Worksheet 4:

Let $F$ be a field of characteristic different to 2 or 3.
Let $x^3 + ax + b$ be a cubic polynomial with coefficients in $F$ that has no repeated roots. An elliptic curve over $F$ is defined as the set of points $(x, y)$ in $F^2$ satisfying the equation

$$y^2 = x^3 + ax + b,$$

together with a single point denoted $O$ and called the point at infinity.

Problem 4.1:

1. How many points does the elliptic curve given by the equation $y^2 = x^3 - x$ over $F_5$ have?
2. How many points does the elliptic curve given by the equation $y^2 = x^3 + x$ over $F_5$ have?
3. Show that no elliptic curve over $F_5$ can have more than 11 points.

Solution 4.1:
For the following problem our field will be the real numbers, thus we can draw the curves. Let $E$ be an elliptic curve, let $P$ and $Q$ be two points in $E$. We will define $P + Q$ and $-P$ by the following rules.

1. If $P = O$, then $-P := O$ and $P + Q := Q$, so in the following cases we will assume that no point is the point at infinity.

2. If the point $P$ has coordinates $(x, y)$, then the point $-P$ is given by the the coordinates $(x, -y)$

3. If $P$ and $Q$ have different $x$-coordinates, then the line $l = PQ$ intersects $E$ at a third point $R$ (in case $l$ is tangent to $E$ at $P$ or $Q$, we define $R$ to be the point of tangency). We define $P + Q := -R$.

4. If $Q = -P$, then $P + Q := O$.

5. If $P = Q$, then let $l$ be the tangent line to $E$ at $P$, let $R$ be the third point of intersection of $l$ and $E$. We define $P + Q := -R$.

These definitions also work in the case of any field, if one takes care of what a tangent curve means in those cases. An example of this can be seen in the following picture:
Problem 4.2:
For the following problem our field will be the real numbers, thus we can draw the curves.
Let $L$ be some line that is not parallel to the $y$-axis, show the following equalities:

1. Assume $L \cap E$ are three different points $A, B, C$. Then
   \[ A + B + C = O \]

2. Assume $L \cap E$ consists of two points $A, B$, where $L$ is tangent to $E$ at $A$. Then $A + A + B = O$.
3. Assume $L \cap E = \{A\}$. Then $A + A + A = O$.

Solution 4.2:
The objective of the next problem is to find a formula for the point $P + Q$, in terms of $a, b$ and the coordinates of $P$ and $Q$.

Let $E$ be the elliptic curve over $\mathbb{R}$ given by the equation $y^2 = x^3 + ax + b$, and $P = (x_1, y_1), Q = (x_2, y_2)$. Assume that $x_1 \neq x_2$.

Let $y = \alpha x + \beta$ be the equation of the line $l$ passing through $P$ and $Q$.

Let $R = (x_3, y_3)$ be the third point of intersection of $l$ and $E$.

**Problem 4.3:**

(1) Show that the $x$-coordinate of the intersection points of $l$ and $E$ satisfy the equation:

$$x^3 - (\alpha x + \beta)^2 + ax + b = 0$$

(2) Show that $x_3 = \alpha^2 - x_1 - x_2 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2$.

(3) Compute the coordinates of $P + Q$.

This can be taken as the definition of $P + Q$, when $P \neq Q$, in any field.

**Solution 4.3:**
Let $E$ be the elliptic curve over $\mathbb{R}$ given by the equation $y^2 = x^3 + ax + b$, and $P = (x_1, y_1)$. Let $y = \alpha x + \beta$ be the equation of the line $l$ tangent to $E$ passing through the point $P$.

The tangent line to $E$ at $P$ has slope $\alpha = \frac{3x_1^2 + a}{2y_1}$.

**Problem 4.4:**

(1) Show that the $x$ coordinates of the intersection points of $l$ and $E$ satisfy the equation:

$$x^3 - (\alpha x + \beta)^2 + ax + b = 0$$

(2) Show that $x_3 = \alpha^2 - 2x_1 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$.

(3) Compute the coordinates of $P + P$.

This formula can be taken as the definition of $P + P$ for an elliptic curve over any field.

**Solution 4.4:**
One can think of the elliptic curve given by equation $y^2 = x^3 + ax + b$ with the point at infinity $O$, as a projective curve in $\mathbb{P}^2_F$, with equation

$$y^2 z = x^3 + axz^2 + bz^3$$

**Problem 4.5**

Show that there exists a bijection between the points of the elliptic curve $E$ (and points $(x, y)$ in $y^2 = x^3 + ax + b$) and points in the projective plane satisfying the equation $y^2 z = x^3 + axz^2 + bz^3$.

What point in the projective plane corresponds to $O$?

**Solution 4.5**
Problem 4.6:
Show that $P + Q + R = O$ if and only if $P, Q, R$ are the intersection points of a line and $E$, when we think of it as a projective curve.
Which cases are we missing if we only consider lines in affine space?
Solution 4.6:
Let $L_1, \ldots, L_6$ be homogeneous linear polynomials in three variables, i.e. $L_i = 0$ is a projective line in $\mathbb{P}^2$. Let $X = L_1L_2L_3$ and $Y = L_4L_5L_6$. Assume that $\{X = 0\} \cap \{Y = 0\}$ are nine different points.

For the following problem, you may use that if an elliptic curve (seen as a projective curve) passes through 8 of the points in $\{X = 0\} \cap \{Y = 0\}$ then the intersection of the degree 3 curve and $\{X = 0\} \cap \{Y = 0\}$ is exactly the 9 points of $\{X = 0\} \cap \{Y = 0\}$.

**Problem 4.7:**

Assuming that the points $P, Q, -(P + Q), O, R, -R, -P, -(Q + R), (P + Q) + R$ are all different, show that $(P + Q) + R = P + (Q + R)$.

**Hint:** Find 6 lines $L_1, \ldots, L_6$, $X = L_1L_2L_3$ and $Y = L_4L_5L_6$ such that $X \cap Y = \{P, Q, -(P + Q), O, R, -R, -P, -(Q + R), (P + Q) + R\}$.

**Solution 4.7:**
Problem 4.8:
Show that the points of an elliptic curve with the addition defined before form an abelian group i.e. show that the operation satisfies associativity, commutativity, there exists a neutral element and any element has an inverse.
Solution 4.8:
An element $P$ of a group $(E,+_E)$ is said to have order $d$ if $d$ is the smallest positive integer such that
\[ dP = P +_E \cdots +_E P = 0 \]

**Problem 4.9:**
Find the order of the point $(2, 3)$ on the elliptic curve $y^2 = x^3 + 1$.

**Solution 4.9:**
Problem 4.10:
Let $P$ be a point in an elliptic curve $E$, different from the point at infinity.

(1) Show that a point has order 2 if and only if it is on the $x$-axis.

(2) Show that a point $P$ has order 3 if and only if the tangent to $E$ at $P$ does not contain any other point of $E$.

(3) Can you find a geometric description of the points of order 4 in $E$?

Solution 4.10:
Problem 4.11:
Let $p$ be an odd prime number, different from 3. Show that there are $p + 1$ different points in the following elliptic curves over $\mathbb{F}_p$:

1. $y^2 = x^3 - x$, for $p \equiv 3 \pmod{4}$.
2. $y^2 = x^3 - 1$, for $p \equiv 2 \pmod{3}$.

Solution 4.11: