

# Baby-Step Giant-Step Algorithmus

**Ziel:** Berechnen von  $\log_g a$  in  $U_n$  in Zeit und Platz  $\mathcal{O}(\sqrt{n} \log n)$ .

**Idee:** Baby-Step Giant-Step Algorithmus

- Sei  $x \equiv \log_g a \pmod{\varphi(n)}$  mit  $0 \leq x < \varphi(n)$ , d.h.  $g^x \equiv a \pmod{n}$ .
- Setze  $A := \lceil \sqrt{\varphi(n)} \rceil$ .
- Schreibe  $x = x_1 A + x_0$  mit  $x_0, x_1 < A \leq \lceil \sqrt{\varphi(n)} \rceil$ .
- Es gilt die Identität  $(g^A)^{x_1} \equiv a \cdot g^{-x_0} \pmod{n}$ .
- Erstelle zwei Listen mit Kandidaten für  $(g^A)^{x_1}$  bzw.  $a \cdot g^{-x_0}$ .
- Zwei gleiche Listenelemente liefern  $(x_0, x_1)$  und damit  $x$ .

# Baby-Step Giant-Step Algorithmus

## Algorithmus Baby-Step Giant-Step

EINGABE:  $n, a$

- 1 Setze  $A := \lceil \sqrt{\varphi(n)} \rceil$ .
- 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  $x \in \{0, \dots, A-1\}$ 
  - 1 Falls  $ag^{-x_0} \bmod n$  in einer der zweiten Komponenten von  $(x_1, (g^A)^{x_1} \bmod n)$  in  $L$  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  $A := \lceil \sqrt{12} \rceil = 4$ . Wir erhalten

$i$	$(2^4)^i \bmod 13$	$5(2^{-1})^i \bmod 13$
0	1	5
1	3	<b>9</b>
2	<b>9</b>	11
3	1	12

- 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  $x^2 \equiv (-1) \pmod{p}$  lösbar gdw  $p \equiv 1 \pmod{4}$ .

### Beweis:

- Sei  $g$  ein Generator von  $U_p$ . Dann gilt

$$g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p} \text{ und } g^{p-1} \equiv 1 \pmod{p}.$$

- D.h.  $g^{\frac{p-1}{2}}$  ist Nullstelle von  $X^2 - 1$  in  $\mathbb{F}_p$ .
- Wegen  $g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ , muss  $g^{\frac{p-1}{2}} \equiv (-1) \pmod{p}$  gelten. D.h.

$$\log_g(-1) \equiv \frac{p-1}{2} \pmod{p-1}.$$

- Die Kongruenz  $x^2 \equiv (-1) \pmod{p}$  ist äquivalent zu

$$2 \log_g x \equiv \log_g(-1) \equiv \frac{p-1}{2} \pmod{p-1}.$$

- Die lineare Kongruenz ist lösbar gdw  $\text{ggT}(2, p-1) \mid \frac{p-1}{2}$ .
- Wegen  $\text{ggT}(p-1, 2) = 2$  bedeutet dies  $2 \mid \frac{p-1}{2}$  bzw.  $p \equiv 1 \pmod{4}$ .

# Lösen allgemeiner quadratischer Gleichungen

**Ziel:** Effiziente Berechnung der Lösungen von

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

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

- Das Lösen von  $ay^2 + by + c \equiv 0 \pmod{p}$  kann für  $a \not\equiv 0 \pmod{p}$  auf das Lösen von  $x^2 \equiv d \pmod{p}$  zurückgeführt werden.

- Wir multiplizieren obiges Polynom mit dem Inversen von  $a$  in  $U_p$ :

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

- Sei  $d = \left(\frac{b}{2a}\right)^2 - \frac{c}{a}$  die Diskriminante. Wir lösen  $x^2 \equiv d \pmod{p}$ .

- Falls  $x$  eine Lösung ist, dann ist auch  $-x$  eine Lösung.

- Beide Lösungen sind für  $p \geq 3$ ,  $x \not\equiv 0 \pmod{p}$  verschieden, denn

$$x \equiv -x \pmod{p} \Leftrightarrow 2x \equiv 0 \pmod{p} \Leftrightarrow x \equiv 0 \pmod{p}.$$

- Für unsere Ausgangskongruenz erhalten wir folgende Lösungen

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

# Quadratische Reste und das Legendre-Symbol

## Definition Quadratischer Rest

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

Sonst heißt  $a$  *quadratischer Nicht-Rest*.

## Definition Legendre-Symbol

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

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

## 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  $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$ ,  $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$  und  $\left(\frac{0}{7}\right) = 0$ .

# Struktur der quadratischen Reste

## Lemma Struktur der quadratischen Reste

Sei  $p \in \mathbb{P} \setminus \{2\}$  und  $g$  ein Generator von  $U_p$ . Ein  $g^i \bmod p$ ,  $i = 0, \dots, p-2$ , 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  $2k \equiv i \bmod p-1$  bzw.

$$i = 2k + c(p-1) = 2(k + c \cdot \frac{p-1}{2}) \text{ f\"ur ein } c \in \mathbb{Z}.$$

- Damit ist  $i$  gerade.

## Korollar

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

- Genau die  $\frac{p-1}{2}$  Elemente  $a \in \{g^0, g^2, \dots, g^{p-3}\}$  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  $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$  (auch für  $p = 2$ ).

② Euler-Identität:  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ .

③  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{falls } p \equiv 1 \pmod{4} \\ -1 & \text{falls } p \equiv 3 \pmod{4} \end{cases}$ .

④ Multiplikativität:  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ .

⑤  $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$  für  $b \not\equiv 0 \pmod{p}$ .



# Eigenschaften des Legendre-Symbols

## Beweis:

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

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

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

(2) Für  $a \not\equiv 0 \pmod{p}$  sind beide Seiten  $\neq 0$ . Sei also  $a \not\equiv 0$ .

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

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

# Eigenschaften des Legendre-Symbols

- (3) Aus (2) folgt  $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ .
- Da beide Seiten in  $\mathbb{Z}$  nur Werte aus  $\pm 1$  annehmen, gilt Gleichheit.
  - Es gilt  $(-1)^{\frac{p-1}{2}} = 1$  gdw  $\frac{p-1}{2} \equiv 0 \pmod{2}$  bzw  $p \equiv 1 \pmod{4}$ .
  - Es gilt  $(-1)^{\frac{p-1}{2}} = (-1)$  gdw  $\frac{p-1}{2} \equiv 1 \pmod{2}$  bzw  $p \equiv 3 \pmod{4}$ .
- (4) Aus (2) folgt  $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$ .
- Die Identität über  $\mathbb{Z}$  folgt wieder aus der  $\pm 1$ -Wertigkeit.
- (5) Aus (4) folgt  $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)^2 = \left(\frac{a}{p}\right)$  für  $b \not\equiv 0 \pmod{p}$ .

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