§ 13. Der diskrete Logarithmus

13.1. Definition. Sei p eine Primzahl. Wie wir in §9 bewiesen haben, ist die multiplikative Gruppe $\mathbb{F}_p^*$ des Körpers $\mathbb{F}_p = \mathbb{Z}/p$ zyklisch. Sei g ein erzeugendes Element von $\mathbb{F}_p^*$ (Primitivwurzel modulo p). Da $\mathbb{F}_p^*$ die Ordnung $p-1$ hat, ist die Abbildung

$$\exp_g : \mathbb{Z}/(p-1) \longrightarrow \mathbb{F}_p^*, \quad k \mapsto g^k,$$

bijektiv und wegen $\exp_g(k+\ell) = \exp_g(k)\exp_g(\ell)$ sogar ein Gruppen-Isomorphismus der additiven Gruppe $(\mathbb{Z}/(p-1), +)$ auf die multiplikative Gruppe $\mathbb{F}_p^*$. Die Umkehrabbildung heißt der *diskrete Logarithmus* zur Basis g,

$$\log_g : (\mathbb{Z}/p)^* \longrightarrow \mathbb{Z}/(p-1).$$

Der Logarithmus genügt der Funktionalgleichung

$$\log(xy) = \log(x) + \log(x)$$

(wir haben zur Vereinfachung den Index g weggelassen) und liefert einen Isomorphismus der multiplikativen Gruppe $\mathbb{F}_p^*$ auf die additive Gruppe $\mathbb{Z}/(p-1)$. Klassischerweise wurde der diskrete Logarithmus als *Index* bezeichnet, Schreibweise $\mathrm{ind}_g(x) = \log_g(x)$, und diente der Zurückführung der Multiplikation modulo p auf die Addition modulo $p-1$. So hat Gauß für seine zahlentheoretischen Untersuchungen Index-Tabellen (= Logarithmen-Tafeln) für alle Primzahlen $p < 100$ aufgestellt.

Beispiel. Für die Primzahl $p = 13$ ist $g = 2$ eine Primitivwurzel. Rechnet man zunächst alle Potenzen von g aus, so erhält man daraus eine Tabelle mit den Logarithmen:

k	0	1	2	3	4	5	6	7	8	9	10	11
$\exp_2(k)$	1	2	4	8	3	6	12	11	9	5	10	7

x	1	2	3	4	5	6	7	8	9	10	11	12
$\log_2(x)$	0	1	4	2	9	5	11	3	8	10	7	6

Für große Primzahlen (hundert und mehr Stellen), wie sie heute in den Anwendungen benutzt werden, ist die Erstellung von Logarithmen-Tafeln natürlich nicht mehr praktikabel. Während die Exponentialfunktion mithilfe des schnellen Potenzierungs-Algorithmus sehr effizient berechnet werden kann, ist es im Allgemeinen viel schwieriger, den diskreten Logarithmus zu berechnen. Diese Asymmetrie wird für einige kryptographische Verfahren benützt.

13.2. Shanks' Algorithmus zur Berechnung des diskreten Logarithmus. Die naive Methode zur Berechnung von $\log_g(x)$ besteht darin, der Reihe nach alle Potenzen $g^k \bmod p$, $k = 0, 1, 2, \ldots$ auszurechnen, bis man auf die Gleichheit $g^k \equiv x \bmod p$ stößt. Dann ist $k = \log_g(x)$. Durchschnittlich wird man dabei etwa $p/2$ Schritte benötigen,

die Komplexität ist also $O(p)$. Shanks hat ein Verfahren erdacht, bei dem man die Komplexität auf etwa $O(\sqrt{p})$ herunterdrücken kann. Dies ist das sog. Giant-Steps-Baby-Steps-Verfahren (GSBS). Wir besprechen es gleich in einer etwas allgemeineren Situation:

Sei G eine (multiplikativ geschriebene) zyklische Gruppe der Ordnung m und g ein erzeugendes Element von G. Dann ist die Abbildung

$$\exp_g : \mathbb{Z}/m \longrightarrow G, \quad k \mapsto g^k,$$

ein Gruppen-Isomorphismus. Es geht um die Berechnung der Umkehrabbildung

$$\log_g : G \to \mathbb{Z}/m.$$

Zu vorgegebenem $x \in G$ muss also ein k bestimmt werden, so dass

$$x = g^k.$$

Wir setzen $r := \lceil \sqrt{m} \rceil$, d.h. r ist die kleinste ganze Zahl $\geqslant \sqrt{m}$. Der unbekannte Logarithmus k lässt sich schreiben als

$$k = \alpha r + \beta \quad \text{mit} \quad 0 \leqslant \alpha, \beta < r.$$

Die Gleichung $g^k = x$ ist äquivalent zu

$$g^{\alpha r} = x g^{-\beta}.$$

Um diese Gleichung zu lösen, berechnen wir zuerst die ‘giant steps’

$$g^{\nu r} = (g^r)^\nu \quad \text{für } \nu = 0, 1, 2, \ldots, r-1$$

und speichern sie ab. Dann berechnen wir die ‘baby steps’

$$x g^{-\mu} \quad \text{für } \mu = 0, 1, 2, \ldots$$

und vergleichen sie mit den giant steps, bis eine Gleichheit

$$g^{\nu r} = x g^{-\mu}$$

gefunden wird. Dann ist $k := \nu r + \mu$ der gesuchte Logarithmus.

Offenbar ist die Gesamtzahl der zu berechnenden giant steps und baby steps $\leqslant 2\sqrt{m}$. Durch geeignete Hash-Techniken bei der Speicherung kann man erreichen, dass ein Vergleich in fast konstanter Zeit (d.h. unabhängig von m) durchgeführt werden kann, so dass also die Gesamtkomplexität $O(\sqrt{m})$ ist.

Die Berechnung des diskreten Logarithmus in G kann noch weiter beschleunigt werden, wenn die Ordnung von G keine Primzahl ist. Dazu brauchen wir zunächst einige Vorbereitungen.

13.3. Satz. *Sei G eine (multiplikative) zyklische Gruppe der Ordnung m mit erzeugendem Element g. Dann gibt es zu jedem Teiler $k \mid m$ genau eine Untergruppe $G(k) \subset G$ der Ordnung k. Diese Untergruppe kann auf folgende Weisen charakterisiert werden:*

(1) $G(k) = \{x \in G : x^k = e\}$.

(2) $G(k) = \mathrm{Im}(G \xrightarrow{\phi} G)$, *wobei* $\phi(x) := x^{m/k}$.

(3) $G(k)$ *ist die von* $g^{m/k}$ *erzeugte zyklische Untergruppe von* G.

Beweis. Wir bezeichnen die durch (1) bis (3) charakterisierten Untergruppen von G mit $G_i(k)$, $i = 1, 2, 3$. Offenbar gilt

$$G_3(k) \subset G_2(k) \subset G_1(k),$$

und die Ordnung von $G_3(k)$ ist gleich k, da sie aus den Elementen $g^{j(m/k)}$ für $j = 0, 1, \ldots, k-1$ besteht. Es ist also nur noch $G_1(k) \subset G_3(k)$ zu zeigen. Sei $x \in G_1(k)$. Es gilt $x = g^\nu$ mit einer gewissen ganzen Zahl ν. Da $x^k = g^{\nu k} = e$, gilt $m \mid \nu k$, also $m/k \mid \nu$. Daraus folgt aber $x = g^\nu \in G_3(k)$, q.e.d.

13.4. Satz. *Sei* G *eine zyklische Gruppe der Ordnung* m. *Es gelte*

$$m = m_1 m_2 \cdot \ldots \cdot m_r$$

mit paarweise teilerfremden $m_i \geqslant 2$. *Sei* $G(m_i) \subset G$ *die eindeutig bestimmte Untergruppe von* G *der Ordnung* m_i *und seien* $\lambda_1, \ldots, \lambda_r$ *ganze Zahlen mit*

$$\lambda_1 \cdot \frac{m}{m_1} + \ldots + \lambda_r \cdot \frac{m}{m_r} = 1.$$

(Die λ_i *existieren, da* $\gcd(m/m_1, m/m_2, \ldots, m/m_r) = 1$.*)*
Man betrachte die Abbildungen

$$G \xrightarrow{\phi} G(m_1) \times G(m_2) \times \ldots \times G(m_r) \xrightarrow{\psi} G,$$

wobei

$$\phi(x) := (x^{m/m_1}, \ldots, x^{m/m_r}) \quad \textit{und} \quad \psi(x_1, \ldots, x_r) := x_1^{\lambda_1} \cdot \ldots \cdot x_r^{\lambda_r}.$$

Dann sind ϕ *und* ψ *Isomorphismen mit* $\psi \circ \phi = id_G$.

Beweis. Die Gleichung $\psi \circ \phi = \mathrm{id}_G$ folgt direkt aus der Definition der λ_i. Da die Gruppen G und $\prod_{i=1}^r G(m_i)$ gleichviele Elemente haben, müssen ϕ und ψ bijektiv, also Isomorphismen sein.

13.5. Pohlig-Hellman-Reduktion. Wir wenden jetzt Satz 13.4 auf das Problem des diskreten Logarithmus an. Wir behalten die Bezeichnungen von 13.4 bei. Sei $g \in G$ ein erzeugendes Element und $x \in G$ ein Element, dessen Logarithmus zur Basis g bestimmt werden soll. Wir zeigen, dass dies auf die Berechnung der diskreten Logarithmen in den Gruppen $G(m_i)$ zurückgeführt werden kann. Dazu wenden wir die Abbildung ϕ auf g und x an:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G(m_1) \times \ldots \times G(m_r) \\ g & \mapsto & (\, g_1 \quad , \ \ldots \ , \quad g_r \,) \quad , \quad g_i := g^{m/m_i} \\ x & \mapsto & (\, x_1 \quad , \ \ldots \ , \quad x_r \,) \quad , \quad x_i := x^{m/m_i} \end{array}$$

Das Element g_i erzeugt die Gruppe $G(m_i)$, also gibt es ganze Zahlen k_i mit

$$x_i = g_i^{k_i} \quad \text{für } i = 1, \ldots, r.$$

Nach Satz 13.4 gilt

$$x = x_1^{\lambda_1} \cdot \ldots \cdot x_r^{\lambda_r} = g_1^{k_1\lambda_1} \cdot \ldots \cdot g_r^{k_r\lambda_r} = g^{k_1\lambda_1 m/m_1 + \ldots + k_r\lambda_r m/m_r};$$

daher ist

$$k := \sum_{i=1}^{r} k_i \, \lambda_i \, \frac{m}{m_i} \bmod m \in \mathbb{Z}/m$$

der diskrete Logarithmus zur Basis g von x.

Da jede natürliche Zahl m in ein Produkt von teilerfremden Primzahlpotenzen zerlegt werden kann, zeigen die obigen Überlegungen, dass das Problem des diskreten Logarithmus in beliebigen zyklischen Gruppen auf das entsprechende Problem in zyklischen Gruppen von Primzahlpotenz-Ordnung zurückgeführt werden kann. Als nächstes zeigen wir, dass man das Problem sogar auf Gruppen mit Primzahl-Ordnung zurückführen kann.

13.6. Zyklische Gruppen von Primzahlpotenz-Ordnung. Sei G eine zyklische Gruppe der Ordnung p^n, (p prim, $n > 1$) mit erzegendem Element g. Nach Satz 13.3 haben wir Untergruppen

$$G(p^k) := \{x \in G : x^{p^k} = e\}, \quad k = 1, \ldots, n,$$

der Ordnung p^k. Die Gruppe $G(p^k)$ ist zyklisch mit erzeugendem Element $g^{p^{n-k}}$ und die Abbildung

$$G \to G(p^k), \quad x \mapsto x^{p^{n-k}},$$

ist ein surjektiver Gruppen-Homomorphismus. Die Gruppen $G(p^k)$ liefern eine sog. Filtrierung von G,

$$\{e\} \subset G(p) \subset G(p^2) \subset \ldots \subset G(p^{n-1}) \subset G(p^n) = G.$$

Wir setzen voraus, dass wir einen Algorithmus haben (z.B. den Shanks'schen GSBS-Algorithmus), um das diskrete Logarithmus-Problem in der Gruppe $G(p)$ zu lösen. Sei $z \in G$ vorgegeben. Um die Gleichung

$$z = g^t, \quad \text{d.h.} \quad t = \log_g(z),$$

in G zu lösen, zeigen wir durch Induktion nach k, wie man ganze Zahlen t_k finden kann, so dass

$$z^{p^{n-k}} = g^{p^{n-k}t_k}.$$

Für $k = n$ haben wir dann $z = g^{t_n}$.

Der *Induktions-Anfang* $k = 1$ ist einfach das diskrete Logarithmus-Problem in $G(p)$, da $z^{p^{n-1}} \in G(p)$, und $g^{p^{n-1}}$ die Gruppe $G(p)$ erzeugt.

Induktionsschritt $k \to k+1$. Aus $z^{p^{n-k}} = g^{p^{n-k}t_k}$ folgt

$$\left(z^{p^{n-k-1}} g^{-p^{n-k-1}t_k}\right)^p = e, \quad \text{d.h.} \quad z^{p^{n-k-1}} g^{-p^{n-k-1}t_k} \in G(p),$$

also können wir ein ν_k finden, so dass

$$z^{p^{n-k-1}} g^{-p^{n-k-1}t_k} = (g^{p^{n-1}})^{\nu_k}.$$

Also ist

$$z^{p^{n-k-1}} = g^{p^{n-k-1}t_{k+1}} \quad \text{mit} \quad t_{k+1} = t_k + p^k\nu_k, \qquad \text{q.e.d.}$$

Zusammenfassend ergibt sich, dass in einer zyklischen Gruppe der Ordnung

$$m = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$$

das diskrete Logarithmus-Problem in etwa $O(\sqrt{p})$ Schritten gelöst werden kann, wobei $p = \max\{p_1, \ldots, p_r\}$. Für die speziellen Gruppen $(\mathbb{Z}/p)^*$ gibt es noch einen anderen unter dem Namen 'Index Calculus' bekannten Algorithmus, der im Allgemeinen noch schneller ist. Es ist jedoch kein Algorithmus bekannt, dessen Komplexität polynomial mit $\log p$, d.h. polynomial mit der Stellenzahl von p wächst.