4. Exercise sheet

Any claim needs a proof or argument.

Exercise 4.1 (“Meet in the middle attack” on DLP). (8 points)

Consider the group $G = \mathbb{Z}_7^\times$ generated by $g = 5$. The aim of this exercise is to find the discrete logarithm of $a = 6$ using the Baby step-giant step-method you learned in the lecture. In other words, we want to find the smallest positive integer $\alpha$, such that

$$g^\alpha = a.$$ 

(i) Compute a table of pairs $(\alpha_0, ag^{-\alpha_0})$ for $0 \leq \alpha_0 < b$ for an appropriate number of steps $b$. \( \square 2 \)

(ii) Compute $(g^b)^{\alpha_1}$ for values $\alpha_1 \geq 0$ until you hit a value that appears in the table. \( \square 2 \)

Such a collision means that you have found values $\alpha_0$ and $\alpha_1$ such that

$$g^{\alpha_0} = a(g^b)^{-\alpha_1}.$$ 

(iii) Compute $g, g^2, \ldots, g^b$ and find the inverse $g^{-b}$ of the last one. \( \square 1 \)

(iv) Compute the value of the discrete logarithm $\alpha$ from this equation. \( \square 3 \)

Exercise 4.2 (Number of points of an elliptic curve). (4 points)

Let $\mathbb{F}_q$ be a (actually, the) field with $q$ elements. Clearly, given $a, b \in \mathbb{F}_q$ the equation $y^2 = x^3 + ax + b$ has at most $q^2$ solutions $(x, y) \in \mathbb{F}_q^2$, since there are no more candidates.

Prove a better bound of order $O(q)$. \( \square 4 \)
Exercise 4.3 (Elliptic curves). (6+3 points)

Let \( p \geq 5 \) be prime and \( a, b \in \mathbb{Z}_p \) with \( 4a^3 + 27b^2 \neq 0 \). Consider the elliptic curve \( E \) given \( y^2 = x^3 + ax + b \), i.e.

\[
E = \{(x, y) \in \mathbb{Z}_p \mid y^2 = x^3 + ax + b\} \cup \{O\}.
\]

Choose any two points \( P_1, P_2 \in E \). If \( P_i = (x_i, y_i) \neq O \) and \( x_1 \neq x_2 \), the line through them is given by an equation \( y = m(x - x_1) + y_1 \). Let \( P_3 = (x_3, y_3) \) be the third point on the intersection of the line with the curve. Define \( P_1 + P_2 = (x_3, -y_3) \) then. If \( P_1 = -P_2 \) then let \( P_1 + P_2 := O \). Further define \( P_1 + O := P_1 \) and \( O + P_2 := P_2 \) and \( O + O := O \).

(i) Prove that the tangent at a point \( P_1 \) has slope \( \alpha = \frac{3x_1^2 + a}{2y_1} \).

(ii*) Prove that the addition is associative at least in case all operations are of the first type. You may use a computer algebra system to perform tedious algebraic computations.

Consider an example: \( p = 5, a = 2, b = 1 \). So we consider the elliptic curve \( E = \{(x, y) \in \mathbb{Z}_5 \mid y^2 = x^3 + 2x + 1\} \cup \{O\} \) over the field \( \mathbb{Z}_5 \) with 5 elements.

(iii) Make a list of all points of the defined curve. Draw a picture. [It is a good idea to use the representation \( \mathbb{Z}_5 = \{-2, -1, 0, 1, 2\} \).]

(iv) Compute \((-2, 2) + (0, 1)\).

(v) Compute \(2(0, 1) := (0, 1) + (0, 1)\).

(vi) Compute \(3(0, 1)\).

(vii) Make a table of the map \( \exp_{(0,1)} \) which maps \( a \in \mathbb{Z}_7 \) to \( a \cdot (0, 1) \). [Hint: In \( \mathbb{Z}_7 \) we have \( 4 = -3 \).]

(viii) Add \((-2, 2)\) and \((0, 1)\) using this table. Does it produce the same result as before? Should it?

Exercise 4.4 (Alternative addition?). (4 points)

For two points \( P, Q \) on an elliptic curve \( E \), define \( P \oplus Q = S \), where \( S \) is the third intersection point of the line through \( P \) and \( Q \) with \( E \), so that \( S = -(P + Q) \) with the ‘usual’ addition on an elliptic curve. Explain why this method does in general not generate a group structure on \( E \).