The University of Oxford

MSc (Mathematics and Foundations of Computer Science)

Elliptic Curves

Hilary Term 2015

The steps of (each) miniproject are for your guidance; if you wish to take an alternative route to the desired goal, you are free to do so. But, if you follow the suggested route and find yourself unable to carry out any particular step, you may simply assume it so that you can continue with the miniproject, but should make this assumption clear in your presentation.

Please write or print on one side of the paper only.

This miniproject explores properties of elliptic curves of the form

$$\mathcal{E}_B : Y^2 = X^3 + B$$

where $B \in \mathbb{Z}$ with $B \neq 0$.

(a) For each admissible value of B describe (with proofs) the torsion group of $\mathcal{E}_B(\mathbb{Q})$.

(b) Let $N(x)$ denote the number of integers $B \in \mathbb{N}$ with $B \leq x$, such that $\mathcal{E}_B(\mathbb{Q})$ has positive rank. By constructing appropriate numbers B, show that

$$\liminf_{x \to \infty} \frac{N(x)}{x^{1/2}} > 0.$$

Can you prove such a statement with an exponent larger than 1/2 ? How much larger ? (Take care to ensure that the numbers B you construct are distinct.)

(c) Suppose that (x, y) lies on $\mathcal{E}_B$. By considering $x' = x^{-2}(x^3 + 4B)$ find a point on $\mathcal{E}_{-27B}$. What can you deduce about the ranks of $\mathcal{E}_B(\mathbb{Q})$ and $\mathcal{E}_{-27B}(\mathbb{Q})$?

(d) Given a solution of $u^3 + v^3 = 2k$ show how to construct a point (x, y) on $\mathcal{E}_{-27k^2}$ with $x = 6k/(u+v)$. What can you deduce about the number of solutions $s, t \in \mathbb{Q}$ of an equation of the type $s^3 + t^3 = A$, for a given integer A?

(e) Show that if $a+b = 2$ with $a, b \in \mathbb{Q}$ then there is a rational point (x, y) on $\mathcal{E}_{(ab)^2}$ with $x = -ab$. What do you deduce about representations of $2ab$ as a sum of two cubes of rational numbers? Find a solution $s, t \in \mathbb{Q}$ of $s^3 + t^3 = 6$.

(f) For any $(s, t) \in \mathcal{E}_B(\mathbb{Q})$ with $s, t \in \mathbb{Q}$ and $s = \frac{c}{d}$, $\gcd(c, d) = 1$, let the height function $h_x(s, t)$ be defined, as usual, by:

$$h_x\big((s,t)\big) = \log\max\big(|c|, |d|\big),$$

and define $h_x(\mathbf{o}) = 0$. Find a constant C_1, which depends only on B and $Q \in \mathcal{E}_B(\mathbb{Q})$, such that $h_x(P+Q) \leq 2h_x(P)+C_1$ for all $P \in \mathcal{E}_B(\mathbb{Q})$. Find a constant C_2, which depends only on B, such that $h_x(2P) \geq 4h_x(P) - C_2$ for all $P \in \mathcal{E}_B(\mathbb{Q})$.

(g) Give an example of an elliptic curve $\mathcal{E}_B$ of positive rank, and for which you are able to find generators for $\mathcal{E}_B(\mathbb{Q})$.