Problem class 6

1. Let E be the elliptic curve defined over $\mathbb{Q}$ given by $y^2 = x^3 + x + 3$. Let $P = (-1 : 1 : 1)$. Compute $-P$, $2\,P$, $3\,P$ and $4\,P$.

2. Let E be the elliptic curve $y^2 = x^3 + 2\,x - 1$ defined over $\mathbb{F}_5$.

   a) Find all points in $E(\mathbb{F}_5)$. (The number of them will be a prime.)

   b) Pick a point P as a generator of this cyclic group and write all other points as a multiple of your P.

3. Let a be an element in a field k of characteristic different from 2 and 3. Consider the cubic
$$C: \qquad Y^2Z + XYZ = X^3 + a\,XZ^2$$
which contains the point $O = (0 : 1 : 0)$ and the point $P = (0 : 0 : 1)$.

   a) For which a is the cubic smooth.

   b) Write out the formula for the point $P + Q$ where $Q = (x_Q : y_Q : 1) \neq P$.

   c) Use this to verify that $(Q + P) + P = Q$.

4. Consider the cubic $Y^2Z = X^3$ over a field k with its unique singular point $(0 : 0 : 1)$. There is a map $\varphi\colon k \to \mathbb{P}^2(k)$ sending u to $(u : 1 : u^3)$ that has its image in $C(k)$.

   a) Show that the image is precisely all non-singular point in $C(k)$.

   b) Prove that the map is a group homomorphism from $\langle k, +\rangle$ to the group of non-singular points in $C(k)$.

   [Hint: start by checking $\varphi(-u) = -\varphi(u)$ and that $\varphi(u)$, $\varphi(v)$ and $\varphi(-u - v)$ lie on one line.]