Problem class 5

1. Let $C : Y^2Z = X^3 + A\,XZ^2 + B\,Z^3$ be a Weierstrass equation over a field k of characteristic not 2. Suppose $\Delta = 0$. Show that $(3B : 0 : -2A)$ is a singular point in $C(k)$ and hence C is not smooth.

2. a) Let $E : y^2 = x^3 + A\,x + B$ be a Weierstrass equation defined over k. Let $D \in k^\times$. Show that there is a transformation between E and the curve $E' : y^2 = x^3 + D^4 A\,x + D^6 B$.

   b) Determine the discriminant Δ' of E' in terms of the discriminant of E. Define the quantity $j = -1728\,(4A)^3/\Delta$ called the **j-invariant**. Prove that this quantity is invariant under this transformation.

   c) Show that every Weierstrass equation E defined over $k = \mathbb{Q}$ can be transformed into a Weierstrass equation with A and B integers.

3. Let E be the cubic curve given by

$$Y^2Z + a_1\,XYZ + a_3\,YZ^2 = X^3 + a_2\,X^2Z + a_4\,XZ^2 + a_6\,Z^3$$

   with $a_1, a_2, a_3, a_4, a_6 \in k$. Suppose that it is non-singular. Let $O = (0 : 1 : 0) \in E(k)$. Let $P = (x_P : y_P : 1)$ and $Q = (x_Q : y_Q : 1)$.

   a) Prove that O is the unique point of E at infinity and that it is an inflection point.

   b) Show that $-P = (x_P, -y_P - a_1\,x_P - a_3)$.

   c) Spell out the procedure to compute $P + Q$.

   d) Do the same for $2\,P$.

4. Let C_1 and C_2 be the cubics defined over $\mathbb{R}$ by

$$C_1\colon\ X^3 + 2\,Y^3 - XZ^2 - 2\,YZ^2 = 0 \text{ and } C_2\colon\ 2\,X^3 - Y^3 - 2\,XZ^2 + YZ^2 = 0.$$

   a) Find the nine points $\{P_1, P_2, \ldots, P_9\}$ of intersection of C_1 and C_2.

   b) (Long!) Set $P_1 = (0 : 0 : 1)$. Prove that if a cubic passes through P_2, P_3, $\ldots$, P_9 then it also passes through P_1.

Chocolate question

5. Let C be a cubic curve with a point $O \in C(k)$. The tangent at O meets the curve in a further point $\hat{O}$, except if O is an inflection point in which case we take $\hat{O} = O$. Consider the following operation using two points P and Q in $C(k)$:

   - Draw the line through P and $\hat{O}$ and call the third intersection point with C the point R.
   - Draw the line through Q and O and call the third intersection point S.
   - Draw the line through R and S and call the third intersection point $P\#Q$.

   Prove $P + Q = P\#Q$ and, surprisingly, the above describes an abelian group law, too.