Strategie 3: Index Calculus

Inhalt: grobe Skizze vom Index-Calculus–Algorithmus

Recap: Grundidee des quadratischen Siebs

- **Vorgehen** (Skizze)

1. Bestimme eine Menge F von **kleinen** Primzahlen
2. Finde Werte b_i, so dass $b_i^2 \pmod n$ nur aus Primfaktoren aus F besteht
   $M :=$ Menge dieser b_i
3. Finde $b_1, \ldots, b_r \in M$,

   gerade Zahlen $\alpha_0, \alpha_1, \ldots, \alpha_r \in \mathbb{Z}$, und

   Primfaktoren $p_1, \ldots, p_k \in F$ so dass

   $$b_1^2 \cdot b_2^2 \cdots b_r^2 = (-1)^{\alpha_0} \cdot (p_1)^{\alpha_1} \cdots (p_k)^{\alpha_k}$$

   setze $x := b_1 \cdots b_r$, $y := (-1)^{\alpha_0/2} \cdot (p_1)^{\alpha_1/2} \cdots (p_k)^{\alpha_k/2}$

Grundidee vom Index-Calculus

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

- **Vorgehen** (Skizze)

1. Bestimme eine Menge F von **kleinen** Primzahlen
2. $M :=$ Menge von gewissen b_i, deren Primfaktoren alle in F liegen.
3. Für jedes $b_i \in M$: Bestimme jeweiligen Logarithmus $x_i := \log_g(b_i)$

   Dies ergibt:

$$\begin{array}{cccccc} b_1, & b_2, & \ldots, & b_s \\ \| & \| & & \| \\ g^{x_1} & g^{x_2} & & g^{x_s} \end{array}$$

4. Finde y, so dass ag^y sich als Produkt aus M darstellen lässt:

$$\begin{aligned} ag^y &= b_1^{e_1} \cdot b_2^{e_2} \cdot \ldots \cdot b_s^{e_s} \\ &= (g^{x_1})^{e_1} \cdot (g^{x_2})^{e_2} \cdot \ldots \cdot (g^{x_s})^{e_s} \\ &= g^{x_1 e_1 + x_2 e_2 + \ldots + x_s e_s} \end{aligned}$$

5. Aus vorherigem Schritt folgt:
   - $a = g^{x_1 e_1 + x_2 e_2 + \ldots + x_s e_s - y}$
   - $x = x_1 e_1 + x_2 e_2 + \ldots + x_s e_s - y$

Grundidee vom Index-Calculus

Bem: Algorithmische Umsetzungen der Schritte auf der letzten Folie:

- sind nicht simpel!
- erfordern Einsatz von komplexen Techniken, z.B.
  - spezielle modulare Gleichungs-Systeme
  - ausgewählte Anwendungen des chinesischen Restsatzes
  - gewisse, besonders effiziente Logarithmus-Berechnungen für spezifische Konstellationen

Zusatz-Bemerkungen

Eigenschaften vom Index-Calculus-Algorithmus

- Der Algorithmus benötigt u.a. eine eindeutige Primfaktorzerlegung (formal ausgedrückt: eine bestimmte Ring-Struktur).
- Der Algorithmus funktioniert in der multiplikativen Gruppe von $\mathbb{Z}_n^*$.

Bem: Für Gruppen, die nicht die Form $\mathbb{Z}_n^*$ haben, gibt es meist keine effiziente Methode, um zu faktorisieren.

- Inhalt des nächsten Kapitels: Beschreibung einer Gruppe, bei welcher der Index-Calculus-Algorithmus nicht anwendbar ist.