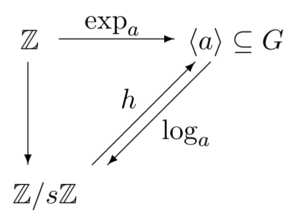
4.1 The Discrete Logarithm

Let G be a group (multiplicatively written) and $a \in G$ be an element of order s (maybe ∞). Then the **exponential function** to base a in G

$$\exp_a \colon \mathbb{Z} \longrightarrow G, \quad x \mapsto a^x,$$

is a group homomorphism (since $a^{x+y} = a^x a^y$) and has period s (since $a^{x+s} = a^x a^s = a^x$ if $s < \infty$). By the homomorphy theorem the induced homomorphism h



is an isomorphism, hence has an inverse map

$$\log_a \colon \langle a \rangle \longrightarrow \mathbb{Z}/s\mathbb{Z}$$

defined on the cyclic subgroup $\langle a \rangle \subseteq G$, the **discrete logarithm** to base a that is an isomorphism of groups. [The case $s = \infty$ fits into this scenario for $s\mathbb{Z} = 0$ and $\mathbb{Z}/s\mathbb{Z} = \mathbb{Z}$.]

We apply this to the multiplicative group $\mathbb{M}_n$: For an integer $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$ the exponential function $\bmod n$ to base a,

$$\exp_a \colon \mathbb{Z} \longrightarrow \mathbb{M}_n, \quad x \mapsto a^x \bmod n,$$

has period $s = \operatorname{ord} a | \lambda(n) | \varphi(n)$. The inverse function

$$\log_a \colon \langle a \rangle \longrightarrow \mathbb{Z}/s\mathbb{Z}$$

is the discrete logarithm $\bmod n$ to base a.

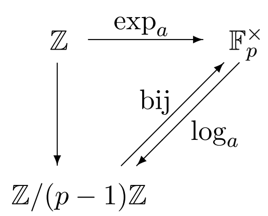
We know of no efficient algorithm that computes the discrete logarithm $\log_a$ for large $s = \operatorname{ord} a$, or to invert the exponential function—not even a probabilistic one.

> **Informal definition:** A function $f : M \longrightarrow N$ is called **one-way function** if for "almost all" images $y \in N$ there is no efficient way to compute a pre-image $x \in M$ with $f(x) = y$.
>
> This definition can be given a mathematically precise (although not completely satisfying) formulation in terms of complexity theory, see Appendix B.

Discrete logarithm assumption: The exponential function $\exp_a \bmod n$ is a one-way function for "almost all" bases a.

Note that this is an unproven conjecture.

The most important special case is a prime module $p \geq 3$, and a primitive element $a \in [2, \ldots, p-2]$, i. e., $\operatorname{ord} a = p - 1$.



To make the computation of discrete logarithms hard in practice we have to choose a prime module p of about the same size as an RSA module. Thus according to the state of the art 1024-bit primes are completely obsolete, 2048-bit primes are safe for short-time applications only.

The book by Shparlinski (see the references for these lecture notes) contains some lower bounds for the complexity of discrete logarithm computations in various computational models.