universität wien

DIPLOMARBEIT / DIPLOMA THESIS

Titel der Diplomarbeit / Title of the Diploma Thesis

„Weniger bekannte Beweise des quadratischen Reziprozitätsgesetzes “

verfasst von / submitted by
Christiane Kroner

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Magistra der Naturwissenschaften (Mag.rer.nat)

Wien, 2016 / Vienna, 2016

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 190 406 482
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	UF Mathematik UF Bewegung und Sport
Betreut von / Supervisor:	ao. Prof. Dr. Christoph Baxa

Vorwort

„Die glücklichen großen Geister, die die Astronomie ebenso wie die anderen schönen Teile der Mathematik geschaffen und erweitert haben, wurden gewiss nicht durch die Aussicht des künftigen Nutzens angefeuert: sie suchten die Wahrheit um ihrer selbst willen und fanden in dem Gelingen ihre Anstrengungen allein schon ihren Lohn und ihr Glück.“

Carl Friedrich Gauß bei seiner Antrittsvorlesung als Astronomieprofessor in Göttingen

Ich konnte beim Verfassen dieser Arbeit auch dieses Glück, von dem Carl Friedrich Gauß spricht, fühlen. Ich freue mich, diese Arbeit des Wissens willens durchgeführt zu haben, ohne den Nutzen im Vorhinein festgelegt zu haben. Insbesondere, weil in der heutigen Zeit dem Nutzen ein meiner Meinung nach zu hoher Stellenwert zugewiesen wird. Umso mehr ich mich mit diesem Thema auseinander gesetzt habe, desto mehr hat es mich fasziniert. Außerdem hat diese intensive Auseinandersetzung mich in meiner Persönlichkeit geformt. Dazu möchte ich von zwei kleinen Erlebnissen berichten:

Bei einem der ersten Treffen zum Besprechen des Themas der Diplomarbeit mit Herrn Professor Baxa erzählte er mir einen Witz: „Zwei Mathematiker sitzen gemeinsam in der Mensa beim Essen. Einer der beiden erzählt dem Anderen von einem trivialen Beispiel. Der Andere hat keine Ahnung wovon sein Kollege spricht. Er geht nach dem Essen sofort in die Bibliothek und vergräbt sich drei Stunden hinter Büchern. Dann stürmt er in das Zimmer seines Kollegen und sagt: „Du hast recht! Das ist trivial!“.“

Ich liege am Sofa und beschäftige mich schon mehrere Stunden mit einer Zeile eines Beweises und versuche nachzuvollziehen, was hier passiert. Immer wieder gehe ich einen Schritt zurück, um vielleicht den fehlenden Puzzelteil zu finden. Und auf einmal aus dem Nichts, kommt mir der richtige Gedanke. Wie ein Vorhang auf der Bühne, fällt die Lösung vom Himmel und ein schwieriges Problem wird zu einer trivialen Umformung. Noch im gleichem Atemzug merke ich, wie in meinem Körper die Glückshormone zu wirken beginnen.

Für diese Momente des Glücks beim Verfassen dieser Arbeit möchte ich mich besonders bei Herrn Professor Baxa und meiner Familie für ihre tolle Unterstützung bedanken!

Inhaltsverzeichnis

0 Einleitung

Diese Arbeit beschäftigt sich mit drei verschiedenen, eher unbekannten Beweisen des quadratischen Reziprozitätsgesetzes. Man sagt, dass es heute mehr als 150 verschiedene Beweise für dieses Gesetz gibt. Alleine Carl Friedrich Gauß hat acht Beweise verfasst. Er war auch der Erste, dem ein vollständiger Beweis gelungen ist. Heute kann man sagen, dass neue Beweise auch neue Richtungen der Forschung herbeigeführt haben. Bei den elementaren Beweisen handelt es sich meistens um Varianten der Gauß'schen Beweise.
Gauß schreibt über das quadratische Reziprozitätsgesetz, welches er auch als Fundamentaltheorem bezeichnet, dass es durch Induktion leicht zu entdecken sei, obwohl sich der Beweis dann als außerordentlich schwierig herausgestellt habe. Dies liege unter anderem daran, dass der Beweis einen anderen Weg, als man vermutet, einschlägt. Gauß meint aber auch, dass das typisch für diesen Zweig der Mathematik sei.
In weiterer Folge öffnen sich, wenn erst einmal ein Weg gefunden wurde, meist weitere Wege, die zu demselben Ziel führen. Die Beweise des quadratischen Reziprozitätsgesetzes unterscheiden sich in ihrer Länge und Direktheit. Teilweise lässt sich kaum eine Verbindung zwischen ihnen herstellen. Aus diesen merkwürdigen Zusammenhängen zwischen versteckten Wahrheiten erschließen sich oft neue Hilfsmittel oder Bereicherungen der Wissenschaft.
Eine Sammlung von verschiedenen Beweisen bietet das Buch „Variationen über ein zahlentheoretisches Thema“ von Herbert Pieper [7]. Die Beweise, welche in der vorliegenden Arbeit vorgestellt werden, finden sich in diesem Buch.

Der erste Beweis, der in dieser Arbeit behandelt wird, ist auch historisch gesehen der Erste, der publiziert wurde (von Carl Friedrich Gauß). Wir erläutern nicht nur die mathematischen Aspekte des Beweises, sondern stellen auch die geschichtlichen Hintergründe vor. Besonders beeindruckend habe ich gefunden, dass der Beweis des Hilfssatzes 3.3 für Gauß eine große Schwierigkeit darstellte, insbesondere der Fall, wenn p von der Form $8m+1$ ist. Dieser kostete, wie Gauß schreibt, ein ganzes Jahr. Auch für mich war dieser Abschnitt der, der am schwersten nachzuvollziehen war. Trotzdem bin ich erstaunt, dass die Voraussetzungen und der Beweis selbst von elementarster Natur sind. Das „schwierigste“ mathematische Konstrukt sind Kongruenzen zweiten Grades.
Die anderen zwei Beweise werden mit Hilfe der Theorie der endlichen Körper durchgeführt und weisen somit natürlich gewisse Gemeinsamkeiten auf. Wie schon beim ersten Beweis, müssen auch für diese Beweise einige Grundlagen geklärt werden, bevor die eigentlichen Beweise folgen können. Im Vergleich zum ersten Beweis sind die anderen beiden sehr

kurz. Der zweite Beweis baut auf der Theorie der Gaußschen Summen auf, welche im neunzehnten Jahrhundert entwickelt wurde. Die Gaußsche Summe ist ein bestimmter Typ einer endlichen Summe von Einheitswurzeln.
Beim dritten Beweis ist es, nicht zuletzt auf Grund der Länge, etwas schwieriger als beim Zweiten, den Überblick zu behalten. Oft erkennt man erst etwas später wofür gewisse Aussagen angeführt und bewiesen wurden. Zwei wichtige Hilfssätze, die beiden Ergänzungssätze, die im Rahmen des ersten und zweiten Beweises gezeigt werden müssen, liefert der dritte Beweis sehr elegant mit.

1 Kurze geschichtliche Einleitung zum ersten Beweis von Gauß

Carl Friedrich Gauß wurde 1777 in Braunschweig geboren. Schon in der frühen Schulzeit bemerkten seine Eltern, Freunde und Lehrer eine außerordentliche Begabung für mathematische Themen und förderten ihn in diesem Bereich besonders. Bereits als Jugendlicher hat er zahlreiche Tabellen aufgeschrieben, um die Teilbarkeit von Zahlen und die Eigenschaften von Primzahlen zu untersuchen. Zum Beispiel stellte er eine Tabelle auf, welche die Primzahlen von 2 bis 997 als Reste in Bezug auf die Primzahlen von 3 bis 503 als Teiler enthält. Dafür musste über 16000mal untersucht werden, ob eine Zahl quadratischer Rest oder Nichtrest ist. Trotzdem entschied sich Gauß erst im Jahre 1796, in dem er die geometrische Konstruierbarkeit des regelmäßigen Siebzehnecks entdeckte, der Mathematik sein Leben zu widmen. Diese und noch viele weiteren Details vom Werdegang von Gauß kann man im Buch von Sartorius von Waltershausen „Gauss zum Gedächtnis“ nachlesen [9].

Wie Pieper bereits in seinem Vorwort [7] beschreibt, wurde das quadratische Reziprozitätsgesetz erstmals von Euler entdeckt. Er publizierte es 1783. Viele Mathematiker haben sich daran versucht es zu beweisen. Fermat, Lagrange, Legendre und natürlich auch Euler selbst, jedoch ist keinem ein vollständiger Beweis gelungen. Zu dem Zeitpunkt, als Gauß den ersten Beweis entwickelte, waren ihm die Resultate von den anderen Mathematikern nicht bekannt. Er leitet 1795 das quadratische Reziprozitätsgesetz induktiv aus seinen unzähligen Zahlentabellen ab. Erst nachdem ihm der Beweis gelungen war, lernte er die Schriften seiner Vorgänger kennen.

Während seines Studiums in Göttingen schrieb Gauß in den Jahren 1796 bis 1798 sein erstes Buch „Disquisitiones arithmeticae“ [3], was „Zahlentheoretische Untersuchungen“ bedeutet. Er war zu diesem Zeitpunkt zwischen 19 und 21 Jahren alt und schuf mit diesem Buch ein bis heute richtungsweisendes Werk, welches die Zahlentheorie zu einer „festbegründeten und zusammenhängend dargestellten Wissenschaft“ werden ließ. 1801 erschien das Buch und mit diesem Zeitpunkt wurde Gauß unter den Mathematiker weltberühmt. In diesem Buch erschienen unter anderem zwei Beweise des quadratischen Reziprozitätsgesetzes, welches man auch als Fundamentaltheorem der quadratischen Reste bezeichnet. Der erste, welcher mittels der Methode der vollständigen Induktion durchgeführt wird, wird im Kapitel Gauß' erster Beweis ausführlich behandelt. Natürlich wurde dieses Werk auch in verschiedene Sprachen übersetzt, zum Beispiel 1889 in Deutsch [4].

Gauß war auch ein begnadeter Astronom, von 1807 bis zu seinem Tod (1855) war er Professor der Astronomie und Direktor der Sternwarte in Göttingen. Er hat in vielen Bereichen der Mathematik, aber auch der Astronomie Ergebnisse präsentiert und wurde nach seinem Tod als „Fürst der Mathematik“ gefeiert. Aus seinem Tagebuch und aus Briefwechsel weiß man, dass Gauß viele seiner Entdeckungen oft gar nicht publiziert hat [7].

Über Gauß gäbe es noch sehr viel zu sagen, wir wollen uns nun aber mit diesem kurzen Überblick zufrieden geben und machen uns auf die Spuren des ersten Beweises des quadratischen Reziprozitätsgesetzes.

2 Grundlagen

Bevor wir uns mit dem quadratischen Reziprozitätsgesetz näher beschäftigen können, müssen noch einige Grundlagen geklärt werden. In diesem Kapitel wird zu Beginn der quadratische Rest und der quadratische Nichtrest definiert. Im Anschluss daran werden wichtige Sätze zu diesem Thema, wie zum Beispiel der kleine Satz von Fermat, angeführt und bewiesen. Abschließen werden wir mit der Beantwortung von zwei Spezialfällen der Frage „Für welche ungeraden Primzahlen p ist eine gegeben Zahl quadratischer Rest?". Auf die allgemeine Beantwortung dieser Frage, in Form des quadratischen Reziprozitätsgesetzes müssen wir noch warten.
Wir folgen grundsätzlich dem Kapitel „Einführung. Quadratische Reste“ von Pieper in „Variationen über ein zahlentheoretisches Thema von Carl Friedrich Gauss“ [7]. Wir werden jedoch die für den ersten Beweis nicht relevanten Ausführungen zum Teil weglassen. Außerdem werden wir allgemeine Definitionen hinzufügen, welche sich auch in der Mitschrift von 2008 zur Vorlesung Zahlentheorie von ao. Prof. Dr. Christoph Baxa finden.

Vorweg möchte ich noch erwähnen, dass in dieser Arbeit die Menge der natürlichen Zahlen einschließlich der 0 gemeint ist. Es ist $x \in \mathbb{N}$ genau dann, wenn $x \in \{0, 1, 2, 3, \ldots\}$.

Bevor wir quadratische Reste und Nichtreste definieren können, werden wir zuerst Teiler und Kongruenzen einführen.

Definition 2.1. (Teiler)
Seien $a, b \in \mathbb{Z}$. Man sagt a teilt $b :\Leftrightarrow \exists d \in \mathbb{Z} : b = ad$. Man schreibt dafür $a \mid b$ und sagt auch: a ist Teiler von b.
Ist a kein Teiler von b, so schreibt man $a \nmid b$.

Definition 2.2. (Kongruenz)
Es seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$. Man sagt a und b seien kongruent modulo m wenn $m \mid (a-b)$. Man schreibt dafür $a \equiv b \pmod{m}$. Die Zahl m heißt Modul. Falls $m \nmid (a - b)$, dann schreibt man $a \not\equiv b \pmod{m}$ und sagt a und b seien inkongruent modulo m.

Beispiel 2.3. *Es ist* 5 *kongruent zu* 25 *modulo* 10*, weil* $5 - 25$ *durch* 10 *geteilt werden kann. Oder* $12 \equiv -2 \pmod{7}$*, da* $7 \mid 14$.

Definition 2.4. (quadratischer Rest)
Es sei $m > 1$ eine natürliche Zahl und a eine ganze Zahl. Gibt es eine ganze Zahl x so, dass $a \equiv x^2 \pmod{m}$ ist, so heißt a quadratischer Rest für die Zahl m. Man sagt die

Zahl a ist modulo m einer Quadratzahl kongruent. Eine ganze Zahl b, die modulo m keiner Quadratzahl kongruent ist, heißt quadratischer Nichtrest für die Zahl m.

Bemerkung. In weiterer Folge ist auch der quadratische Rest beziehungsweise der quadratische Nichtrest gemeint, wenn nur von Rest oder Nichtrest gesprochen wird.

Beispiel 2.5. *Es ist* 2 *quadratischer Rest für* 7*, weil* $2 \equiv 9 (= 3^2) \pmod 7$.

Definition 2.6. (Primzahl)
Sei $p \in \mathbb{Z}$ und $p > 1$. Wenn p nur die Teiler $1, -1, p, -p$ besitzt, dann heißt p Primzahl.

Satz 2.7. *Kleiner Satz von Fermat. Für* $a \in \{0, 1, 2, 3, \ldots, p-1\}$ *mit* p *einer Primzahl gilt*

$$a^p \equiv a \pmod p.$$

Beweis. Für den Fall $a = 0$ stimmt die Kongruenz immer. Wir betrachten nun den Fall, wenn $a \in \{1, 2, \ldots, p-1\}$. Da $\mathrm{ord}(1, 2, 3, \ldots, p-1) = p-1$ und $\mathrm{ord}(a)$ die Ordnung der von a erzeugten Untergruppe bezeichnet, folgt aus dem Satz von Lagrange (siehe Abschnitt 1.2 in [1]), dass $p - 1 = \mathrm{ord}(a) \cdot q$ für eine natürliche Zahl q gilt.
Wir können $a^p = a^{p-1} \cdot a$ schreiben und setzen für $p-1$ ein. Dann erhalten wir

$$a^p = a^{\mathrm{ord}(a) \cdot q} \cdot a = (a^{\mathrm{ord}(a)})^q \cdot a.$$

Laut Definition der Ordnung ist $a^{\mathrm{ord}(a)} \equiv 1 \pmod p$, also gilt

$$a^p = (a^{\mathrm{ord}(a)})^q \cdot a \equiv 1^q \cdot a = a \pmod p.$$

□

Durch Multiplizieren beider Seiten der Kongruenz $a^p \equiv a \pmod p$ mit a^{-1} sehen wir, dass für $a \in \{1, 2, 3, \ldots, p-1\}$ auch $a^{p-1} \equiv 1 \pmod p$ gilt.

Bemerkung. Der kleine Satz von Fermat gilt allgemeiner, nämlich für alle endlichen Gruppen. Vergleiche dazu Satz 6 in Kapitel 1.3 aus dem Buch „Algebra“ von Siegfried Bosch [1].

Satz 2.8. *Unter den* m *Zahlen* $0, 1, 2, 3, \ldots, m-1$ *können nicht mehr als* $\frac{m}{2} + 1$ *Zahlen als Rest bei der Division einer Quadratzahl durch* m *auftreten.*

Beweis. Wir müssen nur Quadratzahlen, welche größer oder gleich Null und kleiner m^2 sind, betrachten, weil auch die Quadrate kongruenter Zahlen einander kongruent sind.

Das heißt, jede Zahl, welche einer Quadratzahl kongruent ist, ist auch einer Quadratzahl in $\{0^2, 1^2, 2^2, \ldots, (m-1)^2\}$ kongruent.
Wenn m gerade ist, gilt

$$\begin{aligned}
0^2 &\equiv 0^2 \pmod{m},\\
1^2 &\equiv 1^2 \pmod{m},\\
&\ldots,\\
\left(\frac{m}{2}-1\right)^2 &\equiv \left(\frac{m}{2}-1\right)^2 \pmod{m},\\
\left(\frac{m}{2}\right)^2 &\equiv \left(\frac{m}{2}\right)^2 \pmod{m},\\
\left(\frac{m}{2}+1\right)^2 &\equiv \left(\frac{m}{2}-1\right)^2 \pmod{m}, \quad (*)\\
\left(\frac{m}{2}+2\right)^2 &\equiv \left(\frac{m}{2}-2\right)^2 \pmod{m},\\
&\ldots,\\
(m-2)^2 &\equiv 2^2 \pmod{m},\\
(m-1)^2 &\equiv 1^2 \pmod{m}.
\end{aligned}$$

Die Kongruenz $(*)$ gilt, weil $(\frac{m}{2}+1)^2 = \frac{m^2}{4}+m+1 \equiv \frac{m^2}{4}-m+1 = (\frac{m}{2}-1)^2 \pmod{m}$.
Analog lassen sich die Kongruenzen in den darauffolgenden Zeilen überprüfen.
Es können nur Zahlen, die schon zu einem der Quadrate $0^2, 1^2, 2^2, \ldots, (\frac{m}{2})^2$ modulo m kongruent sind, zu einer Quadratzahl kongruent werden. Somit gibt es höchstens $\frac{m}{2}+1$ quadratische Reste unter den Zahlen $0, 1, 2, \ldots, m-1$.
Wenn m ungerade ist, gilt genauso, dass jede Zahl, die modul m einer Quadratzahl kongruent wird, zu einem der Quadrate $0^2, 1^2, 2^2, \ldots, (\frac{m-1}{2})^2$ kongruent sein muss. Es gibt also höchstens $\frac{m-1}{2}+1 = \frac{m+1}{2}$ solcher Zahlen unter den Zahlen $0, 1, 2, \ldots, m-1$. □

Satz 2.9. *Es sei p eine ungerade Primzahl. Die Hälfte der Zahlen $1, 2, 3, \ldots, p-1$ wird zu quadratischen Resten für p, die übrigen zu Nichtresten. Das heißt, es gibt genau $\frac{p-1}{2}$ Reste und ebenso viele Nichtreste für p.*

Beweis. Wir zeigen zuerst, dass die $\frac{p-1}{2}$ Zahlen $1^2, 2^2, 3^2, \ldots, (\frac{p-1}{2})^2$ bei der Division durch p auch $\frac{p-1}{2}$ verschiedene Reste haben.
Seien x, y natürliche Zahlen außer Null mit $x > y$ und beide Zahlen sind nicht größer als $\frac{p-1}{2}$. Angenommen es würde für x^2 und y^2 bei der Division durch p der gleiche Rest auftreten, so sieht man leicht durch Nachrechnen, dass auch $x^2 - y^2$ positiv und durch p

teilbar sein muss. Dies ist aber unmöglich, weil $x^2-y^2=(x-y)(x+y)$ und beide Faktoren $x-y$ und $x+y$ kleiner als p sind. Folglich gibt es unter den Zahlen $1,2,3,\ldots,\frac{p-1}{2}$ genau $\frac{p-1}{2}$ verschiedene quadratische Reste.
Nehmen wir jetzt die Null noch dazu entsteht $\frac{p-1}{2}+1=\frac{p+1}{2}$ und dies entspricht der oberen Grenze für die Anzahl der Reste laut Satz 2.8. Aus diesem Grund müssen alle übrigen Zahlen Nichtreste werden und ihre Anzahl ist genauso $\frac{p-1}{2}$. □

Satz 2.10. *(Eulersche Kriterium) Sei p eine ungerade Primzahl und a eine beliebige, nicht durch p teilbare Zahl in $\mathbb{Z}$. Dann ist a quadratischer Rest, wenn $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ist. Und entsprechend ist a quadratischer Nichtrest, wenn $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ ist.*

Beweis. Durch Umformen des kleinen Satzes von Fermat (Satz 2.7) erhalten wir

$$a^{p-1}-1=(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1) \equiv 0 \pmod{p}.$$

Jetzt können wir erkennen, dass $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ oder $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ gelten muss. Falls a quadratischer Rest für p ist, gibt es eine natürliche Zahl x mit $x^2 \equiv a \pmod{p}$. Aus dem kleinen Fermatschen Satz (Satz 2.7) wissen wir, dass $(x^2)^{\frac{p-1}{2}} = x^{(p-1)} \equiv 1 \pmod{p}$. Für quadratische Reste gilt also $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Da diese Kongruenz vom Grad $\frac{p-1}{2}$ höchstens $\frac{p-1}{2}$ Lösungen haben kann und es genau $\frac{p-1}{2}$ quadratische Reste gibt (vgl. Satz 2.9), müssen die quadratischen Nichtreste der Kongruenz $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ genügen. □

Lemma 2.11. *Das Quadrat einer ungeraden Zahl ist stets von der Form $8m+1$ mit m aus den natürlichen Zahlen.*

Beweis. Sei a eine ungerade Zahl. Da das Quadrat einer negativen Zahl gleich dem Quadrat der positiven Zahl ist, können wir $a=2n+1$ mit $n \in \mathbb{N}$ wählen. Es ist

$$a^2=(2n+1)^2=4n^2+4n+1=4(n^2+n)+1$$

und da n^2+n für ein beliebiges $n \in \mathbb{N}$ gerade ist, folgt, dass das Quadrat jeder ungeraden Zahl von der Form $8m+1$ mit $m \in \mathbb{N}$ ist. □

Satz 2.12. *Für $k \in \mathbb{N}$ und $k \geq 3$ ist die ungerade natürliche Zahl a dann und nur dann quadratischer Rest von 2^k, wenn $a \equiv 1 \pmod{8}$ ist.*

Beweis. $\Rightarrow$: Es sei a eine ungerade natürliche Zahl. Wenn $a \not\equiv 1 \pmod{8}$ ist, dann kann a laut Lemma 2.11 kein Rest von 2^k sein, weil es kein Quadrat von einer ungeraden Zahl gibt, welches nicht von der Form $8m+1$ ist. Also muss gelten, wenn a quadratischer Rest

von 2^k ist, dann ist $a \equiv 1 \pmod 8$.
$\Leftarrow$: Zu zeigen: Es sei $a \equiv 1 \pmod 8$. Dann ist a quadratischer Rest von 2^k für k aus den natürlichen Zahlen mit $k \geq 3$.
Wenn die Summe oder die Differenz zweier ganzer Zahlen durch 2^{k-1} teilbar ist, werden die Quadrate dieser Zahlen einander modulo 2^k kongruent. Angenommen eine der beiden Zahlen ist d, so hat die andere Zahl die Form $2^{k-1}h \pm d$, damit die Verknüpfung durch 2^{k-1} teilbar ist. Das Quadrat der zweiten Zahl ist

$$2^{2(k-1)}h^2 \pm 2 \cdot 2^{k-1}hd + d^2 = 2^k(2^{k-2}h^2 \pm hd) + d^2.$$

Jetzt kann man erkennen, dass die Quadrate beider Zahlen modulo 2^k kongruent sind.
Sei a eine ungerade Zahl, die quadratischer Rest von 2^k ist und x^2 ist kongruent zu a modulo 2^k. Hat man außerdem $x \equiv \pm b \pmod{2^{k-1}}$, mit einem b aus den natürlichen Zahlen und $b < 2^{k-2}$ (wenn x existiert, kann man auch immer ein b mit diesen Eigenschaften finden) folgt nach der zuvor angeführten Aussage, dass $b^2 \equiv x^2 \pmod{2^k}$ gilt. Somit ist auch $b^2 \equiv a \pmod{2^k}$ mit einem ungeraden b, welches kleiner als 2^{k-2} ist.
Die Quadrate aller ungeraden Zahlen, welche kleiner sind als 2^{k-2}, sind modulo 2^k inkongruent. Angenommen es wären x und y (mit $x > y$) zwei solche Zahlen mit $x^2 \equiv y^2 \pmod{2^k}$, so wäre auch

$$x^2 - y^2 = (x-y)(x+y) \equiv 0 \pmod{2^k}.$$

Also müsste $(x-y)(x+y)$ durch 2^k teilbar sein. Weil x und y beide ungerade sind, können $x-y$ und $x+y$ nicht gleichzeitig durch 4 teilbar sein. Wenn die Summe der beiden Zahlen nur durch 2 teilbar ist, müsste die Differenz durch 2^{k-1} teilbar werden, damit das Produkt durch 2^k teilbar wäre. Genauso umgekehrt: Wenn die Differenz $x-y$ durch 2 teilbar ist, müsste die Summe durch 2^{k-1} teilbar sein. Da aber x und y kleiner als 2^{k-2} ist, kann weder die Summe noch die Differenz durch 2^{k-1} teilbar werden. Somit sind die Quadrate dieser Zahlen modulo 2^k inkongruent.
Werden die Quadrate aller ungeraden Zahlen, welche kleiner als 2^{k-2} sind, auf ihre kleinsten positiven Reste reduziert, so gibt es 2^{k-3} verschiedene quadratische Reste, die kleiner als 2^k sind, weil 2^{k-3}die Anzahl der ungeraden Zahlen unterhalb von 2^{k-2} ist. Außerdem sind die Zahlen von der Form $8m+1$, weil Quadrate ungerader Zahlen immer von dieser Form sind.
Da es genau $\frac{2^k}{8} = 2^{k-3}$ Zahlen von der Form $8m+1$ gibt, die alle kleiner als 2^k sind, gehören genau diese Zahlen alle zu den Resten. $\square$

Satz 2.13. *Das Produkt aus zwei quadratischen Resten der Primzahl p ist ein Rest.*

Beweis. Seien a und b quadratische Reste für p. Dann gibt es ein x und $y \in \mathbb{N}$ für die gilt $x^2 \equiv a \pmod{p}$ und $y^2 \equiv b \pmod{p}$. Daraus folgt, dass $x^2y^2 = (xy)^2 \equiv ab \pmod{p}$. □

Satz 2.14. *Das Produkt aus einem Rest der Primzahl p und einem Nichtrest für p ist ein Nichtrest.*

Beweis. Es sei a ein quadratischer Rest für p und b ein Nichtrest für p. Es gibt also ein $x \in \mathbb{N}$ mit $x^2 \equiv a \pmod{p}$. Angenommen es gibt auch ein $z \in \mathbb{N}$ mit $z^2 \equiv ab \pmod{p}$, obwohl b Nichtrest ist. Multipliziert man beide Seiten der Kongruenz $x^2 \equiv a \pmod{p}$ mit b folgt

$$x^2b \equiv ab \equiv z^2 \pmod{p}.$$

Weil a modulo p eine prime Restklasse ist und jede prime Restklasse ein Inverses besitzt, kann man $x \cdot x^{-1} \equiv 1 \pmod{p}$ schreiben. Es existiert also ein $y(= x^{-1} \cdot z)$ so, dass $xy \equiv z \pmod{p}$ ist. Dann wäre

$$x^2b \equiv z^2 \equiv x^2y^2 \pmod{p}$$

und somit wäre $b \equiv y^2 \pmod{p}$ und gegen die Annahme ein Rest. Also muss das Produkt ein Nichtrest sein. □

Satz 2.15. *Das Produkt aus zwei Nichtresten der Primzahl p ist ein Rest.*

Beweis. Seien a und b Nichtreste für p. Laut Satz 2.14 erhalten wir $\frac{p-1}{2}$ verschiedene Nichtreste, wenn wir a mit allen Resten, die unter $1, 2, 3, \ldots, p-1$ vorkommen, multiplizieren. Das Produkt ab kann keinem dieser Nichtreste kongruent sein, weil b ein Nichtrest ist. Wäre dieses Produkt nun auch ein Nichtrest, so gäbe es $\frac{p-1}{2} + 1$ verschiedene Nichtreste. Laut Satz 2.9 kann das aber nicht sein und somit muss ab quadratischer Rest sein. □

Mit Hilfe dieser Sätze ist es leicht zu bestimmen, ob das Produkt aus beliebig vielen Faktoren ein Rest oder Nichtrest ist. Ein Rest ist es genau dann, wenn alle einzelnen Faktoren Reste sind oder wenn die Anzahl der unter den Faktoren vorkommenden Nichtreste gerade ist. Ein Nichtrest hingegen ist es genau dann, wenn die Anzahl der unter den Faktoren vorkommenden Nichtreste ungerade ist.

Wenn die Primzahl p als Modul gegeben ist, ist es leicht alle Reste und somit auch alle Nichtreste für p zu bestimmen. Dies wird im folgenden Beispiel demonstriert.

Beispiel 2.16. $p = 13$. *Es müssen alle Quadrate* $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ *bestimmt werden, beziehungsweise die Zahlen, die den Quadraten modulo p kongruent sind. Es ist*
$1^2 \equiv 1 \pmod{13}$, $2^2 \equiv 4 \pmod{13}$, $3^2 \equiv 9 \pmod{13}$, $4^2 = 16 \equiv 3 \pmod{13}$,
$5^2 = 25 \equiv 12 \pmod{13}$ *und* $6^2 = 36 \equiv 10 \pmod{13}$.
Es sind also die Zahlen $1, 3, 4, 9, 10$ *und* 12 *quadratische Reste für* 13.
Die Zahlen $2, 5, 6, 7, 8$ *und* 11 *sind hingegen Nichtreste für* 13.

Wir wollen uns nun der Frage „Für welche ungeraden Primzahlen p ist eine gegebene Zahl quadratischer Rest?“ widmen. Die Zahl $+1$ ist quadratischer Rest für alle Primzahlen. Für -1 gelten folgende Sätze:

Satz 2.17. *Für alle Primzahlen von der Form* $4m+1$ *mit* m *aus den natürlichen Zahlen, ist* -1 *quadratischer Rest.*

Beweis. Es sei p eine Primzahl von der Form $4m+1$ mit $m \in \mathbb{N}$. Wir setzen ins Eulersche Kriterium (Satz 2.10) ein. Es ist $a = -1$ und $p = 4m + 1$. Daraus folgt

$$(-1)^{\frac{p-1}{2}} = (-1)^{2m} = 1$$

und somit haben wir gezeigt, dass -1 quadratischer Rest für alle Primzahlen von der Form $4m + 1$ ist. □

Satz 2.18. *Für alle Primzahlen von der Form* $4m+3$ *mit* m *aus den natürlichen Zahlen, ist* -1 *quadratischer Nichtrest.*

Beweis. Es sei p eine Primzahl von der Form $4m + 3$ mit $m \in \mathbb{N}$. Analog setzen wir ins Eulersche Kriterium (Satz 2.10) ein. Daraus folgt

$$(-1)^{\frac{p-1}{2}} = (-1)^{2m+1} = -1.$$

Also ist -1 Nichtrest für alle Primzahlen von der Form $4m + 3$. □

Bemerkung. Diese zwei Sätze, welche Auskunft darüber geben, ob -1 quadratischer Rest oder Nichtrest einer Primzahl p ist, werden im weiteren Verlauf dieser Arbeit eine wichtige Rolle spielen. Im 5ten Kapitel werden wir sie zum sogenannten ersten Ergänzungssatz zusammenfassen, indem wir ein neues Symbol einführen.

Satz 2.19. *Für alle Primzahlen von der Form* $8m + 3$ *oder von der Form* $8m + 5$ *mit* $m \in \mathbb{N}$ *ist* 2 *Nichtrest.*

Beweis. Multipliziert man Primzahlen von der Form $8m+1$ und $8m+7$ ($m \in \mathbb{N}$) miteinander, so können nur Zahlen der gleichen Form entstehen. Daraus folgt, dass jede Zahl der Form $8m+3$ und $8m+5$ ($m \in \mathbb{N}$) zumindest einen Primfaktor von der Form $8m+3$ oder $8m+5$ haben muss.
Angenommen es gäbe Zahlen der Form $8m+3$ und $8m+5$ für die 2 Rest ist und sei k die kleinste unter diesen Zahlen. Die Zahl 2 ist also Rest für k, aber Nichtrest für jede kleinere Zahl der gleichen Form. Es gibt somit ein $x \in \mathbb{Z}$, sodass $x^2 \equiv 2 \pmod{k}$ gilt. Da k ungerade ist, können wir sicher ein x wählen, welches kleiner als k ist und außerdem auch ungerade ist. (Denn x kann mindestens zwei positive Werte annehmen, die kleiner k sind und deren Summe gleich k ist; eine dieser Zahlen ist ungerade, die andere Zahl ist gerade (vgl. Satz 2.8).) Es sei $x^2 = 2 + ku$ mit $u \in \mathbb{N}$ und kleiner k. Wäre nämlich $u \geq k$, dann wäre auch $ku \geq k^2$ und $x^2 \geq k^2 + 2$, obwohl $x < k$ und somit auch $x^2 < k^2$ gilt, womit wir bei einem Widerspruch angekommen sind. Es muss also $u < k$ gelten.
Wir wissen aber, dass auch $x^2 \equiv 2 \pmod{u}$ gilt, das heißt 2 ist auch Rest für u. Da wir wissen, dass x ungerade ist und somit x^2 von der Form $8m+1$ ist (Lemma 2.11), können wir die Form von u bestimmen. Wenn k von der Form $8m+3$ ist, dann folgt aus der Gleichung $ku = x^2 - 2$, dass u von der Form $8m+5$ sein muss. Umgekehrt folgt, wenn k von der Form $8m+5$ ist, dann hat u die Form $8m+3$. Das heißt u ist auch von der Form $8m+3$ oder $8m+5$ und müsste also nach Wahl von k größer als k sein. Damit stoßen wir auf einen Widerspruch, weil u gleichzeitig größer und kleiner k sein muss. Es gibt keine Zahlen von der Form $8m+3$ oder $8m+5$ für die 2 Rest ist, also gibt es auch keine Primzahlen von dieser Form für die 2 Rest ist. □

Bemerkung. Es wurde also nicht nur für Primzahlen gezeigt, sondern allgemeiner für alle Zahlen von der Form $8m+3$ und $8m+5$.

Definition 2.20. (größter gemeinsame Teiler)
Sind $n_1, \ldots, n_k \in \mathbb{Z}$ nicht alle 0, dann ist

$$\text{ggT}(n_1, \ldots, n_k) := \max\{m \in \mathbb{Z} : m \text{ teilt } n_i \text{ für } 1 \leq i \leq k\}$$

der größte gemeinsamer Teiler von $n_1, ..., n_k$. Bei der Kurzschreibweise wird ggT auch weggelassen.

3 Vorbereitungen für den ersten Beweis

In diesem Kapitel wollen wir noch alle nötigen Vorbereitungen für den ersten Beweis des quadratischen Reziprozitätsgesetz durchführen. Außerdem werden wir erstmals das quadratische Reziprozitätsgesetzes beschreiben und es unter genauer Betrachtung in weitere Fälle unterteilen, welche wir dann im folgenden Kapitel einzeln beweisen werden. Wir halten uns an den ersten Teil des Kapitels „Thema. Beweis des quadratischen Reziprozitätsgesetzes“ von Pieper [7].

Satz 3.1. *Quadratisches Reziprozitätsgesetz.*
Ist p eine Primzahl von der Form $4m+1$, dann gilt:
$+p$ ist Rest aller ungeraden Primzahlen, welche Reste von p sind,
$+p$ ist Nichtrest aller ungeraden Primzahlen, welche Nichtreste von p sind.
Ist q eine Primzahl von der Form $4m+3$, dann gilt:
$-q$ ist Rest aller ungeraden Primzahlen, welche Reste von q sind,
$-q$ ist Nichtrest aller ungeraden Primzahlen, welche Nichtreste von q sind.

Bemerkung. Das quadratische Reziprozitätsgesetz wird normalerweise in einer anderen Form geschrieben. Wir werden in folgenden Kapiteln noch darauf eingehen. Für den „historischen“ Beweis verwenden wir aber natürlich auch diese Schreibweise.

Bevor wir diesen Satz beweisen können, werden wir noch weitere Hilfssätze benötigen. Außerdem werden wir aus Übersichtsgründen folgende Kurzschreibweise einführen: Der Buchstabe R zwischen zwei Zahlen gibt an, dass die erste Zahl Rest der zweiten ist. Der Buchstabe N gibt an, dass die erste Zahl Nichtrest der zweiten ist.

Beispiel 3.2. $\pm 5N13$ *bezeichnet, dass* 5 *und* -5 *Nichtreste für* 13 *sind.*

Satz 3.3. *Es sei p eine Primzahl von der Form $4m+1$ mit $m \in \mathbb{N}$. Dann sind $-p$ und p Nichtreste gewisser Primzahlen. Wenn p größer als 5 ist, gilt, dass $-p$ und p Nichtreste einer kleineren Primzahl als p sind.*

Beweis. (0) Für den Fall $p = 5$ vergleiche das Beispiel 3.2.

Es sei $p > 5$ eine Primzahl der Form $4m + 1$.

(1) Zunächst zeigen wir, dass $-p$ Nichtrest einer gewissen Primzahl $< p$ ist.
Die erste zu überprüfende Zahl ist -13. Da $13R3$ (weil $4^2 \equiv 13 \pmod 3$ ist) und $-1N3$ (vgl. Satz 2.18) folgt, dass $-13N3$. Auf die gleiche Art kann man überprüfen, dass

$-17N5$. Somit können wir $p \geq 29$ setzen. Sei $2a$ die kleinste gerade Zahl, welche $\sqrt{p}$ übertrifft, also ist $2a < \sqrt{p} + 2$ und

$$4a^2 < (\sqrt{p} + 2)^2 = p + 4\sqrt{p} + 4.$$

Da p größer oder gleich 29 ist, folgt dass $\sqrt{p} - 2$ immer echt größer als $\sqrt{8}$ ist und somit auch

$$(\sqrt{p} - 2)^2 = p - 4\sqrt{p} + 4 > 8.$$

Aus dieser Ungleichung sehen wir, dass $p > 4\sqrt{p} + 4$ ist. Es folgt

$$4a^2 < p + \underbrace{4\sqrt{p} + 4}_{<p} < 2p \text{ oder } 4a^2 - p < p.$$

Weil $p \equiv 4a^2 \pmod{4a^2 - p}$, ist p quadratischer Rest von $4a^2 - p$. Außerdem ist $4a^2 - p$ von der Form $4m + 3$ mit $m \in \mathbb{N}$. Da -1 laut Satz 2.18 Nichtrest für Primzahlen der Form $4m + 3$ ist, ist auch $-p$ Nichtrest für $4a^2 - p$, falls $4a^2 - p$ eine Primzahl ist. Wenn $4a^2 - p$ keine Primzahl ist, hat die Zahl mindestens einen Primfaktor von der gleichen Form $(4m + 3)$ und p wird für diesen Primfaktor quadratischer Rest. Somit wird $-p$ für ihn Nichtrest.

Eine Primzahl p der Form $4m + 1$ kann nur $p \equiv 5 \pmod 8$ oder $p \equiv 1 \pmod 8$ sein.

(2) In diesem Abschnitt zeigen wir, dass für $p \equiv 5 \pmod 8$ die Primzahl p Nichtrest einer gewissen Primzahl $< p$ ist.
Sei a eine natürliche Zahl, die kleiner als $\sqrt{\frac{1}{2}p}$ ist. Wenn a gerade ist, dann wird $p - 2a^2$ von der Form $8m + 5$ sein, weil $2a^2$ durch 8 teilbar ist. Wenn a ungerade ist, wird $p - 2a^2$ von der Form $8m + 3$ werden. Das heißt, dass $p - 2a^2$ durch eine Primzahl q von der Form $8m + 5$ oder $8m + 3$ teilbar ist. Dies folgt, weil Produkte beliebig vieler Zahlen der Form $8m + 1$ und $8m + 7$ weder die Form $8m + 3$, noch $8m + 5$ haben können.
Weil q den Ausdruck $p - 2a^2$ teilt, folgt, dass $p \equiv 2a^2 \pmod q$ ist. Wir wissen, dass a^2 nicht durch q teilbar ist, sonst wäre nämlich auch die Primzahl p durch q teilbar. Also ist a^2 ein durch q nicht teilbarer quadratischer Rest. Aus dem Satz 2.19 wissen wir, dass 2 Nichtrest von q ist. Weil Nichtrest mal Rest immer ein Nichtrest ist (Satz 2.14), folgt, dass $2a^2$ Nichtrest von q ist.

(3) Im dritten und letzten Abschnitt diesen Beweises zeigen wir die Existenz einer gewissen Primzahl, welche kleiner p ist, für die $p \equiv 1 \pmod 8$ Nichtrest ist.

Es sei $2k+1 < p$ mit k aus den natürlichen Zahlen. Angenommen p sei quadratischer Rest von allen ungeraden Primzahlen, die nicht größer als $2k+1$ sind. Dann existiert ein $x \in \mathbb{Z}$, sodass $x^2 \equiv p \pmod{l}$ mit $l \leq 2k+1$ und l ist eine ungerade Primzahl.
Weil $p \equiv 1 \pmod{8}$ ist, wissen wir aus Satz 2.12, dass die Kongruenz $x^2 \equiv p \pmod{2^i}$ für beliebiges i aus den natürlichen Zahlen lösbar ist.
Aus diesen beiden Kongruenzen folgt, dass $x^2 \equiv p \pmod{m}$ für jeden Modul m lösbar ist, der nur ungerade, $2k+1$ nicht übertreffende Primfaktoren enthält außer einer beliebigen Potenz von 2.
Wir wählen für m das Produkt aller natürlichen Zahlen von 1 bis $2k+1$, das heißt $m = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2k \cdot (2k+1)$. Ist x_1 eine positive Lösung der Kongruenz $x^2 \equiv p \pmod{m}$, also ${x_1}^2 \equiv p \pmod{m}$, dann gilt

$$\mathrm{ggT}(p, m) = 1 \text{ (weil } p > 2k+1 \text{ ist)}$$

und daraus folgt auch $\mathrm{ggT}(x_1, m) = 1$ (wegen $(p, m) = ({x_1}^2, m) = 1$). Um schlussendlich zu einem Widerspruch zu kommen betrachten wir folgenden Ausdruck näher:

$$\begin{aligned}
&x_1(p-1^2)(p-2^2)\cdot\ldots\cdot(p-k^2)\\
&\equiv x_1({x_1}^2-1^2)({x_1}^2-2^2)\cdot\ldots\cdot({x_1}^2-k^2) \pmod{m}\\
&= x_1(x_1+1)(x_1-1)\cdot\ldots\cdot(x_1+k)(x_1-k)\\
&= (x_1+k)(x_1+k-1)\cdot\ldots\cdot(x_1+1)x_1(x_1-1)\cdot\ldots\cdot(x_1-k)
\end{aligned}$$

Nun wollen wir zeigen, dass $(x_1+k)(x_1+k-1)\cdot\ldots\cdot(x_1+1)x_1(x_1-1)\cdot\ldots\cdot(x_1-k)$ ein Vielfaches von m ist. Angenommen x_1 wäre kleiner oder gleich $2k+1$, dann müsste auch der größte gemeinsame Teiler größer als 1 sein. Also ist $x_1 > 2k+1$. Wir wissen nun, dass aus dem Ausdruck $(x_1+k)(x_1+k-1)\cdot\ldots\cdot(x_1+1)x_1(x_1-1)\cdot\ldots\cdot(x_1-k)$ kein Faktor kleiner als $k+2$ sein kann. Insgesamt sind es $2k+1$ Faktoren, welche sich jeweils immer nur um 1 unterscheiden. Somit kann immer der Faktor m aus diesem Produkt herausgehoben werden. Daraus folgt:

$$(x_1+k)(x_1+k-1)\cdot\ldots\cdot(x_1+1)x_1(x_1-1)\cdot\ldots\cdot(x_1-k) \equiv 0 \pmod{m}.$$

Wir wissen also, dass der Bruch $\frac{(x_1+k)(x_1+k-1)\cdot\ldots\cdot(x_1+1)x_1(x_1-1)\cdot\ldots\cdot(x_1-k)}{1\cdot2\cdot3\cdot\ldots\cdot(2k+1)}$ eine ganze Zahl sein muss. Außerdem folgt, dass

$$x_1(p-1^2)(p-2^2)\cdot\ldots\cdot(p-k^2) \equiv 0 \pmod{m}$$

Wegen $(x_1, m) = 1$ ist sogar $(p-1^2)(p-2^2)\cdot\ldots\cdot(p-k^2) \equiv 0 \pmod{m}$.

Das Produkt $m = 1\cdot 2\cdot 3\cdot\ldots\cdot(2k+1)$ kann durch Umformen auch so geschrieben werden:

$$(k+1)\underbrace{((k+1)^2-1^2)}_{=k(k+2)}\underbrace{((k+1)^2-2^2)}_{=(k-1)(k+3)}\cdot\ldots$$
$$\ldots\cdot\underbrace{((k+1)^2-(k-2)^2)}_{=3(2k-1)}\underbrace{((k+1)^2-(k-1)^2)}_{=2(2k)}\underbrace{((k+1)^2-k^2)}_{=1(2k+1)}.$$

Also muss

$$\frac{(p-1^2)(p-2^2)\cdot\ldots\cdot(p-k^2)}{m} = \frac{1}{k+1}\cdot\frac{p-1^2}{(k+1)^2-1^2}\cdot\frac{p-2^2}{(k+1)^2-2^2}\cdot\ldots\cdot\frac{p-k^2}{(k+1)^2-k^2}$$

eine ganze Zahl sein. Wir können k so wählen, dass $k < \sqrt{p} < k+1$ ist. Das ist möglich weil, $p \equiv 1 \pmod 8$ ist und somit $p \geq 17$ sein muss. Deshalb ist auch $2k+1$ immer kleiner als $2\sqrt{p}+1$ und das ist wiederum kleiner als p für $p \geq 17$. Mit diesem gewählten k ist jeder Faktor des Produkts $\frac{1}{k+1}\cdot\frac{p-1^2}{(k+1)^2-1^2}\cdot\frac{p-2^2}{(k+1)^2-2^2}\cdot\ldots\cdot\frac{p-k^2}{(k+1)^2-k^2}$ ein echter Bruch, da $(k+1)^2$ größer als p ist. Das Produkt der echten Brüche kann keine ganze Zahl sein. Somit sind wir bei einem Widerspruch angelangt. Die Annahme, dass p quadratischer Rest von allen ungeraden Primzahlen, welche nicht größer als $2k+1$ sind, ist falsch. Es gibt immer eine Primzahl $\leq 2k+1 < p$, für die p Nichtrest ist.

□

Im nächsten Abschnitt werden wir einige Folgerungen aus dem, als wahr angenommenen, quadratischen Reziprozitätsgesetzes herleiten. Wir führen eine weitere Kurzschreibweise ein:

$p, p', p'', \ldots$ bezeichnen Primzahlen von der Form $4m+1$,
$q, q', q'', \ldots$ bezeichnen Primzahlen von der Form $4m+3$,
$a, a', a'', \ldots$ bezeichnen natürliche Zahlen von der Form $4m+1$ und
$b, b', b'', \ldots$ bezeichnen natürliche Zahlen von der Form $4m+3$.

Satz 3.1.a. Das quadratische Reziprozitätsgesetz (vgl. Satz 3.1) wird mit diesen Bezeichnung in folgender Form dargestellt: $l \neq p$ ist eine ungerade Primzahl.

a) Ist lRp, dann pRl.
b) Ist lNp, dann pNl.
c) Ist lRq, dann $-qRl$.
d) Ist lNq, dann $-qNl$.

Die Sätze 2.13, 2.14 und 2.15 geben Auskunft darüber, ob das Ergebnis von Multiplikationen von Resten und Nichtresten wiederum ein Rest beziehungsweise ein Nichtrest wird. Außerdem wissen wir aus den Sätzen 2.17 und 2.18, ob -1 Rest oder Nichtrest von bestimmten Primzahlen ist. Wenn man die Ergebnisse dieser Sätze mit dem Gesetz verknüpft, kann man für eine ungerade Primzahl l folgende Zusammenhänge beschreiben:

a) Wenn $\pm lRp$, dann pRl.

b) Wenn $\pm lNp$, dann pNl.

c) Wenn lRq und $-lNq$, dann $-qRl$.

d) Wenn lNq und $-lRq$, dann $-qNl$.

Bemerkung zu a) Weil $-1Rp$ und Rest mal Rest gleich Rest, folgt lRp genau dann, wenn $-lRp$.
Zu b) Wie bei a), weil $-1Rp$ und Rest mal Nichtrest gleich Nichtrest, folgt lNp genau dann, wenn $-lNp$.
Zu c) Da $-1Nq$ und Nichtrest mal Rest gleich Nichtrest, folgt lRq genau dann, wenn $-lNq$.
Zu d) Wie bei c), weil $-1Nq$ und Nichtrest mal Nichtrest gleich Rest, folgt lNq genau dann, wenn $-lRq$.

Satz 3.1.b. Wenn wir nun auch für die Primzahl l eine Unterscheidung vornehmen und einmal Primzahlen der Form $4m+1$ einsetzen und dann Primzahlen der Form $4m+3$, dann erhalten wir folgende acht Aussagen:

$$\text{Wenn } \pm p'Rp, \qquad \text{dann } \pm pRp'. \tag{1}$$

$$\text{Wenn } \pm p'Np, \qquad \text{dann } \pm pNp'. \tag{2}$$

$$\text{Wenn } pRq \text{ und } -pNq, \qquad \text{dann } \pm qRp. \tag{3}$$

$$\text{Wenn } pNq \text{ und } -pRq, \qquad \text{dann } \pm qNp. \tag{4}$$

$$\text{Wenn } \pm qRp, \quad \text{dann } pRq \text{ und } -pNq. \tag{5}$$

$$\text{Wenn } \pm qNp, \quad \text{dann } pNq \text{ und } -pRq. \tag{6}$$

$$\text{Wenn } q'Rq \text{ und } -q'Nq, \quad \text{dann } qNq' \text{ und } -qRq'. \tag{7}$$

$$\text{Wenn } q'Nq \text{ und } -q'Rq, \quad \text{dann } qRq' \text{ und } -qNq'. \tag{8}$$

Dies sind alle Fälle, welche beim Vergleich von zwei Primzahlen auftreten können. Das quadratische Reziprozitätsgesetz kann also auch in dieser Form angeschrieben werden.

Bemerkung zu 1) Diese Aussage folgt aus a), da $-1Rp'$ und Rest mal Rest gleich Rest ist.
Zu 2) Folgt aus b), da $-1Rp'$ und Nichtrest mal Rest gleich Nichtrest ist.
Zu 3) Folgt aus c), da $-1Rp$ und Rest mal Rest gleich Rest ist.
Zu 4) Folgt aus d), da $-1Rp$ und Nichtrest mal Rest gleich Nichtrest ist.
Zu 5) Folgt aus a), da $-1Nq$ und Rest mal Nichtrest gleich Nichtrest ist.
Zu 6) Folgt aus b), da $-1Nq$ und Nichtrest mal Nichtrest gleich Rest ist.
Zu 7) Folgt aus c), da $-1Nq'$ und Rest mal Nichtrest gleich Nichtrest ist.
Zu 8) Folgt aus d), da $-1Nq'$ und Nichtrest mal Nichtrest gleich Rest ist.

Lemma 3.4. *Jede Zahl von der Form $4m+1$ hat Null oder eine gerade Anzahl von Primfaktoren der Form $4m+3$. Jede Zahl von der Form $4m+3$ hat eine ungerade Anzahl von Primfaktoren der Form $4m+3$.*

Satz 3.5. *Wir können nun allgemeinere Aussagen ((9)-(14)) mit Hilfe der angeführten acht Fallunterscheidungen des quadratischen Reziprozitätsgesetzes beweisen. Für die folgenden Beweise nehmen wir an, dass das Gesetz wahr ist, auch wenn der Beweis dafür erst an späterer Stelle steht.*

Wir erinnern uns: a ist eine natürliche Zahl von der Form $4m+1$ und p ist eine Primzahl von der Form $4m+1$. b ist eine natürliche Zahl von der Form $4m+3$ und q ist eine Primzahl von dieser Form.

$$\text{Wenn } pRa \text{ oder } -pRa, \text{ dann ist } \pm aRp. \tag{9}$$

Beweis. Die Zahl a wird aus den Primfaktoren $p', p'', \ldots, q, q', \ldots$ zusammengesetzt. Ist pRa, dann ist p auch Rest aller Faktoren der Zahl a. Es folgt aus den Aussagen 1 und 3, dass die einzelnen Faktoren Reste von p werden. Somit ist auch ihr Produkt a Rest von p. Außerdem ist auch $-aRp$, weil $-1Rp$ (Satz 2.17).
Ist nun hingegen $-pRa$, so folgt, dass $-p$ Rest aller Faktoren $p', p'', \ldots, q, q', \ldots$ ist. Nach der Aussage 1 und 4 werden die Faktoren $p', p'', \ldots$ Reste von p und die Faktoren $q, q', \ldots$ werden Nichtreste. Da die Anzahl der Faktoren $q, q', q'', \ldots$ laut Lemma 3.4 gerade ist, (oder es kommt kein Faktor dieser Form vor) wird das Produkt der Nichtreste auch ein Rest. Somit wird das Produkt aus allen Faktoren, also a, Rest von p. Weiters gilt wie oben wegen $-1Rp$ auch $-aRp$. □

$$\text{Wenn } qRa \text{ oder } -qRa, \text{ dann ist } aRq \text{ und } -aNq. \tag{10}$$

Beweis. Die Zahl a wird aus den Primfaktoren $p, p', \ldots, q', q'', \ldots$ zusammengesetzt. Ist qRa, dann ist q auch Rest aller Faktoren der Zahl a. Es folgt aus den Aussagen 5 und 7, dass die Faktoren $p, p', \ldots$ Reste von q werden und die Faktoren $q', q'', \ldots$ Nichtreste von q werden. Da die Anzahl der Nichtreste gerade sein muss (Lemma 3.4), wird das Produkt aus allen Faktoren, also a, ein Rest von q. Außerdem ist $-a$ Nichtrest von q, weil $-1Nq$ (Satz 2.18).
Ist nun $-qRa$, dann wird $-q$ Rest aller Faktoren und nach den Aussagen 5 und 8 werden alle Primfaktoren Reste von q. Also wird aRq und $-aNq$. □

$$\text{Wenn } pRb, \text{ dann ist } \pm bRp. \tag{11}$$

Beweis. Die Zahl b wird aus den Primfaktoren $p', p'', \ldots, q, q', \ldots$ zusammengesetzt. Ist pRb, dann ist p Rest aller Faktoren der Zahl b. Aus den Aussagen 1 und 3 folgt, dass die Faktoren $p', p'', \ldots, q, q', \ldots$ Reste von p werden. Somit ist auch das Produkt b Rest von p. Da $-1Rp$, ist auch$-bRp$. □

$$\text{Wenn } -pRb, \text{ dann ist } \pm bNp. \tag{12}$$

Beweis. Die Zahl b wird aus den Primfaktoren $p', p'', \ldots, q, q', \ldots$ zusammengesetzt. Wenn $-pRb$, dann ist $-p$ Rest von allen Faktoren der Zahl b. Aus der Aussage 1 folgt, dass alle Faktoren $p', p'', \ldots$ Rest von p sind. Aus der Aussage 4 folgt, dass alle Faktoren $q, q', \ldots$ Nichtreste von p werden.
Da wir aus dem Lemma 3.4 wissen, dass b eine ungerade Anzahl an Primfaktoren von der Form $4m+3$ hat, wird das Produkt b ein Nichtrest von p. Außerdem ist auch $-bNp$, weil $-1Rp$. □

$$\text{Wenn } qRb, \text{ dann ist } -bRq \text{ und } bNq. \tag{13}$$

Beweis. Die Zahl b wird aus den Primfaktoren $p, p', \ldots, q', q'', \ldots$ zusammengesetzt. Wenn qRb, dann ist q Rest von allen Faktoren der Zahl b. Aus der Aussage 5 folgt, dass alle Faktoren $p, p', \ldots$ Rest von q sind. Aus der Aussage 7 folgt, dass alle Faktoren $q', q'', \ldots$ Nichtreste von q werden.
Da wir aus dem Lemma 3.4 wissen, dass b eine ungerade Anzahl an Primfaktoren von der Form $4m+3$ hat, wird das Produkt b ein Nichtrest von q, was wiederum gleichbedeutend ist mit $-bRq$, weil $-1Nq$. □

$$\text{Wenn } -qRb, \text{ dann ist } bRq \text{ und } -bNq. \tag{14}$$

Beweis. Die Zahl b wird aus den Primfaktoren $p, p', \ldots, q', q'', \ldots$ zusammengesetzt. Wenn $-qRb$, dann ist $-q$ Rest von allen Faktoren der Zahl b. Aus der Aussage 5 folgt, dass alle Faktoren $p, p', \ldots$ Rest von q sind. Aus der Aussage 8 folgt, dass alle Faktoren $q', q'', \ldots$ Reste von q werden. Da Rest mal Rest ein Rest wird, wird das Produkt b Rest von q. Also ist (wegen $-1Nq$) $-b$ Nichtrest von q. □

Satz 3.6. *Es seien g und h zwei beliebige ungerade, teilerfremde ganze Zahlen. Wir bezeichnen mit i die Anzahl der Primfaktoren von g, für welche h Nichtrest ist. Wenn eine Primzahl, deren Nichtrest h ist, mehrfach unter den Faktoren von g vorkommt, dann ist er so oft zu zählen, wie er vorkommt. Genauso bezeichnen wir durch j die Anzahl der Primfaktoren von h, für welche g Nichtrest ist.*

a) Die Zahlen i, j werden beide gerade oder beide ungerade, wenn die Zahlen g, h die Formen haben:

i) $+a, +a'$ iv) $+a, -b$

ii) $+a, -a'$ v) $-a, -a'$

iii) $+a, +b$ vi) $+b, -b'$

b) Die eine der Zahlen i, j wird gerade und die andere ungerade, wenn die Zahlen g, h die Formen haben:

vii) $-a, +b$ ix) $+b, +b'$

viii) $-a, -b$ x) $-b, -b'$

Bevor wir diesen Satz beweisen, führen wir ein Beispiel an, um die Aussage des Satzes leichter zu verstehen.

Beispiel 3.7. *Es sind die Zahlen $a = 9$ und $-b = -55$ gegeben. Wir rechnen i und j aus und vergleichen, ob Fall iv) eintritt. Zuerst berechnen wir i. Dafür müssen wir die Anzahl der Primfaktoren von a, für die $-b$ Nichtrest ist bestimmen. Die Primfaktoren von 9 sind zweimal die drei und da $-55N3$ (weil $2N3$) ist $i = 2$. Die Anzahl der Primfaktoren von b (5 und 11), für die a Nichtrest ist, ist j. Wir wissen, dass $9R5$ und $9R11$ und somit ist $j = 0$. Beide Zahlen i, j sind also gerade, Fall iv) ist eingetreten.*

Beweis. Es seien g und h zwei ungerade, teilerfremde ganze Zahlen. Genauso wie oben, bezeichnen wir mit i die Anzahl der Primfaktoren von g, für welche h Nichtrest ist und j ist die Anzahl der Primfaktoren von h, für welche g Nichtrest ist.

(1) Zu Beginn wollen wir g ohne Rücksicht auf sein Vorzeichen in Primfaktoren $l_1, l_2, l_3, \ldots$ zerlegen. Außerdem wird h in irgendeiner Weise in Faktoren zerlegt. Unter diesen Faktoren gibt es m_1, welche Nichtreste von l_1 sind, m_2, welche Nichtreste von l_2 sind und so weiter. Dabei seien $m_1, m_2, \ldots$ aus den natürlichen Zahlen. Die Zahl i gibt an, für wie viele unter den Primfaktoren $l_1, l_2, l_3, \ldots$ h Nichtrest ist. Also gibt sie auch an, wie viele der Zahlen $m_1, m_2, \ldots$ ungerade sind (Dies gilt, weil das Produkt nur ein Nichtrest wird, wenn die Anzahl der Faktoren, welche Nichtreste sind, ungerade ist.)
Wir bezeichnen nun mit s die Anzahl aller Zahlenpaare (f, l), sodass der Faktor f von h Nichtrest des Primfaktors l von g ist. Es gilt $s = m_1 + m_2 + m_3 + \ldots$.
Wir können nun einen Zusammenhang zwischen i und s aufstellen. Wenn i gerade ist, so ist auch s gerade. Hingegen gilt, wenn i ungerade ist, so ist auch s ungerade. Es werden also beide Zahlen gerade oder beide ungerade. Wir wissen somit $i \equiv s \pmod 2$. Dies gilt allgemein, egal auf welche Weise h in Faktoren zerlegt sei.

(2) Wir werden zuerst die Fälle i, iii, iv und vi) betrachten. In diesen Fällen ist g positiv und h von der Form $+a$ oder $-b$. Weiters zerlegen wir g und h in Primfaktoren. Bei den Primfaktoren von h geben wir den Faktoren von der Form p ein positives Vorzeichen und den Faktoren von der Form q ein negatives Vorzeichen. Dann hat h immer die gewünschte Form a oder $-b$.
Wie im oberen Abschnitt bezeichnet s die Anzahl der Zahlenpaare (f, l), in denen der Primfaktor f von h Nichtrest des Primfaktors l von g ist. Ähnlich dazu ist jetzt t die Anzahl der Zahlenpaare (f, l), in denen der Primfaktor l von g Nichtrest des Faktors f von h ist. Aus dem quadratischen Reziprozitätsgesetz und den daraus abgeleiteten Aussagen folgt, dass die Zahlenpaare identisch sind und daher ist $s = t$.
Wir wissen aus dem ersten Abschnitt, dass $i \equiv s \pmod 2$ und aus dem gleichen Grund muss auch $j \equiv t \pmod 2$ sein. Also ist auch $i \equiv j \pmod 2$, womit die Aussagen i), iii), iv) und vi) bewiesen sind.

Die übrigen Behauptungen können wir aus den bereits gezeigten Fällen ableiten. Dazu führen wir aber noch eine Kurzschreibweise ein.

(3) Wir betrachten neben i, j nun auch noch i'. Unter i' verstehen wir die Anzahl der Primfaktoren von g, für welche $-h$ Nichtrest ist. Wenn h negativ ist, dann ist natürlich

$-h$ positiv. Wir teilen alle Primfaktoren von g in vier Klassen auf:

a) in Faktoren der Form p, für welche h Rest ist;

b) in Faktoren der Form q, für welche h Rest ist (ihre Anzahl sei x);

c) in Faktoren der Form p, für welche h Nichtrest ist (ihre Anzahl sei y) und

d) in Faktoren der Form q, für welche h Nichtrest ist (ihre Anzahl sei z).

Somit gilt: $i = y + z$ und $i' = x + y$.
Durch Umformen und einsetzten erhalten wir $i' = i + x - z$.

Wenn g von der Form $\pm a$ ist, dann ist $x + z$ eine gerade Zahl, genauso wie $x - z$ eine gerade Zahl sein muss. Daraus folgt

$$i' = i + x - z \equiv i \pmod 2.$$

Ist hingegen g von der Form $\pm b$, das heißt g hat eine ungerade Anzahl an Primfaktoren von der Form q, dann ist $x + z$ ungerade, genauso wie $x - z$. Somit ist

$$i' = i + x - z \not\equiv i \pmod 2,$$

also i und i' sind modulo 2 inkongruent.

Im letzten Abschnitt des Beweises wenden wir die erarbeiteten Resultate auf die einzelnen Fälle an. Es fehlen noch die Fälle ii), v) und vii)-x).

(4) Um den zweiten Fall zu beweisen, gehen wir zu Beginn davon aus, dass g und h von der Form $+a$ sind. Wie oben bereits angeführt, wird in diesem Fall $i \equiv j \pmod 2$. Weiters wissen wir aus dem Abschnitt (3) auch, dass $i' \equiv i \pmod 2$. Aus diesen beiden Äquivalenzen folgt $i' \equiv j \pmod 2$ und somit ist die zweite Behauptung bewiesen.

Nun wollen wir die fünfte Aussage beweisen. Wenn g von der Form $-a$ und h von der Form $+a$ ist, dann folgt nach der eben bewiesenen Aussage (ii), dass $i \equiv j \pmod 2$. Wieder folgt aus dem dritten Abschnitt des Beweises, dass $i' \equiv i \pmod 2$, also auch $i' \equiv j \pmod 2$, womit v) bewiesen ist.

Wir leiten vii) aus iii) ab. Wir wählen g von der Form b und h ist von der Form a. Dann gilt laut iii), dass $i \equiv j \pmod 2$. Außerdem wissen wir, dass $i' \not\equiv i \pmod 2$, weil g von der Form b ist. Daraus folgt $i' \not\equiv j \pmod 2$, womit vii) gezeigt ist.

Analog dazu kann man aus der vierten Aussage die Achte ableiten. Hier wählt man g von der Form $-b$ und h von der Form a. Dann gelten wie im Absatz davor alle Äquivalenzen und man erhält die Aussage für $-a$ und $-b$.

ix) und x) leiten wir beide aus vi) ab. Aus vi) wissen wir, wenn g von der Form b und h von der Form $-b$ ist, dann ist $i \equiv j \pmod 2$. Da g von der Form b ist wissen wir auch, dass $i' \not\equiv i \pmod 2$. Somit ist auch $i' \not\equiv j \pmod 2$ und ix) ist bewiesen.
Die letzte Aussage wird wieder ganz ähnlich bewiesen. Wir setzten zu Beginn g von der Form $-b$ und h von der Form b. Mit Hilfe der gleichen Äquivalenzen wie im vorangegangenen Abschnitt lässt sich die zehnte und letzte Aussage analog beweisen.

Wir konnten nun alle Aussagen überprüfen, dennoch müssen wir uns dessen Bewusst sein, dass wir für diesen Beweis die Richtigkeit des quadratischen Reziprozitätsgesetzes vorausgesetzt haben. Beziehungsweise können wir durch die Beweismethode erkennen, dass der Satz richtig ist, sobald das Reziprozitätsgesetz für alle miteinander kombinierten Primfaktoren von g und h richtig ist. Auch wenn es nicht allgemein wahr wäre. □

Bemerkung.
Wenn g und h Primzahlen sind, dann kann Satz 3.6 in das quadratische Reziprozitätsgesetz übergeführt werden.
In diesem Fall können i und j nicht größer als 1 werden. Wenn i oder j gerade sein muss, dann können sie nur gleich 0 sein. Ist zum Beispiel $i = 0$, dann ist h Rest von g. Wenn i jedoch ungerade ist ($i = 1$), dann wird h Nichtrest von g. Das gleiche gilt natürlich auch für j.

Aus i) folgt: Wenn p Rest von p' ist, dann ist $i = 0$. Also muss $j = 0$ sein und somit folgt, dass p' Rest von p ist (vgl. Aussage 1 aus Satz 3.1.b). Wenn p Nichtrest von p' ist, also $i = 1$, dann wird p' Nichtrest von p, weil $j = 1$ sein muss (vgl. Aussage 2 aus Satz 3.1.b).

Aus ii) folgt: Ist p Rest von p' ($i = 0$), dann ist $-p'$ Rest von p, weil $j = 0$ sein muss (vgl. Aussage 1). Ist p Nichtrest von p' ($i = 1$), dann ist $-p'$ Nichtrest von p, weil $j = 1$ sein muss (vgl. Aussage 2).

Aus iii) folgt: Ist p Rest von q, so ist q Rest von p (vgl. Aussage 3). Ist p Nichtrest von q, so ist q Nichtrest von p (vgl. Aussage 4).

Aus iv) folgt: Wenn p Rest von q ist, dann ist $-q$ Rest von p (vgl. Aussage 3). Wenn p Nichtrest von q ist, dann folgt dass $-q$ Nichtrest von p ist (vgl. Aussage 4).

Aus v) folgt: Ist $-p$ Rest von p', so ist $-p'$ Rest von p (vgl. Aussage 1). Ist jedoch $-p$ Nichtrest von p', dann ist auch $-p'$ Nichtrest von p (vgl. Aussage 2).

Aus vi) folgt: Ist q Rest von q', dann folgt $-q'$ ist Rest von q (vgl. Aussage 7). Und wenn q Nichtrest von q' ist, dann ist auch $-q'$ Nichtrest von q (vgl. Aussage 8).

Aus vii) folgt: Ist $-p$ Rest von q, also $i = 0$, dann ist q Nichtrest von p, weil $j = 1$ sein muss (vgl. Aussage 4). Wenn $-p$ Nichtrest von q, dann ist hingegen q Rest von p (vgl. Aussage 3).

Aus viii) folgt: Wenn $-p$ Rest von q ist, so ist $-q$ Nichtrest von p (vgl. Aussage 4). Wenn $-p$ Nichtrest von q ist, so ist $-q$ Rest von p (vgl. Aussage 3).

Aus ix) folgt: Ist q Rest von q', so ist q' Nichtrest von q (vgl. Aussage 7). Ist q Nichtrest von q', so ist q' Rest von q (vgl. Aussage 8).

Aus x) folgt: Ist $-q$ Rest von q', so folgt, dass $-q'$ Nichtrest von q ist (vgl. Aussage 8). Ist $-q$ Nichtrest von q', so ist $-q'$ Rest von q (vgl. Aussage 7).
Wählt man also für g und h Primzahlen, dann gehen die Aussagen in jene des quadratischen Reziprozitätsgesetzes über.

4 Gauß' erster Beweis

Wir können uns nun endlich dem Beweis des quadratischen Reziprozitätsgesetzes widmen. Der nun angeführte Beweis war auch historisch gesehen der erste vollständige Beweis dieses Satzes und wurde von Carl Friedrich Gauß in seinem ersten Buch „Disquisitiones arithmeticae“ im Jahre 1801 veröffentlicht. Dieser erfolgt, wie bereits erwähnt, mit Hilfe der Methode der vollständigen Induktion. Dafür sagen wir, dass das quadratische Reziprozitätsgesetz bis zu einer gewissen Zahl m hin richtig ist und zwar genau dann, wenn es für zwei beliebige Primzahlen gilt, von denen jedoch keine m übertrifft. In dieser Art soll es auch bei den Sätzen 3.1.a und b, 3.5 und 3.6 verstanden werden. Wenn man davon ausgeht, dass das Gesetz bis zu einer gewissen Schranke m richtig ist, dann ist es leicht nachzuvollziehen, dass auch die erwähnten Sätze, welche wir ja mit Hilfe des Fundamentaltheorems bewiesen haben, bis zu dieser Schranke hin gültig sind. Die Ausführungen in diesem Kapitel folgen wieder dem Kapitel „Thema. Beweis des quadratischen Reziprozitätsgesetzes“ von Pieper [7].
Für kleine Zahlen konnten wir uns beispielhaft bereits überzeugen, dass das Reziprozitätsgesetz wahr ist. Somit müsste es für den Fall, dass es nicht allgemein wahr ist, eine Schranke t geben, bis zu welcher es gilt, während es bis zur nächst höheren Zahl $t+1$ nicht mehr gilt. Das würde bedeuten, dass zwei Primzahlen gegeben sind, von der die größere $t+1$ ist und die sich dem quadratischen Reziprozitätsgesetz widersprechend verhalten, obwohl alle beliebigen zwei Primzahlen, solange sie nur beide kleiner sind als $t+1$, sich dem Gesetzte entsprechend verhalten. Es folgt daraus, dass die oben erwähnten Sätze genauso bis zur Schranke t gelten.
Um die Richtigkeit des quadratischen Reziprozitätsgesetz nachzuweisen, müssen wir zeigen, dass diese Annahme einer Schranke nicht richtig sein kann.

Wir unterscheiden vier Fälle, abhängig von der Form der zwei Primzahlen, welche sich nicht dem Gesetz entsprechend verhalten. Es bezeichne ab sofort $l = t + 1$, die größere Primzahl und l' die kleinere Primzahl.

Fall A. $l \equiv 1 \pmod 4$ und $l' \equiv 1 \pmod 4$.
Das quadratische Reziprozitätsgesetz wäre falsch, wenn entweder a) $\pm l'Rl$ und $\pm lNl'$, oder b) $\pm l'Nl$ und $\pm lRl'$ wäre.

Fall B. $l \equiv 3 \pmod 4$ und $l' \equiv 3 \pmod 4$.
Das quadratische Reziprozitätsgesetz wird falsch, wenn entweder a) $+l'Rl$ und $-lNl'$

(oder, was das Gleiche ist, $-l'Nl$ und $+lRl'$), oder b) $+l'Nl$ und $-lRl'$ (oder, was das Gleiche ist, $-l'Rl$ und $+lNl'$).

Fall C. $l \equiv 1 \pmod 4$ und $l' \equiv 3 \pmod 4$.
Das quadratische Reziprozitätsgesetz wäre falsch, wenn entweder a) $\pm l'Rl$ und $+lNl'$ (oder $-lRl'$), oder b) $\pm l'Nl$ und $-lNl'$ (oder $+lRl'$) wäre.

Fall D. $l \equiv 3 \pmod 4$ und $l' \equiv 1 \pmod 4$.
Das quadratische Reziprozitätsgesetz wird falsch, wenn entweder a) $+l'Rl$ (oder $-l'Nl$) und $\pm lNl'$, oder b) $+l'Nl$ (oder $-l'Rl$) und $\pm lRl'$.

Wenn wir nun beweisen können, dass keiner dieser acht Fälle eintreten kann, dann haben wir gezeigt, dass das quadratische Reziprozitätsgesetz an keine obere Schranke gebunden ist und somit allgemein gültig sein muss.
Im folgenden Beweis werden die Fälle teils in einer anderen Reihenfolge angeführt als bisher, weil manche Fälle voneinander abhängig sind.

1. Fall. Es sei $l = t + 1$ und $l' < l$ außerdem sind l und l' von der Form $4m + 1$.
Zu zeigen: Wenn $\pm l'Rl$, dann kann nicht $\pm lNl'$ sein. (Fall A, a)).

Beweis. Es sei $\pm l'Rl$, also ist $+l' \equiv x^2 \pmod l$. Wir können dafür immer ein gerades x auswählen, welches außerdem auch kleiner als l ist.

α) Wir beginnen mit dem Fall, dass x durch l' nicht teilbar ist. Wir setzen dann für $x^2 = l' + lf$. Es muss f einen positiven Wert annehmen, da sonst $l' + lf < 0$ werden würde, weil $l' < l$ ist. Da aber jede Quadratzahl positiv sein muss, folgt, dass auch f positiv ist. Außerdem muss f von der Form $4m + 3$ sein. Wir haben x gerade gewählt, also ist x^2 durch 4 teilbar. Damit die Summe $l' + lf$ auch durch 4 teilbar wird, muss f von der Form $4m + 3$ sein.
Weiters ist $f < l$. Würde $f \geq l$ sein, dann wäre $x^2 = l' + lf \geq l' + l^2$, dies kann aber nicht sein, weil wir x kleiner l gewählt haben. Somit ist auch x^2 kleiner l^2. Das heißt f ist kleiner als l.
Es muss $l' \nmid f$ gelten. Angenommen $l' \mid f$, dann würde ein $z \in \mathbb{Z}$ existieren mit: $f = l'z$. Daraus folgt

$$x^2 = l' + ll'z = l' \cdot (1 + lz).$$

Wir erkennen, dass x^2 durch l' geteilt werden würde. Da aber l' eine Primzahl ist, folgt

auch, dass $l' \mid x$ und diese Aussage widerspricht unserer Voraussetzung. Also ist auch f nicht teilbar durch l'.
Aus $x^2 = l' + lf$ folgt auch $x^2 \equiv l' \pmod{f}$ oder anders formuliert $l'Rf$. Genauso folgt $lfRl'$ aus der Gleichung $x^2 = l' + lf$. Wir wissen l' und f sind beide kleiner l. Deshalb gilt die Aussage 11) aus Satz 3.5, das heißt aus $l'Rf$ folgt, dass $\pm fRl'$.
Wir wissen also, dass $\pm fRl'$ und $lfRl'$. Daraus folgt, dass $\pm lRl'$ sein muss (weil Rest mal Rest gleich Rest ist). Also haben wir für den Fall, dass x nicht teilbar durch l' ist gezeigt, dass, wenn $\pm l'$ quadratischer Rest von l ist, $\pm l$ kein Nichtrest von l' werden kann.

β) Jetzt ist x durch l' teilbar, wir setzen $x = yl'$ und $x^2 = l' + ll'h$.
Da wir x gerade gewählt haben und l' ungerade ist, folgt aus der Gleichung $x = yl'$, dass y gerade sein muss. Wir können x^2 durch $y^2l'^2$ ersetzen und erhalten

$$y^2l'^2 = l' + ll'h.$$

Dividieren wir die Gleichung durch l', kommen wir auf

$$y^2l' = 1 + lh.$$

Aus dieser Gleichung folgt, dass h von der Form $4m + 3$ sein muss. Wir überprüfen, dass h zu l' und zu y^2 teilerfremd ist. Dafür betrachten wir die Gleichung $y^2l' = 1 + lh$ genauer. Wenn h mit l' oder y^2 einen gemeinsamen Primteiler p hat, dann müsste p auch y^2l' teilen. Da y^2l' aber nur um 1 größer als lh ist, kann p nicht y^2l' teilen. Also ist h zu y^2 und auch zu l' teilerfremd.
Man kann schnell erkennen, dass $l'y^2$ ein quadratischer Rest von h ist, weil $1^2 = l'y^2 - lh$. Da natürlich auch y^2 quadratischer Rest von h ist, folgt, dass $l'Rh$. Wie in α können wir aus der Aussage 11) aus Satz 3.5 folgern, dass $\pm hRl'$. Damit wir diesen Satz verwenden dürfen müssen wir uns noch kurz davon überzeugen, dass l' und h kleiner l sind. Wir wissen l' ist kleiner l laut Definition und wäre $h \geq l$, dann wäre

$$x^2 = l' + ll'h \geq l' + l^2l',$$

also $x^2 \geq l^2$, was nicht sein kann, weil wir $x < l$ gewählt haben. Also ist h kleiner l.
Es ist $-lhRl'$, weil $1 = l'y^2 - lh$ und somit $1 \equiv -lh \pmod{l'}$. Zusammengefasst folgt aus $\pm hRl'$ und $-lhRl'$, dass $\pm l$ Rest von l' sein muss (weil Rest mal Rest gleich Rest ist). $\square$

2. Fall. Es sei $l = t + 1$ und $l' < l$. Weiter sei $l \equiv 1 \pmod 4$ und $l' \equiv 3 \pmod 4$. Zu zeigen: Wenn $\pm l'Rl$, dann kann weder $+lNl'$ noch $-lRl'$ sein (Fall C, a)).

Beweis. Es sei $\pm l'Rl$ und $x^2 = l' + lf$. Wir können x gerade und kleiner l annehmen.

α) Es sei x durch l' nicht teilbar. Daraus folgt, dass auch f durch l' nicht teilbar ist. Angenommen $l' \mid f$, dann wird x^2 durch l' geteilt und somit gilt auch $l' \mid x$, weil l' eine Primzahl ist. Dies ist ein Widerspruch zu unserer Annahme. Also gilt $l' \nmid f$.
Wäre $f < 0$, dann wäre auch $x^2 = l' + lf < 0$, weil $l > l'$ ist. Da das Quadrat aber nicht negativ sein kann, muss auch $f > 0$ sein. Jedoch kann f nicht größer oder gleich als l werden, sonst würde nämlich wie im ersten Fall auch, $x^2 \geq l^2$ werden und das widerspricht unserer Annahme, dass x kleiner l ist.
Aus der Gleichung $x^2 = l' + lf$ können wir die Form von f bestimmen. Wir wissen, dass x gerade ist, also ist x^2 durch 4 teilbar. Es muss also die Summe $l' + lf$ auch durch 4 teilbar werden. Dies ist genau dann der Fall, wenn f von der Form $4m + 1$ ist.
Wieder aus der Gleichung $x^2 = l' + lf$ können wir ableiten, dass auch $l'Rf$ gilt und auch $lfRl'$. Weil l' und f beide kleiner l sind, können wir Satz 3.5 anwenden (Aussage 10). Das heißt aus $l'Rf$ folgt fRl'.
Da $lfRl'$ und fRl' ist, muss auch lRl' werden (weil Rest mal Rest gleich Rest ist). Wir wissen $-1Nl'$, also ist auch $-lNl'$ und haben somit die Behauptung gezeigt.

β) Nun ist x durch l' teilbar. Es sei $x = yl'$ und $f = l'h$. Also

$$x^2 = y^2 l'^2 = l' + lf = l' + ll'h.$$

Wir dividieren die Gleichung wieder durch l' und erhalten

$$y^2 l' = 1 + lh.$$

Durch Nachrechnen kann man überprüfen, dass h von der Form $4m+3$ sein muss (y muss gerade sein) und positiv, weil sonst $y^2 l'$ negativ sein müsste. Außerdem ist h teilerfremd zu l' und auch zu y^2, dies folgt analog wie im 1. Fall bei β.
Aus der Gleichung $y^2 l' = 1 + lh$ kann man $y^2 l'Rh$ ableiten. Weil $y^2 Rh$ folgt auch $l'Rh$. Da l' und h kleiner l sind, folgt mit Hilfe des Satzes 3.5 (Aussage 13) aus $l'Rh$, dass auch $-hRl'$. Außerdem wissen wir, dass $-lhRl'$, weil $1 \equiv -lh \pmod{l'}$.
Zusammen folgt aus $-hRl'$ und $-lhRl'$, dass lRl' sein muss. Und weil $-1Nl'$ folgt, dass $-lNl'$. □

3. Fall. Es sei $l = t + 1$ und $l' < l$. Weiter sei l und $l' \equiv 1 \pmod 4$.
Zu zeigen: Wenn $\pm l'Nl$, dann kann nicht $\pm lRl'$ sein (Fall A, b)).

Beweis. Für den Beweis bestimmen wir eine Primzahl, welche kleiner als l ist und für die l Nichtrest ist. Die Existenz dieser Primzahl haben wir im Satz 3.3 gezeigt. Jedoch müssen wir eine Unterscheidung durchführen, weil wir in diesem Satz keine Aussage über die Form der Primzahl gemacht haben. Wir wissen also nicht, ob es derartige Primzahlen von der Form $4m + 1$ und von der Form $4m + 3$ gibt.

I) Es sei diese Primzahl von der Form $4m + 1$. Wir bezeichnen sie mit p. Da l Nichtrest für p ist, oder kürzer lNp, muss auch $\pm pNl$ sein. Dies folgt daraus, dass $\pm pRl$ nicht sein kann, weil sonst aus dem ersten Fall, der bereits bewiesen wurde folgen würde, dass $\pm lRp$. Also muss wegen lNp auch $\pm pNl$ sein.
Nach Voraussetzung gilt $\pm l'Nl$ und mit $\pm pNl$ zusammen folgt, dass $\pm pl'Rl$ sein muss (weil Nichtrest mal Nichtrest gleich Rest ist). Es ist also $\pm pl'$ Rest von l. Wir können daher auch schreiben $x^2 \equiv pl' \pmod l$. Wieder können wir hier x gerade und kleiner l wählen.
Diesmal müssen wir sogar vier Fälle unterscheiden:

α) In diesem Fall ist x weder durch l' noch durch p teilbar. Wir setzen $x^2 = pl' \pm lf$ und wählen das Vorzeichen so, dass f immer positiv wird. Es muss f kleiner l sein. Wäre f größer oder gleich l, dann wäre bei dem positiven Vorzeichen $x^2 = pl' + lf \geq pl' + l^2$, also $x^2 \geq l^2$. Das kann aber nicht sein, weil wir $x < l$ gewählt haben und somit auch $x^2 < l^2$ sein muss. Und bei dem negativen Vorzeichen würde $pl' - lf$, wenn $f \geq l$ ist, kleiner Null werden. Das kann aber auch nicht sein, weil x^2 immer größer Null ist. Das heißt, f ist in beiden Fällen kleiner l.
Im nächsten Absatz überprüfen wir, dass f teilerfremd zu p und l' ist. Da p und l' beides Primzahlen sind, genügt es zu zeigen, dass f weder durch p noch durch l' geteilt wird. Angenommen $p \mid f$, dann ist $f = pz$ mit z aus $\mathbb{Z}$. Aus der Gleichung $x^2 = pl' \pm lf$ folgt

$$x^2 = pl' \pm pzl$$
$$x^2 = p \cdot (l' \pm zl).$$

Das heißt $p \mid x^2$. Weil p eine Primzahl ist, folgt daraus $p \mid x$. Dies steht im Widerspruch zu unserer Voraussetzung, also sind f und p teilerfremd.
Analog folgt, dass f zu l' teilerfremd ist. Wie im obigen Absatz nehmen wir an, dass

$l' \mid f$ und erhalten den Widerspruch, dass x durch l' geteilt wird.
Man kann leicht nachrechnen, dass f in der Gleichung $x^2 = pl' + lf$ von der Form $4m+3$ ist (x ist gerade, also muss x^2 durch 4 teilbar sein). Hingegen bei $x^2 = pl' - lf$ ist f von der Form $4m + 1$.
Wir bezeichnen die Anzahl der Primfaktoren von h, für die g Nichtrest ist, mit $[g, h]$.
Aus $x^2 = pl' \pm lf$ wissen wir, dass pl' quadratischer Rest von f ist, kurz $pl'Rf$. Also ist pl' Rest für alle Primfaktoren von f und somit ist $[pl', f] = 0$. Wenn f von der Form $4m+3$ ist, dann wird laut Satz 3.6 iii) $[f, pl']$ gerade. Wenn f von der Form $4m + 1$ ist, dann folgt dies aus i) aus dem Satz 3.6. Da pl' in maximal zwei Primfaktoren zerlegt werden kann, muss $[f, pl']$ gleich 0 oder 2 werden. Das heißt f wird quadratischer Rest von beiden Zahlen p und l' oder von keiner. Der Fall, dass beide quadratische Reste werden, kann nicht eintreten. Es ist $\pm lf$ Rest von p (folgt aus $x^2 = pl' \pm lf$) und laut Voraussetzung ist $\pm lNp$ also wird $\pm fNp$ (weil Nichtrest mal Nichtrest gleich Rest ist). Das heißt aber auch, dass f Nichtrest für l' sein muss.
Wieder wegen $x^2 = pl' \pm lf$ folgt $\pm lfRl'$. Zusammen mit fNl' folgt, dass $\pm lNl'$, was zu zeigen war.

β) In diesem Fall ist x durch l' teilbar, aber nicht durch p. Es sei $x = yl'$ mit $y \in \mathbb{Z}$. Da $x^2 \equiv pl' \pmod{l}$ ist, können wir für x^2 auch $pl' \pm ll'h$ schreiben. Es folgt weiter

$$x^2 = y^2 l'^2 = pl' \pm ll'h.$$

Vereinfacht erhalten wir $y^2 l' = p \pm lh$. Das Vorzeichen wählen wir so, dass h positiv wird. Es ist h kleiner l. Um dies zu zeigen, nehmen wir an, dass h größer oder gleich l ist. Wir müssen wieder zwei Fälle unterscheiden. Bei der Addition folgt

$$x^2 = pl' + ll'h \geq pl' + l^2 l' \geq l^2.$$

Das kann aber nicht sein, weil $x < l$ und somit auch $x^2 < l^2$ sein muss. Bei der Subtraktion ist $x^2 = \underbrace{pl'}_{<l^2} - \underbrace{ll'h}_{\geq l^2}$, also würde $x^2 < 0$ werden, womit wir wieder bei einem Widerspruch angekommen sind.
Nun zeigen wir, dass h zu p, y und l' teilerfremd ist. Da p eine Primzahl ist, reicht es zu zeigen, dass $p \nmid h$. Angenommen $p \mid h$, dann ist $h = pz$ mit z aus den ganzen Zahlen. Es

folgt

$$\begin{aligned} x^2 &= l'p \pm lhl' \\ x^2 = l'p \pm pzll' &= p \cdot (l' \pm zll'). \\ &\Rightarrow p \mid x^2 \Rightarrow p \mid x \end{aligned}$$

Da laut Voraussetzung x nicht durch p teilbar ist und somit auch h nicht durch p teilbar ist, folgt h ist teilerfremd zu p.
Nun nehmen wir an, dass h nicht teilerfremd zu y ist und $h = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ und $y = p'_1 \cdot \ldots \cdot p'_{n'}$. Dann existiert ein Primfaktor von h und von y, wir nennen ihn p_i. Außerdem ist p_i ungleich p, weil $p \nmid h$. Wenn dieses p_i existiert, dann kann $l'y^2 = p \pm lh$ geschrieben werden als

$$\begin{aligned} l'{p_i}^2{y'}^2 &= p \pm lp_ih' \\ p = l'{p_i}^2{y'}^2 \pm lp_ih' &= p_i \cdot (l'p_i{y'}^2 \pm lh'). \\ &\Rightarrow p_i \mid p \end{aligned}$$

Da p eine Primzahl ist, kann p nicht durch p_i geteilt werden. Also muss h teilerfremd zu y sein.
Angenommen h ist nicht teilerfremd zu l', dann ist h durch l' teilbar. Es ist $h = l'z$ mit z aus den ganzen Zahlen. Dann folgt

$$\begin{aligned} l'y^2 &= p \pm ll'z \\ p = l'y^2 \pm ll'z &= l' \cdot (y^2 \pm lz). \\ &\Rightarrow l' \mid p \end{aligned}$$

Die Primzahl p kann aber nicht durch l' geteilt werden, außer $p = l'$, dies kann aber auch nicht sein, weil sonst folgen würde, dass x durch p teilbar wäre, was der Voraussetzung widerspricht. Also folgt schlussendlich h ist teilerfremd zu l'.
Die Form von h muss wieder für beide Vorzeichen getrennt betrachtet werden. In der Gleichung $l'y^2 = p + lh$ muss h von der Form $4m + 3$ sein. Hingegen bei $l'y^2 = p - lh$ muss h von der Form $4m + 1$ sein.
Multipliziert man die Gleichung $y^2l' = p \pm lh$ mit l', so kann man erkennen, dass a) $pl'Rh$ und b) $\pm lhl'Rp$. Wenn man die Gleichung mit p multipliziert, so erhält man c) $lhpRl'$.
Aus a) folgt, dass pl' Rest von allen Primfaktoren von h wird. Also ist $[pl', h] = 0$. Aus dem Satz 3.6 i) und iii) folgt, dass $[h, pl']$ gerade sein muss. Es ist also h Nichtrest von p

und l', oder h ist Rest von beiden Zahlen.
Wir betrachten zuerst den Fall, dass h Nichtrest von p und l' ist. Aus

$$\begin{aligned} hNp, \\ \pm lNp \text{ (Voraussetzung) und} \\ \pm lhl'Rp \ (b) \end{aligned}$$

folgt, dass $\pm l'$ quadratischer Rest von p ist. Da l' und p beide kleiner l sind, folgt aus dem quadratischen Reziprozitätsgesetz $\pm pRl'$. Nun folgt aus

$$\begin{aligned} \pm pRl', \\ hNl' \text{ und} \\ lhpRl' \ (c), \end{aligned}$$

dass $\pm l$ Nichtrest von l' ist, was wir zeigen wollten.
Wenn h Rest von l' und p ist, folgt $\pm lNl'$ sehr ähnlich. Nämlich aus

$$\begin{aligned} \pm lhl'Rp \ (b), \\ hRp \text{ und} \\ \pm lNp \end{aligned}$$

folgt $\pm l'Np$. Wieder folgt aus dem quadratischen Reziprozitätsgesetz, dass $\pm p$ Nichtrest von l' ist. Aus

$$\begin{aligned} lphRl' \ (b), \\ \pm pNl' \text{ und} \\ hRl' \end{aligned}$$

folgt $\pm lNl'$, womit wir am Ende von β) angekommen sind.

γ) Es sei x durch p teilbar, aber nicht durch l'. Der Beweis dieses Falles weicht nur sehr wenig von dem des vorherigen Falles ab. Es sei $x = py$ und da x durch p geteilt wird, wird auch x^2 durch p geteilt. Wir können also x^2 schreiben als $pl' \pm lpj$. Wir erhalten die

Gleichungen

$$p^2y^2 = pl' \pm lpj$$
$$py^2 = l' \pm lj.$$

Wir wählen das Vorzeichen so, dass j immer positiv wird. Es muss $j < l$ sein. Die Argumentation ist analog zu der des vorherigen Falles, wo $h < l$ war.
Jetzt prüfen wir wieder nach, dass j teilerfremd zu p, y und l' ist. Wir beginnen mit der Untersuchung, ob j teilerfremd zu l' ist. Da l' eine Primzahl ist genügt es zu zeigen, dass $l' \nmid j$. Angenommen $l' \mid j$, dann ist $j = l'z$ mit z aus den ganzen Zahlen. Es gilt

$$x^2 = pl' \pm lpj = pl' \pm lpl'z = l' \cdot (p \pm lpz).$$

Das heißt, dass x^2 durch l' geteilt wird und da l' eine Primzahl ist, wird auch x durch l' geteilt. Dies widerspricht der Voraussetzung, also ist j teilerfremd zu l'.
Auch p ist eine Primzahl, also nehmen wir wieder an, dass j durch p geteilt wird. Es existiert ein $z \in \mathbb{Z}$, sodass $j = pz$ gilt. Es folgt

$$py^2 = l' \pm lpz$$
$$py^2 \pm lpz = p \cdot (y^2 \pm lz) = l'.$$

Also $p \mid l'$. Da l' eine Primzahl ist, kann sie nicht von p geteilt werden, außer es gilt $p = l'$. Dann folgt aber aus $l' \nmid j$ sofort, dass auch j von p nicht geteilt wird.
Es fehlt noch zu überprüfen, dass j teilerfremd zu y ist. Wir zerlegen j und y in Primfaktoren. Angenommen j und y sind nicht teilerfremd, dann gibt es einen gemeinsamen Primfaktor p_i, welcher ungleich l' ist (weil j und l' teilerfremd sind). Es gilt

$$py^2 = l' \pm lj$$
$${pp_i}^2y'^2 = l' \pm lp_ij'$$
$${pp_i}^2y'^2 \pm lp_ij' = p_i \cdot (pp_iy'^2 \pm lj') = l'.$$

Das heißt, $p_i \mid l'$. Da l' eine Primzahl ist, kann l' nicht durch p_i geteilt werden. Also ist j auch teilerfremd zu y.
Wieder bestimmen wir die Form von j. Bei negativem Vorzeichen muss j von der Form $4m + 1$ sein und bei positivem von der Form $4m + 3$.
Jetzt multiplizieren wir die Gleichung $py^2 = l' \pm lj$ mit p. Wir erhalten $p^2y^2 = l'p \pm ljp$

und daraus folgt a) $l'pRj$ und c) $\pm ljpRl'$. Aus der mit l' multiplizierten Gleichung $l'py^2 = l'^2 \pm ll'j$ folgt b) $\pm ll'jRp$.
Die restlichen Schlussfolgerungen sind analog zu denen in β). Es reicht dazu, h durch j zu ersetzen. Somit haben wir auch diesen Fall erfolgreich behandelt.

δ) In diesem Fall ist x durch l' und durch p teilbar. Daraus folgt, dass x auch durch pl' teilbar ist. Wenn $p = l'$, dann folgt aus der Annahme (lNp) schon, dass l Nichtrest von l' ist. Also setzen wir $p \neq l'$. Dann sei $x = pl'y$ und $x^2 = l'p \pm lhpl'$. Es folgt

$$\begin{aligned} y^2p^2l'^2 &= l'p \pm lhpl' \text{ und} \\ y^2pl' &= 1 \pm lh. \end{aligned}$$

Wieder folgt, dass h kleiner l ist und für das positive Vorzeichen von der Form $4m+3$ und beim negativen von der Form $4m+1$. Außerdem ist h zu p und zu l' teilerfremd. Da beides Primzahlen sind, genügt es wieder zu zeigen, dass $p \nmid h$ und $l' \nmid h$. Angenommen p teilt h, dann ist $h = pz$ mit z aus den ganzen Zahlen. Es folgt aus $y^2pl' = 1 \pm lh$

$$\begin{aligned} y^2pl' \pm lpz &= 1 \text{ und} \\ p \cdot (y^2l' \pm lz) &= 1. \end{aligned}$$

Das bedeutet, dass $p \mid 1$, womit wir bei einem Widerspruch angekommen sind. Mit Hilfe der gleichen Schritte, kann auch gezeigt werden, dass h teilerfremd zu l' ist.
Aus der Gleichung $y^2pl' = 1 \pm lh$ kann man die Richtigkeit der folgende drei Aussagen erkennen:

$$\begin{aligned} a)&\ pl'Rh \\ b)&\ \pm lhRp \\ c)&\ \pm lhRl' \end{aligned}$$

Wir wissen, dass $[pl', h] = 0$, weil aus a) folgt, dass pl' auch für jeden einzelnen Primfaktor von h Rest ist. Also folgt wieder aus Satz 3.6 (Aussage i) und iii)), dass $[h, pl'] \equiv 0 \pmod 2$. Das bedeutet, entweder ist h Rest für p und für l', oder h ist Nichtrest für p und l'. Im ersten Fall folgt aus hRp und b) $\pm lhRp$, dass l Rest von p ist. Das kann aber nicht sein, weil wir p so gewählt haben, dass lNp gilt. Also muss der zweite Fall eintreten. Es gilt also hNl' und zusammen mit c) $\pm lhRl'$ folgt, dass $\pm lNl'$.

II) Jene Primzahl sei nun von der Form $4m+3$, wir nennen sie q. Wir wissen also, q ist kleiner l und lNq. Weiters wissen wir, dass $\pm qRl$ nicht sein kann, weil sonst nach dem zweiten Fall des bereits bewiesenen quadratischen Reziprozitätsgesetzes folgen würde, dass lRq, was unserer Annahme widerspricht. Also ist $\pm q$ Nichtrest von l. Wir erinnern uns, die Voraussetzung ist $\pm l'Nl$. Da $\pm l'$ und $\pm q$ Nichtreste von l sind, wissen wir, dass $\pm ql'$ quadratischer Rest von l ist. Wir können daher $x^2 \equiv ql' \pmod{l}$ setzen und x gerade und kleiner l annehmen.
Wir müssen nun wieder vier Fälle unterscheiden. Die Beweise dieser Fälle unterscheiden sich nur sehr gering von jenen, bei denen die Primzahl die Form $4m+1$ hatte. Deshalb werden sie in verkürzter Form angeführt.

α) In diesem Fall ist x weder durch l' noch durch q teilbar. Wir setzen für $x^2 = ql' \pm lf$ und wählen das Vorzeichen so, dass f immer positiv wird. Dann ist f kleiner l und teilerfremd zu q und l'. Bei positivem Vorzeichen ist f von der Form $4m+1$, bei negativem von der Form $4m+3$.
Wenn $x^2 = ql' \pm lf$, dann ist $[ql', f] = 0$.
Ist f von der Form $4m+1$, dann wird laut Satz 3.6 iii) $[f, ql']$ gerade. Also wird f für beide Zahlen Rest, oder für beide Zahlen Nichtrest. Wir wissen aus $lfRq$ und lNq, dass f Nichtrest von q ist. Also muss auch $\pm fNl'$ sein. Zusammen mit $lfRl'$ folgt $\pm lNl'$. Hingegen wenn f von der Form $4m+3$ ist, dann folgt aus Satz 3.6 ix), dass $[f, ql'] \equiv 1 \pmod{2}$. Das heißt

1) fRq und fNl' oder,
2) fNq und fRl'.

Da f bei negativem Vorzeichen von dieser Form wird, folgt $-lfRq$. Dies ist gleichbedeutend mit $lfNq$. Außerdem wissen wir, dass lNq. Daraus folgt fRq und somit muss der erste Fall eintreten. Deshalb ist auch fNl'. Zusammen mit $-lfRl'$ folgt $\pm lNl'$.

β) In diesem Fall ist x durch l' teilbar, aber nicht durch q. Es sei $x = yl'$ und $y^2l' = q \pm lh$. Das Vorzeichen wählen wir wieder so, dass h positiv wird. Es ist h kleiner l und zu q, y und l' teilerfremd. In der Gleichung $l'y^2 = q + lh$ muss h von der Form $4m+1$ sein. Hingegen bei $l'y^2 = q - lh$ muss h von der Form $4m+3$ sein.
Wir multiplizieren die Gleichung $y^2l' = q \pm lh$ mit l' und erkennen a) $ql'Rh$ und b) $\pm lhl'Rq$. Außerdem multiplizieren wir die Gleichung mit q und erhalten c) $lhqRl'$.
Aus a) erhalten wir wie in I), dass $[l'q, h] = 0$.

Wenn h von der Form $4m+1$ ist, also das positive Vorzeichen in der Gleichung vorkommt, dann können wir mit Hilfe der dritten Aussage aus dem Satz 3.6 folgern, dass $[h, l'q] \equiv 0 \pmod 2$. Das heißt entweder ist hRl' und hRq, oder hNl' und hNq.
Wir beginnen mit dem ersten Fall. Es ist also hRq und aus b) wissen wir, dass $+lhl'Rq$. Daraus folgt $l'lRq$. Wir wählten q so, dass lNq. Also ist l' auch Nichtrest von q. Da l' und q beide kleiner l sind, können wir das quadratische Reziprozitätsgesetz anwenden und erhalten $\pm qNl'$. Aus c) $lhqRl'$ und weil wir wissen, dass hRl' ist, folgt $\pm lNl'$.
Tritt der zweite Fall ein, ist $l'Rq$, weil

$$hNq,\ lhl'Rq \text{ und } lNq.$$

Es folgt aus dem quadratischen Reziprozitätsgesetz $\pm qRl'$. Aus c) $lhqRl'$, hNl' und $\pm qRl'$ folgt schlussendlich $\pm lNl'$.

Wenn h von der Form $4m+3$ ist, dann folgt aus Satz 3.6 ix), dass $[h, l'q] \equiv 1 \pmod 2$. Das heißt,

1) h ist Rest von l' und h ist Nichtrest von q, oder

2) h ist Nichtrest von l' und h ist Rest von q.

Wir beginnen wieder mit dem ersten Fall. Wenn h von der Form $4m+3$ ist, dann wissen wir, dass b) $-lhl'Rq$ gilt. Dies ist gleichbedeutend mit $lhl'Nq$. Außerdem ist lNq und im ersten Fall ist auch h Nichtrest von q. Aus diesen drei Aussagen folgt, dass l' Nichtrest von q ist. Wir können mit Hilfe des quadratischen Reziprozitätsgesetzes $\pm qNl'$ folgern. Wir können außerdem aus c) $lhqRl'$, hRl' und $\pm qNl'$ erkennen, dass $\pm l$ Nichtrest von l' sein muss.
Genauso folgt auch aus dem zweiten Fall, dass $\pm lNl'$ sein muss.

γ) Es ist x durch q teilbar, aber nicht durch l'. Der Beweis dieses Falles weicht nur sehr wenig von dem des vorherigen Falles ab, deshalb werden wir ihn nicht anführen.

δ) In diesem Fall ist x durch l' und durch q teilbar. Daraus folgt, dass x auch durch ql' teilbar ist. Wenn $q = l'$, dann folgt aus der Annahme (lNq) schon, dass l Nichtrest von l' ist. Also setzen wir $q \neq l'$. Dann sei $x = ql'y$ und $x^2 = l'q \pm lhql'$. Es folgt

$$y^2ql' = 1 \pm lh.$$

Außerdem folgt, dass h kleiner l ist und für das positive Vorzeichen von der Form $4m+3$ und beim negativen von der Form $4m+1$. Es ist h zu q und zu l' teilerfremd.
Aus der Gleichung $y^2ql' \pm lh = 1$ kann man leicht die Richtigkeit der folgenden drei Aussagen erkennen:

$$a)\ ql'Rh$$
$$b)\ \pm lhRq$$
$$c)\ \pm lhRl'$$

Aus a) folgt $[ql', h] = 0$.
Wieder unterscheiden wir, wenn h von der Form $4m+3$, dann folgt aus Satz 3.6 ix), dass $[h, ql'] \equiv 1 \pmod 2$. Das heißt,

1) hRq und hNl', oder
2) hNq und hRl'.

Im zweite Fall führt hNq und b) $-lhRq$ zu dem Widerspruch, dass lRq ist. Das heißt, es tritt der erste Fall ein und wir wissen, dass hNl' sein muss. Außerdem folgt aus c) $-lhRl'$ und h Nichtrest von l', dass auch $\pm l$ Nichtrest von l' ist.

Es bleibt noch der Fall zu überprüfen, wenn h von der Form $4m+1$ ist. Dann folgt wieder aus Satz 3.6 iii), dass $[h, ql'] \equiv 0 \pmod 2$. Das bedeutet, dass entweder h Rest von q und von l' wird, oder h Nichtrest von beiden Zahlen wird. Angenommen hRq, dann folgt aus b) $lhRq$, dass auch l Rest von q wäre, was nicht sein kann. Also ist hNq und somit auch hNl'. Aus c) $lhRl'$ folgt dann lNl' und somit auch $-lNl'$, weil -1 quadratischer Rest von l' ist.
Wir haben nun alle möglichen Fälle überprüft und sind am Ende des Beweises für den dritten Fall angekommen. □

4. Fall. Es sei $l = t + 1$ und $l' < l$. Weiter sei $l \equiv 1 \pmod 4$ und $l' \equiv 3 \pmod 4$.
Zu zeigen: Wenn $\pm l'Nl$, dann kann weder lRl' noch $-lNl'$ sein (Fall C, b)).

Beweis. Der Beweis dieses Falles ist dem des dritten Falles sehr ähnlich. Wir werden in vielen Bereichen auf die analoge Beweisführung verweisen können.

Wir bestimmen eine Primzahl, die kleiner als l ist und für die l Nichtrest ist. Dass es so eine Primzahl auch wirklich gibt, haben wir in Satz 3.3 gezeigt. Wir müssen zwei Fälle getrennt betrachten, je nachdem ob die Primzahl von der Form $4m+1$ oder von der Form

$4m+3$ ist, da wir uns nicht sicher sein können, ob für beide Fälle Primzahlen existieren.

I) Die Primzahl sei von der Form $4m+1$ und wir nennen sie p. Es gilt also lNp. Außerdem muss $\pm p$ Nichtrest von l sein (vgl. 3. Fall). Aus der Voraussetzung wissen wir, dass $\pm l'Nl$, also folgt $\pm pl'Rl$. Wir können $x^2 \equiv pl' \pmod{l}$ setzen. Wieder können wir x gerade und kleiner l annehmen.

α) In diesem Fall ist x weder durch l' noch durch p teilbar. Wie im bereits im dritten Fall setzen wir $x^2 = pl' \pm lf$ und wählen das Vorzeichen so, dass f immer positiv wird. Genauso wird f kleiner l und zu p und l' teilerfremd. Die Form von f ist bei positivem Vorzeichen $4m+1$ und bei negativem Vorzeichen $4m+3$.
Aus $x^2 = pl' \pm lf$ wissen wir, dass pl' quadratischer Rest von f ist, also ist auch $[pl', f] = 0$.

Wenn f von der Form $4m+3$ ist, dann folgt aus Satz 3.6 iii) $[f, pl'] \equiv 0 \pmod{2}$. Das bedeutet, dass

1) f Rest von p und von l' ist, oder
2) f Nichtrest von p und Nichtrest von l' ist.

Im ersten Fall führt fRp und $lfRp$ zu dem Widerspruch, dass l quadratischer Rest von p ist. Das heißt, f ist Nichtrest von p und l'. Aus fNl' und $lfRl'$ folgt, dass l Nichtrest von l' ist.

Ist f von der Form $4m+1$, dann folgt aus Satz 3.6 ix) $[f, pl'] \equiv 1 \pmod{2}$. Das bedeutet, dass

1) f Rest von p und f Nichtrest von l' ist, oder
2) f Nichtrest von p und f Rest von l' ist.

Wieder führt uns der erste Fall zu dem Widerspruch, dass lRp ist. Also ist f quadratischer Rest von l' und aus $-lfRl'$ folgt lNl'.

β) In diesem Fall ist x durch l' teilbar, aber nicht durch p. Es sei $x = yl'$ und $y^2l' = p \pm lh$. Das Vorzeichen sei wieder so gewählt, dass h stets positiv ist.
Somit ist h wieder kleiner l und zu p, y und l' teilerfremd (Beweis vgl. 3. Fall). In der Gleichung $y^2l' = p + lh$ muss h von der Form $4m+3$ sein, bei dem negativen Vorzeichen muss es von der Form $4m+1$ sein.
Aus der mit p beziehungsweise mit l' multiplizierten Gleichung $y^2l' = p \pm lh$ kann man

folgende Aussagen ableiten:

$$\begin{aligned} a)\ & l'pRh \\ b)\ & \pm lhl'Rp \\ c)\ & \mp lphRl' \end{aligned}$$

Aus a) folgt $[pl', h] = 0$.

Wenn h von der Form $4m + 3$ ist, dann folgt aus Satz 3.6 ix) $[h, pl'] \equiv 1 \pmod 2$. Das bedeutet, dass

1) h Rest von p ist und h Nichtrest von l', oder
2) h ist Nichtrest von p und h ist Rest von l'.

Im ersten Fall können wir aus hRp, der Voraussetzung lNp und aus b) $+lhl'Rp$ schließen, dass l' Nichtrest von p ist. Da l' und p beide kleiner l sind, können wir das quadratische Reziprozitätsgesetz anwenden und erhalten pNl'. Nun folgt aus

$$\begin{aligned} & pNl', \\ & hNl' \text{ und} \\ & -lphRl'\ (c), \end{aligned}$$

dass l Nichtrest von l' ist.
Im zweite Fall folgt die Aussage auf analoge Weise.

Es bleibt noch der Fall zu überprüfen, wenn h von der Form $4m+1$ ist. Es folgt aus Satz 3.6 iii), dass $[h, pl'] \equiv 0 \pmod 2$. Das heißt, dass entweder

1) h Rest von p und l' ist, oder
2) h Nichtrest von beiden Zahlen ist.

Wir betrachten den ersten Fall, es folgt aus hRp, lNp (Voraussetzung) und aus b) $-lhl'Rp$, dass l' Nichtrest von p ist. Aus dem quadratischen Reziprozitätsgesetz folgt, dass auch p Nichtrest von l' ist. Das heißt, aus

$$\begin{aligned} & pNl', \\ & hRl' \text{ und} \\ & lphRl'\ (c), \end{aligned}$$

folgt, dass l Nichtrest von l' ist.

Wieder nimmt der zweite Fall genau den Weg, der im vorhergehenden Fall eingeschlagen wurde, also wird er hier nicht mehr angeführt.

γ) Es sei x durch p teilbar, aber nicht durch l'. Der Beweis dieses Falles weicht nur sehr wenig von γ) des dritten Falles ab, sodass wir ihn überspringen.

δ) Es ist x durch l' und durch p teilbar. Daraus folgt, dass x auch durch pl' teilbar ist. Wir setzen $p \neq l'$, wären sie nämlich gleich, würde lNl' aus der Annahme lNp folgen und wir hätten alles gezeigt. Es sei $x = pl'y$ und es folgt $y^2pl' = 1 \pm lh$.
Nun wird h kleiner l und zu p und l' teilerfremd. Wir bestimmen die Form von h und erhalten $4m+3$ bei dem positiven Vorzeichen und $4m+1$ bei dem negativen.
Aus der Gleichung $1 = y^2pl' \mp lh$ folgen die Aussagen:

$$\begin{aligned} a)&\ pl'Rh \\ b)&\ \mp lhRp \\ c)&\ \mp lhRl' \end{aligned}$$

Aus $pl'Rh$ folgt $[pl', h] = 0$.

Für $h = 4m+3$ folgt aus Satz 3.6 ix), dass $[h, pl'] \equiv 1 \pmod 2$. Das heißt,
1) h ist Rest für p und h ist Nichtrest für l', oder
2) h ist Nichtrest für p und Rest für l'.
Der erste Fall führt uns zu einem Widerspruch, weil aus hRp und $-lhRp$ folgt, dass l Rest von p ist. Das heißt, es tritt der zweite Fall ein. Somit folgt aus hRl' und $-lhRl'$, dass l Nichtrest von l' ist.

Ist h von der Form $4m+1$, dann folgt aus Satz 3.6 iii), dass $[h, pl'] \equiv 0 \pmod 2$. Das beteutet, dass
1) h Rest von p und von l' ist, oder
2) h Nichtrest von p und von l' ist.
Wieder kann der erste Fall nicht eintreten, weil hRp und $lhRp$ zu dem Widerspruch führt, dass l Rest von p ist. Also folgt aus hNl' und $lhRl'$, dass l Nichtrest von l' ist.

II) Es bleibt nun der Fall zu überprüfen, wenn jene Primzahl, für die l Nichtrest ist, von der Form $4m+3$ ist. Da die Beweisführung der vorangegangenen sehr ähnelt, wird sie nicht mehr angeführt. □

5. Fall. Es sei $l = t + 1$ und $l' < l$. Weiters seien l und l' von der Form $4m + 3$.
Zu zeigen: Wenn $l'Rl$ oder $-lNl$, dann kann weder lRl' noch $-lNl'$ sein (Fall B, a)).

Beweis. Es ist l' Rest von l. Also sei $x^2 \equiv l' \pmod{l}$, mit x gerade und kleiner l. Wir unterscheiden zwei Fälle.

α) Es ist x nicht durch l' teilbar und $x^2 = l' + lf$. Wir wissen, dass f positiv wird und kleiner l sein muss. Außerdem ist f von der Form $4m + 3$ und zu l' teilerfremd (vgl. 1. Fall α).
Aus der Gleichung $x^2 = l' + lf$ folgt, dass l' quadratischer Rest von f ist. Wir können den Satz 3.5 Aussage 13 verwenden und erhalten $-fRl'$. Es folgt aus $-fRl'$ gemeinsam mit $lfRl'$, dass $-lRl'$, was wiederum gleichbedeutend mit lNl' ist.

β) In diesem Fall ist x durch l' teilbar. Es sei $x = l'y$ und $y^2l' = 1 + lh$. Dann ist h von der Form $4m + 1$ und zu l' teilerfremd (vgl. 1. Fall β).
Aus $y^2l'^2 = l' + lhl'$ wissen wir, dass l' quadratischer Rest von h ist. Wieder können wir den Satz 3.5 verwenden. Diesmal die Aussage 10 und es folgt h ist quadratischer Rest von l'. Aus der Gleichung $y^2l' - lh = 1$ erkennen wir, dass $-lhRl'$. Wir haben hRl' und $-lhRl'$, also folgt lNl', was zu zeigen war.

□

6. Fall. Es sei $l = t + 1$ und $l' < l$. Außerdem sei $l \equiv 3 \pmod{4}$ und $l' \equiv 1 \pmod{4}$.
Zu zeigen: Wenn $l'Rl$ oder $-lNl$, dann kann nicht $\pm lNl'$ sein (Fall D, a)).

Beweis. Dieser Beweis verläuft dem des fünften Falles durchaus ähnlich. Es sei $x^2 \equiv l' \pmod{l}$, mit x gerade und kleiner l.

α) Wenn $l' \nmid x$, dann ist $x^2 = l' + lf$. Wieder ist f positiv und kleiner l. Es wird f von der Form $4m + 1$ und zu l' teilerfremd (vgl. 1. Fall α).
Wir wissen, dass l' quadratischer Rest von f ist. Wir können den Satz 3.5 Aussage 9 verwenden und erhalten fRl'. Es folgt aus fRl' gemeinsam mit $lfRl'$, dass lRl'.

β) In diesem Fall gilt $l' \mid x$. Es sei $x = l'y$ und $y^2l' = 1 + lh$. Dann ist h von der Form $4m + 1$ und zu l' teilerfremd (vgl. 1.Fall β).
Aus $y^2l'^2 = l' + lhl'$ wissen wir, dass l' quadratischer Rest von h ist. Es folgt aus Satz 3.5 Aussage 9, dass h quadratischer Rest von l' ist. Aus der Gleichung $y^2l' - lh = 1$ erkennen wir, dass $\pm lhRl'$. Wir haben hRl' und $lhRl'$, also folgt lRl', was zu zeigen war. □

7. Fall. Es sei $l = t + 1$ und $l' < l$. Es seien l und l' von der Form $4m + 3$.
Zu zeigen: Wenn $l'Nl$ oder $-l'Rl$, dann kann weder lNl' noch $-lRl'$ sein (Fall B, b)).

Beweis. Wir können $-l'Rl$ schreiben als $x^2 \equiv -l' \pmod{l}$. Wobei wir x so wählen, dass es gerade und kleiner l ist.

α) Es ist x nicht durch l' teilbar und $-l' = x^2 - lf$. Es muss f positiv sein und von der Form $4m + 1$. Außerdem ist f zu l' teilerfremd und kleiner l. Es ist $x \leq l - 1$ und l' kleiner $l - 1$. Daraus folgt

$$lf = x^2 + l' < (l-1)^2 + l - 1 = (l-1)(l-1+1) = l^2 - l.$$

Somit ist $f < l - 1$.
Wir erkennen aus der Gleichung $-l' + lf = x^2$, dass $-l'$ quadratischer Rest von f ist und können den Satz 3.5 Aussage 10 anwenden. Dann folgt fRl'. Da auch lf Rest von l' ist, muss l Rest von l' sein und weil -1 Nichtrest von l' ist, folgt auch $-lNl'$.

β) Nun ist x durch l' teilbar und $x = l'y$. Es sei $y^2 l' = -1 + lh$, wobei h immer positiv ist und von der Form $4m + 3$. Wir wissen auch, dass h kleiner l sein muss und zu l' teilerfremd ist.
Wir wissen, dass $-l'$ ein quadratischer Rest von h ist. Aus dem Satz 3.5 Aussage 14 folgt aus $-l'Rh$, dass auch hRl' ist. Weil $lhRl'$ ist muss auch l quadratischer Rest von l' sein. Also haben wir alles gezeigt. □

8. Fall. Es sei $l = t + 1$ und $l' < l$. Es ist $l \equiv 3 \pmod{4}$ und $l' \equiv 1 \pmod{4}$.
Zu zeigen: Wenn $l'Nl$ oder $-l'Rl$, dann kann nicht $\pm lRl'$ sein (Fall D, b)).

Beweis. Der Beweis des letzten Falles verläuft gleich wie der des siebten Falles. In beiden Fällen wird der Satz 3.5 Aussage 12 verwendet. Ansonsten ist die Beweisführung analog. □

Wir haben nun für alle Fälle gezeigt, dass keine obere Schranke existiert. Das heißt, dass das quadratische Reziprozitätsgesetz allgemein gültig ist und somit haben wir auch alle Sätze aus dem vorhergegangenen Kapitel endgültig bewiesen.

Bemerkung. In den Beweisen haben wir für x immer einen geraden Wert gewählt. Man hätte auch den ungeraden Wert verwenden können, jedoch hätte man dann noch zusätz-

liche Unterscheidungen vornehmen müssen.

Dieser Beweis operiert völlig innerhalb der Begriffsbildungen der Theorie der quadratischen Reste. Er lässt zwar die Kürze, welche andere Beweise auszeichnet, vermissen, dies liegt aber nicht in der Methode, sondern in dem Umstand, dass zur Darstellung gewisser Beziehungen kein geeignetes Zeichen benützt wird. Deshalb muss in acht Fälle unterschieden werden, wobei jeder einzelne wieder in Unterabteilungen zerfällt. Durch die Einführung des Legendre-Symbols, eine spezielle Schreibweise und weitere Vereinfachungen kann der Beweis auf zwei Fälle reduziert werden.

Kronecker beschrieb den Beweis als „merkwürdig und scharfsinnige Deduktion, welche ganz direkt mit Überwindung aller Schwierigkeiten auf das Ziel losgehend fast wie eine Kraftprobe Gaußschen Geistes erscheint.“ [6]
Dirichlet schrieb, ihm sei der Beweis „immer merkwürdig erschienen, sowohl wegen des so einfachen Gedankens, welcher demselben zugrunde liegt, als auch deshalb, weil dieser Beweis der einzige ist, in welchem die Betrachtung das Gebiet der Kongruenzen zweiten Gerades, welchem des Satz wesentlich angehört, nirgend verlässt.“ [2]
Gauß hat über seine Beweise folgendes gesagt: „Wiewohl aber alle diese Beweise jeder Anforderung an Strenge genügen, so sind sie doch aus gar zu weit abseits gelegenen Quellen hergeleitet, ausgenommen vielleicht der erste, der dafür wieder mit schwierigen Schlussfolgerungen vorgeht und mit weitläufigen Operationen belastet ist.“ [5]

5 Das Legendre-Symbol

Das Legendre-Symbol ist eine Kurzschreibweise für quadratische Reste und Nichtreste. Es wurde 1798 von dem französischem Mathematiker Adrien-Marie Legendre eingeführt. Dieses Symbol wird uns ab nun bei den folgenden Beweisen des quadratischen Reziprozitätsgesetzes begegnen. Aus diesem Grund werden hier bereits bewiesene Sätze mit Hilfe des Legendre-Symbols beschrieben und die Zusammenhänge erläutert. Am Ende des Kapitels steht auch ein praktisches Beispiel, wie man das Legendre-Symbol berechnen kann, um ein besseres Verständnis für die angeführten Aussagen zu bekommen. Wir folgen im Grunde dem Kapitelanfang „Variation1. Das Legendre-Jacobi-Symbol“ von Pieper [7]. Wir beginnen nun mit der Definition.

Definition 5.1. Sei $p \neq 2$ eine Primzahl, $a \in \mathbb{Z}$ mit $p \nmid a$. Wir setzen

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

$\left(\frac{a}{p}\right)$ heißt Legendre-Symbol.

Wir wollen bereits vorhandene Informationen über quadratische Reste und Nichtreste mit dem Legendre-Symbol verknüpfen und auf diese Weise Eigenschaften des neuen Symbols genauer betrachten.
Wir wissen aus Satz 2.10, dass $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, wenn a ein quadratischer Rest von p ist und wenn a ein Nichtrest ist, dann ist $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Das Euler-Kriterium kann also auch in dieser Form angeschrieben werden

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

Wir können nun auch die Sätze 2.13, 2.14 und 2.15, welche Auskunft über das Produkt von Rest und Nichtrest geben, mit Hilfe des Legendre-Symbols zu einem Satz zusammenfassen und mit Hilfe der obigen Aussage ganz leicht beweisen.

Satz 5.2. *Sei $p \neq 2$ eine Primzahl, $a, b \in \mathbb{Z}$ mit $p \nmid a$, $p \nmid b$. Dann gilt:*

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

Beweis. Es ist

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

Da das Legendre-Symbol aber nur die Werte -1 und 1 annehmen kann, folgt

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

□

Satz 5.3. *Es sei $p \neq 2$ eine Primzahl und $a \in \mathbb{Z}$, mit $p \nmid a$, dann gilt*

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Beweis. Dies folgt sofort aus Satz 2.9, der besagt, dass es gleich viele Reste und Nichtreste gibt, so wie der Definition des Legendre-Symbols. □

Wir können auch die Sätze 2.17 und 2.18, welche bestimmen, ob -1 quadratischer Rest oder Nichtrest ist, zu dem ersten Ergänzungssatz zusammenfassen.

Satz 5.4. *(Erster Ergänzungssatz) Es sei p eine ungerade Primzahl. Dann gilt*

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

Das heißt, wenn p von der Form $4m+1$ ist, dann ist $\frac{p-1}{2}$ gerade und folglich ist dann -1 Rest von p. Wenn hingegen p von der Form $4m+3$ ist, dann ist $\frac{p-1}{2}$ ungerade und -1 Nichtrest von p.

Satz 5.5. *(Zweiter Ergänzungssatz) Es sei p eine ungerade Primzahl. Dann gilt*

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

Der zweite Ergänzungssatz besagt, wenn $p \equiv 1 \pmod 8$, oder $p \equiv 7 \pmod 8$ ist, dann ist 2 quadratischer Rest für p. Außerdem ist 2 Nichtrest für p, wenn $p \equiv 3 \pmod 8$ oder $p \equiv 5 \pmod 8$. Dies folgt, weil $\frac{(8m\pm1)^2-1}{8} = 8m^2 \pm 2m$ und somit gerade ist und weil $\frac{(8m\pm3)^2-1}{8} = 8m^2 \pm 6m + 1$ und somit ungerade ist.

Bemerkung. Einen Teil des zweiten Ergänzungssatzes (2 ist Nichtrest für Primzahlen von der Form $8m+3$ oder $8m+5$) haben wir bereits mit Satz 2.19 bewiesen. Einen vollständigen Beweis werden wir erst im nächsten Kapitel anführen, weil wir ihn mit Hilfe der Theorie der endlichen Körper durchführen werden.

Satz 5.6. *(Quadratisches Reziprozitätsgesetz) Sind p und q verschiedene ungerade Primzahlen, dann gilt*

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

Wenn wir das quadratische Reziprozitätsgesetz in dieser Form etwas näher betrachten, können wir erkennen, dass es leicht in die Form von Satz 3.1 übergeführt werden kann. Wir wissen, dass $\frac{p-1}{2} \cdot \frac{q-1}{2}$ nur dann ungerade ist, wenn beide Primzahlen p und q die Form $4m+3$ haben. Der Bruch wird gerade, sobald eine der Primzahlen von der Form $4m+1$ ist. Das heißt:
Wenn $p \equiv 3 \pmod 4$ und $q \equiv 3 \pmod 4$, dann ist $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$. Das bedeutet qRp genau dann, wenn pNq.
Wenn $p \equiv 1 \pmod 4$ oder $q \equiv 1 \pmod 4$, so ist $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. Also ist qRp genau dann, wenn pRq.

Bemerkung. Spätestens jetzt ist es leicht zu erkennen, dass durch die Einführung des Legendre-Symbols weniger Fallunterscheidungen nötig sind und somit die Beweise in kürzerer Form aufgeschrieben werden können.

Beispiel 5.7. *Für die Berechnung des Legendre-Symbols $\left(\frac{6557}{7919}\right)$ verwenden wir die Ergänzungssätze und das quadratische Reziprozitätsgesetz (vgl. Sätze 5.4, 5.5 und 5.6).*

Wir können 6557 *schreiben als* $79 \cdot 83$. *Da* $7919, 79$ *und* 83 *Primzahlen sind, können wir zweimal das quadratische Reziprozitätsgesetz anwenden. Das heißt*

$$\left(\frac{6557}{7919}\right) = \left(\frac{79}{7919}\right)\left(\frac{83}{7919}\right) = \left(\frac{7919}{79}\right)\left(\frac{7919}{83}\right)(-1)^2.$$

Es ist $7919 \equiv 19 \pmod{79}$ *und* $7919 \equiv 34 \pmod{83}$. *Außerdem ist* 19 *eine Primzahl, also wenden wir wieder das Reziprozitätsgesetz an und* 34 *zerlegen wir in Primfaktoren.*

$$\left(\frac{7919}{79}\right)\left(\frac{7919}{83}\right) = \left(\frac{19}{79}\right)\left(\frac{34}{83}\right) = \left(\frac{79}{19}\right)(-1)\left(\frac{2}{83}\right)\left(\frac{17}{83}\right).$$

Wieder ist $79 \equiv 3 \pmod{19}$ *und wir können* $\left(\frac{2}{83}\right)$ *mit dem zweiten Ergänzungssatz lösen. Da* $3, 17, 19$ *und* 83 *Primzahlen sind folgt*

$$\left(\frac{79}{19}\right)(-1)\left(\frac{2}{83}\right)\left(\frac{17}{83}\right) = \left(\frac{3}{19}\right)(-1)(-1)^{861}\left(\frac{83}{17}\right)(-1)^{328} = \left(\frac{19}{3}\right)\left(\frac{83}{17}\right).$$

Es ist $19 \equiv 1 \pmod{3}$ *und* $83 \equiv -2 \pmod{17}$*. Aus dem ersten und dem zweiten Ergänzungsatz folgt*

$$\left(\frac{1}{3}\right)\left(\frac{-2}{17}\right) = 1 \cdot \left(\frac{-1}{17}\right)\left(\frac{2}{17}\right) = 1 \cdot 1 = 1$$

Das heißt 6557 *ist quadratischer Rest für* 7919*.*

6 Endliche Körper

Die folgenden zwei Beweise bauen auf der Theorie der endlichen Körper auf. In diesem Kapitel werden wir somit einen Ausflug in die Algebra machen. Wir werden eine kurze Einführung zur Klärung der notwendigen Begriffe geben und uns mit den wichtigen Aussagen über endliche Körper beschäftigen. Außerdem wird der Zusammenhang zwischen quadratischen Resten und endlichen Körper hergestellt und wir werden den zweiten Ergänzungssatz beweisen (vergl. Kapitel 10.3 aus dem Buch Elementare Algebra und Zahlentheorie [8]). Am Ende des Kapitels steht eine körpertheoretische Formulierung des quadratischen Reziprozitätsgesetzes. In diesem Kapitel halten wir uns an den Anhang über endliche Körper von Pieper [7] und an das Kapitel „Endliche Körper“, sowie einige Grundlagen aus vorhergegangenen Abschnitten aus dem Buch „Algebra“ von Bosch [1]. Wir beginnen mit der Definition von Körper.

Definition 6.1. (Körper)
Ein Körper ist eine Menge K zusammen mit zwei Verknüpfungen $+$ und $\cdot$, für die folgendes gilt:
1) $(K, +)$ ist eine abelsche Gruppe. Das neutrale Element wird mit 0 und das Negative von $a \in K$ mit $-a$ bezeichnet.
2) $(K\backslash\{0\}, \cdot)$ ist eine abelsche Gruppe. Das neutrale Element wird mit 1 und das Inverse von $a \in K$ mit a^{-1} bezeichnet.
3) Es gelten folgende Distributivgesetze:
$a \cdot (b + c) = a \cdot b + a \cdot c$ für alle $a, b, c \in K$
$(a + b) \cdot c = a \cdot c + b \cdot c$ für alle $a, b, c \in K$

Definition 6.2. (Endliche Körper)
Ein Körper K, der nur aus endlich vielen Elementen besteht, heißt endlicher Körper.

Wenn K ein Körper und K' eine Teilmenge von K, die bezüglich der in K erklärten Addition und Multiplikation selbst einen Körper bildet, so heißt K eine Körpererweiterung von K', oder K' ein Teilkörper von K.

Wir betrachten die Restklassenringe $\mathbb{Z}/m\mathbb{Z}$ mit $m > 0$. Dann ist $\mathbb{Z}/m\mathbb{Z}$ ein kommutativer Ring mit 1 mit m Elementen.

Satz 6.3. *Es ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper, genau dann wenn p eine Primzahl ist.*

Beweis. Wir bezeichnen mit $\bar{x} \in \mathbb{Z}/p\mathbb{Z}$ die zu einem Element x in $\mathbb{Z}$ gehörige Restklasse modulo $p\mathbb{Z}$.

$\Leftarrow$: Es sei p eine Primzahl. Das heißt aber auch, dass p größer 1 sein muss und $\mathbb{Z}/p\mathbb{Z}$ somit nicht der Nullring sein kann. Es ist leicht zu sehen, dass $(\mathbb{Z}/p\mathbb{Z}, +)$ eine abelsche Gruppe ist. Um zu sehen, dass $(\mathbb{Z}/p\mathbb{Z}\backslash\{0\}, \cdot)$ eine abelsche Gruppe ist, müssen wir noch zeigen, dass es zu jedem Element ein Inverses gibt.
Es seien $a, b \in \mathbb{Z}$ und $\bar{a} \cdot \bar{b} = 0$, dann ist $ab \in p\mathbb{Z}$. Durch die Primfaktorzerlegung sieht man, dass p ein Teiler von a oder von b ist. Daraus folgt, dass $a \in p\mathbb{Z}$ oder $b \in p\mathbb{Z}$ und weiter, dass $\bar{a} = 0$ oder $\bar{b} = 0$ sein muss. Wir wissen also, dass $\mathbb{Z}/p\mathbb{Z}$ nullteilerfrei ist. Aus der Nullteilerfreiheit folgt, dass für jedes $\bar{a} \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ die Abbildung $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $\bar{x} \mapsto \bar{a} \cdot \bar{x}$ injektiv ist. Wegen der Endlichkeit von $\mathbb{Z}/p\mathbb{Z}$ folgt die Bijektivität. Insbesondere ist das Einselement von $\mathbb{Z}/p\mathbb{Z}$ im Bild dieser Abbildung enthalten und wir wissen, das jedes $\bar{a}$ ein inverses Element bezüglich der Multiplikation hat. Somit ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper.
$\Rightarrow$: Es sei $\mathbb{Z}/p\mathbb{Z}$ ein Körper und somit auch nullteilerfrei. Dann folgt $\mathbb{Z}/p\mathbb{Z} \neq 0$ und p größer 1. Wir wollen zeigen, dass p eine Primzahl ist und betrachten daher einen Teiler $d \in \mathbb{N}$ von p. Es gilt die Gleichung $p = da$ und es folgt $\bar{d} \cdot \bar{a} = 0$. Wegen der Nullteilerfreiheit von $\mathbb{Z}/p\mathbb{Z}$ ist $\bar{d} = 0$ oder $\bar{a} = 0$. Wenn $\bar{d} = 0$, dann ist p ein Teiler von d und somit ist $d = p$. Wenn hingegen $\bar{a} = 0$, dann ist p ein Teiler von a und $a = p$. Das heißt aber auch, dass $d = 1$ sein muss. Die Zahl p hat somit höchstens sich selbst und 1 als Teiler und ist eine Primzahl. □

Beispiel 6.4. *Die Menge aller Restklassen modulo p, mit p einer Primzahl bilden einen Körper, wie wir im vorherigen Satz gesehen haben. Wir bezeichnen ihn mit* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. *Der Körper besitzt endlich viele Elemente, nämlich p, und ist somit ein endlicher Körper.*

Definition 6.5. Es sei K ein endlicher Körper. Ist $a \in K$, so sind auch die Potenzen $a^2, a^3, a^4, \ldots$ und $a^{-1}, a^{-2}, \ldots$ in K enthalten. Die kleinste natürliche Zahl k, für die $a^k = 1$ gilt, heißt Ordnung des Elements $a \neq 0$. Kurzschreibweise: $\mathrm{ord}(a) = k$.

Bemerkung. Da K nur endlich viele Elemente enthält, können nicht alle Potenzen verschieden sein. Ist k die Ordnung des Elements a, so sind die Potenzen $1, a, a^2, \ldots, a^{k-1}$ verschieden.

Beispiel 6.6. *Wir berechnen die Ordnung von* $a = 3$ *und* $b = 4$ *in* $\mathbb{F}_5$.
Es ist $3^4 \equiv 1 \pmod 5$ *(und* $3^1, 3^2, 3^3 \not\equiv 1 \pmod 5$*), also ist* $\mathrm{ord}(3) = 4$.
Die Ordnung von b hingegen ist 2, *weil* $4^2 \equiv 1 \pmod 5$.

Satz 6.7. *Es sei K ein endlicher Körper mit q Elementen und n ist die größte Ordnung, die ein Element von* $K\backslash\{0\}$ *hat. Dann ist*

$$n = q - 1.$$

Beweisskizze. Es seien $a, b \in K$ und $b \neq 0$, wobei die $\text{ord}(a) = n$ und $\text{ord}(b) = k$. Man kann zeigen, dass die maximale Ordnung n durch die Ordnung jedes anderen Elements$\neq 0$ von K teilbar ist, das heißt es gilt $k \mid n$. Diese Aussage erhält man am besten indem man indirekt annimmt, dass k kein Teiler von n wäre und durch betrachten der Ordnung von ab einen Widerspruch erhält.
Weil $k \mid n$ ist jedes Element von $K\backslash\{0\}$ eine Nullstelle der Gleichung $x^n - 1 = 0$. Diese Gleichung kann nicht mehr als n Nullstellen haben, also folgt $q - 1 \leq n$. Andererseits ist $n \leq q - 1$, weil K die n Potenzen $a, a^2, \ldots, a^{n-1}, a^n = 1$, die alle $\neq 0$ sind, enthält. Es muss somit ein Element a in K geben mit der Ordnung $q - 1$. □

Für jedes Element maximaler Ordnung $a \in K$ stellen die Elemente $1, a, a^2, \ldots, a^{n-1}$, die alle untereinander verschieden sind, mit 0 alle Elemente von K dar. Jedes Element eines Körpers mit q Elementen ist Nullstelle der Gleichung

$$x^q - x = x(x^{q-1} - 1) = 0.$$

Für die Elemente ungleich 0 genügt sogar die Gleichung $x^{q-1} - 1 = 0$.

Definition 6.8. Es sei K ein endlicher Körper. Ist $a \in K\backslash\{0\}$, so sind auch die Summen $2a, 3a, 4a, \ldots$ in K enthalten. Die kleinste natürliche Zahl $p > 0$, für die $p \cdot a = 0$ gilt, heißt Charakteristik oder additive Ordnung von K. Die Kurzschreibweise ist $p = \text{char } K$.

Bemerkungen. Da K nur endlich viele Elemente enthält, können nicht alle Summen verschieden sein. Insbesondere existiert die additive Ordnung.
Wenn $pa = 0$ für $a \in K$, dann gilt auch $pb = paa^{-1}b = 0$ für jedes $b \in K$. Es haben also alle von Null verschiedenen Elemente von K die gleiche additive Ordnung, insbesondere gilt dies auch für das Einselement.
Außerdem muss p eine Primzahl sein. Wäre $p = p_1 p_2$ mit p_1 und p_2 kleiner p, so wäre $p_2 \cdot a \neq 0$ und hätte die kleinere additive Ordnung p_1, oder umgekehrt.
Für allgemeine Körper kann es passieren, dass es keine natürliche Zahl $p > 0$ gibt, für die $p \cdot a = 0$ gilt, zum Beispiel für $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. In diesem Fall definiert man die Charakteristik als 0.

Beispiel 6.9. *Der Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mit p Elementen und p einer Primzahl hat die Charakteristik p.*

Beispiel 6.10. *Für jeden Teilkörper T eines Körpers K gilt:* $\text{char } K = \text{char } T$. *Da das Einselement 1_T und das Nullelement 0_T vom Teilkörper T mit denen des Körpers K übereinstimmen, ist $p \cdot 1_T = 0_T$ in T genau dann, wenn $p \cdot 1_K = 0_K$ in K ist.*

Definition 6.11. Wir wissen, dass der Durchschnitt von Teilkörpern eines Körpers K wieder ein Teilkörper ist. Deshalb enthält K einen eindeutig bestimmten kleinsten Teilkörper P als Durchschnitt aller Teilkörper. Wir nennen P Primkörper von K.

Beispiel 6.12. *In jedem endlichen Körper der Charakteristik p ist $\mathbb{F}_p$ als Teilkörper enthalten, da wir ihn als additives Erzeugnis von 1 erhalten. Es ist $\mathbb{F}_p$ der kleinste Teilkörper von K, also Primkörper von K.*

Lemma 6.13. *Ist p eine Primzahl und $1 \leq k \leq p-1$, dann gilt $p \mid \binom{p}{k}$.*

Beweis. Nach Definition gilt

$$\binom{p}{k} = \frac{p(p-1)\cdot\ldots\cdot(p-k+1)}{1\cdot 2\cdot\ldots\cdot k}.$$

Das heißt, der Nenner N ist teilerfremd zu p, weil er aus Faktoren besteht, die alle kleiner als p sind. Der Zähler $Z = p(p-1)\cdot\ldots\cdot(p-k+1) = p\cdot M$ ist ein Vielfaches von p. Wir schreiben $\binom{p}{k} = p\frac{M}{N}$, das heißt, pM wird von N geteilt, weil der Binomialkoeffizient immer eine ganze Zahl ist.
Da N und p teilerfremd sind, ist $Nx + py = 1$ mit $x, y \in \mathbb{Z}$ lösbar, vergleiche dazu Satz 3.12 aus dem Buch Elementare Algebra und Zahlentheorie [8]. Es gilt $NMx + pyM = M(Nx + py) = M$. Aus $N \mid pM$ und der Gleichung $M = pyM + NMx$ folgt $N \mid M$. Somit ist

$$\frac{M}{N} = \frac{\binom{p}{k}}{p}$$

eine ganze Zahl. □

Satz 6.14. *In einem endlichen Körper K der Charakteristik p gilt für alle $a, b \in K$*

$$(a \pm b)^p = a^p \pm b^p.$$

Beweis. Es gilt nach der binomischen Formel

$$(a \pm b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i (\pm b)^{p-i}.$$

Für $1 \leq i \leq p-1$ ist der Binomialkoeffizient $\binom{p}{i}$ nach Lemma 6.13 eine natürliche durch p teilbare Zahl. Aus der Definition der Charakteristik folgt, dass alle Mittelglieder $\binom{p}{i} a^i (\pm b)^{p-i}$ für $1 \leq i \leq p-1$ in K gleich 0 sind. Somit folgt $(a \pm b)^p = a^p \pm b^p$. □

Definition 6.15. Ein Automorphismus eines Körpers K ist eine bijektive Abbildung $\phi : K \to K$ für die für alle x, y in K gilt:
$\phi(x + y) = \phi(x) + \phi(y)$
$\phi(xy) = \phi(x)\phi(y)$ für alle $x, y \in K$.

Satz 6.16. *Die Abbildung $\sigma_p : a \to a^p$ ist ein Automorphismus von $\mathbb{F}_p$.*

Beweis. Wir beginnen mit den Homomorphieeigenschaften.
Die Abbildung σ_p ist verträglich mit der Multiplikation in $\mathbb{F}_p$. Es gilt

$$\sigma_p(x \cdot y) = (x \cdot y)^p = x^p \cdot y^p = \sigma_p(x) \cdot \sigma_p(y).$$

Außerdem ist $\sigma_p(1) = 1^p = 1$.
Weiters gilt

$$\sigma_p(x + y) = \sigma_p(x) + \sigma_p(y),$$

weil, wie wir bereits aus Satz 6.14 wissen, $(x + y)^p = x^p + y^p$ gilt.
Somit ist σ_p ein Homomorphismus. Es bleibt zu zeigen, dass σ_p auch eine bijektive Abbildung ist. Wir beginnen damit, die Injektivität zu zeigen. Seien a und b in K mit $\sigma_p(a) = \sigma_p(b)$, also $a^p - b^p = 0$. Aus Satz 6.14 wissen wir, dass $a^p - b^p = (a - b)^p$ ist und $(a - b)^p$ ist genau dann Null, wenn $a = b$. Also ist σ_p injektiv.
Weil die Abbildung injektiv ist und weil unser Körper endlich ist, folgt die Surjektivität. Also ist σ_p bijektiv und somit ein Automorphismus. □

Bemerkung. Die Abbildung σ_p von $K \to K$, mit K einem Körper der Charakteristik $p > 0$ wird auch Frobenius-Abbildung genannt. Wir schreiben

$$\mathrm{Frob}_p(x) := x^p.$$

Definition 6.17. Es sei K ein Körper. Dann ist der Polynomring $K[X]$ über dem Körper K die Menge aller Polynome mit Koeffizienten aus dem Körper K und der Unbestimmten X zusammen mit der üblichen Addition und Multiplikation von Polynomen.

Beispiel 6.18. *Der Polynomring $\mathbb{F}_p[X]$ besteht aus allen Polynomen $a_0 + a_1x + \ldots + a_kx^k$ mit $k \in \mathbb{N}$ und $a_0, \ldots, a_k \in \mathbb{F}_p$.*

Satz 6.19. *Sei K ein Körper der Charakteristik $p > 0$. Für den Primkörper $\mathbb{F}_p$ von K gilt*

$$\mathbb{F}_p = \{x \in K \mid \mathrm{Frob}_p(x) = x\}.$$

Das heißt, ein Element x aus K gehört dann und nur dann zu $\mathbb{F}_p$, wenn $\mathrm{Frob}_p(x) = x$, also $x^p = x$ ist.

Beweis. Wir wissen aus dem kleinen Satz von Fermat (Satz 2.7), dass $x^p = x$ für alle $x \in \mathbb{F}_p$. Außerdem wissen wir, dass das Polynom $X^p - X$ in K maximal p Nullstellen haben kann. Somit müssen die Mengen schon gleich sein und es gilt

$$\mathbb{F}_p = \{x \in K \mid x^p = x\}.$$

□

Definition 6.20. Sei K ein Körper, $f \in K[X]$ nicht konstant. Ein Erweiterungskörper Z von K heißt Zerfällungskörper von f über K, wenn f in $Z[X]$ vollständig in Linearfaktoren zerfällt, also

$$f = a_n \prod_{j=1}^{n} (X - \beta_j) \qquad \text{mit } \beta_j \in Z,$$

und Z von K und den Elementen $\beta_1, \ldots, \beta_n$ erzeugt wird, das heißt $Z = K(\beta_1, \ldots, \beta_n)$.

Definition 6.21. Es sei $K \subset L$ eine Körpererweiterung. Dann bezeichnet man die Vektorraumdimension $[L : K] := \dim_K L$ als den Grad von L über K. Die Körpererweiterung heißt endlich oder unendliche, je nachdem, ob $[L : K]$ endlich oder unendlich ist.

Bemerkung. Es gilt $L = K$ genau dann wenn $[L : K] = 1$.

Im folgenden Abschnitt wollen wir uns mit fundamentalen Aussagen über endliche Körper beschäftigen. Wir wollen für jede Potenz q von p, also für $q = p^n$ mit einer natürlichen Zahl $n > 0$, einen Körper $\mathbb{F}_q$ mit q Elementen konstruieren. Außerdem werden wir sehen, dass man jeden endlichen Körper auf diese Weise erhält.

Bemerkung. Der Körper $\mathbb{F}_q$ mit $q = p^n$ und $n > 1$ ist grundverschieden von dem Restklassenring $\mathbb{Z}/p^n\mathbb{Z}$. Der Restklassenring besitzt Nullteiler und ist somit kein Körper.

Satz 6.22. *Es sei $\mathbb{F}$ ein endlicher Körper. Dann hat $\mathbb{F}$ den Primkörper $\mathbb{F}_p$ und es gilt $p = \mathrm{char}\ \mathbb{F} > 0$. Weiter besteht $\mathbb{F}$ aus genau $q = p^n$ Elementen, wobei $n = [\mathbb{F} : \mathbb{F}_p]$. Es ist $\mathbb{F}$ Zerfällungskörpers des Polynoms $X^q - X$ über $\mathbb{F}_p$.*

Beweis. Aus der Endlichkeit von $\mathbb{F}$ folgt einerseits, dass der zugehörige Primkörper $\mathbb{F}_p$ mit $p = \mathrm{char}\ \mathbb{F} > 0$ endlich ist und andererseits, dass auch der Grad $n = [\mathbb{F} : \mathbb{F}_p]$ endlich ist.

Wir können nun einen Isomorphismus von $\mathbb{F}_p$-Vektorräumen $\mathbb{F} \simeq (\mathbb{F}_p)^n$ verwenden. Wir wissen, dass $\mathbb{F}_p$ genau p Elemente hat. Da ein Isomorphismus eine bijektive Abbildung ist, folgt, dass $\mathbb{F}$ genau $q = p^n$ Elemente haben muss.
Die Ordnung der multiplikativen Gruppe $\mathbb{F}^*$ ist die Anzahl der Elemente dieser Gruppe und somit gleich $q - 1$. Wir verwenden den Satz 6.7 und erkennen, dass jedes Element aus $\mathbb{F}^*$ eine Nullstelle des Polynoms $X^{q-1} - 1$ ist. Des weiteren folgt, dass $\mathbb{F}$ aus $q = p^n$ Nullstellen des Polynoms $X^q - X$ besteht. Da dieses Polynom aber nicht mehr als q Nullstellen haben kann wissen wir, dass $X^q - X$ über $\mathbb{F}$ vollständig in Linearfaktoren zerfällt. Das heißt $\mathbb{F}$ ist Zerfällungskörper des Polynoms $X^q - X \in \mathbb{F}_p[X]$. □

Satz 6.23. *Es sei p eine Primzahl. Dann existiert zu jedem $n \in \mathbb{N}$ ein Erweiterungskörper $\mathbb{F}_q/\mathbb{F}_p$ mit $q = p^n$ Elementen. Es ist $\mathbb{F}_q$ bis auf Isomorphie eindeutig charakterisiert als Zerfällungskörper des Polynoms $X^q - X$ über $\mathbb{F}_p$ und $\mathbb{F}_q$ besteht genau aus den Nullstellen von $X^q - X$.*
Jeder endliche Körper der Charakteristik p ist isomorph zu genau einem endlichen Körper des Typs $\mathbb{F}_q$.

Beweisskizze. Zuerst muss die Existenz eines Körpers der Charakteristik p mit $q = p^n$ Elementen gezeigt werden. Dies zeigt man, indem man den Zerfällungskörper des Polynoms $f = X^q - X$ über $\mathbb{F}_p$ bildet, also muss man nachweisen, dass die q Nullstellen von dem Polynom einen Körper mit q Elementen bilden. Man prüft nach, dass $(a \pm b)^q$ mit $a, b \in \mathbb{F}_p$ wieder eine Nullstelle von f ist und dass auch die Verknüpfung mit dem Inversen $(ab^{-1})^q$ für $b \neq 0$ eine Nullstelle in f ist.
Die Eindeutigkeit dieser Körper folgt aus Satz 6.22. □

Beispiel 6.24. *Wir konstruieren den endlichen Körper mit vier Elementen. Wir betrachten $\mathbb{F}_2[X]/(x^2 + x + 1)\mathbb{F}_2[X]$, ähnlich wie in Satz 6.3 kann man für diesen Körper die Körperaxiome nachrechnen. Wir benötigen hierfür nur, dass das Polynom $x^2 + x + 1$ irreduzibel (ein Polynom, das sich nicht als Produkt zweier nicht invertierbarer Polynome schreiben lässt) ist. Die Koeffizienten sind aus $\mathbb{F}_2$ und somit 0 oder 1. Außerdem folgt aus $x^2 + x + 1 = 0$, dass $x^2 = -x - 1$ und wir können hiermit jedes beliebige Polynom auf die folgenden vier Elemente (Polynome) reduzieren:*

$$\mathbb{F}_4 = \mathbb{F}_2 \cdot X + \mathbb{F}_2 = \{0, 1, x + 1, x\}.$$

Das heißt, das Polynom $3x^3 + x + 5$ wird in $\mathbb{F}_2[X]$ reduziert zu: $x^3 + x + 1$. Weiters ist $x^3 = x^2 \cdot x = (x + 1)x = x^2 + x = x + 1 + x = 2x + 1 = 1$, also folgt insgesamt $x^3 + x + 1 = x + 2 = x$.

Bemerkungen. Abschließend werden noch einige Bemerkungen ohne Beweis angeführt. Es sei $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0$ ein irreduzibles Polynom (ein Polynom, das sich nicht als Produkt zweier nicht invertierbarer Polynome schreiben lässt), wobei alle Koeffizienten aus $\mathbb{F}_p$ sind, dann hat $f(x)$ im Körper $\mathbb{F}_{p^m}$ mit p^m Elementen eine Nullstelle α. Außerdem haben alle Nullstellen von $f(x)$ die Form α^{p^i}.
Es folgt, wenn $f(x)$ irgendein (nicht notwendig irreduzibles) Polynom mit Koeffizienten aus $\mathbb{F}_p$ ist, so existiert eine Erweiterung von $\mathbb{F}_p$, in der ein irreduzibler Faktor von $f(x)$ und damit $f(x)$ eine Nullstelle besitzt. Somit ergibt sich die Existenz eines Körpers, in dem $f(x)$ sich in lauter Linearfaktoren zerlegen lässt.
Für ein quadratisches Polynom $f(x) = x^2 + ax + b = (x - \alpha_1)(x - \alpha_2)$ mit Koeffizienten in $\mathbb{F}_p$ ist die Diskriminante $D(f) = a^2 - 4b$. Die Nullstellen α_1 und α_2 liegen dann und nur dann in $\mathbb{F}_p$, wenn $D(f)$ ein Quadrat in $\mathbb{F}_p$ ist.

Wir haben nun ausreichend Theorie der endlichen Körper und wollen den Beweis des zweiten Ergänzungssatzes (Satz 5.5) durchführen. Wir erinnern uns:

Satz. *Es sei p eine ungerade Primzahl, dann gilt*

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

Beweis. Sei α in $\mathbb{F}_{p^2}$ ein Element der Ordnung 8 in der multiplikativen Gruppe $\mathbb{F}_{p^2}^*$, das heißt $\alpha^8 = 1$. Wir können α^8 auch als $\alpha^{2\cdot 4}$ schreiben und erkennen, dass α^2 die Ordnung 4 hat. Wir wissen, dass $\alpha^4 \cdot \alpha^4 = 1$, also ist $\alpha^4 = (\alpha^2)^2 = -1$ und $\alpha^{-2} = -\alpha^2$.
Wir betrachten $\gamma = \alpha + \alpha^{-1}$ in $\mathbb{F}_{p^2}$. Es ist

$$\begin{aligned}\gamma^2 &= (\alpha + \alpha^{-1})^2 \\ &= \alpha^2 + \alpha^{-2} + 2 \\ &= 2.\end{aligned}$$

Daraus folgt, dass

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

Wir müssen ein Fallunterscheidung vornehmen:

I) Es sei p kongruent ± 1 modulo 8.

Daraus folgt

$$\gamma^p = (\alpha + \alpha^{-1})^p = \alpha^p + \alpha^{-p} = \alpha + \alpha^{-1} = \gamma.$$

Somit ist $2^{\frac{p-1}{2}} = \gamma^{p-1} = 1$ in $\mathbb{F}_p$, also ist $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ in $\mathbb{Z}$. Wir wissen aus dem Eulerschen Kriterium, dass somit 2 quadratischer Rest modulo p ist.

II) Es sei $p \equiv \pm 3 \pmod{8}$.
Daraus folgt

$$\gamma^p = (\alpha + \alpha^{-1})^p = \alpha^p + \alpha^{-p} = \alpha^3 + \alpha^{-3}.$$

Wäre $\alpha^3 + \alpha^{-3} = \alpha + \alpha^{-1}$, dann müsste $(\alpha^3 + \alpha^{-3}) \cdot (\alpha + \alpha^{-1}) = 2$, weil $(\alpha^3 + \alpha^{-3})^2 = 2$ ist. Wir berechnen also

$$\begin{aligned}(\alpha^3 + \alpha^{-3}) \cdot (\alpha + \alpha^{-1}) &= \alpha^4 + \alpha^{-4} + \alpha^2 + \alpha^{-2} \\ &= -1 - 1 + \alpha^2 - \alpha^2 \\ &= -2 \neq 2.\end{aligned}$$

Wir wissen also, dass $\alpha^3 + \alpha^{-3} \neq \alpha + \alpha^{-1}$, also auch $(\alpha + \alpha^{-1})^p \neq \alpha + \alpha^{-1}$.
Somit ist

$$\begin{aligned}2^{\frac{p-1}{2}} &= (\gamma^2)^{\frac{p-1}{2}} \\ &= (\alpha^1 + \alpha^{-1})^{p-1} \neq 1\end{aligned}$$

in $\mathbb{F}_p$, also muss $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ in $\mathbb{Z}$ gelten und wieder aus dem Eulerschen Kriterium folgt, dass 2 diesmal Nichtrest für p ist. □

Um das quadratische Reziprozitätsgesetz körpertheoretisch formulieren zu können müssen wir kurz klären, was es bedeutet, wenn eine Zahl quadratischer Rest einer anderen Zahl ist. Es seien p, q zwei verschiedene, ungerade Primzahlen. Dann gilt:

pRq genau dann, wenn p ein Quadrat in $\mathbb{F}_q$ ist.

Wir können also das quadratische Reziprozitätsgesetz folgendermaßen formulieren:

Satz 6.25. *Es seien p und q ungerade und verschiedene Primzahlen.*

a) Ist wenigstens eine dieser Primzahlen von der Form $4m + 1$, so ist p ein Quadrat in $\mathbb{F}_q$ genau dann, wenn q ein Quadrat in $\mathbb{F}_p$ ist.

b) Sind beide Primzahlen von der Form $4m + 3$, so ist entweder p ein Quadrat in $\mathbb{F}_q$ oder q ein Quadrat in $\mathbb{F}_p$.

7 Zweiter Beweis

Wir nähern uns langsam dem nächsten Beweis des quadratischen Reziprozitätsgesetzes. Hierfür müssen wir noch den Begriff der Einheitswurzel und den der Gaußschen Summen einführen. Dabei halten wir uns an den Beginn des Kapitels „Variation 10. Gaußsche Summen (mit Vorzeichenbestimmung)“ von Pieper [7]. Nach der Berechnung des Quadrats der Gaußschen Summe können wir das Fundamentaltheorem in der, bereits im vorhergegangenen Kapitel angeführten Form (Satz 6.25) beweisen. Dieser Beweis befindet sich auch im Kapitel „Variation 12. Gaußsche Summen in endlichen Körpern“ von Pieper [7].

Definition 7.1. Es sei K ein endlicher Körper, ζ in K und $p \geq 1$ eine natürliche Zahl. Wenn

$$\zeta^p = 1,$$

dann heißt ζ p-te Einheitswurzel.

Eine p-te Einheitswurzel ζ heißt primitiv, falls $\zeta^m \neq 1$ für $m = 1, \ldots, p-1$ gilt.

Bemerkung. Ist ζ eine primitive p-te Einheitswurzel, dann sind $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$ alle Lösungen der Gleichung $x^p - 1 = 0$. Es kommen keine neuen Lösungen mehr dazu, wenn man die negativen Exponenten beziehungsweise Exponenten größer oder gleich p betrachtet.

Beispiel 7.2. *Zum besseren Verständnis vereinfachen wir ζ^{-2} und ζ^{p+3}:*
$\zeta^{-2} = \frac{1}{\zeta^2} = \frac{\zeta^p}{\zeta^2} = \zeta^{p-2}$,
$\zeta^{p+3} = \zeta^p \zeta^3 = \zeta^3$.

Wir können die Gleichung $x^p - 1 = 0$ auf eine Gleichung $(p-1)$-ten Grades zurückführen:

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + 1) = 0.$$

Somit ist entweder $x = 1$ oder $x^{p-1} + x^{p-2} + \ldots + 1 = 0$. Da die zweite Gleichung $\zeta, \zeta^2, \ldots, \zeta^{p-1}$, also insbesondere ζ als Nullstellen besitzt, gilt:

$$\zeta^{p-1} + \zeta^{p-2} + \ldots + 1 = 0.$$

Diesen Zusammenhang werden wir noch öfter brauchen.

Definition 7.3. Es seine p eine ungerade Primzahl, ζ ein p-te Einheitswurzel und $\left(\frac{x}{p}\right)$ das Legendre-Symbol. Die Summen

$$\tau_k = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^{kx},\ 1 \leq k \leq p-1,$$

heißen Gaußsche Summen.

Satz 7.4. *Es seien τ_k Gaußsche Summen. Es gilt*

$$\tau_k = \left(\frac{k}{p}\right) \tau_1.$$

Beweis. Es ist

$$\tau_1 = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^{x}.$$

Wir führen die Summationstransformation $kx \equiv y \pmod{p}$ durch, das heißt

$$\left(\frac{y}{p}\right) = \left(\frac{kx}{p}\right) = \left(\frac{k}{p}\right)\left(\frac{x}{p}\right), \text{ also gilt umgekehrt } \left(\frac{x}{p}\right) = \left(\frac{k}{p}\right)\left(\frac{y}{p}\right).$$

Nun setzen wir in τ_k ein. Wir erhalten

$$\tau_k = \sum_{y=1}^{p-1} \left(\frac{k}{p}\right)\left(\frac{y}{p}\right) \zeta^{y} = \left(\frac{k}{p}\right) \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) \zeta^{y} = \left(\frac{k}{p}\right) \tau_1.$$

□

Satz 7.5. *Es sei $\tau = \tau_1$ eine Gaußsche Summe. Dann ist*

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

Beweis. Nach Definition der Gaußschen Summe können wir τ^2 schreiben als

$$\tau^2 = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^{x} \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) \zeta^{y} = \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \left(\frac{xy}{p}\right) \zeta^{x+y} = \sum_{y=1}^{p-1} \sum_{x=1}^{p-1} \left(\frac{xy}{p}\right) \zeta^{x+y}.$$

Nun substituieren wir x durch yu, das heißt

$$\tau^2 = \sum_{y=1}^{p-1} \sum_{u=1}^{p-1} \left(\frac{y^2 u}{p}\right) \zeta^{yu+y} = \sum_{u=1}^{p-1} \left(\frac{u}{p}\right) \sum_{y=1}^{p-1} \zeta^{y(u+1)}.$$

Wir betrachten zuerst die Summe $\sum_{y=0}^{p-1} \zeta^{y(u+1)}$. Wenn $u \not\equiv -1 \pmod{p}$ ist, dann ist

$$\sum_{y=0}^{p-1} \zeta^{y(u+1)} = \zeta^0 + \zeta^1 + \ldots + \zeta^{p-1} = 0.$$

Ist $u \equiv -1 \pmod{p}$, dann folgt

$$\sum_{y=0}^{p-1} \zeta^{y(u+1)} = \sum_{y=0}^{p-1} \zeta^0 = \sum_{y=0}^{p-1} 1 = p.$$

Daraus folgt

$$\sum_{y=1}^{p-1} \zeta^{y(u+1)} = \begin{cases} -1 & \text{für } u \not\equiv -1 \pmod{p}, \\ p-1 & \text{für } u \equiv -1 \pmod{p}. \end{cases}$$

Wir können nun den Fall $u \equiv -1 \pmod{p}$ aus der Summe herausziehen und durch weiteres Umformen erhalten wir

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

Durch Herausheben und weil wir wissen, dass es gleich viele quadratische Reste wie Nichtreste gibt und somit die Summe von $\left(\frac{u}{p}\right)$ gleich Null sein muss, können wir weiter vereinfachen und erhalten die zu beweisende Aussage

$$\left(\frac{-1}{p}\right) \cdot (p-1) - \left(\sum_{u=1}^{p-1} \left(\frac{u}{p}\right) - \left(\frac{-1}{p}\right)\right) = \left(\frac{-1}{p}\right) \cdot p - \sum_{u=1}^{p-1} \left(\frac{u}{p}\right) = \left(\frac{-1}{p}\right) \cdot p.$$

Somit haben wir gezeigt, dass $\tau^2 = \left(\frac{-1}{p}\right) \cdot p$.
Das zweite Gleichheitszeichen, $\left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$, folgt direkt aus dem ersten Ergänzungssatz 5.4. □

Bemerkung. Für $\tau = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^x$ gilt also

$$\tau^2 = \left(\frac{-1}{p}\right) \cdot p = \begin{cases} p & \text{falls } p \equiv 1 \pmod{4}, \\ -p & \text{falls } p \equiv 3 \pmod{4}. \end{cases} \tag{15}$$

Wir werden nun das quadratische Reziprozitätsgesetz, wie wir es in Satz 5.6 angeführt haben, beweisen:

Satz. *Sind p und q verschiedene ungerade Primzahlen, dann gilt*

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

Beweis. Es seien p, q zwei verschiedene ungerade Primzahlen. $\mathbb{F}_q$ sei der endliche Körper mit q Elementen.
Es liegt entweder in $\mathbb{F}_q$ oder einem Erweiterungskörper von $\mathbb{F}_q$ eine primitive p-te Einheitswurzel ζ, denn für jedes $e \geq 1$ enthält die Körpererweiterung $\mathbb{F}_{q^e}$ mit q^e Elementen ein Element α der Ordnung $q^e - 1$ (vgl. Satz 6.7). Wenn e die kleinste Zahl ist, für die $q^e \equiv 1 \pmod{p}$ gilt, dann ist $\zeta = \alpha^{\frac{q^e-1}{p}}$ ein Element der Ordnung p in $\mathbb{F}_{q^e}$, also eine primitive p-te Einheitswurzel, weil $\zeta^p = 1$ und $\zeta^i \neq 1$ für $0 < i < p$.
Weiters sei τ die Gaußsche Summe

$$\tau = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^x.$$

Es ist τ eine Summe in einem Erweiterungskörper von $\mathbb{F}_q$ mit der Charakteristik q, also gilt

$$\tau^q = \left[\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^x\right]^q = \sum_{x=1}^{p-1} \left[\left(\frac{x}{p}\right) \zeta^x\right]^q = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^{qx} = \left(\frac{q}{p}\right) \left[\sum_{x=1}^{p-1} \left(\frac{qx}{p}\right) \zeta^{qx}\right].$$

In weiterer Folge führen wir eine Substitution durch. Wir setzen $y = qx$ und wissen, dass auch qx alle Zahlen von 1 bis $p-1$ durchläuft, da x alle diese Zahlen durchläuft. Deshalb folgt

$$\tau^q = \left(\frac{q}{p}\right) \left[\sum_{x=1}^{p-1} \left(\frac{qx}{p}\right) \zeta^{qx}\right] = \left(\frac{q}{p}\right) \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) \zeta^y = \left(\frac{q}{p}\right) \tau.$$

Das heißt

$$\tau^q = \left(\frac{q}{p}\right) \tau \qquad \Leftrightarrow \qquad \tau^{q-1} = \left(\frac{q}{p}\right). \tag{16}$$

Wenn $\left(\frac{q}{p}\right) = 1$, dann folgt aus (16) $\tau^q = \tau$, das heißt τ gehört zu $\mathbb{F}_q$.
Wenn $\left(\frac{q}{p}\right) = -1$, so folgt wieder aus (16), dass $\tau^q = -\tau$. Somit ist $\tau^{q^2} = (\tau^q)^q = (-\tau)^q = -(-\tau) = \tau$, das heißt τ liegt in $\mathbb{F}_{q^2}$.

Wir wissen aus (15), dass $(\tau^2)^q = \left(\frac{-1}{p}\right)^q p^q$. Aus dem kleinen Fermatschen Satz (Satz 2.7) folgt $\left(\frac{-1}{p}\right)^q p^q = \left(\frac{-1}{p}\right) p = \tau^2$. Somit gehört τ^2 zu $\mathbb{F}_q$.

Nach dem Eulerschen Kriterium (Satz 2.10) gilt in $\mathbb{F}_q$ die Gleichung

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

für alle a in $\mathbb{F}_q$. Da wir wissen, dass τ^2 in $\mathbb{F}_q$ ist, können wir in der obigen Gleichung $a = \tau^2$ setzen und es gilt

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

Andererseits wissen wir, dass

$$(\tau^2)^{\frac{q-1}{2}} = \tau^{\frac{2\cdot(q-1)}{2}} = \tau^{q-1},$$

also ist wegen (16)

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

In (15) haben wir τ^2 bestimmt. Wir setzen dieses Ergebnis in $\left(\frac{\tau^2}{q}\right)$ ein, durch Umformen erhalten wir

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

Zusammengefügt ergibt sich

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

Wir können die rechte Seite der Gleichung aufspalten und erhalten

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

Aus dem Eulerschen Kriterium (Satz 2.10) folgt

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

Somit haben wir das quadratische Reziprozitätsgesetz bewiesen, weil

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

□

8 Dritter Beweis

In diesem Kapitel wird ein weiterer Beweis vorgestellt, der auf der Theorie der endlichen Körper aufbaut. Außerdem werden wir den ersten und den zweiten Ergänzungssatz durch minimalen zusätzlichen Aufwand erhalten. Wir folgen im Groben dem Kapitel „Variation 13.“ von Pieper [7]. Da wir schon alle notwendigen Vorbereitungen getroffen haben, können wir diesmal sofort mit dem Beweis beginnen.

Es seien l und q verschiedene Primzahlen. Wir setzen voraus, dass l entweder die einzige gerade Primzahl 2 ist oder eine ungerade Primzahl p, außerdem ist q eine ungerade Primzahl und von der Form $4m \pm 1$.
Es sei $e \geq 1$ die kleinste Zahl, für die $l^e \equiv 1 \pmod{q}$ gilt. Wir betrachten den endlichen Körper $\mathbb{F}_{l^e}$. Dieser Körper besitzt l^e Elemente und enthält ein Element α mit der Ordnung $l^e - 1$. Weiters ist dann $\zeta = \alpha^{\frac{l^e-1}{q}}$ eine primitive q-te Einheitswurzel in $\mathbb{F}_{l^e}$.
Wir bezeichnen mit σ die Summe

$$\sigma = \sum_{aRq} \zeta^a \text{ für } 0 < a < q$$

und mit σ' die Summe

$$\sigma' = \sum_{bNq} \zeta^b \text{ für } 0 < b < q.$$

Somit durchläuft a die $\frac{q-1}{2}$ verschiedenen quadratischen Reste und b die $\frac{q-1}{2}$ quadratischen Nichtreste.

Wir betrachten den Ausdruck $1 + \sigma + \sigma'$. Es gilt

$$1 + \sigma + \sigma' = 1 + \sum_{aRq} \zeta^a + \sum_{bNq} \zeta^b = \sum_{i=0}^{q-1} \zeta^i = 1 + \zeta + \zeta^2 + \ldots + \zeta^{q-1} = 0,$$

also folgt

$$\sigma + \sigma' = -1. \tag{17}$$

Nun betrachten wir $\sigma\sigma' = \sum_{aRq} \sum_{bNq} \zeta^{a+b}$. Es ist leicht zu sehen, dass hier $\frac{q-1}{2} \cdot \frac{q-1}{2}$ Summanden auftreten. Um diesen Ausdruck näher beschreiben zu können überlegen wir uns, wie oft sich jedes r aus $\{0, 1, 2, \ldots, q-1\}$ in der Form $r \equiv a + b \pmod{q}$ mit aRq und bNq darstellen lässt. Wir beginnen mit den Darstellungen für $r = 0$, indem wir unterscheiden, ob -1 Rest oder Nichtrest für q ist:

$-1Rq$: Wenn -1 quadratischer Rest von q ist, dann besitzt 0 keine solchen Darstellungen. Angenommen 0 besitzt eine Darstellung, das heißt es existieren a und b, für die $0 \equiv a+b \pmod{q}$ mit aRq und bNq gilt, insbesondere ist a ungleich b. Da aus $-1Rq$ und aRq folgt, dass auch $-a$ quadratischer Rest von q ist und genauso aus bNq und $-1Rq$ folgt, dass $-b$ Nichtrest von q ist, kann es keine Darstellung in dieser Form geben.

$-1Nq$: Wenn $-1Nq$ ist, dann folgt aus aRq, dass $-a$ Nichtrest von q ist. Außerdem schließen wir aus bNq, dass $-bRq$ ist und es somit $\frac{q-1}{2}$ verschiedene Darstellungen für $r = 0$ gibt.
Als nächstes betrachten wir $r = 1$, das heißt $1 \equiv a + b \pmod{q}$, wobei aRq und bNq ist. Daraus folgt aber auch, dass für jedes $r \in \{1, 2, \ldots, q-1\}$ die Kongruenz $r \equiv ar + br \pmod{q}$ gilt. Je nach dem, ob r Rest von q ist, wird ar beziehungsweise br Rest oder Nichtrest von q. Die Anzahl der Darstellungen jedes r ungleich Null stimmt mit der Anzahl der Darstellung von 1 überein.

Wir erinnern uns, dass es insgesamt $\frac{(q-1)^2}{4}$ Summanden in $\sigma\sigma'$ gibt und unterscheiden wieder:

$-1Rq$: Da in diesem Fall für Null keine Darstellungen existieren, müssen für jeden der $q-1$ Reste $r = 1, 2, \ldots, q-1$ genau $\frac{q-1}{4}$ Darstellungen existieren, weil $(q-1)\cdot\frac{q-1}{4} = \frac{(q-1)^2}{4}$. Jedes $r \in \{1, 2, \ldots, q-1\}$ hat $\frac{q-1}{4}$ verschiedene Darstellungen. Das heißt aber auch, weil die Anzahl eine ganze Zahl sein muss, dass q von der Form $4m+1$ ist, beziehungsweise, dass $q \equiv 1 \pmod{4}$ gelten muss.

$-1Nq$: Ähnlich können wir auch in diesem Fall die Anzahl der Darstellungen eines jeden Restes r bestimmen, diesmal hat Null aber $\frac{q-1}{2}$ Darstellungen. Durch Nachrechnen überzeugen wir uns, dass jedes r ungleich Null genau $\frac{q-3}{4}$ Darstellungen besitzt:

$$\frac{q-1}{2} + \frac{q-3}{4} \cdot (q-1) = \frac{2q - 2 + q^2 - 4q + 3}{4} = \frac{q^2 - 2q + 1}{4} = \frac{(q-1)^2}{4}.$$

Aus dem gleichen Grund wie oben muss in diesem Fall $q \equiv 3 \pmod{4}$ sein.

An dieser Stelle fassen wir die bisherigen Ergebnisse zusammen und werden gleich erkennen, dass wir hiermit den ersten Ergänzungssatz (Satz 5.4) bewiesen haben:

Wenn $-1Rq$, dann $q \equiv 1 \pmod{4}$.

Wenn $-1Nq$, dann $q \equiv 3 \pmod{4}$.

Da die Kontraposition der Aussagen die umgekehrte Richtung der jeweils anderen Aussage liefert, folgt somit der erste Ergänzungssatz.

Wir können nun $\sigma\sigma'$ weiter vereinfachen:

Wenn $-1Rq$, dann gilt

$$\sigma\sigma' = \frac{q-1}{4} \cdot \underbrace{\sum_{r=1}^{q-1} \zeta^r}_{=-1, \text{ weil } 1+\zeta+\ldots+\zeta^{q-1}=0} = \frac{q-1}{4} \cdot (-1) = \frac{1-q}{4}.$$

Hier muss $q \equiv 1 \pmod 4$ sein.

Wenn $-1Nq$, dann gilt

$$\sigma\sigma' = \frac{q-1}{2} + \frac{q-3}{4} \cdot \underbrace{\sum_{r=1}^{q-1} \zeta^r}_{=-1} = \frac{q-1}{2} + \frac{q-3}{4} \cdot (-1) = \frac{2q-2-(q-3)}{4} = \frac{q+1}{4}.$$

Hier ist $q \equiv -1 \pmod 4$.

Wir werden diese zwei Fälle zusammenfassen. Es sei q von der Form $4m \pm 1$, dann gilt

$$\sigma\sigma' = -\left(\frac{-1}{q}\right) m = \frac{1 - \left(\frac{-1}{q}\right) q}{4}. \tag{18}$$

Wir rechnen zuerst nach, dass $-\left(\frac{-1}{q}\right) m = \frac{1-\left(\frac{-1}{q}\right)q}{4}$, wenn $q = 4m \pm 1$.
Für m können wir $\frac{q \mp 1}{4}$ schreiben. Wir ersetzen m und formen weiter um:

$$-\left(\frac{-1}{q}\right) m = -\left(\frac{-1}{q}\right) \frac{q \mp 1}{4} = \frac{-\left(\frac{-1}{q}\right) q \pm \left(\frac{-1}{q}\right)}{4}$$

Der Ausdruck $\pm\left(\frac{-1}{q}\right)$ wird in beiden Fällen 1. Wenn das positive Vorzeichen in der Gleichung vorkommt, dann ist $q = 4m+1$ und somit ist -1 quadratischer Rest von q, also ist $+\left(\frac{-1}{q}\right) = 1$. Wenn hingegen das negative Vorzeichen vorkommt, dann ist $q = 4m-1$ und -1 Nichtrest von q, das heißt $-\left(\frac{-1}{q}\right) = -(-1) = 1$.
Also ist $-\left(\frac{-1}{q}\right) m$ auch wirklich gleich $\frac{1-\left(\frac{-1}{q}\right)q}{4}$.
Wir müssen uns jetzt noch davon überzeugen, dass $-\left(\frac{-1}{q}\right) m$ auch wirklich $\sigma\sigma'$ entspricht. Dazu unterscheiden wir wieder, ob -1 Rest oder Nichtrest von q ist.

Wenn $-1Rq$, dann ist $\left(\frac{-1}{q}\right) = 1$, also ist $\frac{1-\left(\frac{-1}{q}\right)q}{4} = \frac{1-q}{4} = \sigma\sigma'$.

Wenn $-1Nq$, dann ist $\left(\frac{-1}{q}\right) = -1$, also ist $\frac{1-\left(\frac{-1}{q}\right)q}{4} = \frac{1+q}{4} = \sigma\sigma'$.

Wir fassen zusammen, was wir bis jetzt herausgefunden haben (Aussage 17 und 18):

$\sigma + \sigma' = -1$, also auch $\sigma' = -1 - \sigma$, und

$\sigma\sigma' = -\left(\frac{-1}{q}\right) m$.

Damit erhalten wir:

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

Das heißt, $\sigma^2 + \sigma - \left(\frac{-1}{q}\right) m = 0$. Das Gleiche gilt auch für σ'. Somit sind σ und σ' Nullstellen der Gleichung $x^2 + x - \left(\frac{-1}{q}\right) m = 0$.

Im folgenden Absatz werden wir uns davon überzeugen, dass σ ungleich σ' sein muss. Wäre $\sigma = \sigma'$, dann würde aus $\sigma + \sigma' = -1$ folgen, dass $\sigma = -\frac{1}{2}$ und $\sigma^2 = \frac{1}{4} = -\left(\frac{-1}{q}\right) m$. Durch Umformen kommen wir auf die Gleichung $-1 = 4\left(\frac{-1}{q}\right) m$. Wir unterscheiden wieder zwei Fälle:

Für $q \equiv 1 \pmod 4$ ist $m = \frac{q-1}{4}$ und $-1Rq$. Aus der Gleichung $-1 = 4\left(\frac{-1}{q}\right) m$ folgt also $-1 = 4 \cdot \frac{q-1}{4} = q - 1$. Somit ist $q = 0$.

Für $q \equiv -1 \pmod 4$ ist $m = \frac{q+1}{4}$ und -1 Nichtrest von q. Das heißt, $-1 = 4 \cdot (-1)\frac{q+1}{4} = -q - 1$ und somit ist $q = 0$.

Also ist in beiden Fällen $q = 0$ in $\mathbb{F}_l$. Das ist gleichbedeutend mit $q \equiv 0 \pmod l$. Dies ist aber ein Widerspruch, weil q und l zwei verschiedene Primzahlen sind. Somit sind σ und σ' verschieden.

Wir prüfen, ob die Summe σ in $\mathbb{F}_l$ liegt und werden sehen, wenn lRq, dann liegt σ in $\mathbb{F}_l$, hingegen wenn lNq, dann liegt σ nicht in $\mathbb{F}_l$.

Also beginnen wir damit, dass l quadratischer Rest von q ist, dann ist

$$\sigma^l = \left(\sum_{aRq} \zeta^a\right)^l = \sum_{aRq} \zeta^{al},$$

weil die Summe in einem Körper der Charakteristik l liegt (Satz 6.14). Wir werden al durch a' ersetzen. Es durchläuft a' alle Reste von q, weil lRq und damit auch $alRq$. Also ist

$$\sum_{aRq} \zeta^{al} = \sum_{a'Rq} \zeta^{a'} = \sigma.$$

Das heißt, dass σ zu $\mathbb{F}_l$ gehört (vgl. Satz 6.19).

Jetzt sei l quadratischer Nichtrest von q:

$$\sigma^l = \left(\sum_{aRq} \zeta^a\right)^l = \sum_{aRq} \zeta^{al}.$$

Wir ersetzen al durch b'. Diesmal durchläuft b' alle Nichtreste von q, weil $alNq$. Somit ist

$$\sum_{aRq} \zeta^{al} = \sum_{b'Nq} \zeta^{b'} = \sigma'$$

und wie wir oben nachgewiesen haben, gilt $\sigma \neq \sigma'$, also liegt σ nicht in $\mathbb{F}_l$.

Wir haben bereits festgestellt, dass die Summe σ Nullstelle der Gleichung $x^2 + x - \left(\frac{-1}{q}\right) m = 0$ ist. Es ist leicht zu sehen, dass die Koeffizienten dieser Gleichung in $\mathbb{F}_l$ liegen. Das heißt aber auch, dass sie dann und nur dann in $\mathbb{F}_l$ liegt, wenn das Polynom $x^2 + x - \left(\frac{-1}{q}\right) m$ in $\mathbb{F}_l$ in Linearfaktoren zerfällt. Andererseits haben wir gerade festgestellt, dass σ genau dann, wenn l quadratischer Rest von q ist, in $\mathbb{F}_l$ liegt. Das heißt:

I) Das Polynom $x^2 + x - \left(\frac{-1}{q}\right) m$ zerfällt in $\mathbb{F}_l$ in Linearfaktoren genau dann, wenn $\left(\frac{l}{q}\right) = 1$ ist.

Am Anfang haben wir l ungerade oder gleich zwei gewählt. Wir betrachten jetzt den Fall wenn $l = p$ ungerade ist. Aus dem Kapitel der endlichen Körper wissen wir, dass, wenn das Quadrat der Diskriminante D unseres quadratischen Polynoms $x^2+x-\left(\frac{-1}{q}\right) m$ in $\mathbb{F}_p$ liegt, dann auch die Nullstellen des Polynoms in $\mathbb{F}_p$ liegen. Außerdem wissen wir, wenn die Nullstellen des Polynoms in $\mathbb{F}_p$ liegen, dann zerfällt das Polynom in Linearfaktoren in $\mathbb{F}_p$. Das heißt, wir müssen herausfinden, wann $\left(\frac{D}{p}\right) = 1$, weil DRp genau dann, wenn D ein Quadrat in $\mathbb{F}_p$ ist.
Die Diskriminante eines quadratischen Polynoms $x^2 + ux + v = 0$ ist $D = u^2 - 4v$. Die

Diskriminante von $x^2 + x - \left(\frac{-1}{q}\right) m$ ist

$$D = 1 + 4\left(\frac{-1}{q}\right) m = 1 + 4\frac{\left(\frac{-1}{q}\right) q - 1}{4} = \left(\frac{-1}{q}\right) q.$$

II) Das Polynom $x^2 + x - \left(\frac{-1}{q}\right) m$ zerfällt in $\mathbb{F}_l$ in Linearfaktoren genau dann, wenn $\left(\frac{\left(\frac{-1}{q}\right) q}{p}\right) = 1$ ist.

Verknüpfen wir nun I) und II) mit $l = p$ folgt

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

Diese Aussage ist gleichbedeutend mit dem quadratischen Reziprozitätsgesetz und durch Umformen erhalten wir das Gesetz in bereits bekannter Form

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

Zuletzt sei $l = 2$. Wir betrachten wieder das Polynom $x^2 + x - \left(\frac{-1}{q}\right) m$. Wenn $m \equiv 0 \pmod 2$ gilt, dann ist das betrachtete Polynom $x^2 + x = x(x+1)$ in $\mathbb{F}_2$. Wenn $m \equiv 1 \pmod 2$ ist, dann ist das Polynom $x^2 + x + 1$ (irreduzibel).

III) In $\mathbb{F}_2$ zerfällt das Polynom in Linearfaktoren genau dann, wenn $m \equiv 0 \pmod 2$.

Wir wollen die Form von q bestimmen, wenn $m \equiv 0 \pmod 2$ ist:

1.Fall: $q = 4m + 1 \Leftrightarrow m = \frac{q-1}{4}$.

$$\begin{aligned} m &\equiv 0 \pmod 2 \Leftrightarrow \\ \frac{q-1}{4} &= 2k \Leftrightarrow \\ q &= 8k + 1 \end{aligned}$$

2.Fall: $q = 4m - 1 \Leftrightarrow m = \frac{q+1}{4}$.

$$\begin{aligned} m \equiv 0 \pmod 2 \Leftrightarrow \\ \frac{q+1}{4} = 2k \Leftrightarrow \\ q = 8k - 1 \end{aligned}$$

Wenn $m \equiv 0 \pmod 2$, dann ist q von der Form $8k \pm 1$.

Wir setzen in I) für $l = 2$ und mit der Aussage aus III) folgt:
$\left(\frac{2}{q}\right) = 1$ genau dann, wenn $q \equiv \pm 1 \pmod 8$ ist. Somit haben wir auch den zweiten Ergänzungssatz (vgl. Satz 5.5) bewiesen.

Literatur

[1] Siegfried Bosch. *Algebra.* Berlin: Springer, 2009.

[2] Peter Gustav Lejeune Dirichlet. *G. Lejeune Dirichlet's Werke.* Berlin: Königliche Akademie der Wissenschaften, 1889-1897.

[3] Carl Friedrich Gauß. *Disquisitiones arithmeticae.* Leipzig: G. Fleischer, 1801.

[4] Carl Friedrich Gauß. *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik.* Berlin: Springer, 1889.

[5] Carl Friedrich Gauß. *Sechs Beweise des Fundamentaltheorems über quadratische Reste.* Leipzig: Teubner, 1901.

[6] Leopold Kronecker. *Monatsberichte der Königlichen Preussische Akademie der Wissenschaften zu Berlin.* Berlin: Königliche Akademie der Wissenschaften, 1876.

[7] Herbert Pieper. *Variationen über ein zahlentheoretisches Thema von Carl Friedrich Gauss*, volume 33. Berlin: Springer, 2013.

[8] R. Schulze-Pillot. *Elementare Algebra und Zahlentheorie.* Berlin: Springer, 2007.

[9] W.S. von Waltershausen. *Gauss zum Gedächtniss.* Leipzig: S. Hirzel, 1856.

Zusammenfassung

Diese Arbeit beschäftigt sich mit drei verschiedenen, eher unbekannten Beweisen des quadratischen Reziprozitätsgesetzes. Man sagt, dass es heute mehr als 150 verschiedene Beweise für dieses Gesetz gibt.

Der als erste angeführte Beweis ist auch historisch gesehen der Erste, der publiziert wurde (von Carl Friedrich Gauß). Es wird nicht nur auf die mathematischen Aspekte des Beweises, sondern auch auf die geschichtlichen Hintergründe eingegangen. Erstaunlich ist, dass die Voraussetzungen und der Beweis selbst von elementarster Natur sind. Das „schwierigste“ mathematische Konstrukt sind Kongruenzen zweiten Grades.
Die anderen zwei Beweise werden mit Hilfe der Theorie der endlichen Körper durchgeführt und weisen somit natürlich gewisse Gemeinsamkeiten auf. Im Vergleich zum ersten Beweis sind sie sehr kurz. Der zweite Beweis baut auf der Theorie der Gaußschen Summen auf, welche im neunzehnten Jahrhundert entwickelt wurde. Die Gaußsche Summe ist ein bestimmter Typ einer endlichen Summe von Einheitswurzeln.
Beim dritten Beweis ist es, nicht zuletzt auf Grund der Länge, etwas schwieriger als beim Zweiten, den Überblick zu behalten. Oft erkennt man erst etwas später wofür gewisse Aussagen angeführt und bewiesen wurden. Zwei wichtige Hilfssätze, die beiden Ergänzungssätze, die im Rahmen des ersten und zweiten Beweises gezeigt werden müssen, liefert der dritte Beweis sehr elegant mit.

Abstract

This paper deals with three different, lesser known proofs of the law of quadratic reciprocity. It is said that there are more than 150 different proofs of this law today.

The first cited proof is also historically the first and was published by Carl Friedrich Gauss. Aside from the mathematical aspects of the proof, the historical background is discussed. It is amazing that the conditions and the proof itself are of the most elementary nature. The most "difficult" mathematical construct are congruences of the second degree.
The two other proofs use the theory of finite fields and they have naturally similarities. Compared with the first proof, they are very short. The second proof is based on the theory of Gaussian sums, which are certain types of finite sums of roots of unity.
The third proof is, not least due to its length, more difficult to follow than the second. Often you only see afterwards why certain statements were given and proved. Two important lemmas, the two supplementary laws, which have to been shown in the course of the first and second proof, come as a by-product of the third proof, without additional expenses.