Quadratische Reste

Michael Partheil

19. Mai 2008

Inhaltsverzeichnis

1 Hintergrund

Lemma 1.1 *Sei p eine Primzahl und $i \in \mathbb{Z}$ mit $1 \leq i \leq p-1$. Dann gilt:*

$$\binom{p}{i} \equiv 0 \ mod\ p$$

Beweis Es gilt:

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

Da p und $i!$ teilerfremd sind (beachte: $i \leq p-1$), aber $\binom{p}{i}$ eine ganze Zahl ist, folgt, dass auch

$$\frac{(p-1) \cdot (p-2) \cdot \ldots \cdot (p-i+1)}{i!}$$

eine ganze Zahl ist und somit

$$p \mid \binom{p}{i}$$

□

Lemma 1.2 *Sei p eine Primzahl und $x_1, \ldots, x_n \in \mathbb{Z}$. Dann gilt:*

$$(x_1 + \ldots + x_n)^p \equiv x_1^p + \ldots + x_n^p \ mod\ p$$

Beweis Der Beweis ist per Induktion über n.
Die Behauptung stimmt offensichtlich für $n = 1$.
Induktionsschluss von n nach $n+1$: Für ein $n \in \mathbb{N}$ gelte bereits: $(x_1 + \ldots + x_n)^p \equiv x_1^p + \ldots + x_n^p \bmod p$ (IV). Dann gilt:

$$\begin{aligned}
(x_1 + \ldots + x_{n+1})^p &\equiv \sum_{i=0}^{p} \binom{p}{i} (x_1 + \ldots + x_n)^i \cdot x_{n+1}^{p-i} \bmod p \\
&\overset{1.1}{\equiv} \binom{p}{0} (x_1 + \ldots + x_n)^0 \cdot x_{n+1}^p + \binom{p}{p} (x_1 + \ldots + x_n)^p \cdot x_{n+1}^0 \bmod p \\
&\equiv x_{n+1}^p + (x_1 + \ldots + x_n)^p \bmod p \\
&\overset{IV}{\equiv} x_1^p + \ldots x_n^p + x_{n+1}^p \bmod p
\end{aligned}$$

□

Lemma 1.3 *Sei $F \in \mathbb{Z}[X]$ ein primitives Polynom. Ist F irreduzibel in $\mathbb{Z}[X]$, dann ist F auch in $\mathbb{Q}[X]$ irreduzibel.*

BEWEIS Angenommen, F wäre reduzibel in $\mathbb{Q}[X]$. Dann gilt $F = g_1 g_2$ mit g_1, g_2 Polynome aus $\mathbb{Q}[X]$, die beide nicht konstant sind. Diese Polynome lassen sich darstellen als $g_i = a_i G_i$ mit $a_i \in \mathbb{Q}$ und G_i primitiven Polynomen aus $\mathbb{Z}[X]$. Damit:

$$F = a_1 a_2 G_1 G_2$$

Da das Produkt zweier primitiver Polynome ebenfalls wieder primitiv ist, ist auch $G_1 G_2$ primitiv. Die Darstellung eines Polynoms aus $\mathbb{Q}[X]$ als primitives Polynom aus $\mathbb{Z}[X]$ ist bis auf das Vorzeichen eindeutig, woraus $a_1 a_2 = \pm 1$ folgt. Damit wäre F aber auch in $\mathbb{Z}[X]$ reduzibel, ein Widerspruch zur Voraussetzung. □

Satz 1.4 (Irreduzibilitätskriterium von Eisenstein) *Sei*

$$F = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$$

und p eine Primzahl mit $p \mid a_i$ für $i = 0, \ldots, n-1$ und $p^2 \nmid a_0$. Dann ist F irreduzibel in $\mathbb{Z}[X]$ (und nach Lemma 1.3 auch in $\mathbb{Q}[X]$).

BEWEIS Angenommen, F wäre reduzibel. Dann gibt es Polynome $G = \sum_{i=0}^{r} b_i X^i, H = \sum_{i=0}^{s} c_i X^i \in \mathbb{Z}[X]$ die nicht konstant sind mit $F = G \cdot H$. Es folgt, dass $a_n = b_r c_s$ und damit $p \nmid b_r$, $p \nmid c_s$. Außerdem gilt $a_0 = b_0 c_0$. Da $p \mid a_0$ aber $p^2 \nmid a_0$ teilt p entweder b_0 oder c_0. Wir nehmen o.B.d.A. $p \mid b_0$ und $p \nmid c_0$ an.

Sei nun t maximal mit $p \mid b_i$ für $i = 0, \ldots, t$. Somit ist $0 \leq t \leq r-1$ und

$$a_{t+1} = \sum_{i=0}^{t+1} b_i c_{t+1-i} = \underbrace{b_{t+1} c_0}_{\notin (p)} + \underbrace{\sum_{i=0}^{t} b_i c_{t+1-i}}_{\in (p)}$$

Somit: $p \nmid a_{t+1}$, also $t+1 = n$. Damit gilt aber $r = n$ (wegen $0 \leq t \leq r-1$) und $s = 0$ (da $n = r + s$), ein Widerspruch zu H nicht konstant.

Also ist F irreduzibel in $\mathbb{Z}[X]$. □

Korollar 1.5 *Sei p eine Primzahl und*

$$\phi_p(X) := X^{p-1} + X^{p-2} + \ldots + X + 1$$

ein Polynom.

Dann ist $\phi_p(X)$ irreduzibel in $\mathbb{Q}[X]$.

BEWEIS Es gilt

$$\phi_p(X) = \frac{X^p - 1}{X - 1}$$

Das Polynom $G(X) := \phi_p(X+1)$ ist irreduzibel genau dann wenn $\phi_p(X)$ irreduzibel ist (denn $\phi_p(X)$ reduzibel $\Rightarrow \phi_p(X) = f(X)g(X) \Rightarrow \phi_p(X+1) = f(X+1)g(X+1) \Rightarrow \phi_p(X+1)$ reduzibel. Analog folgt aus $\phi_p(X+1)$ reduzibel, dass $\phi_p(X)$ reduzibel ist.)

Ferner:

$$\begin{aligned} G(X) &= \frac{(X+1)^p - 1}{X} = \frac{\sum_{i=0}^{p} \binom{p}{i} X^i - 1}{X} \\ &= \frac{\sum_{i=1}^{p} \binom{p}{i} X^i}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1} \\ &\overset{j:=i-1}{=} \sum_{j=0}^{p-1} \binom{p}{j+1} X^j \end{aligned}$$

Da $\binom{p}{p} = 1$, $\binom{p}{1} = p$ und nach Lemma 1.1 $p \mid \binom{p}{i}$ für $i = 1, \ldots, p-1$ ist $G(X)$ irreduzibel nach dem Eisenstein'schen Irreduzibilitätskriterium.

Also ist auch $\phi_p(X)$ irreduzibel in $\mathbb{Q}[X]$. □

2 Quadratische Reste

Definition 2.1 (Potenzreste :-) Seien $N, m \geq 2$ natürliche Zahlen.

Eine zu m teilerfremde Zahl $a \in \mathbb{Z}$ heißt *N-ter Potenzrest Modulo m*, wenn ein $x \in \mathbb{Z}$ existiert mit $x^N \equiv a \bmod m$.

Ist insbesondere $N = 2$, so heißt *a quadratischer Rest mod m*, andernfalls nennt man *a* einen *quadratischen Nichtrest.*

Beispiel 2.2 In $\mathbb{Z}_3^*$ ist 1 quadratischer Rest, da $1 \equiv 1^2 \bmod 3$ und 2 ist quadratischer Nichtrest, da $2^2 \equiv 1 \not\equiv 2 \bmod 3$.

Lemma 2.3 *Sei p eine ungerade Primzahl. In $\mathbb{Z}_p^*$ gibt es genau $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste.*

BEWEIS Sei $r := \frac{p-1}{2}$. Die Elemente $1^2, \ldots, r^2$ sind offensichtlich quadratische Reste in $\mathbb{Z}_p^*$ und paarweise inkongruent mod p, denn aus $1 \leq i < j \leq r$ und $i^2 \equiv j^2 \bmod p$ folgt $j^2 - i^2 \equiv (j-i)(j+i) \equiv 0 \bmod p$, also $p \mid (j-i)(j+i)$ und da p prim ist somit entweder $p \mid j-i$ oder $p \mid j+i$, was nicht möglich ist da $j-i$ und $j+i$ echt kleiner als p sind.

Also gibt es mindestens $\frac{p-1}{2}$ quadratische Reste in $\mathbb{Z}_p^*$.

Die restlichen Elemente $(r+1)^2, \ldots, (r+r)^2$ sind nochmals die selben Reste $r^2, \ldots, 1^2$ denn

$$(p-i)^2 \equiv p^2 - 2pi + i^2 \equiv i^2 \bmod p, \text{ für } i = 1, \ldots, r$$

Somit gibt es genau $\frac{p-1}{2}$ quadratische Reste und damit auch $\frac{p-1}{2}$ quadratische Nichtreste in $\mathbb{Z}_p^*$. □

Anderer Beweis Die Abbildung $\phi : \mathbb{Z}_p^* \to \mathbb{Z}_p^*, x \mapsto x^2$ ist ein Gruppenhomomorphismus, da $\phi(xy) \equiv (xy)^2 \equiv x^2y^2 \equiv \phi(x)\phi(y) \bmod p$.

Nun ist die Anzahl der Quadrate in $\mathbb{Z}_p^*$ gleich der Ordnung des Bildes von ϕ. Da gilt $Ord(\mathbb{Z}_p^*) = Ord(Bild(\phi)) \cdot Ord(Kern(\phi))$ und $Kern(\phi) = \{\pm 1\}$ (beachte: $p \neq 2$) folgt

$$Ord(Bild(\phi)) = \frac{Ord(\mathbb{Z}_p^*)}{Ord(Kern(\phi))} = \frac{p-1}{2}$$

□

Definition 2.4 (Legendre-Symbol) Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann definiert man das *Legendre-Symbol* $\left(\frac{a}{p}\right)$ durch

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

Satz 2.5 (Satz von Euler) *Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann gilt:*

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

Beweis Für $p \mid a$ stimmt die Behauptung offensichtlich. Wir können also $p \nmid a$ und damit a, p teilerfremd (beachte: p ist prim!) voraussetzen.

Ist a ein quadratischer Rest, so gibt es ein zu p teilerfremdes $b \in \mathbb{Z}$ mit $a \equiv b^2 \bmod p$. Damit:

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \overset{Fermat}{\equiv} 1 \bmod p$$

Sei nun a quadratischer Nichtrest und g eine Primitivwurzel von $\mathbb{Z}_p^*$. Damit gilt $a \equiv g^{2k+1} \bmod p$ für ein geeignetes $k \in \mathbb{N}$ (der Exponent von g muss ungerade sein, da a sonst ein quadratischer Rest wäre). Es ergibt sich:

$$a^{\frac{p-1}{2}} \equiv g^{(2k+1)\frac{p-1}{2}} \equiv g^{k(p-1)} g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \bmod p$$

Da g die Ordnung $p-1$ hat, ist $g^{\frac{p-1}{2}} \not\equiv 1 \bmod p$, aber $(g^{\frac{p-1}{2}})^2 \equiv g^{p-1} \equiv 1 \bmod p$. Die Gleichung $x^2 = 1$ hat in $\mathbb{Z}_p$ nur die Lösungen $x = \pm 1$, es folgt $g^{\frac{p-1}{2}} \equiv -1 \bmod p$, also

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p$$

□

Korollar 2.6 *Sei p eine ungerade Primzahl und $a, b \in \mathbb{Z}$.*

1. $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
2. *Aus $a \equiv b$ mod p folgt* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
3. $\left(\frac{a^2}{p}\right) = 1$ *wenn* $p \nmid a$.

Beweis Die Behauptungen folgen direkt aus dem Satz von Euler sowie der Definition des Legendre-Symbols. □

Satz 2.7 *Sei p eine ungerade Primzahl. Dann gilt:*

1. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & \text{wenn } p \equiv 1 \bmod 4 \\ -1 & \text{wenn } p \equiv 3 \bmod 4 \end{cases}$
2. $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & \text{wenn } p \equiv \pm 1 \bmod 8 \\ -1 & \text{wenn } p \equiv \pm 3 \bmod 8 \end{cases}$

Beweis Der erste Teil des Satzes folgt aus Satz 2.5 und $p \geq 3$.

Zu 2.) Im Ring der ganzen Gauß'schen Zahlen $\mathbb{Z}[i]$ gilt

$$(1+i)^2 = 2i$$

also

$$2 = -i(1+i)^2$$

Aus dem Satz von Euler folgt

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-i)^{\frac{p-1}{2}} \frac{(1+i)^p}{1+i} \overset{1.2}{\equiv} (-i)^{\frac{p-1}{2}} \frac{1+i^p}{1+i} \bmod p$$

Da gilt $i^p = i^{p-1}i = (i^2)^{(p-1)/2}i = (-1)^{(p-1)/2}i$ ist also

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

Fall 1: $p \equiv 1 \bmod 4$

$$\left(\frac{2}{p}\right) \equiv (-i)^{\frac{p-1}{2}} \equiv ((-i)^2)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{4}} \overset{2\nmid\frac{p+1}{2}}{\equiv} ((-1)^{\frac{p-1}{4}})^{\frac{p+1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \bmod p$$

Fall 2: $p \equiv 3 \bmod 4$

$$\begin{aligned}\left(\frac{2}{p}\right) &\equiv (-i)^{\frac{p-1}{2}} \frac{1-i}{1+i} \equiv (-i)^{\frac{p-1}{2}} \frac{(1-i)^2}{1-i^2} \equiv (-i)^{\frac{p+1}{2}} \bmod p \\ &\equiv (-1)^{\frac{p+1}{4}} \overset{2\nmid\frac{p-1}{2}}{\equiv} ((-1)^{\frac{p+1}{4}})^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \bmod p\end{aligned}$$

Da p als ungerade vorausgesetzt wurde, haben wir alle möglichen Fälle behandelt und es folgt Behauptung 2. □

Beispiel 2.8 Ist die Gleichung $x^2 \equiv -8 \bmod 13$ lösbar?

$$\left(\frac{-8}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = (-1)^{\frac{13-1}{2}}\left(\frac{2}{13}\right)\left(\frac{2^2}{13}\right) = 1 \cdot (-1) \cdot 1 = -1$$

da $13 \equiv 5 \bmod 8$.

Also ist die Gleichung nicht lösbar.

3 Gauß'sche Summen

Definition 3.1 Sei p eine ungerade Primzahl und

$$\zeta_p := e^{2\pi i/p} \in \mathbb{C}$$

ζ_p ist eine p-te Einheitswurzel, es gilt $\zeta_p^p = 1$ und jede andere Lösung der Gleichung $x^p = 1$ ist eine Potenz von ζ_p.

Lemma 3.2 *Seien p und ζ_p wie in Definition 3.1. Es gilt*

$$\sum_{k=0}^{p-1} \zeta_p^k = 0$$

BEWEIS Durch Multiplikation der Behauptung mit $\zeta_p - 1$ erhält man

$$\sum_{k=0}^{p-1} \zeta_p^k = 0 \iff \sum_{k=1}^{p} \zeta_p^k - \sum_{k=0}^{p-1} \zeta_p^k = 0 \iff \zeta_p^p - 1 = 0 \iff 1 - 1 = 0$$

□

Lemma 3.3 *Jedes Polynom f des Ringes $\mathbb{Z}[\zeta_p]$ lässt sich durch*

$$f = \sum_{i=0}^{p-2} a_i \zeta_p^i \quad \textit{mit } a_i \in \mathbb{Z}$$

darstellen und die Darstellung ist eindeutig.

BEWEIS Da ζ_p eine p-te Einheitswurzel ist, gilt für $k \in \mathbb{N}_0$

$$\zeta_p^{p+k} = \zeta_p^p \cdot \zeta_p^k = \zeta_p^k$$

Durch wiederholte Anwendung lassen sich so alle Potenzen ζ_p^m für $m \geq p$ auf Potenzen kleiner gleich $p-1$ reduzieren. Ferner gilt nach Lemma 3.2

$$\sum_{k=0}^{p-1} \zeta_p^k = 0 \iff \zeta_p^{p-1} = -\sum_{k=0}^{p-2} \zeta_p^k$$

Damit wäre der erste Teil der Behauptung bewiesen.

Eindeutigkeit der Darstellung: Die Zahlen $1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}$ sind in $\mathbb{Q}$ linear unabhängig. Andernfalls gäbe es ein Polynom $F \in \mathbb{Q}[X]$, $\mathrm{Grad}(F) \leq p-2$, $F \neq 0$ mit $F(\zeta_p) = 0$. Das Polynom $\phi_p := X^{p-1} + X^{p-2} + \ldots + X + 1$ ist nach Korollar 1.5 irreduzibel in $\mathbb{Q}[X]$ und da $\mathbb{Q}[X]$ Hauptidealring ist auch ein Primelement. Ferner gilt $\phi_p(\zeta_p) = 0$ nach Lemma 3.2. Da ϕ_p prim ist, sind F und ϕ_p teilerfremd (beachte: Da $Grad(F) < Grad(\phi_p)$ ist F auch kein Vielfaches von ϕ_p) und es gibt somit Polynome $A, B \in \mathbb{Q}[X]$ mit $A(X)F(X) + B(X)\phi_p(X) = 1$. Setzt man darin $X = \zeta_p$ folgt der Widerspruch $0 = 1$.

Sei nun

$$f' = a'_{p-2}\zeta_p^{p-2} + a'_{p-3}\zeta_p^{p-3} + \ldots + a'_1\zeta_p + a'_0 \quad \text{mit } a'_i \in \mathbb{Z}$$

eine andere Darstellung von f. Aus der linearen Unabhängigkeit von $1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}$ erhält man

$$f' - f = 0 \iff \sum_{i=0}^{p-2} (a'_i - a_i)\zeta_p^i = 0 \iff a'_i - a_i = 0, \text{ für alle } i = 0, \ldots, p-2$$

Also ist $a'_i = a_i$ für alle $i = 0, \ldots, p-2$, die Darstellung von f also eindeutig. $\square$

Definition 3.4 (Gauß'sche Summe)

$$S(p) := \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta_p^k \quad \in \mathbb{Z}[\zeta_p]$$

heißt Gauß'sche Summe.

Satz 3.5 *Seien p, q ungerade Primzahlen, $p \neq q$ und $S(p)$ die Gauß'sche Summe. Dann gilt:*

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

Beweis Im Folgenden wird statt ζ_p einfach nur ζ verwendet.

Bemerkung: Ist $k \not\equiv 0 \bmod p$ und durchläuft m die Zahlen $1, \ldots, p-1$, so tut dies auch $km \bmod p$, nur evtl. in anderer Reihenfolge.

$$\begin{aligned}
S(p)^2 &= \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k \cdot \sum_{l=1}^{p-1} \left(\frac{l}{p}\right) \zeta^l = \sum_{k=1}^{p-1} \sum_{l=1}^{p-1} \left(\frac{kl}{p}\right) \zeta^{k+l} \\
&= \sum_{k=1}^{p-1} \sum_{l=1}^{p-1} \left(\frac{kkl}{p}\right) \zeta^{k+kl} = \sum_{k=1}^{p-1} \sum_{l=1}^{p-1} \left(\frac{l}{p}\right) \zeta^{k(1+l)} \\
&= \sum_{l=1}^{p-1} \left(\frac{l}{p}\right) \sum_{k=1}^{p-1} \zeta^{k(1+l)} = \sum_{l=1}^{p-2} \left(\frac{l}{p}\right) \sum_{k=1}^{p-1} \zeta^{k(1+l)} + \left(\frac{p-1}{p}\right) \sum_{k=1}^{p-1} \zeta^{kp} \\
&= \sum_{l=1}^{p-2} \left(\frac{l}{p}\right) \left(\sum_{k=0}^{p-1} \zeta^{k(1+l)} - 1 \right) + \left(\frac{-1}{p}\right) \sum_{k=1}^{p-1} \underbrace{(\zeta^p)^k}_{=1} \\
&\overset{3.2}{=} -\sum_{l=1}^{p-2} \left(\frac{l}{p}\right) + \left(\frac{-1}{p}\right)(p-1) = -\left(\sum_{l=1}^{p-1} \left(\frac{l}{p}\right) - \left(\frac{p-1}{p}\right) \right) + \left(\frac{-1}{p}\right)(p-1)
\end{aligned}$$

Nach Lemma 2.3 gibt es gleich viele quadratische Reste wie Nichtreste, also gilt $\sum_{l=1}^{p-1} \left(\frac{l}{p}\right) = 0$. Damit folgt schließlich

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

Zu 2.)

$$\begin{aligned} S(p)^q &\equiv \left(\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta^k\right)^q \overset{1.2}{\equiv} \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta^{kq} \bmod q \\ &\equiv \sum_{k=1}^{p-1}\left(\frac{kqq}{p}\right)\zeta^{kq} \equiv \left(\frac{q}{p}\right)\sum_{k=1}^{p-1}\left(\frac{kq}{p}\right)\zeta^{kq} \bmod q \\ &\overset{Bem.}{\equiv} \left(\frac{q}{p}\right)\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta^k \overset{Def.}{\equiv} \left(\frac{q}{p}\right)S(p) \bmod q \end{aligned}$$

□

4 Quadratisches Reziprozitätsgesetz

„Das Quadratische Reziprozitätsgesetz gibt (...) ein Verfahren an, um (...) zu entscheiden, ob eine Zahl ein quadratischer Rest oder ein quadratischer Nichtrest ist. Die Entdeckung des quadratischen Reziprozitätsgesetzes durch Euler und der Beweis durch Gauß waren die Ausgangspunkte der Entwicklung der modernen Zahlentheorie.“
Quelle: Wikipedia[1]

Satz 4.1 (Quadratisches Reziprozitätsgesetz) *Seien p, q ungerade Primzahlen, $p \neq q$. Dann gilt:*

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

Beweis Multipliziert man die zweite Behauptung von Satz 3.5 mit $S(p)$ so erhält man

$$S(p)^{q+1} \equiv \left(\frac{q}{p}\right)S(p)^2 \bmod q \iff (S(p)^2)^{(q+1)/2} \equiv \left(\frac{q}{p}\right)S(p)^2 \bmod q$$

Ebenfalls nach Satz 3.5 gilt $S(p)^2 = \left(\frac{-1}{p}\right)p$, also

$$\left(\frac{-1}{p}\right)^{(q+1)/2} p^{(q+1)/2} \equiv \left(\frac{q}{p}\right)\left(\frac{-1}{p}\right)p \bmod q$$

[1] http://de.wikipedia.org/wiki/Quadratisches_Reziprozitätsgesetz, Stand: 2. April 2008

Kürzen von p (beachte: p, q teilerfremd) und $\left(\frac{-1}{p}\right)$ liefert

$$\left(\frac{-1}{p}\right)^{(q-1)/2} p^{(q-1)/2} \equiv \left(\frac{q}{p}\right) \bmod q$$

Nach dem Satz von Euler gilt $p^{(q-1)/2} \equiv \left(\frac{p}{q}\right) \bmod q$ und $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, es folgt

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

Da beide Seiten der Kongruenz ± 1 sind und $q \geq 3$ gilt sogar Gleichheit. □

Beispiel 4.2 Ist $x^2 \equiv -15 \bmod 71$ lösbar? (Beachte: 71 ist eine Primzahl!)

Nach dem Quadratischen Reziprozitätsgesetz gilt

$$\left(\frac{3}{71}\right) \cdot \left(\frac{71}{3}\right) = (-1)^{1 \cdot 35} \Rightarrow \left(\frac{3}{71}\right) = (-1)\left(\frac{71}{3}\right)$$

und

$$\left(\frac{5}{71}\right) \cdot \left(\frac{71}{5}\right) = (-1)^{2 \cdot 35} \Rightarrow \left(\frac{5}{71}\right) = \left(\frac{71}{5}\right)$$

Also:

$$\begin{aligned} \left(\frac{-15}{71}\right) &= \left(\frac{-1}{71}\right)\left(\frac{3}{71}\right)\left(\frac{5}{71}\right) = (-1)^{35}(-1)\left(\frac{71}{3}\right)\left(\frac{71}{5}\right) \\ &= \left(\frac{2}{3}\right)\left(\frac{1}{5}\right) \overset{Euler}{=} (-1) \cdot 1 = -1 \end{aligned}$$

Also ist die Kongruenz nicht lösbar.

5 Literaturverzeichnis

Eric Bach, Jeffrey Shallit Algorithmic Number Theory – Volume 1: efficient algorithms. The MIT Press, 1996

Otto Forster Algorithmische Zahlentheorie. vieweg, 1996

Hendrik Kasten Persönliche Notizen zur Übung zur Algebraische Zahlentheorie

Jürgen Sander Skript zur Vorlesung Zahlentheorie Wintersemester 2004/2005. http://www.blu7.com/Skripte/ZahlentheorieWS0405Skript.pdf

Michiel Smid Primality testing in polynomial time. http://citeseer.ist.psu.edu/smid03primality.html

Wikipedia Verschiedene Artikel. http://de.wikipedia.org/wiki/Hauptseite