5.1 Discrete Logarithm and Factorization

Let $a \in \mathbb{M}_n$, $\operatorname{ord} a = s$, and consider the exponential function

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

The problem of computing discrete logarithms $\bmod n$ is to find an algorithm that for each $y \in \mathbb{M}_n$

- outputs "no" if $y \notin \langle a \rangle$,
- else outputs an $r \in \mathbb{Z}$ with $0 \le r < s$ and $y = a^r \bmod n$.

Proposition 15 (E. Bach) *Let $n = pq$ with different primes $p, q \ge 3$. Then factoring n admits a probabilistic efficient reduction to the computation of discrete logarithms $\bmod n$.*

Proof. We have $\varphi(n) = (p-1)(q-1)$. For a randomly chosen $x \in \mathbb{M}_n$ always $x^{\varphi(n)} \equiv 1 \pmod{n}$. Let $y := x^n \bmod n$, thus

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

The discrete logarithm yields an r with $0 \le r < \operatorname{ord} x \le \lambda(n)$ and $y = x^r \bmod n$. Hence

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

Since $|r - (p+q-1)| < \lambda(n)$ the probability is high that $r = p + q - 1$. This happens for example if $\operatorname{ord} x = \lambda(n)$. Otherwise choose another x.

From the two equations

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

we easily compute the factors p and q. $\diamond$