Elliptic Curves. Sheet 1. To be handed in during 2nd Week.

1. For each of the following elliptic curves, find all the points (including, as always, the point at infinity) over $\mathbb{F}_5$. Draw a complete group table in each case and describe each group as a product of cyclic groups.

(a). $Y^2 = X^3 + 2X$.

(b). $Y^2 = X^3 + 1$.

2. Show that the point $(2, 4)$ is of order 4 on $Y^2 = X^3 + 4X$, defined over $\mathbb{Q}$.

3.

(a). Let $m \in \mathbb{N}$ be odd or $f_m \in (\mathbb{Q}^*)^2$ (or both). Show that the curve

$$Y^2 = f_m X^m + f_{m-1} X^{m-1} + \ldots + f_0, \text{ where all } f_i \in \mathbb{Q} \text{ and } f_m \neq 0,$$

can be birationally transformed over $\mathbb{Q}$ to a curve of the form

$$Y^2 = X^m + g_{m-1} X^{m-1} + \ldots + g_0, \text{ with all } g_i \in \mathbb{Z}.$$

(b). Birationally transform over $\mathbb{Q}$ the curve $Y^2 = \frac{1}{5}X^3 + 3X^2 + 1$ to a curve of the form $Y^2 = X^3 + AX + B$, where $A, B \in \mathbb{Z}$.

4.

(a). Let $p \equiv 2 \pmod 3$ be prime and let $A \in \mathbb{F}_p^*$. Show that the number of points (including the point at infinity) on the curve $Y^2 = X^3 + A$ over $\mathbb{F}_p$ is exactly $p + 1$.

(b). Let $p \equiv 3 \pmod 4$ be prime and let $B \in \mathbb{F}_p^*$. Show that the number of points (including the point at infinity) on the curve $Y^2 = X(X^2 + B)$ over $\mathbb{F}_p$ is exactly $p + 1$.

The following question is compulsory for students taking the MSc in MFoCS (Mathematics and the Foundations of Computer Science). For everyone else, it is optional.

5.

(a). Let $\mathcal{C} : Y^2 = Q(X) = X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$, where all $f_i \in \mathbb{Q}$. Show that the curve $\mathcal{C}$ can be birationally transformed over $\mathbb{Q}$ to a curve of the form $Y^2 = X^3 + AX + B$, where $A, B \in \mathbb{Z}$. [Begin by finding $G(X)$ and $H(X)$ such that $Q(X) = G(X)^2 + H(X)$, with G quadratic and H linear, and let $T = Y + G(X)$, $S = X\big(Y + G(X)\big)$.]

(b). Birationally transform over $\mathbb{Q}$ the curve $\mathcal{C}_1 : Y^2 = 2X^4 + 9$ to the standard form $Y^2 = X^3 + AX + B$, with $A, B \in \mathbb{Z}$. Show that $\mathcal{C}_2 : Y^2 = 2X^4 + 7$ can also be birationally transformed over $\mathbb{Q}$ to the same form. [Hint: In each case, first transform to the form $Y^2 = Q(X)$ of part (a).]

(c). Birationally transform over $\mathbb{Q}(i)$ the curve $Y^2 = -X^4 - 1$ to the standard form $Y^2 = X^3 + AX + B$, with $A, B \in \mathbb{Z}$. Is this possible over $\mathbb{R}$? Is this possible over $\mathbb{Q}(\sqrt{-2})$?