Strategie 4: Pollard ρ-Methode

Ziel: Lösung bestimmen der Gleichung $g^x = a$
(in einer Gruppe G mit Erzeugendem g).

Grund-Idee

- Ermitteln von s und t mit der Eigenschaft $a^s = g^t$.
  (Einsetzen in die Ursprungs-Gleichung liefert $g^{sx} = g^t$.)
- Lösen der Gleichung $sx = t \pmod{|G|}$

Vorüberlegung: Modulare Äquivalenzen

Beobachtung

Falls $u = v \pmod{n}$ und d ein Teiler von v und n ist, dann gilt

- $d \mid u$, und
- $\frac{u}{d} = \frac{v}{d} \left(\mod \frac{n}{d}\right)$

Begründung:

- $u = v \pmod{n}$ bedeutet, dass u die Form $u = v + k \cdot n$ hat (für eine ganze Zahl k).
- Division durch k ergibt $\frac{u}{d} = \frac{v}{d} + k \cdot \frac{n}{d}$.

Vorüberlegung: Modulare Lineare Gleichungen

Betrachtete Gleichung: $ax = b \pmod{n}$
Notation: $d := \mathrm{ggT}(a, n)$.

- Fall 1: $d = 1$. Dann ist $x = a^{-1} \cdot b \pmod{n}$ [einzige Lösung]
- Fall 2: $d > 1$. Gemäss vorheriger Beobachtung:
  - Falls $d \nmid b$: Die Gleichung hat keine Lösung.
  - Falls $d \mid b$: $\frac{a}{d}x = \frac{b}{d} \left(\mathrm{mod}\ \frac{n}{d}\right)$.
    - Da $\frac{a}{d}$ und $\frac{n}{d}$ teilerfremd sind, entspricht diese Gleichung Fall 1.
    - Mit $z := \left(\frac{a}{d}\right)^{-1} \left(\mathrm{mod}\ \frac{n}{d}\right)$ ist die Lösung somit $x = z \cdot \frac{b}{d} \left(\mathrm{mod}\ \frac{n}{d}\right)$.
    - Alle Lösungen der ursprünglichen Gleichung: $z \cdot \frac{b}{d} + k \cdot \frac{n}{d} \pmod{n}$ $(*)$ mit $k \in \{0, 1, 2, \ldots, d-1\}$.

Vorüberlegung: Modulare Lineare Gleichungen

Aufgabe: Löse die Gleichung $119x = 203 \pmod{273}$

Pollard ρ-Methode, Schritt 1

Ziel: Lösung für die Gleichung $g^x = a$ finden (in einer Gruppe G)

Schritt 1

1. Zerlege G in drei ungefähr gleich grosse Teilmengen G_1, G_2, G_3.
2. Bilde eine Folge $x_0, x_1, x_2, \ldots$ via $x_0 = 1$ und

$$x_{i+1} = \begin{cases} ax_i, & \text{falls } x_i \in G_1 \\ x_i^2, & \text{falls } x_i \in G_2 \\ gx_i, & \text{falls } x_i \in G_3 \end{cases}$$

Beobachtung: Für jedes Element x_i dieser Folge gibt es Zahlen r, s, so dass $x_i = a^r \cdot g^s$.

Pollard ρ-Methode, Schritt 1

Beobachtung

Hat x_i die Form $x_i = a^r g^s$, so ist $x_{i+1} = a^{\tilde{r}} g^{\tilde{s}}$ mit

$$\tilde{r} = \begin{cases} \tilde{r} = r + 1, & \tilde{s} = s & \text{falls } x_i \in G_1 \\ \tilde{r} = 2r, & \tilde{s} = 2s, & \text{falls } x_i \in G_2 \\ \tilde{r} = r, & \tilde{s} = s + 1, & \text{falls } x_i \in G_3 \end{cases}$$

Speichert man in jedem Schritt x_i und die zugehörigen Exponenten r_i und s_i, so kann man x_{i+1}, r_{i+1} und s_{i+1} jeweils effizient berechnen!

Pollard ρ-Methode, Schritt 1

Analyse der Folge $x_0, x_1, x_2, \ldots$ von vorhin.

Hinweis

- Die Folge $x_0, x_1, x_2, \ldots$ ist so konstruiert, dass sie sich ähnlich wie eine Folge von zufälligen Elementen verhält.
- Analog zum Pollard-ρ-Algorithmus für die Faktorisierung lässt sich zeigen, dass bei $k \geq 1.2\sqrt{|G|}$ Elementen mit Wahrscheinlichkeit > 0.5 ein Paar mit $x_i = x_j$ dabei ist.

Pollard ρ-Methode, Schritt 2

- Schritt 1 liefert ein Paar $x_i = x_j$.
- Es gibt Zahlen $r, s, \tilde{r}, \tilde{s}$, so dass $x_i = a^r g^s$ und $x_j = a^{\tilde{r}} g^{\tilde{s}}$.
- Gleichsetzen ergibt $a^r g^s = a^{\tilde{r}} g^{\tilde{s}}$ resp. $a^{r-\tilde{r}} = g^{\tilde{s}-s}$.
- Also: $a^t = g^u$ mit $t := r - \tilde{r}$ und $u := \tilde{s} - s$.
- Einsetzen von $g^x = a$ in die obige Gleichung liefert $g^{tx} = g^u$.
- Dies ist äquivalent zur Gleichung $tx = u \pmod{(|G|)}$.
  Diese Gleichung kann via $(*)$ von Folie 3 bestimmt werden.
  (Auswählen derjeniger Lösung, die $g^x = a$ erfüllt.)

  Hinweis: Da g ein erzeugendes Element ist, hat die obige Gleichung auf alle Fälle eine Lösung.

Pollard ρ-Methode, Schritt 2

Aufgabe: Wir setzen $p = 29$, $g = 2$ und $a = 5$. Ausserdem zerlegen wir die Gruppe $\mathbb{Z}_p^*$ in $G_1 = \{1, 2, \ldots, 10\}$, $G_2 = \{11, 12, \ldots, 19\}$ und $G_3 = \{20, 21, \ldots, 28\}$. Bestimme den Logarithmus von a bezüglich g in $\mathbb{Z}_p^*$ mit Hilfe der obigen Pollard ρ - Methode.

Effizienz-Aspekte

- Analog zum Pollard ρ-Algorithmus für die Faktorisierung lässt sich zeigen, dass eine Kollision der Form $x_i = x_{2i}$ in ungefähr gleich vielen Schritten wie *irgendeine* Kollision $x_i = x_j$ gefunden wird.
- Somit reicht es, die Tripel (x_i, r_i, s_i) jeweils nur solange zu speichern, bis der Index i die nächst-höhere Zweier-Potenz erreicht hat.
- Damit ist der Pollard ρ-Algorithmus deutlich Speicher-effizienter als der Babystep-Giantstep Algorithmus.