Legendre-Symbol von 2

Lemma Legendre-Symbol von 2

Sei $p \in \mathbb{P} \setminus \{2\}$. Dann gilt

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

Beweis:

- Nach Euler-Identität wissen wir, dass $(\frac{2}{p}) \equiv 2^{\frac{p-1}{2}} \bmod p$.
- In $\mathbb{Z}[i]$ gilt $2 = (-i) \cdot 2i = (-i)(1+i)^2$. Damit folgt
$$2^{\frac{p-1}{2}} = (-i)^{\frac{p-1}{2}}(1+i)^{p-1} = (-i)^{\frac{p-1}{2}} \frac{(1+i)^p}{(1+i)}.$$
- Modulo p (für Real-/Imaginärteil separat) gilt $(1+i)^p \equiv (1+i^p)$.
- Wir schreiben $p = 2k+1$ mit $k \in \mathbb{N}$ und erhalten
$$2^{\frac{p-1}{2}} \equiv (-i)^k \cdot \frac{1+i^{2k+1}}{1+i} = (-i)^k \cdot \frac{1+(-1)^k i}{1+i} \bmod p \quad (*).$$

Legendre-Symbol von 2

Beweis: (Fortsetzung)

- Der Term $\frac{1+(-1)^k i}{1+i}$ ist 1 für gerades k. Für ungerade k gilt
$$\frac{1-i}{1+i} = \frac{(1-i)^2}{1-i^2} = \frac{-2i}{2} = (-i).$$
- In $\mathbb{Z}[i]$ ist $\operatorname{ord}(-i) = 4$. D.h. es genügt, $k \bmod 4$ zu betrachten.
- Für $k \equiv 0, 1, 2, 3$ liefert die rechte Seite von $(*)$ die Werte
$$(-i)^0 = 1,\ (-i)^2 = (-1),\ (-i)^2 = (-1) \text{ und } (-i)^4 = 1.$$
- Aus $k \equiv \frac{p-1}{2} \bmod 4$ folgt $p \equiv 2k + 1 \bmod 8$.
- Für $k \equiv 0, 3$ erhalten wir $(\frac{2}{p}) = 1$ und $p \equiv \pm 1 \bmod 8$.
- Für $k \equiv 1, 2$ erhalten wir $(\frac{2}{p}) = (-1)$ und $p \equiv \pm 3 \bmod 8$.

Übung: Zeigen Sie $(-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{falls } p \equiv \pm 1 \bmod 8 \\ -1 & \text{falls } p \equiv \pm 3 \bmod 8 \end{cases}$.

Gaußsumme

Definition Gaußsumme

Sei $p \in \mathbb{P} \setminus \{2\}$ und $\xi = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ eine p-te Einheitswurzel. Für $a \in \mathbb{Z}$ mit $a \not\equiv 0 \bmod p$ definieren wir die *Gaußsumme*

$$g_a = \sum_{j=1}^{p-1} (\tfrac{j}{p}) \xi^{aj} \in \mathbb{Z}[\xi].$$

Lemma Gaußsumme

Seien $p, q \in \mathbb{P} \setminus \{2\}$ verschieden und $a \in \mathbb{Z}$, $a \not\equiv 0 \bmod p$. Dann gilt

1. $g_a = (\frac{a}{p}) g_1 \in \mathbb{Z}[\xi]$
2. $g_1^2 = (\frac{-1}{p}) p \in \mathbb{Z}$
3. $g_1^q \equiv g_q \bmod q$ in $(\mathbb{Z}/q\mathbb{Z})[\xi]$ (mod q komponentenweise).

Gaußsumme

Beweis:

(1) Wegen $(\frac{a}{p}) = (\frac{a}{p})^{-1}$ zeigen wir $(\frac{a}{p})g_a = g_1$. Es gilt

$$(\tfrac{a}{p})g_a = \sum_{j=1}^{p}(\tfrac{a}{p})(\tfrac{j}{p})\xi^{aj} = \sum_{i=1}^{p-1}(\tfrac{aj}{p})\xi^{aj}.$$

- Für $a \not\equiv 0 \bmod p$ ist $U_p \to U_p, \bar{j} \mapsto \overline{aj}$ ein Isomorphismus.
- D.h. $\overline{aj}$ durchläuft für $j = 1, \ldots, p-1$ alle Elemente $\bar{1}, \ldots, \overline{p-1}$.
- Damit folgt $(\frac{a}{p})g_a = \sum_{j=1}^{p-1}(\frac{aj}{p})\xi^{aj} = \sum_{\ell=1}^{p-1}(\frac{\ell}{p})\xi^{\ell} = g_1$.

(2) Wir betrachten zunächst $\sum_{j=1}^{p-1}\xi^{\ell j}$. Für $\ell \not\equiv 0 \bmod p$ ist dies

$$(-1) + \sum_{j=0}^{p-1}(\xi^{\ell})^j = (-1) + \frac{(\xi^{\ell})^p - 1}{\xi^{\ell} - 1} = (-1) + \frac{(\xi^p)^{\ell} - 1}{\xi^{\ell} - 1} = (-1).$$

- Für $\ell \equiv 0 \bmod p$ gilt $\sum_{j=1}^{p-1}\xi^{\ell j} = \sum_{j=1}^{p-1} 1^j = p - 1$. Wir rechnen

$$g_1^2 = \left(\sum_{j=1}^{p-1}(\tfrac{j}{p})\xi^j\right)\left(\sum_{k=1}^{p-1}(\tfrac{k}{p})\xi^k\right) = \sum_{j=1}^{p-1}\sum_{k=1}^{p-1}(\tfrac{jk}{p})\xi^{j+k}.$$

Gaußsumme

Beweis: (Fortsetzung)

- Wir nutzen wieder den Isomorphismus $\bar{k} \mapsto \overline{jk}$ für $\bar{j} \in U_p$

$$\begin{aligned}\sum_{j=1}^{p-1}\sum_{k=1}^{p-1}\left(\frac{jk}{p}\right)\xi^{j+k} &= \sum_{k=1}^{p-1}\sum_{j=1}^{p-1}\left(\frac{j^2k}{p}\right)\xi^{j+jk} \\ &= \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\sum_{j=1}^{p-1}\xi^{j(1+k)}.\end{aligned}$$

- Unter Ausnutzen unserer Identitäten für $\sum_{j=1}^{p-1}\xi^{\ell j}$ formen wir um zu

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

- Genau die Hälfte aller $\bar{a} \in U_p$ sind quadratische Reste.
- Somit enthält die Summe je $(\frac{p-1}{2})$-mal die Summanden 1 und -1.
- Wir erhalten insgesamt $g_1^2 = \left(\frac{p-1}{p}\right)p - \sum_{k=1}^{p-1}\left(\frac{k}{p}\right) = \left(\frac{-1}{p}\right)p$.

(3) Mit unserer Binomischen Formel mod q (Frobenius) erhalten wir

$$\begin{aligned}g_1^q &= \left(\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\xi^j\right)^q \equiv \sum_{j=1}^{p-1}\left(\left(\frac{j}{p}\right)\xi^j\right)^q = \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)^q\xi^{jq} \\ &= \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\xi^{jq} = g_q \bmod q.\end{aligned}$$

Quadratisches Reziprozitätsgesetz (Gauß)

Satz Quadratisches Reziprozitätsgesetz (Gauß)

Seien $p, q \in \mathbb{P} \setminus \{2\}$ mit $p \neq q$. Dann gilt

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{für } p \equiv q \equiv 3 \bmod 4 \\ \left(\frac{p}{q}\right) & \text{sonst} \end{cases}.$$

Beweis:

- In $\mathbb{Z}[\xi]$ gilt nach dem vorigen Lemma
$$(\tfrac{q}{p})g_1 = g_q \equiv g_1^q = g_1(g_1^2)^{\frac{q-1}{2}} \equiv g_1 \left(\frac{g_1^2}{q}\right) \bmod q.$$
- Multiplikation mit g_1 liefert $(\frac{q}{p})g_1^2 \equiv g_1^2 \left(\frac{g_1^2}{q}\right) \bmod q$.
- Alle Terme sind nun in $\mathbb{Z}$. Wegen $p \neq q$ gilt $g_1^2 = (\frac{-1}{p})p \not\equiv 0 \bmod q$.
- Kürzen von g_1^2 liefert

$$\begin{aligned} \left(\frac{q}{p}\right) &\equiv (\tfrac{g_1^2}{q}) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \cdot (\tfrac{p}{q}) \equiv \left((-1)^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}} \cdot (\tfrac{p}{q}) \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot (\tfrac{p}{q}) \bmod q \end{aligned}$$

Quadratisches Reziprozitätsgesetz (Gauß)

Beweis: (Fortsetzung)

- Alle Terme sind ± 1, d.h. die Kongruenz ist eine Gleichheit.
- Der Exponent von (-1) ist ungerade gdw $\frac{p-1}{2}$ und $\frac{q-1}{2}$ ungerade.
- Es gilt $\frac{p-1}{2} \equiv 1 \bmod 2$ gdw $p \equiv 3 \bmod 4$. (analog für q)

Bsp:

- Frage: Besitzt die Gleichung $x^2 \equiv 19 \bmod 31$ Lösungen?
- Dazu berechnen wir

$$\left(\frac{19}{31}\right) = -\left(\frac{31}{19}\right) = -\left(\frac{12}{19}\right) = -\left(\frac{2}{19}\right)\left(\frac{2}{19}\right)\left(\frac{3}{19}\right) = \left(\frac{19}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

- Durch Ausprobieren erhalten wir die beiden Lösungen

$$(\pm 9)^2 = 81 \equiv 19 \bmod 31.$$

Problem:

Berechnung des Legendre-Symbols erfordert Faktorisierung in $\mathbb{Z}$.

Das Jacobi-Symbol

Definition Jacobi-Symbol

Sei $n \in \mathbb{N}$ ungerade mit Primfaktorzerlegung $n = \prod_{i=1}^{s} p_i^{r_i}$. Wir definieren das *Jacobi-Symbol* $\left(\frac{a}{n}\right) := \prod_{i=1}^{s} \left(\frac{a}{p_i}\right)^{r_i}$.

Anmerkungen:

- Falls a quadratischer Rest mod n ist, dann gilt $a \equiv b^2 \bmod n$ und
$$\left(\frac{a}{n}\right) = \left(\frac{b^2}{n}\right) = \prod_{i=1}^{s} \left(\frac{b^2}{p_i}\right)^{r_i} = \prod_{i=1}^{s} \left(\frac{b}{p_i}\right)^{2r_i} = 1.$$
- Falls $\left(\frac{a}{n}\right) = 1$, dann muss a kein quadratischer Rest mod n sein.
- Es gilt z.B. $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)^2 = 1$.
- Nach CRT müsste jede Lösung von $x^2 \equiv 2 \bmod 15$ auch eine Lösungen von $x^2 \equiv 2 \bmod 3$ und $x^2 \equiv 2 \bmod 5$ sein.
- Beide Kongruenzen besitzen aber keine Lösungen.

Übung:

$\left(\frac{a}{n}\right)$ ist multiplikativ in a und n. D.h. für $a = a_1 a_2$ und $n = n_1 n_2$ gilt
$$\left(\frac{a}{n}\right) = \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right) = \left(\frac{a_1}{n_1}\right)\left(\frac{a_2}{n_1}\right)\left(\frac{a_1}{n_2}\right)\left(\frac{a_2}{n_2}\right).$$

Reziprozität für Jacobi-Symbol

Satz Reziprozität

Seien $m \neq n \geq 3$ ungerade natürliche Zahlen. Dann gilt

1. $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$.
2. $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$.
3. $(\frac{m}{n}) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}(\frac{n}{m})$.

Beweis:

- Obige Identitäten gelten für prime n, m. Die linken Seiten sind multiplikativ in n, m, können also in die Primteiler zerlegt werden.
- Genügt zu zeigen: Die rechten Seiten sind multiplikativ in n, m.
- Sei $n = n_1 n_2$ ungerade, d.h. n_1, n_2 sind ebenfalls ungerade.

(1) Wir zeigen $(-1)^{\frac{n_1 n_2 - 1}{2}} = (-1)^{\frac{n_1-1}{2}} \cdot (-1)^{\frac{n_2-1}{2}}$. Dies ist äquivalent zu

$$\frac{n_1 n_2 - 1}{2} \equiv \frac{n_1 + n_2 - 2}{2} \bmod 2$$
$$\Leftrightarrow \quad n_1 n_2 - n_1 - n_2 + 1 = (n_1 - 1)(n_2 - 1) \equiv 0 \bmod 4$$

- Da $n_1 - 1$ und $n_2 - 1$ beide gerade sind, folgt die Korrektheit.

Reziprozität für Jacobi-Symbol

Beweis: (Fortsetzung)

(2) zu zeigen: $(-1)^{\frac{n_1^2 n_2^2 - 1}{8}} = (-1)^{\frac{n_1^2-1}{8}} (-1)^{\frac{n_2^2-1}{8}}$. Dies ist äquivalent zu

$$\frac{n_1^2 n_2^2 - 1}{8} \equiv \frac{n_1^2-1}{8} + \frac{n_2^2-1}{8} \bmod 2 \Leftrightarrow n_1^2 n_2^2 - n_1^2 - n_2^2 + 1 \equiv 0 \bmod 16.$$

- Wir formen weiter um zu

$$(n_1^2 - 1)(n_2^2 - 1) = (n_1 + 1)(n_1 - 1)(n_2 + 1)(n_2 - 1) \equiv 0 \bmod 16.$$

- Die Korrektheit folgt, da alle vier Terme $n_1 \pm 1$, $n_2 \pm 1$ gerade sind.

(3) Aus (1) folgt die Multiplikativität von

$$(-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} = \left((-1)^{\frac{m-1}{2}}\right)^{\frac{n-1}{2}} \text{ in } n \text{ und } m.$$

Anmerkung: Für ungerades n und $m = 2^k m'$ mit ungeradem m' gilt

$$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^k \cdot \left(\frac{m'}{n}\right) = \left(\frac{2}{n}\right)^k \cdot (-1)^{\frac{(m'-1)(n-1)}{4}} \left(\frac{n}{m'}\right).$$