Zweiter Beweis des quadratischen Reziprozitätssatzes und Quadratische Gaußsummen

Armin Sawicki

3. Mai 2017

Inhaltsverzeichnis

1 Erinnerung, Hilfssätze

Definition. *Das Legendre-Symbol:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, falls\ \exists\ x \not\equiv 0(p) : x^2 \equiv a(p) \\ -1, falls\ \ \nexists\ x \not\equiv 0(p) : x^2 \equiv a(p) \\ 0, falls\ p \mid a \end{cases}$$

Satz 1.1. *Einige Rechenregeln für das Legendre-Symbol:*

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

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

$$(c) \qquad a \equiv b(p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

Satz 1.2. *Seien $\omega_1, \omega_2 \in \Omega,\ p \in \mathbb{Z}$ prim. Dann gilt:*

$$(\omega_1 + \omega_2)^p \equiv {\omega_1}^p + {\omega_2}^p(p)$$

Satz 1.3 (Wilsons Theorem)**.** $(p-1)! \equiv -1(p)$

Theorem (Quadratisches Reziprozitätsgesetz)**.** *Seien p, q ungerade und prim, $p \neq q$. Dann gilt:*

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

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

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

2 Die quadratische Eigenschaft der 2

Sei $\zeta = e^{2\pi i/8}$ und schreibe $\tau = \zeta + \zeta^{-1}$.

Offenbar gilt: $\zeta^2 = e^{\pi i/2} = i$.

Damit folgt die quadratische Eigenschaft der 2 durch

$$\tau^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = i + 2 - i = 2$$

Bemerkung. *Als Nullstelle des Polynoms $x^8 - 1 \in \mathbb{Z}[x]$ ist ζ algebraisch und τ als Summe zweier algebraischer Zahlen ist ebenfalls algebraisch.*

Damit lässt sich nun Teil (b) des quadratischen Reziprozitätsgesetzes zeigen:

Beweis. Sei $p \in \mathbb{Z}$ ungerade und prim, dann gilt:

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

Andererseits gilt nach Satz 1.2 und wegen $\zeta^3 = -\zeta^{-1}$:

$$\Rightarrow\; \tau^p = (\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} = \begin{cases} \zeta + \zeta^{-1} = \tau, falls\, p \equiv \pm 1(8) \\ -(\zeta + \zeta^{-1}) = -\tau, falls\, p \equiv \pm 3(8) \end{cases}$$

Insgesamt folgt somit für $\varepsilon \equiv \frac{p^2-1}{8}(2)$

$$\begin{aligned} (-1)^\varepsilon \tau &\equiv \left(\frac{2}{p}\right)\tau(p) \mid \cdot\tau \\ (-1)^\varepsilon 2 &\equiv \left(\frac{2}{p}\right)2(p) \mid : 2 \\ (-1)^\varepsilon &\equiv \left(\frac{2}{p}\right)(p) \\ \Rightarrow (-1)^\varepsilon &= \left(\frac{2}{p}\right) \end{aligned}$$

□

3 Quadratische Summen von Gauß

Sei $p \in \mathbb{Z}$ ungerade und prim und sei $\zeta = e^{2\pi i/p}$.

Lemma 3.1. $\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} p, falls\ a \equiv 0(p) \\ 0, falls\ a \not\equiv 0(p) \end{cases}$

Beweis. Für $a \equiv 0(p)$ folgt $\zeta^a = 1$ und damit $\sum_{t=0}^{p-1} \zeta^{at} = p$.

Ist $a \not\equiv 0(p)$, so ist $\zeta^a \neq 1$ und damit folgt

$$\sum_{t=0}^{p-1} \zeta^{at} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = 0.$$

□

Daraus folgt direkt folgendes

Korollar 3.2. $p^{-1} \sum_{t=0}^{p-1} \zeta^{(x-y)t} = \delta(x,y) := \begin{cases} 1, falls\ x \equiv y(p) \\ 0, falls\ x \not\equiv y(p) \end{cases}$

Lemma 3.3. *Sei (t/p) das Legendre-Symbol, dann gilt:*

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

Beweis. Nach Definition gilt $(0/p) = 0$. Von den verbleibenden $p-1$ Summanden ist jeweils eine Hälfte $+1$ und die andere Hälfte -1, da die Anzahl der quadratischen Reste und Nichtreste modulo p gleich ist. □

Definition. *Die quadratische Gaußsumme ist definiert durch:*

$$g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}$$

Notation. *Setze* $g := g_1$.

Satz 3.4. $g_a = (a/p)g$

Beweis. Ist $a \equiv 0(\mathrm{p})$, so gilt $\zeta^{at} = 1$ für alle t und mit Lemma 3.3 folgt:

$$g_{\mathrm{a}} = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0 = \left(\frac{a}{p}\right) g$$

Sei nun $a \not\equiv 0(\mathrm{p})$. Da t alle Werte $0, ..., p-1$ annimmt und p nicht a teilt, folgt, dass at auch alle Werte $0, ..., p-1$ durchläuft. Es folgt:

$$\left(\frac{a}{p}\right) g_{\mathrm{a}} = \sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at} = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \zeta^{x} = g,$$

Durch Multiplikation mit (a/p) folgt die Behauptung. □

Bemerkung. *Aus Satz 3.4 folgt für $a \not\equiv 0(p)$: ${g_a}^2 = g^2$.*

Satz 3.5. $g^2 = (-1)^{\frac{p-1}{2}} p$

Beweis. Wir berechnen dafür die Summe $\sum_{a=0}^{p-1} g_{\mathrm{a}} g_{\text{-a}}$ auf zwei Weisen:
Zum einen gilt:

$$\sum_{a=0}^{p-1} g_{\mathrm{a}} g_{\text{-a}} = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \sum_{a=1}^{p-1} \left(\frac{-1}{p}\right) g^2 = (p-1)\left(\frac{-1}{p}\right) g^2$$

Andererseits gilt $g_{\mathrm{a}} g_{\text{-a}} = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \zeta^{a(x-y)}$ und mit Korollar 3.2 folgt:

$$\sum_{a=0}^{p-1} g_{\mathrm{a}} g_{\text{-a}} = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \delta(x,y) p = p \sum_{x=0}^{p-1} \left(\frac{x^2}{p}\right) = p(p-1)$$

Damit gilt:

$$\begin{aligned} & (p-1)\left(\frac{-1}{p}\right) g^2 = p(p-1) \\ \Leftrightarrow \quad & \left(\frac{-1}{p}\right) g^2 = p \\ \Leftrightarrow \quad & g^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p \end{aligned}$$

□

Nun können wir mithilfe der quadratischen Gaußsummen auch Teil (c) des quadratischen Reziprozitätsgesetzes zeigen.

Beweis. Sei $g^2 = p^* := (-1)^{\frac{p-1}{2}} p$ und sei q $\neq$ p ungerade und prim. Dann gilt:

$$\begin{aligned} g^{q-1} = (g^2)^{\frac{q-1}{2}} = (p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right)(q) \\ \Rightarrow\ g^q \equiv \left(\frac{p^*}{q}\right) g(q) \end{aligned}$$

Nach Satz 1.2 und 3.4 folgt andererseits:

$$g^q = \left(\sum_{t=0}^{p-1} \left(\frac{t}{p}\right)\zeta^t\right)^q \equiv \sum_{t=0}^{p-1} \left(\frac{t}{p}\right)^q \zeta^{qt} \equiv g_{\mathrm{q}} \equiv \left(\frac{q}{p}\right) g(q)$$

Also:

$$\begin{aligned} \left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g(q) \mid \cdot g \\ \Leftrightarrow \left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^*(q) \\ \Rightarrow \left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right)(q) \end{aligned}$$

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

□

4 Das Vorzeichen der Gaußschen Summe

Theorem. *Der Wert der quadratischen Gaußsumme ist gegeben durch:*

$$g = \begin{cases} \sqrt{p}, falls\ p \equiv 1(4) \\ i\sqrt{p}, falls\ p \equiv 3(4) \end{cases}$$

Sei $\zeta = e^{2\pi i/p}$. Dann sind $1, \zeta, ..., \zeta^{p-1}$ die Nullstellen von $x^p - 1 \in \mathbb{Z}[x]$.

Satz 4.1. *Es gilt:*

$$\prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)})^2 = (-1)^{\frac{p-1}{2}} p$$

Beweis. Es gilt $x^p - 1 = (x-1)\prod_{j=1}^{p-1}(x - \zeta^j)$.

Division durch $x - 1$ und Einsetzen von $x = 1$ liefert:

$$\begin{aligned} p &= \prod_{j=1}^{p-1}(1 - \zeta^j) \\ &= \prod_{k=1}^{\frac{p-1}{2}}(1 - \zeta^{4k-2})(1 - \zeta^{-(4k-2)}) \\ &= \prod_{k=1}^{\frac{p-1}{2}}(\zeta^{-(2k-1)} - \zeta^{2k-1})(\zeta^{2k-1} - \zeta^{-(2k-1)}) \\ &= (-1)^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}}(\zeta^{2k-1} - \zeta^{-(2k-1)})^2 \end{aligned}$$

□

Satz 4.2. *Es gilt:*

$$\prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)}) = \begin{cases} \sqrt{p}, falls\ p \equiv 1(4) \\ i\sqrt{p}, falls\ p \equiv 3(4) \end{cases}$$

Beweis. Nach Satz 4.1 müssen wir nur das Vorzeichen bestimmen. Wir können das Produkt auch schreiben als:

$$i^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} 2 \cdot sin\left(\frac{(4k-2)\pi}{p}\right)$$

Wegen $1 \leq k \leq \frac{p-1}{2}$ ist $sin\left(\frac{(4k-2)\pi}{p}\right) < 0$ genau dann, wenn $1 < \frac{4k-2}{p} \leq 2$. $\Leftrightarrow \frac{p+2}{4} < k \leq \frac{p+1}{2}$. Daher hat das Produkt $\frac{p-1}{2} - \left\lfloor \frac{p+2}{4} \right\rfloor$ negative Faktoren, also $\begin{cases} \frac{p-1}{4}, falls\ p \equiv 1(4). \\ \frac{p-3}{4}, falls\ p \equiv 3(4). \end{cases}$ □

Nach Satz 3.5 und 4.1 haben wir nun für $\varepsilon = \pm 1$ gezeigt:

$$g = \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)}) \tag{1}$$

Satz 4.3. $\varepsilon = +1$

Beweis. Betrachte das Polynom

$$f(x) = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \cdot x^j - \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (x^{2k-1} - x^{p-(2k-1)})$$

Dann gilt $f(\zeta) = 0$ nach (1) und $f(1) = 0$ nach Lemma 3.3. Da die zugehörigen Minimalpolynome $1 + x + ... + x^{p-1}$ und $x - 1$ relativ prim sind, folgt somit $x^p - 1 \mid f(x)$, schreibe also $f(x) = (x^p - 1)h(x)$ und substituiere $x = e^z$:

$$\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \cdot e^{jz} - \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (e^{(2k-1)z} - e^{(p-(2k-1))z}) = (e^{pz} - 1)h(e^z)$$

Übergang zur Reihendarstellung:

$$\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\cdot\left(\sum_{l=0}^{\infty}\frac{j^l}{l!}\cdot z^l\right)-\varepsilon\prod_{k=1}^{\frac{p-1}{2}}\left(\sum_{l=0}^{\infty}\frac{(2k-1)^l-(p-(2k-1))^l}{l!}\cdot z^l\right)$$
$$=\left(\sum_{l=1}^{\infty}\frac{p^l}{l!}\cdot z^l\right)h(e^z)$$

Koeffizientenvergleich bei $z^{\frac{p-1}{2}}$ und Reduktion modulo p liefert dann:

$$\frac{\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)j^{\frac{p-1}{2}}}{(\frac{p-1}{2})!}-\varepsilon\prod_{k=1}^{\frac{p-1}{2}}(4k-2-p)\equiv 0(p)$$
$$\Leftrightarrow\ \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)j^{\frac{p-1}{2}}\equiv\varepsilon\cdot\left(\frac{p-1}{2}\right)!\prod_{k=1}^{\frac{p-1}{2}}(4k-2)(p)$$
$$\equiv\varepsilon\cdot(2\cdot 4\cdot 6\cdot\ldots\cdot(p-1))\prod_{k=1}^{\frac{p-1}{2}}(2k-1)(p)$$
$$\equiv\varepsilon\cdot(p-1)!$$
$$\equiv-\varepsilon(p)$$

nach Wilsons Theorem.

Nach Satz 1.1(a) gilt andererseits $j^{\frac{p-1}{2}}\equiv(j/p)(p)$, somit:

$$p-1=\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)^2\equiv-\varepsilon(p)$$

Damit folgt $\varepsilon\equiv 1(p)$, also $\varepsilon=+1$. □