Elliptic Curves. Sheet 6. To be handed in during 7th Week.

1. Find the torsion group over $\mathbb{Q}$ for each of:
(a). $Y^2 = X^3 + 1$.
(b). $Y^2 = X(X-1)(X-2)$.
(c). $Y^2 = X^3 + 1/3^6$.
(d) [optional]. $Y^2 = X^3 - 219X + 1654$.
Note: (d) requires significant computation (you should do an initial search for points with x-coordinate in the range $|x| \leqslant 20$, with $x \in \mathbb{Z}$) and is of course much more time consuming than anything which would be asked in a timed exam. It is mainly intended to demonstrate that interesting torsion groups can occur.

2. Let, as usual, $\mathcal{C} : Y^2 = X(X^2 + aX + b)$ and $\mathcal{D} : Y^2 = X(X^2 + a_1 X + b_1)$, where $a, b \in \mathbb{Z}$, $a_1 = -2a, b_1 = a^2 - 4b$ and $b(a^2 - 4b) \neq 0$. Let $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ denote the set of torsion elements of $\mathcal{C}(\mathbb{Q})$ which have odd order, and let $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ denote the set of torsion elements of $\mathcal{D}(\mathbb{Q})$ which have odd order. Show that $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ and $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ are isomorphic.

3. Let $\mathcal{C}$ and $\mathcal{D}$ be as in question 2. Let the homomorphism $\phi, \hat{\phi}$ be defined as usual by

$$\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x, y) \mapsto \Big(\big(\frac{y}{x}\big)^2, y - \frac{by}{x^2}\Big),$$

$$\hat{\phi} : \mathcal{D}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) : (u, v) \mapsto \Big(\frac{1}{4}\big(\frac{v}{u}\big)^2, \frac{1}{8}\big(v - \frac{b_1 v}{u^2}\big)\Big).$$

What are the preimages of $(0,0)$ under $\hat{\phi}$? Show that $(0,0) \in 2\mathcal{C}(\mathbb{Q})$ if and only if there exist $m, n \in \mathbb{Z}$ such that $b = m^2$ and $a + 2m = n^2$.

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.

4. Show that any elliptic curve over $\mathbb{Q}$ with a rational point of order 4 is birationally equivalent to:

$$Y^2 + XY + vY = X^3 + vX^2,$$

for some $v \in \mathbb{Q}$.