DUPLICATION FORMULA AND POINTS OF ORDER THREE

We recall a number of useful formulas. If \( P_i = (x_i, y_i) \) are the points of intersection of a line with the elliptic curve \( E : y^2 = f(x) = x^3 + ax^2 + bx + c \), then we have

\[
x_1 + x_2 + x_3 = m^2 - a,
\]

where \( m \) is the slope of the line. This is the most efficient way to calculate the \( x \) coordinate of the point \( P_1 + P_2 \). Now observe if the line is the tangent line at the point \( P = (x, y) \), we get

\[
m^2 = \frac{f'(x)^2}{(2y)^2} = \frac{f'(x)^2}{4f(x)},
\]

using \( y^2 = f(x) \). Hence we get the duplication formula for the \( x \)-coordinate \( x(2P) \) of the point \( 2P \), by setting \( x_1 = x_2 = x \) and solving for \( x_3 = x(2P) \)

\[
x(2P) = \frac{f'(x)^2}{4f(x)} - a - 2x = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.
\]

**Points of order three** As we have seen in the lecture by geometric considerations, if a point \( P = (x, y) \) has order three, then \( 2P = -P \) and \( x(2P) = x \). Plugging this into the duplication formula, multiplying by the denominator we get the polynomial identity

\[
0 = \Psi_3(x) = 2f(x)f''(x) - f'(x)^2 = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2).
\]

Hence a point \( P = (x, y) \) can have order 3 only if its \( x \)-coordinate satisfies \( \Psi_3(x) = 0 \).

**Lemma** If the discriminant \( \Delta = \Delta(f) \) is not equal to 0, then \( \Psi_3 \) has four distinct roots.

By the Repeated Root Theorem (see below), it suffices to show that \( \Psi_3 \) and \( \Psi_3' \) have no common zeros. Now observe that

\[
\Psi_3'(x) = 2f'(x)f''(x) + 2f(x)f'''(x) - 2f'(x)f''(x) = 2f(x)f'''(x) = 12f(x),
\]

where the last equality follows from \( f'''(x) = 6 \) (as \( f(x) \) is a polynomial of order 3 with leading coefficient 1). Assume now there exists a point \( x_o \) for which \( \Psi_3(x_o) = 0 - \Psi_3'(x_o) \). Then the last equality implies that \( 12f(x_o) = 0 \), i.e. \( f(x_o) = 0 \). Plugging this into the formula for \( \Psi_3(x) \), we obtain

\[
0 = \Psi_3(x_o) = 2f(x_o)f''(x_o) - f'(x_o)^2 = -f'(x_o)^2.
\]

Hence \( x_o \) would be a common root of \( f(x) \) and \( f'(x) \) as well, contradicting the fact that the discriminant of \( f(x) \) is nonzero.

**Repeated Root Theorem** The following statements are equivalent:

(a) The polynomial \( f(x) \) of degree \( n \) has \( n \) distinct roots.

(b) The polynomials \( f(x) \) and \( f'(x) \) have no common root.
(c) The discriminant of the polynomial \( f(x) \) is nonzero

Recall that for a polynomial \( f(x) = x^3 + bx + c \), the discriminant is given by \( \Delta(f) = -4b^3 - 27c^2 \). If \( f(x) = x^2 + bx + c \), then \( \Delta(f) = b^2 - 4c \).

**Theorem** Let \( E : y^2 = f(x) = x^3 + ax^2 + bx + c \) be an elliptic curve with \( \Delta(f) \neq 0 \). Then there exist exactly eight points \( P \) in \( E(\mathbb{C}) \), the set of complex solutions of \( E \) of order 3. In particular, these points together with \( \infty \) form a group which is isomorphic to \( \mathbb{Z}/3 \times \mathbb{Z}/3 \).

**Proof.** We have shown that if \( P = (x,y) \) has order 3, then its \( x \)-coordinate must be one of the four distinct roots of the polynomial \( \Psi_3(x) \). For each of these values, we have two values \( \pm y \) which satisfy \( E \). If \( P_1 \) and \( P_2 \) are two points of order three, then we also have \( 3(P_1 + P_2) = 3P_1 + 3P_2 = \infty \), i.e. also the order of their sum must divide 3 and hence must again be one of the points of order 3 or the point \( \infty \). Hence we get a group of nine elements all of which have order at most 3. It is shown in algebra that this group must be isomorphic to \( \mathbb{Z}/3 \times \mathbb{Z}/3 \).

**Exercises:**

1. Let \( E : y^2 = x^3 + 6x \) with \( b > 0 \). Calculate all real points of order 3. Are there any rational points of order 3?
2. Let \( E : y^2 = x^3 - bx \), with \( b > 0 \).
   (a) Calculate all real points of order 4. **Hint:** If \( P \) has order 4, then \( 2P \) has order 2.
   (b) Calculate all rational points of order four on \( E \).
3. Let \( E : y^2 = f(x) = x^3 + ax^2 + bx = c \) be an elliptic curve with nonzero discriminant. The goal of this exercise is to show that there are at most two real points of order 3 on \( E \).
   (a) Show that its real points (i.e. what we draw on paper) have either one or two connected components, depending on whether \( f(x) \) has one or three real solutions.
   (b) Assume that we have two components, and that \( P_1, P_2 \) are points in the component \( C_1 \) which does not contain the point \( \infty \). Show that \( P_1 + P_2 \) is in \( C_0 \), the component which contains \( \infty \). **Hint:** You may want to consider some geometric argument.
   (c) Show that if \( P \) has odd order, then it must be in \( C_0 \).
   (d) Show that the polynomial \( \Psi_3(x) \) has only one real root \( \alpha \) for which \( f(\alpha) > 0 \) **(Hint:** Use that \( \Psi_3' = 12f(x) \)).
   (e) Prove in general that there are exactly two real points on \( E \) which have order three.