Fachseminar Zahlentheorie

Elegante Beweise der Zahlentheorie

Abstract
Dieser Vortrag thematisiert eine Auswahl der Sammlung besonders elegante, mathematische Beweise der Zahlentheorie aus dem BUCH der Beweise. Im Bereich der analytischen Zahlentheorie wird ein Beweis vorgeführt, der neben dem Satz von Euklid die Unendlichkeit der Primzahlen aufzeigt. Ein weiterer hier aufgeführter Beweis zu dem Zwei-Quadrate-Satz von Fermat beantwortet eine der wohl ältesten Fragen der Zahlentheorie, welche Zahlen als Summe von zwei Quadraten dargstellt werden können. Eine effiziente Berechnung des Legendre-Symbols und ein dadurch gegebenens Verfahren, ob eine Zahl ein quadratischer Rest oder ein Nichtrest einer anderen Zahl darstellt, wird durch das quadratische Reziprozitätsgesetz gegeben. Dies wird in diesem Vortrag anhand einiger Beispiele betrachtet.

verfasst von

Nena Kimpfler

Seminarleitung:
Prof. Dr. Salma Kuhlmann

Universität Konstanz
Sommersemester 2021

Inhaltsverzeichnis

1 Die Unendlichkeit der Primzahlen nach Euler

Primzahlen p sind natürliche Zahlen mit $p \geq 2$, die nur durch sich selbst und die Eins teilbar sind. Nach dem Fundamentalsatz der Arithmetik, auch Hauptsatz der elementaren Zahlentheorie genannt, existiert für jede Zahl $n \in \mathbb{N}$, mit $n > 1$ eine eindeutige Primfaktorzerlegung.
Schnell kommt hierbei die Fragestellung auf „Wie viele Primzahlen gibt es?“. Euklid bewies den Satz, mit der Aussage, dass es mehr Primzahlen gibt, als jede vorgelegte Anzahl von Primzahlen, erstmals im Jahr 300 v. Chr. (siehe [1]). Mit dieser Frage beschäftigten sich jedoch im laufe der Jahre mehrere bekannte Mathematiker wie Euler, Goldbach und Erdös. Alle kamen auf verschiedene Weise zu demselben Befund: Es gibt unendlich viele Primzahlen.

In diesem Vortrag wird der Beweis zur Unendlichkeit der Primzahlen von Euler aufgezeigt (siehe [2, 4–5]). Dieser beschäftigte sich 1748 mit der Fragestellung und zeigte die Unendlichkeit durch einen Beweis mithilfe der analytischen Zahlentheorie.

Satz 1.1 (Satz des Euklid)**.** *Es gibt mehr Primzahlen als jede vorgelegte Anzahl von Primzahlen.*

Beweis nach Euler. Es ist $\mathbb{P} = \{2, 3, 5, 7, 11, \cdots\}$ die Menge der Primzahlen und $\mathbb{N} = \{1, 2, 3, \cdots\}$ die Menge der natürlichen Zahlen. Sei $\pi(x) := \{p \leq x : p \in \mathbb{P}\}$ die Anzahl der Primzahlen, die kleiner oder gleich der reellen Zahl x sind. Wir nummerieren die Primzahlen $\mathbb{P} = \{p_1, p_2, p_3, \cdots\}$ in aufsteigender Größe. Es sei $\log x$ der natürliche Logarithmus, definiert als $\log x = \int_1^x \frac{1}{t} dt$. Nun führen wir eine Abschätzung durch ein Integral durch, indem die Fläche unter dem Graphen der Fuktion $f(t) = \frac{1}{t}$ mit einer oberen Treppenfunktion verglichen wird.

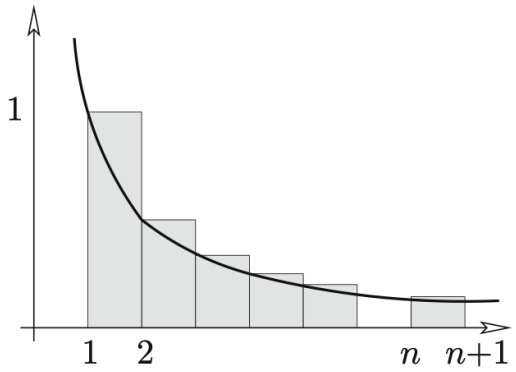

Abbildung 1: Obere Treppenfunktion für $f(t) = \frac{1}{t}$ (siehe [2, 4]).

Für $n \leq x < n+1$ haben wir

$$\begin{aligned} \log x &\leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n}, \\ &\leq \sum \frac{1}{m} \end{aligned}$$

In dieser Summe werden alle $m \in \mathbb{N}$ aufsummiert, für welche die Primteiler kleiner oder gleich x sind, also $p \leq x$.
Nach dem Hauptsatz der elementaren Zahlentheorie kann jedes dieser $m \in \mathbb{N}$ auf eindeutige Weise als ein Produkt der Form $\prod_{p \leq x} p^{k_p}$ geschrieben werden.

Die letzte Summe ist somit gleich

$$\prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(\sum_{k \geq 0} \frac{1}{p^k} \right).$$

Die innere Summe stellt mit $q = \frac{1}{p^k}$, $|q| < 1$ eine geometrische Reihe dar, welche gegen den Grenzwert $\frac{1}{1-q}$ konvergiert. Für die Abschätzung folgt insgesamt

$$\log x \leq \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{1 - \frac{1}{p}} = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1} \tag{1}$$

Offensichtlich gilt $p_k \geq k+1$ und daher

$$\frac{p_k}{p_k - 1} = \frac{p_k - 1 + 1}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k}. \tag{2}$$

Mit den Erkenntnissen (1) und (2) erhalten wir

$$\log x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1$$

Wir wissen, dass die natürliche Logarithmusfunktion $\log x$ nicht beschränkt ist, und folgern daraus, dass $\pi(x)$ ebenso unbeschränkt ist. Es gibt also unendliche viele Primzahlen. ■

2 Zwei-Quadrate-Satz von Fermat

Der Zwei-Quadrate-Satz von Fermat beschäftigt sich mit der Fragestellung, welche Zahlen als Summe von zwei Quadraten dargestellt werden können.
Diese Fragestellung ist in der Zahlentheorie äußerst beliebt und wahrscheinlich so alt wie die Zahlentheorie selbst. (siehe [2, 21–28])
Jede positive reelle Zahl lässt sich durch das Quadrat einer anderen Zahl ausdrücken. Mit dem Vier-Quadrate-Satz bewies Langrange 1770, dass sich jede natürliche Zahl als Summe von vier Quadraten ausdrücken lässt. Degens Acht-Quadrate-Satz zeigt auf, dass ein Produkt von zwei Zahlen, die sich als Summe von acht Quadraten darstellen lassen, selbst eine Summe von acht Quadraten ist (siehe [3]).
Mit dem Zwei-Quadrate-Satz zeigt Fermat, dass sich natürliche Zahlen unter gewissen Voraussetzungen auch als Summe von nur zwei Quadraten darstellen lassen.

Um den Zwei-Quadrate-Satz jedoch beweise zu können, benötigen es etwas Vorarbeit, die uns den Beweis ermöglicht.(siehe [2, 21–28])
Zunächst erinnern wir uns daran, dass für jede Primzahl p die Menge
$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ mit Addition und Multiplikation „modulo p“ einen endlichen Körper bildet. Für diesen Primkörper gelten die folgenden Eigenschaften:

- Für $x \in \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, $x \neq 0$, ist das Inverse bezüglich Addition (Notation: „$-x$“) durch $p - x \in \{1, 2, \ldots, p-1\}$ gegeben. Wenn $p > 2$ ist, dann sind x und $-x$ verschiedene Elemente von $\mathbb{Z}_p$.

Beweis. Ein Körper ist ein Ring und deshalb eine Gruppe bezüglich Addition. Sei $x \in \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, $x \neq 0$. Damit $-x+x \equiv 0 \pmod{p}$ gilt, muss die Summe der beiden durch p teilbar sein. Demnach gilt $p - x = -x$. Da in Gruppen jedes Element genau ein Inverses besitzt, existiert für jedes $x \in \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, $x \neq 0$ ein eindeutiges Inverses Element in $\mathbb{Z}_p$. ■

- Jedes $x \in \mathbb{Z}_p \backslash \{0\}$ hat ein eindeutiges multiplikatives Inverses $\overline{x} \in \mathbb{Z} \backslash \{0\}$, mit $x\overline{x} \equiv 1 \pmod{p}$.

  Beweis. Die Abbildung $\mathbb{Z}_p \to \mathbb{Z}_p$, $z \mapsto xz$ für $x \neq 0$ ist injektiv. Auf der endlichen Menge $\mathbb{Z}_p \backslash \{0\}$ somit auch surjektiv. Demnach existiert für jedes x ein eindeutiges $\overline{x} \neq 0$ mit $x\overline{x} \equiv 1 \pmod{p}$. ■

- Die Quadrate $0^2, 1^2, 2^2, \cdots, h^2$ definieren verschiedene Elemente von $\mathbb{Z}_p$, für $h = \lfloor \frac{p}{2} \rfloor$.

  Beweis. Seien $x, y \in \mathbb{Z}_p$, $x, y < h$. Für die Quadrate $x^2 \equiv y^2 \pmod{\text{p}}$ bzw. $(x+y)(x-y) \equiv 0 \pmod{p}$ folgt mit dem Satz vom Nullprodukt, dass entweder $x \equiv y$ oder $x \equiv -y$. Demnach sind alle Quadrate in $\mathbb{Z}_p$ für $h = \lfloor \frac{p}{2} \rfloor$ verschieden. ■

Alle Primzahlen p lassen sich in drei verschiedene Klassen einteilen.

$$\begin{aligned} p &= 2, \\ p &= 4m + 1, \\ p &= 4m + 3, \end{aligned}$$

mit $m \in \mathbb{N}$.
Im Folgenden wird das erste für den Zwei-Quadrate-Satz von Fermat benötigte Lemma 2.1 aufgezeigt.

Lemma 2.1. *Für jede Primzahl p der Form $p = 4m + 1$ hat die Gleichung $s^2 \equiv -1 \pmod{p}$ zwei Lösungen $s \in \{1, 2, \cdots, p-1\}$. Für $p = 2$ gibt es genau eine solche Lösung, während es für Primzahlen von der Form $p = 4m + 3$ keine Lösung gibt.*

Beweis. Für die Primklasse $p = 2$ ist $-1 \equiv 1 \pmod 2$ und $s \equiv 1 \pmod 2$. Für ungerade p wird eine Äquivalenzrelation auf der Menge $\{1, 2, \cdots, p-1\}$ konstruiert. Hierfür wird jedes Element $x \in \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ mit seinem additiven $(-x)$ und multiplikativen $(\overline{x})$ Inversen in $\mathbb{Z}_p$ in Relation gesetzt. Eine solch vierelementige Menge

$$\{x, -x, \overline{x}, -\overline{x}\}$$

besitzt die Inversen für all ihre Elemente und wird als „allgemeine“ Äquivalenzklasse bezeichnet. Sind Elemente in der allgemeinen Äquivalenzklasse nicht verschieden, so können auch kleinere Äquivalenzklassen auftreten. Hierbei können folgende Entsprechungen eintreten

- $x \equiv -x \pmod p$ für ungerades p unmöglich.
- $x \equiv \overline{x} \pmod p$ ist äquivalent zu $x^2 \equiv 1 \pmod p$. Hierfür existieren die Lösungen $x = 1$ und $x = p - 1$ und entsprechen der Äquivalenzklasse $\{1, p-1\}$ der Größe 2.
- $x \equiv -\overline{x} \pmod p$ ist äquivalent zu $x^2 \equiv -1$ da $x \in \mathbb{Z}_p$ und $\mathbb{Z}_p$ ein Körper ist, hat diese Gleichung entweder keine Lösung oder eine Lösung in Form eines Produkts von zwei verschiedenen Linearfaktoren $x_0, p - x_0$. Die entsprechende Äquivalenzklasse der Größe 2 lautet $\{x_0, p - x_0\}$.

Die $p-1$ elementige Menge $\{1, 2, \cdots, p-1\}$ lässt sich in Quadrupel, Äquivalenzklassen der Größe 4, und ein bzw. zwei Paare, Äquivalenzklassen der Größe 2, einteilen. Erinnern wir uns an die drei verschiedenen Primklassen, denen eine Primzahl p zuzuordnen ist. Für $p = 2$ ist $1 \equiv -1$ und $\overline{1} \equiv 1 (\mathrm{mod}\, 2)$. Für $p - 1 = 4m + 2$ folgt, dass sich die $p - 1$ Elemente in m Quadrupel einteilen lassen und eine Äquivalenzklasse der Größe 2, welche die Äquivalenz $x^2 \equiv 1 \pmod p$ erfüllt. Für $p - 1 = 4m$ existiert ebenso das Paar $\{1, p-1\}$ welches die Äquivalenz $x^2 \equiv 1$ bedient. Die restlichen $p - 3$ Elemente eine Primzahl der Form $p = 4m+1$ lassen sich somit in $m-1$ Quadrupel einteilen. Des Weiteren muss ein zweites Paar geben. Dieses besteht aus den Lösungen $\{x_0, p - x_0\}$ der Gleichung $s^2 \equiv -1 \pmod p$. ■

Nach den Eigenschaften eines Primkörpers (siehe [2, 20] gibt es $\lfloor \frac{p}{2} \rfloor + 1$ verschiedene Quadrate x^2 in $\mathbb{Z}_p$ und somit ebenso $\lfloor \frac{p}{2} \rfloor + 1$ verschiedene

Elemente der Form $-(1+y^2)$. Für ungerade p gilt

$$\begin{aligned} \lfloor\frac{p}{2}\rfloor + 1 + \lfloor\frac{p}{2}\rfloor + 1 &= p - 1 + 2, \\ &= p + 1, \\ &> p. \end{aligned}$$

Der Primkörper $\mathbb{Z}_p$ besteht aus p Elementen. Demnach sind die beiden Mengen von Zahlen zu groß um disjunkt zu sein und es gibt ein x^2 mit $x^2 = -(1+y^2)$. Nach dem Schubfachprinzip gibt es demnach ein x und y mit $x^2 \equiv -(1+y^2) \pmod{p}$. Für alle Primzahlen gibt es also eine Lösung der Gleichung $x^2 + y^2 \equiv -1 \pmod{p}$.
Ebenso hilfreich für den Beweis des Zwei-Quadrate-Satz von Fermat ist folgendes Lemma 2.2.

Lemma 2.2. *Keine Zahl $n = 4m+3$ ist eine Summe von zwei Quadraten.*

Beweis. Sei $k \in \mathbb{N}$ und $2k$ eine gerade Zahl. Es ist $(2k)^2 = 4k^2 \equiv 0 \pmod{4}$. Für Quadrate von ungeraden Zahlen gilt $(2k+1)^2 = 4(k^2+k)+1 \equiv 1 \pmod{4}$. Es ist somit jede Summe von Quadraten zu 0, 1 oder 2 (mod 4) kongruent. Da eine Zahl der Form $n = 4m+3 \equiv 3 \pmod{4}$, kann diese keine Summe zweier Quadrate sein. ■

Primzahlen der Form $p = 4m+3$ sind somit „schlecht“ und wir konzentrieren und auf die „guten“ Primzahlen der Klasse $p = 4m+1$. Folgende Proposition 2.1 ist der bedeutendste Schritt für den Beweis des Zwei-Quadrate-Satz von Fermat.

Proposition 2.1. Jede Primzahl der Form $p = 4m+1$ ist eine Summe von zwei Quadraten, sie kann also als $p = x^2 + y^2$ dargestellt werden, mit natürlichen Zahlen x und y.

Beweis. Betrachten wir die Paare (x', y') von ganzen Zahlen mit $0 \leq x', y' \leq \sqrt{p}$, das heißt $x', y' \in \{0, 1, \cdots \lfloor\sqrt{p}\rfloor\}$, dann gibt es für $(x', y') \neq (y', x')$ genau $(\lfloor\sqrt{p}\rfloor + 1)^2$ solche Paare. Mit der Abschätzung

$$\lfloor x \rfloor > x - 1 \quad \text{für } x = \sqrt{p} \tag{3}$$

wird deutlich, dass es mehr als p solche Paare von ganzen Zahlen gibt.

$$\begin{aligned}(\lfloor\sqrt{p}\rfloor+1)^2 &= \lfloor\sqrt{p}\rfloor^2+2\lfloor\sqrt{p}\rfloor+1^2,\\ &\overset{(3)}{>} (\sqrt{p}-1)^2+2(\sqrt{p}-1)+1,\\ &= p-p+1+p-2+1,\\ &= p.\end{aligned}$$

Also können für ein festes $s\in\mathbb{Z}$ die Werte $x'-sy'$, die aus den Paaren (x',y') erzeugt werden, nicht modulo p verschieden sein können (Schubfachprinzip). Für jedes s gibt es somit mindestens zwei verschiedene Paare

$$(x',y'),(x'',y'')\in\{0,1,\cdots,\lfloor\sqrt{p}\rfloor\}^2$$

mit

$$x'-sy'\equiv x''-sy'' \pmod{p}.$$

Definieren wir

$$x:=|x'-x''|,\quad y:=|y'-y''|,$$

so erhalten wir

$$(x,y)\in\{0,1,\cdots,\lfloor\sqrt{p}\rfloor\}^2 \quad\text{mit}\quad x\equiv\pm sy \pmod{p}.$$

Da nach dem Schubfachprinzip die Paare verschieden sind, gilt $x,y\neq 0$. Nach Lemma 2.1 existiert ein s mit $s^2\equiv -1 \pmod{p}$ für Primzahlen der Form $p=4m+1$. Es folgt

$$x^2\equiv s^2y^2\equiv -y^2 \pmod{p}$$

und wir erhalten

$$(x,y)\in\mathbb{Z}^2 \quad\text{mit}\quad 0<x^2+y^2<2p \quad\text{und}\quad x^2+y^2\equiv 0 \pmod{p}.$$

Nach Definition einer Primzahl p ist diese jedoch die einzige Zahl zwischen 0 und $2p$, welche durch p teilbar ist. Es gilt $x^2+y^2=p$. ■

Nun sind wir in der Lage, den Zwei-Quadrate-Satz von Fermat zu beweisen.

Definition 2.1. Wir nennen eine Zahl n *darstellbar*, wenn sie eine Summe von zwei Quadraten ist, das heißt, wenn $n = x^2 + y^2$ für ganzzahlige x, y ist.

Satz 2.3 (Zwei-Quadrate-Satz von Fermat)**.** *Eine natürliche Zahl n kann genau dann als Summe von zwei Quadraten dargestellt werden, wenn jeder Primfaktor der Form $p = 4m + 3$ in der Primfaktorzerlegung von n mit geradem Exponenten auftritt.*

Beweis. „$\Leftarrow$“:
Sei n eine beliebige natürliche Zahl und jeder Primfaktor der Form $p = 4m+3$ in der Primfaktorzerlegung von n taucht mit geradem Exponenten a auf.

1. Die natürlichen Zahlen $1 = 0^2 + 1^1$ und $2 = 1^2 + 1^2$ sind offensichtlich darstellbar. Nach Proposition 2.1 ist jede Primzahl der Form $p = 4m+1$ darstellbar.

2. Das Produkt von zwei darstellbaren Zahlen $n_1 = x_1^2 + y_1^2$ und $n_2 = x_2^2 + y_2^2$ ist darstellbar, denn es gilt
$$\begin{aligned} n_1 n_2 &= (x_1 + y_1)^2 \cdot (x_2 + y_2)^2, \\ &= x_1^2 x_2^2 + x_1^2 y_2^2 + y_1^2 x_2^2 + y_1^2 y_2^2, \\ &= (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - x_2 y_1)^2. \end{aligned}$$

3. Wenn $n = x^2 + y^2$ darstellbar ist, dann ist auch $nz^2 = (xz)^2 + (yz)^2$ darstellbar.

Für die beliebige, natürlich Zahl n mit $b, c, d, f, g, h, k, l, m \in \mathbb{N}$ gilt
$$\begin{aligned} n &= 2 \cdot (4b + 1) \cdot (4c + 1) \cdot (4d + 3)^2, \\ &\overset{(1)}{=} (1^2 + 1^2) \cdot (f^2 + g^2) \cdot (h^2 + k^2) \cdot (4d + 3)^2, \\ &\overset{(2)}{=} (l^2 + m^2) \cdot (4d + 3)^2, \\ &= l^2 \cdot (4d + 3)^2 + m^2 \cdot (4d + 3)^2, \\ &\overset{(3)}{=} (l(4d + 3))^2 + (m(4d + 3))^2. \end{aligned}$$

„$\Rightarrow$“:
Sei n darstellbar.

1. Wenn $p = 4m + 3$ eine Primzahl ist, die eine darstellbare Zahl $n = x^2 + y^2$ teilt, dann teilt p sowohl x als auch y, und damit ist n auch durch p^2 teilbar. Wenn nämlich $x \not\equiv 0 \pmod{p}$ wäre, dann könnten wir ein $\overline{x}$ finden mit $x\overline{x} \equiv 1 \pmod{p}$, dann die Gleichung $x^2 + y^2 \equiv 0 \pmod{p}$ mit $\overline{x^2}$ multiplizieren, und damit $1 + y^2\overline{x^2} = 1 + (\overline{x}y)^2 \equiv 0 \pmod{p}$ erhalten, was ein Widerspruch für $p = 4m + 3$ zu Lemma 2.1 ist.

2. Wenn n darstellbar und durch $p = 4m + 3$ teilbar ist, dann ist n auch durch p^2 teilbar und n/p^2 ist ebenfalls darstellbar, da n nach ausreichender Division durch p nur noch von darstellbaren Primzahlen ausgedrückt wird, weil die Primzahl der Klasse $p = 4m + 3$ mit geradem Exponenten in der Primfaktorzerlegung von n auftaucht.

■

3 Das Quadratische Reziprozitätsgesetz

Das am häufigsten bewiesene Theorem in der Mathematik ist das quadratische Reziprozitätsgesetz der Zahlentheorie. 1801 publizierte Carl Friedrich Gauß in seinem Werk Disquisitiones Arithmeticae den ersten Beweis des quadratischen Reziprozitätsgesetz von Euler. Dies wird auch als Ausgangspunkt der Entwicklung der modernen Zahlentheorie bezeichnet (siehe [4]).
Franz Lemmermeyer führte im Jahr 2000 in einer Monografie 196 Beweise an, die das quadratische Reziprozitätsgesetz beweisen [2, 29–33].

Mithilfe des von Euler aufgestellten Theorems lassen sich Aussagen über die Lösbarkeit einer quadratischen Gleichung machen, indem das Legendre-Symbol berechnet wird. Somit kann entschieden werden, ob eine Zahl ein quadratischer Rest oder Nichtrest einer anderen Zahl darstellt. Für Gleichungen höheren Grades dienen höhere Reziprozitätsgesetze (siehe [4]).
In diesem Vortrag wird über die Anwendung des quadratischen Reziprozitätsgesetz diskutiert und diese beispielhaft aufgezeigt. Genauere Informationen und der Beweis selbst sind im Buch „Das BUCH der Beweise“ von Martin Aigner und Günter M. Ziegler [2] auf Seite 29 bis 33 zu finden.

Um über das quadratische Reziprozitätsgesetz diskutieren zu können, vorab ein paar Definitionen und Hilfssätze.

Definition 3.1 (quadratischer Rest und Nichtrest)**.** Es sei $a \not\equiv 0 \pmod{p}$ gegeben, das heißt $p \nmid a$. wir nennen a einen quadratischen Rest modulo p, wenn $a \equiv b^2 \pmod{p}$ ist für ein b, und anderenfalls einen quadratischen Nichtrest. Die verschiedenen quadratischen Reste sind $1^2, 2^2, \cdots, (\frac{p-1}{2})^2$. Es gibt $\frac{p-1}{2}$ quadratische Reste und Nichtreste.

Definition 3.2 (Legendre-Symbol)**.** Es sei $a \not\equiv 0 \pmod{p}$, dann ist

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

Satz 3.1. *Für jede ungerade Primzahl p gilt:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \textit{für} \quad p \equiv 1 \pmod{4}, \\ -1, & \textit{für} \quad p \equiv -1 \pmod{4}. \end{cases}$$

Satz 3.2. *Für jede ungerade Primzahl p gilt:*

$$\left(\frac{2}{p}\right) = (-1)^{\lceil \frac{p-1}{4} \rceil} = \begin{cases} 1, & \textit{falls} \quad \lceil \frac{p-1}{4} \rceil \quad \textit{gerade} \quad \textit{also} \quad p \equiv 1, 7 \pmod{8}, \\ -1, & \textit{falls} \quad \lceil \frac{p-1}{4} \rceil \quad \textit{ungerade} \quad \textit{also} \quad p \equiv 3, 4 \pmod{8}. \end{cases}$$

Angenommen $a \equiv b^2 \pmod{p}$ ist ein quadratischer Rest. Aus dem Euler-Kriterium (siehe [2, 30]) folgt die wichtige Produktregel

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \tag{4}$$

Nun kennen wir alle wichtigen Aussagen, um das quadratische Reziprozitätsgesetz anwenden zu können.

Satz 3.3 (Quadratisches Reziprozitätsgesetz)**.** *Seien p und q verschiedene ungerade Primzahlen. Dann gilt*

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

Ist $p \equiv 1 \pmod 4$ oder $q \equiv 1 \pmod 4$, so ist $\frac{p-1}{2}$ (bzw. $\frac{q-1}{2}$) gerade, und es folgt $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$, d.h. $(\frac{q}{p}) = (\frac{p}{q})$. Im Fall $p \equiv q \equiv 3 \pmod 4$ haben wir $(\frac{p}{q}) = -(\frac{q}{p})$. Somit gilt für ungerade Primzahlen stets $(\frac{p}{q}) = (\frac{q}{p})$ außer wenn **beide** p und $q \equiv 3 \pmod 4$ sind.

Wenden wir nun das quadratische Reziprozitätsgesetz anhand folgender Beispiele an [4].
Beispiel 1:
Ist die Kongruenz $x^2 \equiv 10 \pmod{13}$ lösbar? Es muss geprüft werden, ob 10 ein quadratischer Rest ist.

$$\left(\frac{10}{13}\right) \overset{(4)}{=} \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) \overset{3.2}{=} -1\left(\frac{5}{13}\right).$$

$$\left(\frac{5}{13}\right) \overset{3.3}{=} \left(\frac{13}{5}\right) = \left(\frac{13-2\cdot 5}{5}\right) = \left(\frac{3}{5}\right) \overset{3.3}{=} \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) \overset{3.2}{=} -1.$$

Es gilt demnach

$$\left(\frac{10}{13}\right) = (-1)(-1) = 1$$

und 10 ist ein quadratischer Rest. Die obige Gleichung besitzt eine Lösung, nämlich $6^2 \equiv 10 \pmod{13}$.
Beispiel 2:
Ist die Kongruenz $x^2 \equiv 57 \pmod{127}$ lösbar? Es muss geprüft werden, ob 57 ein quadratischer Rest ist.

$$\left(\frac{57}{127}\right) \overset{(4)}{=} \left(\frac{3}{127}\right)\left(\frac{19}{127}\right).$$

$$\left(\frac{3}{127}\right) \overset{3.3}{=} (-1)\left(\frac{127}{3}\right) = (-1)\left(\frac{127-3\cdot 42}{3}\right) = (-1)\left(\frac{1}{3}\right) \overset{3.1}{=} -1$$

$$\begin{aligned}\left(\frac{19}{127}\right) &\overset{3.3}{=} (-1)\left(\frac{127}{19}\right) = (-1)\left(\frac{127-19\cdot 6}{19}\right) = (-1)\left(\frac{13}{19}\right) \overset{3.3}{=} (-1)\left(\frac{19}{13}\right)\\ &= (-1)\left(\frac{6}{13}\right) \overset{(4)}{=} (-1)\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) \overset{3.2,3.3}{=} (-1)(-1)\left(\frac{13}{3}\right)\\ &= (-1)(-1)\left(\frac{1}{3}\right) \overset{3.1}{=} 1\end{aligned}$$

Es gilt demnach

$$\left(\frac{57}{127}\right) = (-1)1 = -1$$

und 57 ist kein quadratischer Rest. Die Gleichung $x^2 \equiv 57 \pmod{127}$ besitzt keine Lösung.

Literatur

[1] Benno Artmann. *Euclid—The Creation of Mathematics* -. Springer Science and Business Media, Berlin, 2012.

[2] Martin Aigner and Günter M. Ziegler. *Das BUCH der Beweise* -. Springer-Verlag, Berlin, 2013.

[3] Guido Walz. *Lexikon der Mathematik: Band 4 - Moo bis Sch*. Springer Berlin, Wiesbaden, 2016.

[4] Komaravolu Chandrasekharan. *Introduction to Analytic Number Theory - Grundlehren der mathematischen Wissenschaften 148*. Springer Berlin, Wiesbaden, 2012.