5. The Discrete Logarithm

5.1. Definition. Let p be a prime. As we have proved in chapter 4, the multiplicative group $(\mathbb{Z}/p)^*$ is cyclic. A generator g of this group is called a *primitive root* modulo p. The map

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

is an isomorphism of the additive group $\mathbb{Z}/(p-1)$ onto the multiplicative group $(\mathbb{Z}/p)^*$. Its inverse is called the *discrete logarithm* with respect to base g,

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

Classically, $\log_g(x)$ is also called the *index* of x with respect to the primitive root g.

In this chapter we will discuss the discrete logarithm in a slightly more general setting: Let G be a (multiplicative) cyclic group of order m and g a generator of G. Again we have a group isomorphism

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

and we are interested in its inverse

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

By definition

$$\log_g(x) = k \quad \Longleftrightarrow \quad x = g^k.$$

Whereas the exponential map can be efficiently calculated using the fast exponentiation algorithm, it is in general much more complicated to calculate the discrete logarithm. This asymmetry is used by some cryptographic systems.

5.2. Shanks' Giant-Step-Baby-Step Method. The naive method to calculate the discrete logarithm of x is to calculate g^k for $k = 0, 1, 2, 3, \ldots$ until one finds a match $g^k = x$. The complexity of this method is $O(m)$.

Shanks has devised a quite general method which reduces this complexity to about $O(\sqrt{m})$, which we will now describe.

Let G be a cyclic group of order m with generator g. We want to calculate the discrete logarithm of a given element $x \in G$, i.e. find an integer k with $0 \le k < m$ and

$$g^k = x.$$

Set $r := \lceil \sqrt{m} \rceil$, i.e. r is the least integer $\ge \sqrt{m}$. The unknown logarithm k can be written as

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

The equation $g^k = x$ is equivalent to

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

To solve this equation, we first calculate the 'giant steps'

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

and store them. Next we calculate the 'baby steps'

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

and compare them with the giant steps until a match $g^{\alpha r} = x g^{-\beta}$ is found. Then $k = \alpha r + \beta$ is the discrete logarithm of x.

What is the complexity of this method? The calculation of the giant steps and baby steps has a complexity of $O(\sqrt{m})$. The critical point is comparing the baby steps with the giant steps. Since we have up to $\sqrt{m}$ baby steps, it is not acceptable to do every time a linear search in the table of giant steps. A better way is to use binary search which needs $O(\log m)$ steps for one search. This supposes the table of giant steps to be sorted, which can be done (e.g. by a suitable quicksort algorithm) in $O(\sqrt{m}\log m)$ steps. This leads to an overall complexity of $O(\sqrt{m}\log m)$. Still better is to use appropriate hashing techniques. Then a lookup in the table of giant steps can be done in almost constant time, so we get a complexity of $O(\sqrt{m})$.
A disadvantage of this method is the high space requirement of order $O(\sqrt{m})$ for the table of giant steps. There is a probabilistic variant of the algorithm (which we will discuss in a later chapter) which needs only a small constant amount of space.

If the order m of the group G is not a prime number, one can reduce the discrete logarithm problem for G to smaller groups. For this purpose we need some preparations.

5.3. Theorem. *Let G be a (multiplicative) cyclic group of order m with generator g. Then for every positive divisor $k \mid m$ there exists exactly one subgroup $G(k) \subset G$ of order k. This group can be described in the following ways:*

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

ii) $G(k) = \mathrm{Im}(\phi)$, *where ϕ is the map*

$$\phi : G \longrightarrow G, \quad x \mapsto x^{m/k}.$$

iii) *$G(k)$ is the cyclic subgroup of G generated by $g^{m/k}$.*

Proof. Define $G_1 := \{x \in G : x^k = e\}$. Certainly any subgroup of G with k elements is contained in G. If we can show that G_1 has k elements, we have proved unicity.
Every element $x \in G$ has the form $x = g^\nu$ with $0 \le \nu < m$. We have

$$x = g^\nu \in G_1 \iff g^{\nu k} = e \iff m \mid \nu k \iff (m/k) \mid \nu.$$

This shows that $G_1 = \{g^{(m/k)\mu} : 0 \le \mu < k\}$ which has indeed k elements and is the group described in iii). Because G is generated by g, the group $\mathrm{Im}(\phi)$ in ii) is generated by $g^{m/k}$, which implies that the groups described in ii) and iii) coincide. This completes the proof of the theorem.

5.4. Theorem. *Let G be a cyclic group of order m. Suppose that*

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

with pairwise coprime $m_i \ge 2$ and let G_i be the uniquely determined subgroup of G of order m_i. Since $\gcd(m/m_1, m/m_2, \ldots, m/m_r) = 1$, there exist integers λ_i with

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

Consider the maps

$$G \xrightarrow{\phi} G_1 \times G_2 \times \ldots \times G_r \xrightarrow{\psi} G,$$

where ϕ and ψ are defined by

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

Then ϕ and ψ are isomorphisms with $\psi \circ \phi = id_G$.

Proof. The equation $\psi \circ \phi = \mathrm{id}_G$ follows directly from the definition of the integers λ_i. Since the groups G and $G_1 \times G_2 \times \ldots \times G_r$ have the same number of elements, it follows that ϕ and ψ are isomorphisms.

5.5. Pohlig-Hellman reduction. We now apply theorem 5.4 to the discrete logarithm problem. We keep the notations of 5.4. Let $g \in G$ be a generator and $x \in G$ an element whose discrete logarithm is to be calculated. We apply the map ϕ to g and x.

$$\begin{array}{ccl} G & \xrightarrow{\phi} & G_1 \times \ldots \times G_r \\ g & \mapsto & (g_1, \ldots, g_r), \quad g_i = g^{m/m_i} \\ x & \mapsto & (x_1, \ldots, x_r), \quad x_i = x^{m/m_i} \end{array}$$

The element g_i is a generator of the group G_i of order m_i, therefore we can solve the discrete logarithm problem in G_i with respect to base g_i and get integers k_i with

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

By theorem 5.4 we have

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

therefore

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

is the discrete logarithm of $x \in G$ with respect to base g.

Since every positive integer m can be decomposed into a product of prime powers, $m = \prod_{i=1}^{r} p_i^{k_i}$, we see that the discrete logarithm problem in an arbitrary finite cyclic group can be reduced to the discrete logarithm problem in cyclic groups of prime power order. We will show next how to further reduce the problem to groups of prime order.

5.6. Cyclic groups of prime power order. Let G be a cyclic group of order p^n, where p is a prime and n an integer ≥ 2. Let g be a generator of G. We want to solve the discrete logarithm problem in G, i.e. given an element $z \in G$, find an integer t such that $g^t = z$. For $k = 1, 2, \ldots, n$ we define the subgroups

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

By theorem 5.3, $G(p^k)$ is a cyclic group of order p^k and the map

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

is surjective. We have the filtration

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

We suppose that we have an algrithm to solve the discrete logarithm problem in $G(p)$ (for example Shanks' giant-step-baby-step method). Given $z \in G$, we will show by induction on k how to find integers t_k such that

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

The case $k = n$ solves the discrete logarithm problem in G. Since $g^{p^{n-1}}$ is a generator of $G(p)$, the case $k = 1$ is the discrete logarithm problem in $G(p)$.

Induction step $k \to k+1$. By induction hypothesis we have

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

Therefore

$$y_k := (zg^{-t_k})^{p^{n-k-1}} \in G(p),$$

and solving the discrete logarithm problem in $G(p)$ yields an integer τ_k with

$$(g^{p^{n-1}})^{\tau_k} = y_k = (zg^{-t_k})^{p^{n-k-1}}.$$

This implies

$$(zg^{-t_k - \tau_k p^k})^{p^{n-k-1}} = e \implies (g^{t_k + \tau_k p^k})^{p^{n-k-1}} = z^{p^{n-k-1}}.$$

With $t_{k+1} := t_k + \tau_k p^k$, this is the induction assertion for $k+1$, q.e.d.

5.7. Conclusion. Let G be a cyclic group of order m and let

$$m = \prod_{i=1}^{r} p_i^{k_i}$$

be the prime factorization of m. Then, using the Pohlig-Hellman reduction and Shanks' giant-step-baby-step method, the discrete logarithm in G can be calculated in about $O(\sqrt{p})$ steps, where $p = \max\{p_i : 1 \leq i \leq r\}$.