} \setminus \{0\}$ mit $a, b \geq 3$ und $\mathrm{ggT}(a, b) = 1$. Dann gilt:*

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

Beweis. Der Beweis des Reziprozitätsgesetzes basiert erneut auf der Induktion nach n beziehungsweise t. Zusätzlich wird eine Fallunterscheidung vorgenommen:
1. Fall: Es sei $a \in \mathbb{P}$. Weiters sei b eine beliebige ungerade Zahl mit Primfaktorzerlegung $b = p_1 \cdot p_2 \cdot \ldots \cdot p_n$.
Falls $n = 1$ gilt, entspricht die Aussage dem quadratischen Reziprozitätsgesetzes für das Legendre-Symbols und wurde somit schon in einem früheren Kapitel der Arbeit bewiesen.
Es sei nun $n > 1$. Weiters sei die Behauptung für alle ganzen Zahlen b' mit $n-1$ Primfaktoren bereits bewiesen. Setzt man nun wieder $b' = p_2 \cdot \ldots p_n$ so ist $b = p_1 \cdot b'$. Wegen $\mathrm{ggT}(a, b) = 1$ gilt außerdem $\mathrm{ggT}(a, p_1) = \mathrm{ggT}(a, b') = 1$. Aufgrund der Induktionsvoraussetzung und der Rechenregeln für das Jacobi-Symbol (Satz 6.1 ii) und iii)) folgt damit:

$$\begin{aligned}\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) &= \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{b'}\right) \cdot \left(\frac{p_1}{a}\right) \cdot \left(\frac{b'}{a}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{p_1}{a}\right) \cdot \left(\frac{a}{b'}\right) \cdot \left(\frac{b'}{a}\right) \\ &= (-1)^{\frac{a-1}{2} \cdot \frac{p_1-1}{2}} \cdot (-1)^{\frac{a-1}{2} \cdot \frac{b'-1}{2}} = (-1)^{\frac{a-1}{2} \cdot (\frac{p_1-1}{2} + \frac{b'-1}{2})}\end{aligned}$$

Da p_1 und b' ungerade sind, ergibt sich aus dem Hilfssatz sofort

$$\frac{p_1-1}{2} + \frac{b'-1}{2} \equiv \frac{p_1 \cdot b'-1}{2} = \frac{b-1}{2} \pmod 2$$

und damit folgt die Behauptung für b.
Fall 2: Es sei nun $b \geq 3$ eine beliebige vorgegebene ungerade Zahl und a eine

beliebige ungerade Zahl mit $a = q_1 \cdot q_2 \cdot \ldots \cdot q_t$ mit $q_1, q_2, \ldots, q_t \in \mathbb{P}$.
Falls $t = 1$ gilt liegt der Fall 1 eins vor und die Gültigkeit der Aussage ist klar. Es sei nun $t > 1$. Weiters sei die Behauptung für alle Zahlen a' mit $t - 1$ Primfaktoren bereits bewiesen. Setzt man nun $a' = q_2 \cdot \ldots \cdot q_t$ so ist $a = q_1 \cdot a'$. Wegen $\text{ggT}(a, b) = 1$ gilt außerdem $\text{ggT}(q_1, b) = \text{ggT}(a', b) = 1$. Aufgrund der Induktionsvoraussetzung und der Rechenregeln für das Jacobi-Symbol (Satz 6.1 ii) und iii)) folgt damit:

$$\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = \left(\frac{q_1}{b}\right) \cdot \left(\frac{a'}{b}\right) \cdot \left(\frac{b}{q_1}\right) \cdot \left(\frac{b}{a'}\right) = \left(\frac{q_1}{b}\right) \cdot \left(\frac{b}{q_1}\right) \cdot \left(\frac{a'}{b}\right) \cdot \left(\frac{b}{a'}\right)$$
$$= (-1)^{\frac{q_1-1}{2} \cdot \frac{b-1}{2}} \cdot (-1)^{\frac{a'-1}{2} \cdot \frac{b-1}{2}} = (-1)^{(\frac{q_1-1}{2} + \frac{a'-1}{2}) \cdot \frac{b-1}{2}}$$

Da q_1 und a' ungerade sind, ergibt sich aus dem Hilfssatz sofort

$$\frac{q_1 - 1}{2} + \frac{a' - 1}{2} \equiv \frac{q_1 \cdot a' - 1}{2} = \frac{a - 1}{2} \pmod 2$$

und damit folgt die Behauptung für a.

□

6.2 Anwendung des Reziprozitätsgesetzes für das Jacobi-Symbol

In diesem abschließenden Abschnitt der Arbeit soll in Anlehung an Remmert und Ullrich (2008) [10] nun demonstriert werden, wie sich die Bestimmung der Werte des Legendre-Symbols durch die Anwendung des quadratischen Reziprozitätsgesetzes für das Jacobische Restsymbol vereinfacht und daher schneller eine Aussage über die Lösbarkeit der quadratischen Kongruenzgleichung
$x^2 \equiv a \pmod p$ getroffen werden kann.

Beispiel (1). Es soll erneut der Wert des Legendre-Symbols $\left(\frac{35}{281}\right)$ bestimmt werden, diesmal jedoch ohne die Zahl 35 in ihre Primfaktoren zu zerlegen und das Legendre-Symbol für jeden Primfaktor einzeln zu berechnen.
Mithilfe der Erkenntnisse über das Jacobi-Symbol folgt sofort:

$$\left(\frac{35}{281}\right) \cdot \left(\frac{281}{35}\right) = (-1)^{\frac{35-1}{2} \cdot \frac{281-1}{2}}$$
$$\iff \left(\frac{35}{281}\right) = (-1)^{\frac{35-1}{2} \cdot \frac{281-1}{2}} \cdot \left(\frac{281}{35}\right) = (-1)^{17 \cdot 140} \cdot \left(\frac{1}{35}\right) = 1$$

Somit konnte durch die Anwendung des quadratischen Reziprozitätsgesetzes für das Jacobische Restsymbol deutlich schneller gezeigt werden, dass 35 ein quadratischer Rest modulo 281 ist und die Kongruenzgleichung $x^2 \equiv 35 \pmod{281}$ daher lösbar ist.

Beispiel (2). Im nächsten Beispiel soll nun der Wert des Legendre-Symbols $\left(\frac{65}{307}\right)$ bestimmt werden.

$$\left(\frac{65}{307}\right)\cdot\left(\frac{307}{65}\right) = (-1)^{\frac{65-1}{2}\cdot\frac{307-1}{2}} \Longleftrightarrow \left(\frac{65}{307}\right) = (-1)^{\frac{65-1}{2}\cdot\frac{307-1}{2}}\cdot\left(\frac{307}{65}\right)$$
$$= (-1)^{32\cdot 153}\cdot\left(\frac{47}{65}\right) = \left(\frac{47}{65}\right) = 1^{23\cdot 32}\cdot\left(\frac{65}{47}\right) = \left(\frac{18}{47}\right) = \left(\frac{2\cdot 9}{47}\right) = \left(\frac{2}{47}\right)$$

Aus dem zweiten Ergänzungssatz für Jacobische Restsymbol folgt nun:

$$\left(\frac{2\cdot 9}{47}\right) = (-1)^{\frac{47^2-1}{8}} = (-1)^{\frac{46\cdot 48}{8}} = 1$$

Somit wurde mit nur einer Rechnung gezeigt, dass 65 ein quadratischer Rest modulo 307 ist.

Beispiel (3). Das dritte und letzte Beispiel soll nun verdeutlichen, dass das Jacobische Restsymbol auch bei der Bestimmung des Legendre-Symbols von großen Zahlen überaus hilfreich ist. Es soll entschieden werden, ob die quadratische Kongruenz $x^2 \equiv 49337 \pmod{129061}$ lösbar ist. (Dabei gilt $129061 \in \mathbb{P}$ und $\mathrm{ggT}(49337, 129061) = 1$) Bei der Berechnung des Wertes von $\left(\frac{49337}{129061}\right)$ werden sowohl die beiden Ergänzungssätz als auch das quadratische Reziprozitätsgesetz für das Jacobi-Symbol herangezogen.

$$\left(\frac{49337}{129061}\right)\cdot\left(\frac{129061}{49337}\right) = (-1)^{\frac{49337-1}{2}\cdot\frac{129061-1}{2}} \Longleftrightarrow \left(\frac{49337}{129061}\right) = \left(\frac{129061}{49337}\right)$$
$$= \left(\frac{-18950}{49337}\right) = \left(\frac{-1}{49337}\right)\cdot\left(\frac{18950}{49337}\right) = \left(\frac{5^2\cdot 758}{49337}\right) = \left(\frac{758}{49337}\right)$$
$$= \left(\frac{2}{49337}\right)\cdot\left(\frac{379}{49337}\right) = \left(\frac{379}{49337}\right) = \left(\frac{49337}{379}\right) = \left(\frac{67}{379}\right) = (-1)\cdot\left(\frac{379}{67}\right)$$
$$= (-1)\cdot\left(\frac{-23}{67}\right) = \left(\frac{23}{67}\right) = (-1)\cdot\left(\frac{67}{23}\right) = (-1)\cdot\left(\frac{-2}{23}\right) = \left(\frac{2}{23}\right) = 1$$

Literatur

[1] Hölzle A. *Quadratische Reste und das quadratische Reziprozitätsgesetz*. 2007. URL: https://docplayer.org/40371842-Quadratische-reste-und-das-quadratische-reziprozitaetsgesetzt.html (besucht am 20. 05. 2023).

[2] Schüler A. *Quadratische Reste*. Mathematisches Institut: Universität Leipzig, 2003. URL: https://lsgm.uni-leipzig.de/KoSemNet/pdf/schueler-03-1.pdf (besucht am 20. 05. 2023).

[3] Trost E. *Primzahlen*. 2. Aufl. Basel: Springer Basel AG, 1968.

[4] Lemmermeyer F. *Reciprocity Laws: from Euler to Eisenstein*. Berlin: Springer Verlag, 2000.

[5] Aigner M.; Ziegler G. *Das Buch der Beweise*. 5. Aufl. Deutschland: Springer Verlag, 2018.

[6] Pieper H. *Variationen über ein zahlentheoretisches Thema von Carl Friedrich Gauss*. Basel, Stuttgart: Birkenhäuser Verlag, 1978.

[7] Fulmek M. *Vorlesungsskript der VO Zahlentheorie*. 2019. URL: https://www.mat.univie.ac.at/~mfulmek/scripts/ZT/skriptum.pdf (besucht am 20. 05. 2023).

[8] Lohrey M. *Übungsblatt 8*. Hrsg. von Universität Siegen Lehrstuhl Theoretische Informatik. Strukturelle Komplexitätstheorie. 2020/21. URL: https://www.eti.uni-siegen.de/ti/lehre/ws2021/komplexitaetstheorie/comp_08_sol.pdf (besucht am 20. 05. 2023).

[9] Bundschuh P. *Einführung in die Zahlentheorie*. 6. Aufl. Berlin, Heidelberg: Springer Verlag, 2008.

[10] Remmert R.; Ullrich P. *Elementare Zahlentheorie*. 3. Aufl. Basel, Boston, Berlin: Birkenhäuser Verlag, 2008.