Baby-Step Giant-Step Algorithmus

Algorithmus Baby-Step Giant-Step

EINGABE: n, a

1. Setze $A := \lceil \sqrt{n} \rceil$.
2. Erstelle Liste L mit Einträgen $(x_1, (g^A)^{x_1} \bmod n)$ für $0 \leq x_1 < A$.
3. Sortiere L nach der zweiten Komponente.
4. Für alle $x \in \{0, \ldots, A-1\}$
   1. Falls $ag^{-x0} \bmod n$ in einer der zweiten Komponenten $(x_1, (g^A)^{x_1} \bmod n)$ von L auftaucht, EXIT.

AUSGABE: $x = x_1 A + x_0 \equiv \log_g a \bmod \varphi(n)$

Laufzeit:

- Wir vernachlässigen hier die Berechnung der Gruppenoperation.
- Schritt 2: $\mathcal{O}(A)$, Schritt 3: $\mathcal{O}(A \log A)$, Schritt 4: $\mathcal{O}(A \log A)$.
- Damit ist die Gesamtlaufzeit $\mathcal{O}(A \log A) = \mathcal{O}(\sqrt{n} \log n)$.

Bsp. Diskreter Logarithmus mit Baby-Step Giant Step

Bsp:

- Wir berechnen $\log_2 \bar{5}$ in U_{13}.
- Setze $A := \lceil \sqrt{13} \rceil = 4$. Wir erhalten

i	$(2^4)^i \bmod 13$	$5(2^{-1})^i \bmod 13$
0	1	5
1	3	**9**
2	**9**	12
3	1	6

- Wir erhalten für $(x_1, x_0) = (2, 1)$ das gleiche Element 9.
- Damit folgt $x = x_1 A + x_0 = 2 \cdot 4 + 1 = 9$.
- Wir testen, dass $2^9 = (2^3)^3 \equiv (-1) \cdot 8 \equiv 5 \bmod 13$.

Die Wurzeln der (-1)

Lemma Wurzeln der (-1)

Für $p \in \mathbb{P} \setminus \{2\}$ ist $x^2 \equiv (-1) \bmod p$ ist lösbar gdw $p \equiv 1 \bmod 4$.

Beweis:

- Sei g ein Generator von U_p. Dann gilt
$$g^{\frac{p-1}{2}} \not\equiv 1 \bmod p \text{ und } g^{p-1} \equiv 1 \bmod p.$$
- D.h. $g^{\frac{p-1}{2}}$ ist Nullstelle von $X^2 - 1$ in $\mathbb{F}_p$.
- Wegen $g^{\frac{p-1}{2}} \not\equiv 1 \bmod p$, muss $g^{\frac{p-1}{2}} \equiv (-1) \bmod p$ gelten. D.h.
$$\log_g(-1) \equiv \frac{p-1}{2} \bmod p - 1.$$
- Die Kongruenz $x^2 \equiv (-1) \bmod p$ ist äquivalent zu
$$2 \log_g x \equiv \log_g(-1) \equiv \frac{p-1}{2} \bmod p - 1.$$
- Die lineare Kongruenz ist lösbar gdw $\mathrm{ggT}(2, p-1) | \frac{p-1}{2}$.
- Wegen $\mathrm{ggT}(p-1, 2) = 2$ bedeutet dies $2 | \frac{p-1}{2}$ bzw. $p \equiv 1 \bmod 4$.

Lösen allgemeiner quadratischer Gleichungen

Ziel: Effiziente Berechnung der Lösungen von

$$X^2 \equiv d \bmod p \text{ für } p \in \mathbb{P}, d \in \mathbb{Z}.$$

Beobachtung: Sei $p \in \mathbb{P} \setminus \{2\}$.

- Das Lösen von $ay^2 + by + c \equiv 0 \bmod p$ kann für $a \not\equiv 0 \bmod p$ auf das Lösen von $x^2 \equiv d \bmod p$ zurückgeführt werden.
- Wir multiplizieren obiges Polynom mit dem Inversen von a in U_p:

$$y^2 + \frac{b}{a}y + \frac{c}{a} \equiv 0 \bmod p \Leftrightarrow \left(y + \frac{b}{2a}\right) \equiv \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \bmod p.$$

- Sei $d = \left(\frac{b}{2a}\right)^2 - \frac{c}{a}$ die Diskriminante. Wir lösen $x^2 \equiv d \bmod p$.
- Falls x eine Lösung ist, dann ist auch $-x$ eine Lösung.
- Beide Lösungen sind für $p \geq 3$, $x \not\equiv 0 \bmod p$ verschieden, denn

$$x \equiv -x \bmod p \Leftrightarrow 2x \equiv 0 \bmod p \Leftrightarrow x \equiv 0 \bmod p.$$

- Für unsere Ausgangskongruenz erhalten wir folgende Lösungen

$$\begin{cases} -\frac{b}{2a} \bmod p & \text{falls } d \equiv 0 \bmod p. \\ -\frac{b}{2a} \pm x_{1,2} \bmod p & \text{falls } x_{1,2} \text{ Lösungen von } x^2 \equiv d \bmod p \text{ sind.} \\ \text{keine Lösung} & \text{sonst.} \end{cases}$$

Quadratische Reste und das Legendre-Symbol

Definition Quadratischer Rest

Sei $p \in \mathbb{P}$. Ein $a \in \mathbb{Z}$ mit $a \not\equiv 0 \bmod p$ heißt *quadratischer Rest modulo* p, falls ein $b \in \mathbb{Z}$ existiert mit $b^2 \equiv a \bmod p$.
Sonst heißt a *quadratischer Nicht-Rest*.

Definition Legendre-Symbol

Für $p \in \mathbb{P}$, $a \in \mathbb{Z}$ definieren wir das *Legrendre-Symbol* als

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{falls } a \text{ quadratischer Rest modulo } p. \\ -1 & \text{falls } a \text{ quadratischer Nicht-Rest modulo } p. \\ 0 & \text{falls } a \equiv 0 \bmod p. \end{cases}$$

Bsp:

- In U_7 gilt $\bar{1}^2 = \bar{6}^2 = \bar{1}$, $\bar{2}^2 = \bar{5}^2 = \bar{4}$ und $\bar{3}^2 = \bar{4}^2 = \bar{2}$. Damit ist
$$\left(\tfrac{1}{7}\right) = \left(\tfrac{2}{7}\right) = \left(\tfrac{4}{7}\right) = 1, \left(\tfrac{3}{7}\right) = \left(\tfrac{5}{7}\right) = \left(\tfrac{6}{7}\right) = (-1) \text{ und } \left(\tfrac{0}{7}\right) = 0.$$

Struktur der quadratischen Reste

Lemma Struktur der quadratischen Reste

Sei $p \in \mathbb{P} \setminus \{2\}$ und g ein Generator von U_p. Ein $g^i \bmod p$, $i = 0, \ldots, p-2$, ist quadratischer Rest gdw i gerade ist.

Beweis:

$\Leftarrow$: Sei $i = 2k$, $k \in \mathbb{N}$, dann ist $(g^k)^2 \equiv g^i \bmod p$.

$\Rightarrow$: Sei $g^i \bmod p$ ein quadratischer Rest.

- Dann existiert ein $b \in \mathbb{Z}$ mit $b^2 \equiv g^i \bmod p$.
- Da g Generator von U_p, existiert ein $k \in \mathbb{N}$ mit $g^k \equiv b \bmod p$.
- Es folgt $2k = i \bmod p - 1$ bzw.
$$i = 2k + c(p-1) = 2(k + c \cdot \tfrac{p-1}{2}) \text{ für ein } c \in \mathbb{Z}.$$
- Damit ist i gerade.

Korollar

Für genau die Hälfte aller $\bar{a} \in U_p$ gilt $(\frac{a}{p}) = 1$.

- Genau die $\frac{p-1}{2}$ Elemente $a \in \{g^2, g^4, \ldots, g^{p-1}\}$ liefern $\left(\frac{a}{p}\right) = 1$.

Eigenschaften des Legendre-Symbols

Satz Eigenschaften des Legendre-Symbols

Sei $p \in \mathbb{P} \setminus \{2\}$ und $a, b \in \mathbb{Z}$. Es gilt

1. $a \equiv b \bmod p \Rightarrow (\frac{a}{p}) = (\frac{b}{p})$ (auch für $p = 2$).
2. Euler-Identität: $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \bmod p$.
3. $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{falls } p \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv 3 \bmod 4 \end{cases}$.
4. Multiplikativität: $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.
5. $(\frac{ab^2}{p}) = (\frac{a}{b})$ für $b \not\equiv 0 \bmod p$.

Eigenschaften des Legendre-Symbols

Beweis:

(1) Für $a \equiv b \equiv 0 \bmod p$ ist die Aussage klar. Ansonsten gilt

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow \exists c \in \mathbb{Z} \text{ mit } c^2 \equiv a \equiv b \bmod n \Leftrightarrow \left(\frac{b}{p}\right) = 1.$$

- D.h. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, da das Legendre-Symbol nur Werte ± 1 annimmt.

(2) Für $a \equiv 0 \bmod p$ sind beide Seiten 0. Sei also $a \not\equiv 0$.

- Wir schreiben $a \equiv g^i \bmod p$ für einen Generator g von U_p.
- Lemma Folie 120: Für die linke Seite gilt $\left(\frac{g^i}{p}\right) = 1 \Leftrightarrow i \equiv 0 \bmod 2$.
- Behauptung: $a^{\frac{p-1}{2}} \equiv g^{i\frac{p-1}{2}} \equiv 1 \bmod 2 \Leftrightarrow i \equiv 0 \bmod 2$.
- Aus dieser Behauptung folgt die Euler-Identität.
- $\Leftarrow$: Für gerades $i = 2k$ gilt $g^{i\frac{p-1}{2}} \equiv g^{k(p-1)} \equiv 1 \bmod p$.
- $\Rightarrow$: Sei $g^{i\frac{p-1}{2}} \equiv 1 \bmod p$. Dann gilt

  $p - 1 \mid i\frac{p-1}{2}$ bzw. $i\frac{p-1}{2} \equiv 0 \bmod p - 1$ und damit $i \equiv 0 \bmod 2$.