5.1 Diskreter Logarithmus und Faktorisierung

Für $a \in \mathbb{M}_n$ mit $\operatorname{Ord} a = s$ und zugehöriger Exponentialfunktion

$$\exp_a : \mathbb{Z} \longrightarrow \mathbb{M}_n$$

besteht das Problem des diskreten Logarithmus darin, einen Algorithmus zu finden, der für jedes $y \in \mathbb{M}_n$

- „nein“ ausgibt, wenn $y \notin \langle a \rangle$,
- sonst ein $r \in \mathbb{Z}$ ausgibt mit $0 \leq r < s$ und $y = a^r \bmod n$.

Satz 1 (E. Bach) *Sei $n = pq$ mit verschiedenen Primzahlen $p, q \geq 3$. Dann ist die Faktorisierung von n probabilistisch effizient auf das Problem des diskreten Logarithmus* mod n *reduzierbar.*

Beweis. Es ist $\varphi(n) = (p-1)(q-1)$. Für ein zufällig gewähltes $x \in \mathbb{M}_n$ ist stets $x^{\varphi(n)} \equiv 1 \pmod{n}$. Sei $y := x^n \bmod n$, also

$$y \equiv x^n \equiv x^{n-\varphi(n)} = x^{pq-(p-1)(q-1)} = x^{p+q-1} \pmod{n}.$$

Der diskrete Logarithmus liefert ein r mit $0 \leq r < \operatorname{Ord} x \leq \lambda(n)$ und $y = x^r \bmod n$. Also ist

$$x^{r-(p+q-1)} \equiv 1 \pmod{n}, \quad \operatorname{Ord} x \mid r - (p+q-1).$$

Da $|r - (p+q-1)| < \lambda(n)$, besteht eine große Wahrscheinlichkeit, dass $r = p + q - 1$; z. B. tritt das ein, wenn $\operatorname{Ord} x = \lambda(n)$. Andernfalls wird ein anderes x gewählt.

Aus den beiden Gleichungen

$$\begin{aligned} p + q &= r + 1, \\ p \cdot q &= n \end{aligned}$$

sind die Faktoren p und q bestimmbar. $\diamond$