The University of Oxford

MSc (Mathematics and Foundations of Computer Science)

Elliptic Curves

Hilary Term 2024

The steps of (each) mini project 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 mini project, but should make this assumption clear in your presentation.

The different parts of this miniproject are largely independent, and are likely to be of quite different lengths. Give clear and precise references to any results you use from the lecture notes, example sheets, books, on-line resources, or elsewhere, and justify all answers. Please include your own examples in addition to those gathered from other sources.

(a) If $\mathcal{E}$ is an elliptic curve defined over $\mathbb{Q}$, we begin by asking whether one can have $\mathcal{E}(\mathbb{F}_p) \cong \mathcal{E}(\mathbb{F}_q)$ for distinct primes p and q. Show by example that this can happen when $p = 5$ and $q = 7$. Prove in contrast that it can never happen for $p = 101$ and $q = 151$.

(b) Suppose that the elliptic curve $\mathcal{E}_{a,b}$ is given by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Give an example of congruence conditions on a and b which will ensure that $\mathcal{E}_{a,b}$ has only trivial torsion (over $\mathbb{Q}$). Deduce that a positive proportion of elliptic curves over $\mathbb{Q}$ have trivial torsion, in the sense that if

$$N(X) := \#\{(a, b) \in \mathbb{Z} : |a|, |b| \leq X, \, \mathcal{E}_{a,b} \text{ has trivial torsion}\}$$

then

$$\liminf_{X \to \infty} X^{-2} N(X) > 0.$$

Do you expect the proportion of curves with non-trivial torsion groups to be positive, or zero? You should discuss your answer, **but you are not expected to prove anything**.

(c) For any integer $n \in \mathbb{N}$ we write $\omega(n)$ to denote the number of distinct prime factors of n, so that $\omega(36) = 2$, for example. Let $\mathcal{E} : y^2 = x(x^2 + ax + b)$ be an elliptic curve with $a, b \in \mathbb{Z}$ satisfying $b > 0$ and $a^2 - 4b > 0$. Show how to give a bound for the rank of $\mathcal{E}$ in terms of $\omega(b)$ and $\omega(a^2 - 4b)$.

If b and $a^2 - 4b$ are distinct primes, under what circumstances can you show that $\mathcal{E}$ must have rank zero? Can you say anything about the rank being zero in the case in which $b = p_1 p_2$ and $a^2 - 4b = p_3$, for distinct primes p_1, p_2, p_3?

Prove that if b and $a^2 - 4b$ are distinct primes, then the torsion group must have size at most 100, and say to what extent this bound can be improved.

(d) Let E_n be the elliptic curve

$$y^2 = x^3 - nx.$$

where n is a non-zero integer.

For a non-zero point $P \in E_n(\mathbb{Q})$, with x-coordinate $x(P) = \frac{p}{q}$ written in lowest terms, we define $h(P) = \log(\max(|p|, |q|))$. We also define $h(O) = 0$.

(i) Let $Q \in E_n(\mathbb{Q})$. Write $Q = (a/d^2, b/d^3)$, where a, b, d are coprime integers. Find explicitly a constant C_1 that depends only on n and Q such that

$$h(P + Q) \leq 2h(P) + C_1$$

for all $P \in E_n(\mathbb{Q})$.

(ii) Find explicitly a constant C_2 that depends only on n such that

$$h(2P) \geq 4h(P) - C_2$$

for all $P \in E_n(\mathbb{Q})$.

(iii) Find as many n as possible such that $E_n(\mathbb{Q})$ has positive rank, and for which you can determine completely a set of generators for $E_n(\mathbb{Q})$.