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

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

Rekursive Berechnung des Jacobi Symbols

Definition $a \bmod n$

Sei $a \in \mathbb{Z}$ und $n \in \mathbb{N}$. Dann bezeichnen wir mit $a \bmod n$ dasjenige $b \in \mathbb{Z}$ mit $b \equiv a \bmod n$ und $0 \leq b < n$. D.h. $b = a - \lfloor \frac{a}{n} \rfloor \cdot n$.

Algorithmus Jacobi-Symbol

EINGABE: m, n mit n ungerade und $\mathrm{ggT}(m, n) = 1$.

1. Falls $m = 1$, Ausgabe 1.
2. Sei $m = 2^k m'$ mit m' ungerade.
3. Ausgabe $(-1)^{\frac{k(n^2-1)}{8}} \cdot (-1)^{\frac{(m'-1)(n-1)}{4}} \cdot \text{Jacobi-Symbol}(n \bmod m', m')$

AUSGABE: $\left(\frac{m}{n}\right)$

Laufzeit:

- Analog zum Euklidischen Alg. erhalten wir $\mathcal{O}(\log \max\{m, n\})$ rekursive Aufrufe, jeder dieser benötigt $\mathcal{O}(\log^2 \max\{m, n\})$.
- D.h. die Gesamtlaufzeit ist $\mathcal{O}(\log^3 \max\{m, n\})$.

Berechnung von Wurzeln für $p \equiv 3 \bmod 4$

Bsp: Berechnung von $(\frac{22}{39})$

$$(\tfrac{22}{39}) = (\tfrac{2}{39}) \cdot (\tfrac{11}{39}) = -(\tfrac{39}{11}) = -(\tfrac{6}{11}) = -(\tfrac{2}{11}) \cdot (\tfrac{3}{11}) = -(\tfrac{11}{3}) = -(\tfrac{2}{3}) = 1.$$

Ziel: Falls $x^2 \equiv d \bmod p$ mit $(\frac{d}{p}) = 1$, berechne beide Lösungen.

Satz Wurzeln für $p \equiv 3 \bmod 4$

Sei $p \in \mathbb{P}$ mit $p \equiv 3 \bmod 4$ und $d \in \mathbb{Z}$ mit $(\frac{d}{p}) = 1$. Dann sind die Lösungen von $x^2 \equiv d \bmod p$ von der Form $\pm d^{\frac{p+1}{4}}$.

Beweis:

- Es gilt $(\pm d^{\frac{p+1}{4}})^2 = d^{\frac{p+1}{2}} = d^{\frac{p-1}{2}} \cdot d \equiv (\frac{d}{p}) \cdot d = d \bmod p$.
- Es gilt $d^{\frac{p+1}{4}} \not\equiv -d^{\frac{p+1}{4}} \bmod p$, da $\overline{d^{\frac{p+1}{4}}} \in U_p$ und $p > 2$.
- Da $\mathbb{F}_p$ ein Körper ist, sind dies die einzigen beiden Lösungen.

Berechnen allgemeiner Quadratwurzel

Idee des Algorithmus von Tonelli und Shanks:

- Sei $p - 1 = 2^s \cdot q$ mit q ungerade.
- Erster Ansatz: Berechne $a \equiv d^{\frac{q+1}{2}} \bmod p$. Dann gilt
$$a^2 \equiv (d^{\frac{q+1}{2}})^2 = d^q \cdot d \bmod p.$$
- Falls $d^q \equiv 1 \bmod p$, dann ist a bereits die gesuchte Quadratwurzel.
- Es gilt $U_p \cong \mathbb{Z}/\varphi(p)\mathbb{Z} \cong \mathbb{Z}/2^s\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Wir schreiben $x \cong (x_1, x_2)$.
- Für die Abbildung $f : U_p \to U_p, x \mapsto x^q$ gilt
$$f(x) = x^q \cong q(x_1, x_2) = (qx_1, qx_2) = (qx_1, 0) \in \mathbb{Z}/2^s\mathbb{Z} \times 0.$$
- D.h. q-ten Potenzen sind in einer Untergruppe H der Ordnung 2^s.
- Wir wollen nun einen Erzeuger g von H konstruieren.
- Sei $z \in U_p$ mit $(\frac{z}{p}) = (-1)$. Dann gilt $g :\equiv z^q \bmod p \in H$ und
$$g^{2^{s-1}} \equiv z^{q2^{s-1}} = z^{\frac{p-1}{2}} \equiv (-1) \bmod p \text{ und } g^{2^s} \equiv z^{p-1} \equiv 1 \bmod p.$$
- D.h. g ist Generator von H und $d^q \equiv g^\ell \bmod q$ für ein $0 \leq \ell < 2^s$.
- ℓ ist gerade, da $g^\ell \equiv d^q \equiv \frac{a^2}{d} \bmod p$ quadratischer Rest ist. Es folgt
$$(a \cdot g^{-\frac{\ell}{2}})^2 \equiv d \bmod p.$$
- Damit ist $a \cdot g^{-\frac{\ell}{2}}$ unsere gesuchte Quadratwurzel.

Berechnen des Diskreten Logarithmus modulo 2^s

Lemma Berechnen des Diskreten Logarithmus modulo 2^s

Sei p prim mit $p-1=2^s q$, q ungerade. Sei $H=\langle g\rangle \subseteq U_p$ mit $\mathrm{ord}(g)=2^s$. Für $x=g^\ell \in H$ kann ℓ in $\mathcal{O}(\log^4 p)$ berechnet werden.

Beweis:

- Wir schreiben $\ell=\sum_{i=0}^{s-1}\ell_i\cdot 2^i$ und berechnen $\ell_0,\ldots,\ell_{s-1}$.
- Berechnung von ℓ_0: Wir berechnen $x^{2^{s-1}} \bmod q$. Es gilt
$$x^{2^{s-1}} \equiv g^{\ell\cdot 2^{s-1}} = g^{\sum_{i=0}^{s-1}\ell_i\cdot 2^{s-1+i}} \equiv g^{\ell_0 2^{s-1}} \bmod p.$$
- Da $x^{2^s}\equiv 1 \bmod p$, muss $x^{2^{s-1}}\equiv \pm 1 \bmod p$ gelten.
- Falls $x^{2^{s-1}}\equiv (-1) \bmod p$, dann ist $\ell_0=1$, sonst ist $\ell_0=0$.
- Sei nun $\ell_0,\ldots,\ell_{j-1}$ bekannt. Wir wollen ℓ_j berechnen.
- Berechnung von ℓ_j: Es $g^{\sum_{i=j}^{s-1}\ell_i 2^i} \equiv x g^{-\sum_{i=0}^{j-1}\ell_i 2^i} := x'$. Damit ist
$$(x')^{2^{s-1-j}} \equiv g^{\sum_{i=j}^{s-1}\ell_i\cdot 2^{s-1-j+i}} \equiv g^{\ell_j 2^{s-1}} \bmod p.$$
- Damit gilt analog wie zuvor $\ell_j=1$ gdw $(x')^{2^{s-1-j}}\equiv(-1) \bmod p$.
- Jedes ℓ_j kann in Zeit $\mathcal{O}(\log^3 p)$ berechnet werden.