Proseminar
"Quadratisches Reziprozitätsgesetz"

Daniel Wiens

November 2019

1 Einführung

Die grundlegende Fragestellung beim Quadratischen Reziprozitätsgestz besteht darin, ob es für ein bestimmtes $a \in \mathbb{Z}$ eine Lösung von $x^2 \equiv a \pmod{p}$ gibt. Diese Frage ist nicht so leicht zu beantworten, wie zum Beispiel in $\mathbb{R}$, wo es die $a \in \mathbb{R}_{\geq 0}$ oder in $\mathbb{C}$, wo es alle $a \in \mathbb{C}$ sind.
Im folgenden werden wir eine effiziente Berechnung herleiten, welche uns erlaubt zu sagen ob eine Lösung existiert oder nicht.

2 Herleitung von Eulers Kriterium

Im folgenden sei p eine ungerade Primzahl und $a \not\equiv 0 \pmod{p}$, das heißt $a \nmid p$. Dann nennen wir a einen *quadratischen Rest* modulo p, wenn $a \equiv b^2 \pmod{p}$ ist für ein $b \in \mathbb{Z}$ und andersfalls einen *quadratischen Nichtrest*.

Bemerkung. Wir betrachten nur ungerade Primzahlen, da für den Fall $p = 2$ die Beweise nicht in dieser Art funktionieren, was aber nicht schlimm ist, da für $p = 2$, die Quadrate immer existieren.

Lemma 1. *Die quadratischen Reste sind* $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$. *Es gibt also* $\frac{p-1}{2}$ *quadratische Reste und* $\frac{p-1}{2}$ *quadratische Nichtreste*

Beispiel. Für $p = 5$ sind $1^2 = 1,\ 2^2 = 4,\ 3^2 = 4,\ 4^2 = 1$ die Quadrate, also sind 1 und 4 quadratische Reste und 2 und 3 quadratische Nichtreste.

Beweis. Für alle $i \in \mathbb{Z}$

$$\begin{aligned} & i^2 \equiv (p-i)^2 \pmod{p} && \mid 2.\ \textit{binomische Formel} \\ \iff & i^2 \equiv p^2 - 2pi + i^2 \pmod{p} && \mid \textit{Rechnen modulo } p \\ \iff & i^2 \equiv i^2 \pmod{p} \end{aligned}$$

Lassen wir i von 1 bis $\frac{p-1}{2}$ laufen sehen wir dass es höchsten $\frac{p-1}{2}$ quadratische Reste geben kann. Nun müssen wir nur noch zeigen, dass alle diese Quadrate unterschiedlich sind:
Falls $i^2 \equiv j^2 \pmod{p}$ ist mit $1 \leq i, j \leq \frac{p-1}{2}$, so $p \mid i^2 - j^2 = (i+j)(i+j)$, da $1 \leq i + j \leq p - 1$, folgt $p \nmid i + j$, also $p \mid i - j$, das heißt $i \equiv j \pmod{p}$.
□

Führen nun das *Legendre-Symbol* ein. Sei $a \not\equiv 0 \pmod{p}$, dann ist

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

Nun versuchen wir einen neuen Ausdruck für das Legendre-Symbol zu finden, dies führt uns zu Fermats "kleinem Satz":

Satz (Fermats kleiner Satz)**.** *Für* $a \not\equiv 0 \ (mod\ p)$ *gilt*

$$a^{p-1} \equiv 1 \ (mod\ p)$$

Beispiel. Sei $a = 3,\ p = 5$ *dann* $3^4 \equiv 81 \equiv 1 \pmod{p}$

Beweis. Die Menge $\{1a, 2a, \ldots, (p-1)a\}$ durchläuft alle Reste $r \not\equiv 0 \pmod{p}$, da wenn $i \equiv j \pmod{p}$ und $ai \not\equiv aj \pmod{p}$ folgt, wenn wir mit a^{-1} multiplizieren $i \not\equiv j \pmod{p}$, ein Widerspruch**!**
Damit sind $1a, 2a, \ldots, (p-1)a$ paarweise verschieden. Also:

$$\begin{aligned} (1a)(2a)\ldots((p-1)a) &\equiv 1 \cdot 2 \cdots (p-1) \pmod{p} && \mid Umstrukturieren \\ \iff (p-1)! \cdot a^{p-1} &\equiv (p-1)! \pmod{p} && \mid durch\ (p-1)!\ teilen \\ \iff a^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

□

Mit anderen Worten das *Polynom* $x^{p-1} \in \mathbb{Z}_p[x]$ hat als Nullstellen alle Restklassen ungleich 0. Mit der der dritten Binomischen Formel erhalten wir:

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

Angenommen $a \equiv b^2 \pmod{p}$ ist ein quadratischer Rest, dann gilt nach dem kleinen Satz von Fermat $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$. Die quadratischen Reste sind daher die Nullstellen des ersten Faktors $x^{\frac{p-1}{2}} - 1$, dann sind die quadratischen Nichtreste die Nullstellen des zweiten Faktors $x^{\frac{p-1}{2}} + 1$. Ein Vergleich mit der Definition des Legendre-Symbols führt zu folgender wichtigen Beziehung:

Lemma 2 (Euler Kriterium)**.** *Für* $a \not\equiv 0 \ (mod\ p)$ *gilt*

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

Daraus folgt sofort wichtige *Produktregel*:

$$(\frac{ab}{p}) = (ab)^{\frac{p-1}{2}} (\text{mod } p) = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} (\text{mod } p) = (\frac{a}{p})(\frac{b}{p})$$

Das erlaubt uns bei der Überprüfung ob eine Zahl $a \not\equiv 0 \pmod{p}$ ein quadratischer Rest ist, diese in ihre Primfaktoren zu zerlegen. Also müssen wir nur noch $(\frac{-1}{p})$, $(\frac{2}{p})$ und $(\frac{q}{p})$ für ungerade Primzahlen q bestimmen.
$(\frac{-1}{p})$ können wir schon jetzt mit dem Euler Kriterium berechnen:

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & , falls\ \frac{p-1}{2}\ gerade\ ist\ also\ p \equiv 1 \pmod{4} \\ -1 & , falls\ \frac{p-1}{2}\ ungerade\ ist\ also\ p \equiv 3 \pmod{4} \end{cases}$$

Bemerkung. Ungerade Zahlen können nur 1 oder 3 sein modulo 4, da sie ansonsten gerade wären.
Beispiel.

$$(\frac{1}{5}) = 1,\ (\frac{2}{5}) = -1,\ (\frac{3}{5}) = 3^2 = 4 = -1 \pmod{5}, (\frac{4}{5}) = (\frac{2}{5})(\frac{2}{5}) = (-1)(-1) = 1$$

Den Fall $(\frac{2}{p})$ werden wir im nachfolgenden mit dem Lemma von Gauß berechnen, welcher für den ersten Beweis des quadratischen Reziprozitätsgesetzes von Bedeutung ist.

3 Quadratisches Reziprozitätsgesetz

Theorem (Quadratisches Reziprozitätsgesetz)**.** *Seien p und q verschiedene ungerade Primzahlen. Dann gilt:*

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

Ist $p \equiv 1 \pmod{4}$ oder $q \equiv 1 \pmod{4}$, so ist $\frac{p-1}{2}$ (bzw. $\frac{q-1}{2}$) gerade, daraus folgt:

$$\begin{aligned} (\frac{q}{p})(\frac{p}{q}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1 \qquad & | \ durch\ (\frac{p}{q})\ teilen \\ \iff (\frac{q}{p}) = (\frac{p}{q}) \qquad & | \ da\ (\frac{p}{q}) = \pm 1 \end{aligned}$$

Ist $p \equiv q \equiv 3 \pmod{p}$ so ist $\frac{p-1}{2}$ und $\frac{q-1}{2}$ ungerade und $\frac{p-1}{2}\frac{q-1}{2}$ damit auch ungerade. Also:

$$\begin{aligned} (\frac{q}{p})(\frac{p}{q}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1 \qquad & | \ durch\ (\frac{p}{q})\ teilen \\ \iff (\frac{q}{p}) = -(\frac{p}{q}) \qquad & | \ da\ (\frac{p}{q}) = \pm 1 \end{aligned}$$

Mit der Bemerkung (2) gilt für ungerade Primzahlen stets $(\frac{q}{p}) = (\frac{p}{q})$, außer wenn $p \equiv q \equiv 3 (\mathrm{mod}\ 4)$ ist

Beispiel.

$$(\frac{10}{13}) = (\frac{2}{13})(\frac{5}{13}) = -(\frac{5}{13}) = -(\frac{13}{5}) = -(\frac{3}{5}) = -(\frac{5}{3}) = 1$$

Stimmt da $6^2 \equiv 36 \equiv 10 \pmod{13}$, die Formel für $(\frac{2}{p})$ wird im folgenden geliefert.

3.1 Erster Beweis

Beweis. Der erste Beweis baut auf dem Lemma von Gauß auf:

Lemma 3 (Lemma von Gauß)**.** *Es sei $a \not\equiv 0 \pmod p$. Man betrachte die Zahlen $1a, 2a, \ldots, \frac{p-1}{2}a$ und reduziere sie modulo p auf die Restklassen mit kleinstem absolut Wert, also $ia \equiv r_i \pmod p$ mit $-\frac{p-1}{2} \leq r_i \leq \frac{p-1}{2}$ für alle i. Dann gilt:*

$$(\frac{a}{p}) = (-1)^s \text{ mit } s = \#\{i : r_i < 0\}$$

Beweis. Seien $u_1, \ldots, u_s$ die Reste modulo p die kleiner als 0 sind und $v_1, \ldots, v_{\frac{p-1}{2}-s}$ jene, die größer als 0 sind. Dann liegen die Zahlen $-u_1, \ldots, -u_s$ zwischen 1 und $\frac{p-1}{2}$ und sind alle von den $v_j's$ verschieden. Denn sei $-u_i = v_j$, d.h $u_i + v_j \equiv 0 \pmod p$. Aus $u_i \equiv ka, v_j \equiv la \pmod p$ mit $1 \leq k, l \leq \frac{p-1}{2}$ folgt $p \mid (k+l)a$, und da $p \nmid a$, muss $p \mid k+l$, da aber $1 \leq k+l \leq p-1$ folgt $p \nmid k+l$. Ein Wiederspruch!
Also ist $\{-u_1, \ldots, -u_s, v_1, \ldots, v_{\frac{p-1}{2}-s}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. Wir haben daher:

$$\prod_i (-u_i) \prod_j v_j = \frac{p-1}{2}!$$

$$\iff (-1)^s \prod_i u_i \prod_j v_j \equiv \frac{p-1}{2}! \pmod p$$

Errinnern uns das die u_i und die v_j Reste von $1a, \ldots, \frac{p-1}{2}a$ sind:

$$(\frac{p-1}{2})! \equiv (-1)^s \prod_i u_i \prod_j v_j \equiv (-1)^s (\frac{p-1}{2})!\, a^{\frac{p-1}{2}} \pmod p$$

Teilen durch $(\frac{p-1}{2})!$ und $(-1)^s$ liefert mit Euler Kriterium(2):

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \equiv (-1)^s \pmod p$$

Da p ungerade ist, folgt die Gleichheit $(\frac{a}{p}) = (-1)^s$

□

Berechnen nun $(\frac{2}{p})$: Die Zahlen $1 \cdot 2, 2 \cdot 2, \ldots, \frac{p-1}{2} \cdot 2$ liegen alle zwischen 1 und $p-1$, dann sind die $\{i : \frac{p-1}{2} < 2i \leq p-1\}$ die i mit Resten kleiner Null, denn bei denen ist der positive Rest größer als der Betrag des negativen Rests. Daraus folgt:

$$\begin{aligned} s &= \#\{i : \frac{p-1}{2} < 2i < p-1\} = \#\{i : 2i < p-1\} - \#\{i : 2i \leq \frac{p-1}{2}\} \\ &= \frac{p-1}{2} - \#\{i : 2i \leq \frac{p-1}{2}\} = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor = \left\lceil \frac{p-1}{4} \right\rceil \end{aligned}$$

Dann ist:

$$(\frac{2}{p}) = (-1)^{\lceil \frac{p-1}{4} \rceil} = \begin{cases} 1 & , falls \ \lceil \frac{p-1}{4} \rceil \ gerade \ ist \ also \ p \equiv 1, 7 \pmod 8 \\ -1 & , falls \ \lceil \frac{p-1}{4} \rceil \ ungerade \ ist \ also \ p \equiv 3, 5 \pmod 8 \end{cases}$$

Nun kommen wir zum sehr eleganten Teil des Beweises:
Seien p und q ungerade Primzahlen und $(\frac{q}{p})$ das Legendre-Symbol Sei iq ein Vielfaches von q, das wie im Lemma von Gauß (3) auf einen negativen Rest $r_i < 0$ reduziert wird. Das bedeutet es gibt eine eindeutige bestimmte ganze Zahl j mit $-\frac{p}{2} < iq - jp < 0$, wobei $0 < j < \frac{q}{2}$, wegen $0 < i < \frac{p}{2}$, da die i wie bei (3) gewählt wurden.
Es gilt also $(\frac{q}{p}) = (-1)^s$, wobei s die Anzahl der Gitterpunkte $(x, y) \in \mathbb{N}^2$ ist, mit $-\frac{p}{2} < qx - py < 0$, multiplizieren mit -1 ergibt äquivalente Aussage:

$$0 < py - qx < \frac{p}{2}, x < \frac{p}{2}, y < \frac{q}{2} \tag{1}$$

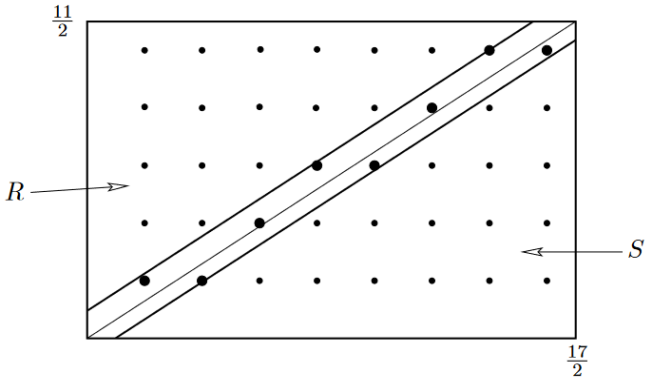
Analog ist $(\frac{p}{q}) = (-1)^t$, wobei t die Anzahl der Gitterpunkte $(x, y) \in \mathbb{N}^2$ ist, mit $-\frac{q}{2} < py - qx < 0$, multiplizieren mit -1 ergibt äquivalente Aussage:

$$0 < qx - py < \frac{q}{2}, x < \frac{p}{2}, y < \frac{q}{2} \tag{2}$$

Betrachten nun das Rechteck mit den Seitenlängen $\frac{p}{2}$,$\frac{q}{2}$ und ziehen zwei Geraden parallel zur Diagonalen $py = qx \iff y = \frac{q}{p}x$, mit den Gleichungen $y = \frac{q}{p}x + \frac{1}{2}$ oder nach Termumformung $py - qx = \frac{p}{2}$, bzw. $y = \frac{p}{q}(x + \frac{1}{2})$ oder $qx - py = \frac{q}{2}$.

Die Skizze zeigt die Situation für $p = 17,\ q = 11$.

$p = 17 \quad q = 11$
$s = 5 \quad t = 3$
$(\frac{q}{p}) = (-1)^5 = -1$
$(\frac{p}{q}) = (-1)^3 = -1$



Machen folgende Beobachtungen:

1. Es liegen keine Gitterpunkte auf der Diagonalen und auf den zwei Parallelen. Aus $py = qx$ würde nämlich $qx \equiv 0 \pmod{p}$ folgen, da q eine Primzahl ist folgt $p \mid x$, ein Wiederspruch, da $0 < x < \frac{p}{2}$. Für die Diagonalen bemerken wir das $py - qx \in \mathbb{Z}$ ist, während $\frac{p}{2}, \frac{q}{2} \in \mathbb{Q}$ sind.

2. Die Gitterpunkte, die (1) erfüllen, sind genau die Punkte zwischen $py - qx = 0 \iff py = qx$ und $py - qx = \frac{p}{2}$ liegen, also der obere Streifen $0 < py - qx < \frac{p}{2}$ und jene, die (2) erfüllen sind genau die Punkte zwischen $qx - py = 0 \iff qx = py$ und $qx - py = \frac{q}{2}$ liegen, also der untere Streifen $0 > py - qx > -\frac{q}{2} \iff 0 < qx - py < \frac{q}{2}$. Die Gesamtzahl der Gitterpunkte in den beiden Streifen ist daher $s + t$

3. Die äußeren Regionen $R : py - qx > \frac{p}{2}$ und $S : qx - py > \frac{q}{2}$ enthalten *dieselbe* Anzahl von Punkten. Dafür betrachtet man die Abbildung: $\varphi : R \to S,\ (x, y) \mapsto (\frac{p+1}{2} - x, \frac{q+1}{2} - y)$, sie ist eine Involution und damit eine Bijektion zwischen R und S.

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

Da die Gesamtzahl der Gitterpunkte im Rechteck gleich $\frac{p-1}{2} \cdot \frac{q-1}{2}$ ist folgt:

$$\begin{aligned}
(-1)^{\frac{p-1}{2}\frac{q-1}{2}} &= (-1)^{s+t}(-1)^{|R|}(-1)^{|S|} && \mid da\ |R| = |S| \\
(-1)^{\frac{p-1}{2}\frac{q-1}{2}} &= (-1)^{s+t}(-1)^{2|R|} \\
(-1)^{\frac{p-1}{2}\frac{q-1}{2}} &= (-1)^{s+t}
\end{aligned}$$

Und damit

$$(\frac{q}{p})(\frac{p}{q}) = (-1)^{s+t} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

□

3.2 Zweiter Beweis

Jetzt kommen wir zu dem zweiten Beweis, dieser beruht auf "Gaußsche Summen". Auf diese kam Gauß beim Studium der Gleichung $x^p - 1 = 0$ und der arithmetischen Eigenschaften des Körpers $\mathbb{Q}(\zeta)$ (Ein sogennanter Kreisteilungskörper), wobei ζ eine p-te Einheitswurzel ist.
Zunächst stellen wir ein paar Tatsachen über endliche Körper zusammen:

1. Es seien p und q verschiedene ungerade Primzahlen und F der endliche Körper mit q^{p-1} Elementen. Dieser besitzt Charakteristik q , also $qa = 0$ für jedes $a \in F$. Das impliziert $(a+b)^q = a^q + b^q$, da jeder Binominalkoeffizient $\binom{q}{i} = \frac{q!}{i!(q-i)!}$ ein Vielfaches von q ist im Binomischen Lehrsatz für $0 < i < q$ und daher 0 in F.

2. Die multiplikative Gruppe $F^* = F\backslash\{0\}$ ist zyklisch, mit $q^{p-1} - 1$ Elementen. Nach kleinem Fermat ist p ein Teiler von $q^{p-1} - 1$, somit existiert ein Element $\zeta \in F$ der Ordnung p, das heißt es gilt $\zeta^p = 1$ und ζ erzeugt die Untegruppe $\{\zeta, \zeta^1, \ldots, \zeta^p = 1\}$ von F^*. Man bemerke, dass jedes ζ^i mit $(i \neq p)$ wieder ein erzeugendes Element dieser Untergruppe ist. Wir erhalten also die Faktorisierung $x^p - 1 = (x - \zeta)(x - \zeta^2) \cdots (x - \zeta^p)$ (siehe grauer Kasten S.36).

Beweis. Im folgenden betrachten wir die *Gaußsche Summe*

$$G := \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)\zeta^i \in F,$$

wobei $\left(\frac{i}{p}\right)$ das Legendre-Symbol ist. Für den Beweis leiten wir zwei verschiedene Ausdrücke für G^q ab und setzen diese dann gleich.

Erster Ausdruck

$$G^q = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)^q \zeta^{iq} = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)\zeta^{iq} = \left(\frac{q}{p}\right) \sum_{i=1}^{p-1} \left(\frac{iq}{p}\right)\zeta^{iq} = \left(\frac{q}{p}\right)G \tag{3}$$

Die erste Gleichheit kommt von $(a + b)^q = a^q + b^q$ angewandt auf die Summanden, die zweite aufgrund $\left(\frac{i}{p}\right)^q = \left(\frac{i}{p}\right)$, da q ungerade ist und wir uns erinnern das $\left(\frac{i}{p}\right) = 1$ oder -1 ist. Das dritte aus $\left(\frac{i}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{iq}{p}\right) = \left(\frac{i}{p}\right)\left(\frac{q^2}{p}\right)$, wobei $\left(\frac{q^2}{p}\right) = 1$, da q^2 schon quadratischer Rest ist. Das letzte folgt, daraus das iq alle Reste ungleich 0 durchläuft.

Zweiter Ausdruck
Angenommen es gilt:

$$G^2 = (-1)^{\frac{p-1}{2}} p \tag{4}$$

Dann gilt mit Euler Kriterium (2):

$$G^q = G(G^2)^{\frac{q-1}{2}} = G(-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} = G(\frac{p}{q})(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{5}$$

Setzen nun die Ausdrücke (3) und (5) gleich

$$\begin{aligned}
(\frac{q}{p})G &= G(\frac{p}{q})(-1)^{\frac{p-1}{2}\frac{q-1}{2}} && \mid \textit{teilen durch } G \\
(\frac{q}{p}) &= (\frac{p}{q})(-1)^{\frac{p-1}{2}\frac{q-1}{2}} && \mid \textit{teilen durch } (\frac{p}{q}) \\
(\frac{q}{p})(\frac{p}{q}) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}
\end{aligned}$$

Müssen also nur noch (4) zeigen. Machen dazu zwei Beobachtungen:

- $\sum_{i=1}^{p} \zeta^i = 0$ und daher $\sum_{i=1}^{p-1} \zeta^i = -1$. Dies folgt aus der Tatsache, dass $-\sum_{i=1}^{p} \zeta^i$ der Koeffizient von x^{p-1} in $x^p - 1 = \prod_{i=1}^{p}(x - \zeta^i)$ ist, und daher gleich 0 ist.
- $\sum_{k=1}^{p-1}(\frac{k}{p}) = 0$ und daher $\sum_{k=1}^{p-2}(\frac{k}{p}) = -(\frac{-1}{p})$, da es gleich viele quadratische Reste wie Nichtreste gibt nach Lemma (1).

Wir haben:

$$G^2 = \left(\sum_{i=1}^{p-1}(\frac{i}{p})\zeta^i\right)\left(\sum_{j=1}^{p-1}(\frac{j}{p})\zeta^j\right) = \sum_{i,j}(\frac{ij}{p})\zeta^{i+j}$$

Setzten wir $j \equiv ik \pmod p$ (Bemerke das ik alle Restklassen ungleich 0 durchläuft und diese Substitution daher möglich ist).

$$G^2 = \sum_{i,k}(\frac{i^2k}{p})\zeta^{i+ik} = \sum_{i,k}(\frac{k}{p})\zeta^{i(1+k)} = \sum_{k=1}^{p-1}(\frac{k}{p})\sum_{i=1}^{p-1}\zeta^{i(1+k)}$$

Für $k \equiv p-1 \equiv -1 \pmod p$ ergibt dies $(\frac{-1}{p})(p-1)$, da $\zeta^{1+k} = \zeta^p = 1 = \zeta^{pi}$. Damit

$$G^2 = (\frac{-1}{p})(p-1) + \sum_{k=1}^{p-2}(\frac{k}{p})\sum_{i=1}^{p-1}\zeta^{i(1+k)}$$

Mit der ersten Beobachtung sehen wir das für $k \neq p-1 : \sum_{i=1}^{p-1} \zeta^i = -1$ gilt. Dann ist unser zweiter Summand $-\sum_{k=1}^{p-2} \frac{k}{p} = (\frac{-1}{p})$ nach der zweiten Beobachtung. Es folgt:

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

mit Eulers Kriterium (2), was zu zeigen war.

□

4 Literartur

M. Aigner, G. M. Ziegler, Das Buch der Beweise. Springer, 5. Auflage. (S.30-38)