The University of Oxford

MSc (Mathematics and Foundations of Computer Science)

Elliptic Curves

Hilary Term 2010

The steps of the 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 consists of two independent parts. You should attempt both.

Part 1

This section of the miniproject is designed to investigate the question — If $\mathcal{E}$ is an elliptic curve defined over $\mathbb{Q}$, to what extent is $\mathcal{E}(\mathbb{Q})$ dense in $\mathcal{E}(\mathbb{R})$ (with the usual topology of $\mathbb{R}^2$)? If there are parts of your analysis that you are unable to make completely rigorous then you should give a partly rigorous argument.

Begin by taking $\mathcal{E}$ in the form $w = z^3 + Aw^2z + Bw^3$. Draw sketches of $\mathcal{E}(\mathbb{R})$ in the cases $A = 1, B = 0$ and $A = -1, B = 0$. Describe the group law geometrically, taking $\mathbf{o} = (0, 0)$. How do you find twice a point, and the inverse of a point? What can you say about points of order 2?

Given $P \in \mathcal{E}(\mathbb{Q})$, when can you say that the sequence $P, 2P, 3P, \ldots$ must contain a convergent subsequence in $\mathcal{E}(\mathbb{R})$? If there is a subsequence tending to one of the points at infinity, show that there is a subsequence converging to $\mathbf{o} = (0, 0)$. Equally, if there is a subsequence tending to a finite point of $\mathcal{E}(\mathbb{R})$, show that there is a subsequence converging to $\mathbf{o}$.

Now suppose a large value of H is chosen. Show that there is a small value $\eta = \eta(H) > 0$ such that the map $(Q, R) \mapsto Q + R$ from

$$\big(\mathcal{E}(\mathbb{R}) \cap [-H, H]^2\big) \times \big(\mathcal{E}(\mathbb{R}) \cap [-\eta, \eta]^2\big)$$

to $\mathcal{E}(\mathbb{R})$ is continuous, and deduce that for any $\varepsilon > 0$ there is a corresponding $\delta > 0$ so that if $Q \in \mathcal{E}(\mathbb{R}) \cap [-H, H]^2$ and $R \in \mathcal{E}(\mathbb{R}) \cap [-\delta, \delta]$ then the distance from $Q + R$ to Q (in the real metric) is at most ε. Show that if in addition $R \neq \mathbf{o}$, then there is a value $\varpi(R) > 0$ such that the distance from $Q + R$ to Q is at least $\varpi(R)$.

Show that, for suitable Q and R, there must be a multiple of R within ε of Q.

What do you conclude about the density of rational points on $\mathcal{E} : y^2 = x^3 + Ax + B$? Give explicit examples where the different cases hold.

Part 2

In this part of the miniproject you will investigate integral points on the elliptic curve $\mathcal{E} : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$.

Show that if $P \in \mathcal{E}(\mathbb{Q})$ and $nP \in \mathcal{E}(\mathbb{Z})$ for some non-zero integer n, then $P \in \mathcal{E}(\mathbb{Z})$. If $n = 2$, show that if $P = (x, y)$ with $y \neq 0$ then $y^2 | \Delta$, where $\Delta = 4A^3 + 27B^2$.

Suppose now that $x^3 + Ax + B$ has three real roots $e_1 < e_2 < e_3$. Show that if P and Q are points on $\mathcal{E}$ with $x(P), x(Q) \geq e_3$ then $x(P + Q) \geq e_3$. Show similarly that if $e_1 \leq x(P), x(Q) \leq e_2$ then $x(P+Q) \geq e_3$. Suppose in addition that $\mathcal{E}(\mathbb{Q})$ has rank 1. Under what additional assumption can you deduce that if $P \in \mathcal{E}(\mathbb{Q})$ has $x(P) \geq e_3$ then $P = 2Q$ for some $P \in \mathcal{E}(\mathbb{Q})$?

Formulate conditions on $\mathcal{E}$ arising from the above considerations, under which you can give an algorithm to determine all integer solutions to $y^2 = x^3 + Ax + B$, and describe your algorithm. How would it help if you knew that $A \equiv 2 \pmod 5$ and $B \equiv 0 \pmod 5$?

Find all integers a and b for which $a(a + 1) = b(b + 1)(b + 2)$. (You may assume that the relevant elliptic curve has rank 1).