5. Tutorial: Discrete logarithms (2)

The goal of this whole exercise sheet is to compute the discrete logarithm of \( \alpha = 259 \) in base \( g = 2 \) of the subgroup of \( \mathbb{Z}_{391}^\times \) generated by \( g \). Multiple techniques are involved, hence different exercises, which are in fact more or less independent.

**Exercise 5.1** (Chinese remaindering).

(i) Noting that 391 = 23 \( \cdot \) 17, what is the order of \( \mathbb{Z}_{391}^\times \)? Give also its factored expression.

(ii) Compute the order \( d \) of \( g = 2 \) in \( \mathbb{Z}_{391}^\times \). You should use only a few operations to obtain the result.

(iii) What is the order of the subgroup \( G = \langle 2 \rangle < \mathbb{Z}_{391}^\times \)?

(iv) Using the Chinese remainder theorem, show that \( G \cong S_1 \times S_2 \), where \( S_1 \) and \( S_2 \) are subgroups of \( G \), with \( \#S_1 = 11 \) and \( \#S_2 = 8 \). Give generators for \( S_1 \) and \( S_2 \).

(v) Conclude on how to compute the discrete logarithm of \( \alpha \) in \( G \), using discrete logarithms in \( S_1 \) and \( S_2 \).

**Exercise 5.2** (Pollard’s \( \rho \) method).

We now focus on solving the first part of the discrete logarithm in \( G \), namely compute \( \text{dlog}_{g_1}(\alpha_1) \), with \( \alpha_1 = \alpha^{d/d_1} \).

(i) Recall Pollard’s \( \rho \) method to compute discrete logarithms.

(ii) Apply it to our example, starting for instance with \( x_0 = y_0 = g_1^2 \cdot \alpha_1^3 \).
Exercise 5.3 (Pohlig-Hellman algorithm).

Now only the computation of the discrete logarithm in $S_2$ remains.

We first consider the subgroup $S'_2$ of $S_2$ generated by $g'_2 = g_2^{2^2}$.

(i) Show that $z \in S_2$ is in $S'_2$ if and only if $z^2 = 1$.

(ii) What is the order of this subgroup?

(iii) Show that $x_0 = \alpha_2^{2^2}$ is in $S'_2$.

(iv) Compute the discrete logarithm $a_0$ of $x_0$ in base $g'_2$ in $S'_2$.

(v) Similarly, compute $a_1$, the discrete logarithm of $x_1 = \alpha_2^{2^1} \cdot g_2^{-a_0 \cdot 2^1}$. Verify first that $x_1$ is in $S'_2$.

(vi) Same question for $a_2$, the discrete logarithm of $x_2 = \alpha_2^{2^0} \cdot g_2^{-a_1 \cdot 2^1 - a_0 \cdot 2^0}$.

(vii) Conclude on the discrete logarithm of $\alpha_2$ in $S_2$.

Exercise 5.4 (Putting it all together).

(i) What is the discrete logarithm $k$ of $\alpha$ in $G$?