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: Setze $g^{\sum_{i=j}^{s-1}\ell_i 2^i}\equiv x g^{-\sum_{i=0}^{j-1}\ell_i 2^i} := x'$. 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.

Algorithmus von Tonelli und Shanks

Algorithmus Berechnen von Quadratwurzeln mod p

EINGABE: $p \in \mathbb{P}$, d mit $(\frac{d}{p}) = 1$

1. Sei $p - 1 = 2^s q$ mit q ungerade.
2. Setze $x \equiv d^q \bmod p$ und $\ell = 0$.
3. Wähle $z \bmod p$ zufällig bis $(\frac{z}{p}) = (-1)$. Setze $g :\equiv z^q \bmod p$.
4. For $j = 1$ to $s - 1$
   1. If $((x \cdot g^{-\ell})^{2^{s-1-j}} \equiv (-1) \bmod p)$ then $\ell := \ell + 2^j$.
5. Berechne $a \equiv d^{\frac{q+1}{2}} g^{-\frac{\ell}{2}} \bmod p$.

AUSGABE: a mit $a^2 \equiv d \bmod p$

- **Korrektheit:** Folgt aus den beiden Folien zuvor.
- **Laufzeit:** Erwartete Laufzeit $\mathcal{O}(\log^4 p)$.

Übung: Modifizieren Sie den Algorithmus zum Berechnen 3. Wurzeln.

Algorithmus von Tonelli und Shanks

Bsp: Wir berechnen die Lösungen von $y^2 \equiv 2 \bmod 41$.

- Es gilt $41 - 1 = 2^3 \cdot 5$.
- Wir setzen $x \equiv 2^5 = 32 \equiv -9 \bmod 41$.
- Es gilt $(\frac{3}{41}) = (\frac{41}{3}) = (\frac{2}{3}) = (-1)$.
- Wir setzen $g = 3^5 = 81 \cdot 3 \equiv (-3) \bmod 41$.
- Damit gilt $g^{-1} \equiv (-14) \bmod 41$.
- Für $j = 1$ ist $x^2 = (-9)^2 = 81 \equiv (-1) \bmod 41$, d.h. $\ell_1 = 1$.
- Für $j = 2$ ist $x \cdot g^{-\ell} = (-9) \cdot (-14)^2 \equiv (-1) \bmod 41$, d.h. $\ell_2 = 1$.
- Damit gilt $\ell = 6$ und $a \equiv 2^3(-14)^3 \equiv 24 \bmod 41$.
- Wir testen $(\pm 24)^2 \equiv 2 \bmod 41$.

Kettenbrüche

Definition Kettenbruch

Ein *endlicher Kettenbruch* ist eine Sequenz $[a_0, \ldots, a_n]$ mit $a_i \in \mathbb{R}$ und

$$\text{Wert } [a_0] := a_0 \text{ und } [a_0, \ldots, a_n] := [a_0, \ldots, a_{n-1} + \tfrac{1}{a_n}] \text{ für } n \in \mathbb{N}.$$

Der Wert ist eines *unendlichen Kettenbruchs* $[a_0, a_1, \ldots]$ ist definiert als $\lim_{n\to\infty}[a_0, \ldots, a_n]$.

Anmerkung: Aus der Definition folgt

$$[a_0, \ldots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots + \frac{1}{a_n}}}.$$

Ziel: Konstruiere $[a_0, a_1, \ldots]$ mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ für $i \geq 1$.

Bsp:

- $\frac{43}{30} = 1 + \frac{13}{30} = 1 + \frac{1}{\frac{30}{13}} = 1 + \frac{1}{2 + \frac{4}{13}} = 1 + \frac{1}{2 + \frac{1}{\frac{13}{4}}} = 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4}}} = [1, 2, 3, 4]$.
- Sei $\Phi = [1, 1, \ldots]$. Für den Grenzwert muss gelten $\Phi = 1 + \frac{1}{\Phi}$.
- Positive Lösung von $\Phi^2 - \Phi - 1 = 0$ ist der goldene Schnitt $\frac{1+\sqrt{5}}{2}$.