

## Quadratische Reziprozität: Rechnungen mit Gaußschen Summen

Wir wollen die Formel  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$  beweisen, wobei  $p$  eine ungerade Primzahl ist.

Dazu betrachten wir den endlichen Körper  $F_{p^2}$  und ein erzeugendes Element  $\zeta$  von dessen multiplikativer Gruppe. Da  $p^2-1$  jedenfalls durch 8 teilbar ist, also  $p^2-1=8k$  ist  $\eta=\zeta^k$  eine primitive achte Einheitswurzel. Damit ist  $\eta^8=1$  und  $\eta^4 \neq 1$ , also  $\eta^4=-1$ .

Wir setzen für  $n \in \mathbb{Z}$   $f(n) := \begin{cases} 1 & \text{falls } n \equiv 1,7 \pmod{8} \\ -1 & \text{falls } n \equiv 3,5 \pmod{8} \\ 0 & \text{sonst} \end{cases} = \begin{cases} (-1)^{\frac{n^2-1}{8}} & \text{falls } n \text{ ungerade} \\ 0 & \text{sonst} \end{cases}$ .

Die Abbildung  $f: \mathbb{Z} \rightarrow \{-1,1\}$  ist multiplikativ, d.h.  $\forall m, n \in \mathbb{Z}: f(mn) = f(m)f(n)$ .

In  $F_{p^2}$  bildet man die *Gauss-Summe*  $G = \sum_{i=0}^{p-1} f(i)\eta^i = \eta - \eta^3 - \eta^5 + \eta^7 = 2(\eta - \eta^3)$ .

Jetzt errechnet man  $G^2 = 4(\eta - \eta^3)^2 = 4(\eta^2 - 2\eta^4 + \eta^6) = 4 \cdot 2 = 8$ , wobei  $8 = 8 \cdot 1 = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 \in F_{p^2}$ .

Außerdem ist  $G^p = 2^p(\eta - \eta^3)^p = 2(\eta^p - \eta^{3p})$ ; es ist  $2^p = 2$  weil 2 liegt ja bereits im Unterkörper  $\mathbb{Z}_p$  von  $F_{p^2}$  liegt, und in diesem gilt  $\forall x \in \mathbb{Z}_p: x^p = x$ , außerdem fallen in einem Körper der Charakteristik  $p$  die gemischten Terme in der binomischen Formel weg.

Man rechnet jetzt einfach nach, daß:

$$G^p = 2(\eta^p - \eta^{3p}) = \begin{cases} 2(\eta - \eta^3) = G & \text{falls } p \equiv 1,7 \pmod{8} \\ -2(\eta - \eta^3) = -G & \text{falls } p \equiv 3,5 \pmod{8} \end{cases}$$

Bei dieser Rechnung wurden nur die Formeln  $\eta^8=1$ ,  $\eta^4=-1$  benutzt.

Es ist aber auch

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

Weil  $G \neq 0$ , ergibt sich durch Kürzen:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv 1,7 \pmod{8} \\ -1 & \text{falls } p \equiv 3,5 \pmod{8} \end{cases}$$

was zu beweisen war.

Nach dieser Vorübung beweist man mit derselben Technik das quadratische Reziprozitätsgesetz:

Seien  $p, q$  ungerade Primzahlen. Dann ist

$$\begin{aligned} \left(\frac{p}{q}\right) &= -\left(\frac{q}{p}\right) \text{ falls } p \text{ und } q \text{ beide kongruent } 3 \text{ modulo } 4 \text{ sind. In allen anderen F\u00e4llen gilt} \\ \left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right) \end{aligned}$$

Zum Beweis nimmt man sich zun\u00e4chst einen endlichen K\u00f6rper  $K$  der Charakteristik  $p$  her, in welchem es eine primitive  $q$ -te Einheitswurzel gibt. Z.B. eignet sich  $F_{p^{q-1}}$ . Die multiplikative Gruppe dieses K\u00f6rpers besitzt  $p^{q-1} - 1$  Elemente. Nun gilt  $\forall x \in \mathbb{Z}_q: x^{q-1} = 1$ ; dies hei\u00dft aber, da\u00df insbesondere  $p^{q-1} - 1$  durch  $q$  teilbar ist, d.h. man hat eine Darstellung  $p^{q-1} - 1 = qk$ . F\u00fcr ein erzeugendes Element  $\zeta$  der multiplikativen Gruppe von  $F_{p^{q-1}}$  setzen wir  $\eta := \zeta^k$ , so da\u00df  $\eta$  eine primitive  $q$ -te Einheitswurzel ist.

Im Folgenden sei also  $K$  ein endlicher K\u00f6rper der Charakteristik  $p$ , und  $\eta \in K$  sei eine primitive  $q$ -te Einheitswurzel. In  $K$  bilden wir die Gau\u00df-Summe

$$G = \sum_{i=1}^{q-1} \left(\frac{i}{q}\right) \eta^i$$

Vor den Potenzen  $\eta^i$  steht also wieder eine multiplikative Funktion mit Werten in  $\{-1, 1\}$ ! Wir vorher wenden wir die binomische Formel an, beachten, da\u00df die gemischten Terme wegfallen:

$$G^p = \sum_{i=1}^{q-1} \left(\frac{i}{q}\right)^p \eta^{ip} = \sum_{i=1}^{q-1} \left(\frac{i}{q}\right) \eta^{ip}$$

Die Abbildung  $\mathbb{Z}_q^* \rightarrow \mathbb{Z}_q^*, i \rightarrow ip$  ist bijektiv. Setzen wir  $j = ip$  und  $p'$  f\u00fcr das Inverse von  $p$  in  $\mathbb{Z}_q$ , so erhalten wir durch Indexumbenennung die Gleichung:

$$G^p = \sum_{i=1}^{q-1} \left(\frac{i}{q}\right) \eta^{ip} = \sum_{j=1}^{q-1} \left(\frac{j p'}{q}\right) \eta^j$$

Nun ist  $\left(\frac{j p'}{q}\right) = \left(\frac{j}{q}\right) \left(\frac{p'}{q}\right) = \left(\frac{j}{q}\right) \left(\frac{p}{q}\right)$ , so da\u00df insgesamt

$$G^p = \sum_{i=1}^{q-1} \left(\frac{i}{q}\right) \eta^{ip} = \sum_{j=1}^{q-1} \left(\frac{j p'}{q}\right) \eta^j = \left(\frac{p}{q}\right) \sum_{i=1}^{q-1} \left(\frac{j}{q}\right) \eta^j = \left(\frac{p}{q}\right) G$$

Wie vorher rechnen wir auch  $G^2$  aus:

$$G^2 = \left(\sum_{i=1}^{q-1} \left(\frac{i}{q}\right) \eta^i\right) \cdot \left(\sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \eta^j\right) = \left(\sum_{i=1}^{q-1} \sum_{j=1}^{q-1} \left(\frac{ij}{q}\right) \eta^{i+j}\right)$$

In  $\mathbb{Z}_q^*$  setzen wir f\u00fcr festes  $i$ :  $k = j i^{-1}$ , haben damit  $j = ki$  und rechnen weiter:

$$\dots \left(\sum_{i=1}^{q-1} \sum_{k=1}^{q-1} \left(\frac{i^2 k}{q}\right) \eta^{i+ki}\right) = \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \sum_{i=1}^{q-1} \eta^{i(1+k)} = \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \left(\sum_{i=0}^{q-1} (\eta^{1+k})^i - 1\right) = \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \sum_{i=0}^{q-1} (\eta^{1+k})^i - \sum_{k=0}^{q-1} \left(\frac{k}{q}\right)$$

Nun ist aber  $\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) = 0$ , weil die Anzahl der Quadrate mod  $q$  gleich der Anzahl der Nicht-Quadrate ist.

Wir haben also:  $G^2 = \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \sum_{i=0}^{q-1} (\eta^{1+k})^i$

Nun ist für  $k \neq q-1 = -1$  die Summe  $\sum_{i=0}^{q-1} (\eta^{1+k})^i$  gleich Null<sup>1</sup>, während sie für  $k = q-1 = -1$  den durch  $q$ -fache Summation von 1 den Wert  $q$  besitzt. Es ergibt sich daher schließlich :

$$G^2 = \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \sum_{i=0}^{q-1} (\eta^{1+k})^i = \left(\frac{-1}{q}\right) q .$$

Diese Formel wird zu einer zweiten Berechnung von  $G^p$  herangezogen:

$$G^p = G G^{p-1} = G (G^2)^{\frac{p-1}{2}} = G \left( \left( (-1)^{\frac{q-1}{2}} \right)^{\frac{p-1}{2}} \right) q^{\frac{p-1}{2}} . \text{ Vorher hatten wir erhalten:}$$

$$G^p = G \cdot \left(\frac{p}{q}\right) ,$$

so daß sich das quadratische Reziprozitätsgesetz durch Gleichsetzen und Kürzen von  $G$  ergibt.

---

<sup>1</sup> Man setze  $\vartheta = \eta^{1+k} \neq 1$  und erhält nach Umordnen  $\vartheta \sum_{i=0}^{q-1} \vartheta^i = \sum_{i=0}^{q-1} \vartheta^i$ , also  $(\vartheta - 1) \sum_{i=0}^{q-1} \vartheta^i = 0$ , also  $\sum_{i=0}^{q-1} \vartheta^i = 0$ .