**Exercise sheet 5, 11 March 2021**

The addition law on Weierstrass curves $y^2 = x^3 + ax + b$ is given by $\infty$ being the neutral element, $-(x, y) = (x, -y)$ and

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),$$

where

$$\lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} \\ \frac{3x_1^2 + a}{2y_1} \end{cases} \quad \text{for} \quad \begin{cases} P_1 \neq \pm P_2 \\ P_1 = P_2 \neq -P_2 \end{cases}$$

1. Let
$$E/\mathbb{Q} : y^2 = x^3 + 1$$
and observe that $(-1, 0), (0, 1) \in E(\mathbb{Q})$.
   (a) Compute $(-1, 0) + (0, 1)$ using addition law.
   (b) Compute $2(0, 1)$ using the addition law.
   (c) Compute the order of $(0, 1)$. (Note that over the rationals a point need not have finite order, but this one does.

2. Let
$$E_1/\mathbb{F}_{17} : y^2 = x^3 + 1, \qquad E_2/\mathbb{F}_{17} : y^2 = x^3 - 10.$$
and
$$E_3/\mathbb{F}_{17} : y^2 = x^3 + 2x + 5.$$
   (a) Check that
   $$f : (x, y) \mapsto ((x^3 + 4)/x^2, (x^3 y - 8y)/x^3)$$
   defines a map $E_1 \to E_2$.
   (b) Detemine the kernel of $f$.
   (c) What is the degree of $f$?
   (d) Calculate the points in the preimage of $(3, 0)$ under $f$.
   (e) Compute the number of points on $E_1(\mathbb{F}_{17})$, $E_2(\mathbb{F}_{17})$, and $E_3(\mathbb{F}_{17})$.
   (f) Compute $j(E_1)$, $j(E_2)$, and $j(E_3)$.
   (g) Show that $E_1$ and $E_2$ are not isomorphic over $\mathbb{F}_{17}$ but that they are isomorphic over $\mathbb{F}_{17^2}$.

(h) Check that

$$g : (x, y) \mapsto ((x^2 + x + 3)/(x + 1), (x^2 y + 2xy + 15y)/(x^2 + 2x + 1))$$

defines a map $E_1 \to E_3$.

(i) Determinne the kernel of $g$.

(j) What is the degree of $g$?

3. Let $\ell$ be a prime. Show that there are $\ell + 1$ size-$\ell$ subgroups of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.