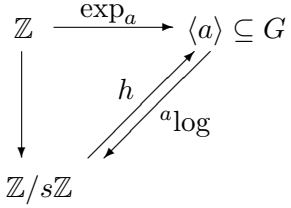
4.1 Der diskrete Logarithmus

Sei G eine Gruppe (multiplikativ geschrieben) und $a \in G$ ein Element der Ordnung s (die auch ∞ sein kann). Dann ist die **Exponentialfunktion** in G zur Basis a

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

ein Gruppenhomomorphismus und hat die Periode s. Nach dem Homomorphiesatz ist der induzierte Homomorphismus h



ein Isomorphismus. Es gibt also eine Umkehrabbildung

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

auf der zyklischen Untergruppe $\langle a \rangle \subseteq G$, den **diskreten Logarithmus** in G zur Basis a, der ein Gruppenisomorphismus ist. [Der Fall $s = \infty$ passt, wenn man $\mathbb{Z}/s\mathbb{Z} = \mathbb{Z}$ setzt.]

Das wird auf die multiplikative Gruppe $\mathbb{M}_n$ angewendet: Für eine ganze Zahl $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a, n) = 1$ hat die Exponentialfunktion $\bmod n$ zur Basis a,

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

die Periode $s = \operatorname{Ord} a | \lambda(n) | \varphi(n)$. Die Umkehrfunktion

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

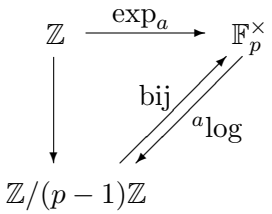
ist der diskrete Logarithmus $\bmod n$ zur Basis a.

Es ist kein effizienter Algorithmus bekannt, den diskreten Logarithmus ${}^a\log$ für große $s = \operatorname{Ord} a$ zu bestimmen, d. h., die Exponentialfunktion umzukehren – auch kein probabilistischer.

> **Informelle Definition:** Eine Funktion $f \colon M \longrightarrow N$ heißt **Einwegfunktion**, wenn für „fast alle“ Bilder $y \in N$ ein Urbild $x \in M$ mit $f(x) = y$ nicht effizient bestimmbar ist.
>
> Eine mathematisch präzise Formulierung dieser Definition lässt sich im Rahmen der Komplexitätstheorie geben, siehe später.

Diskreter-Logarithmus-Vermutung: Die Exponentialfunktion $\exp_a \bmod n$ ist für „fast alle“ Basen a eine Einwegfunktion.

Der wichtigste Spezialfall ist: Der Modul ist eine Primzahl $p \geq 3$ und $a \in [2, \ldots, p-2]$ ist ein primitives Element für p, d. h., $\operatorname{Ord} a = p - 1$.



Damit der diskrete Logarithmus praktisch nicht effizient zu berechnen ist, muss man den Primzahlmodul p etwa in der Größenordnung wie einen RSA-Modul wählen, d. h. nach dem heutigen Stand der Technik reichen 1024-Bit-Primzahlen als Modul nicht aus, 2048-Bit-Primzahlen gelten noch als für ein paar Jahre sicher.

Eine ganze Reihe unterer Schranken für die Komplexität der Berechnung des diskreten Logarithmus in verschiedenen Berechnungsmodellen enthält das – im Literaturverzeichnis der Vorlesung genannte – Buch von Shparlinski.