Eigenschaften des Legendre-Symbols

(3) Aus (2) folgt $(-1) \equiv (-1)^{\frac{p-1}{2}} \bmod p$.
- Da beide Seiten in $\mathbb{Z}$ nur Werte aus ± 1 annehmen, gilt Gleichheit.
- Es gilt $(-1)^{\frac{p-1}{2}} = 1$ gdw $\frac{p-1}{2} \equiv 0 \bmod 2$ bzw $p \equiv 1 \bmod 4$.
- Es gilt $(-1)^{\frac{p-1}{2}} = (-1)$ gdw $\frac{p-1}{2} \equiv 1 \bmod 2$ bzw $p \equiv 3 \bmod 4$.

(4) Aus (2) folgt $(\frac{ab}{p}) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (\frac{a}{p})(\frac{b}{p}) \bmod p$.
- Die Identität über $\mathbb{Z}$ folgt wieder aus der ± 1-Wertigkeit.

(5) Aus (4) folgt $(\frac{ab^2}{p}) = (\frac{a}{p})(\frac{b}{p})^2 = (\frac{a}{p})$ für $b \not\equiv 0 \bmod p$.

Übung: $(\frac{a}{p})$ kann in Zeit $\mathcal{O}(\log^2(\max\{a, p\}) \cdot \log p)$ berechnet werden.

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 wir $p = 2k+1$ 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 $\mathrm{ord}(-i) = 4$. 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 $a \not\equiv 0 \mod p$ definieren wir die *Gaußsumme*

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

Lemma Gaußsumme

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

1. $g_a = \left(\frac{a}{p}\right) g_1 \in \mathbb{Z}[\xi]$
2. $g_1^2 = \left(\frac{-1}{p}\right) p \in \mathbb{Z}$
3. $g_1^q \equiv g_q \mod q$ in $\mathbb{Z}[\xi] = \bigoplus_{i=0}^{p-1} \mathbb{Z}\xi^i$ (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 $a \not\equiv 0 \mod p$ 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 $\ell \not\equiv 0 \mod p$ 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 $\ell \equiv 0 \mod p$ 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 $\bar{j} \in U_p$

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

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

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

- 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

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

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
$$\left(\frac{q}{p}\right)g_1 = g_q \equiv g_1^q = g_1(g_1^2)^{\frac{q-1}{2}} = g_1(g_1^2)^{\frac{q-1}{2}} \equiv g_1 \left(\frac{g_1^2}{q}\right) \bmod q.$$
- Multiplikation mit g_1 liefert $\left(\frac{q}{p}\right)g_1^2 \equiv g_1^2 \left(\frac{g_1^2}{q}\right) \bmod q$.
- Alle Terme sind nun in $\mathbb{Z}$. Wegen $p \neq q$ gilt $g_1^2 = \left(\frac{-1}{p}\right)p \not\equiv 0 \bmod q$.
- Kürzen von g_1^2 liefert
$$\begin{aligned}\left(\frac{q}{p}\right) &\equiv \left(\frac{g_1^2}{p}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right) \equiv \left((-1)^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right) \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot \left(\frac{p}{q}\right) \bmod q\end{aligned}$$

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 von Zahlen.