The University of Oxford

MSc (Mathematics and Foundations of Computer Science)

Elliptic Curves

Hilary Term 2022

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 mini project 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.

Question 1.

(i) Find an $x \in \mathbb{Z}$ such that $|x^2 + 6|_5 < 5^{-3}$.

(ii) Let $\alpha = 1 \cdot 5^{-1} + 2 \cdot 5^0 + 1 \cdot 5^1 + 4 \cdot 5^2 + 1 \cdot 5^3 + 4 \cdot 5^4 + \ldots \in \mathbb{Q}_5$. Express α in the form a/b, where $a, b \in \mathbb{Z}$.

(iii) Determine the primes p for which there exist $x, y \in \mathbb{Z}_p$ such that $y^2 = x^3 + 2x + 2$. Are there $x, y \in \mathbb{Z}$ such that $y^2 = x^3 + 2x + 2$?

(iv) Construct examples of elliptic curves $y^2 = x^3 + f_2x^2 + f_1x + f_0$, where $f_0, f_1, f_2 \in \mathbb{Z}$, which are satisfied by some $x, y \in \mathbb{Z}_p$ with $|y|_p = 1$, for all primes p except $3, 5, 7$. Find other examples of similar types, and explain what method you are using to construct your examples.

Question 2.

(i) Find the torsion group over $\mathbb{Q}$ for the elliptic curve: $Y^2 = X(X + 1)(X + 4)$.

(ii) Find the torsion group over $\mathbb{Q}$ for the elliptic curve:

$Y^2 = X(X+1)(X-8)$.

Are you able to compute this using only reductions modulo p? Are you able to compute this using only the fact that the order of $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ divides the order of every $\widetilde{\mathcal{E}}(\mathbb{F}_p)$? Find other examples of a similar type, explaining how you construct them.

Question 3.

(i) Show that any elliptic curve over $\mathbb{Q}$ with a rational point of order 5 is birationally equivalent to: $Y^2+(1+v)XY+vY = X^3+vX^2$, for some $v \in \mathbb{Q}$.

(ii) Discuss variations of the same idea, for different values of order N. Find elliptic curves over $\mathbb{Q}$ with a point of order N, for various choices of N; for each such curve, compute the whole of the torsion group over $\mathbb{Q}$.

Question 4.

(i) Find the rank of the elliptic curve $Y^2 = X(X^2+6X+1)$.

(ii) Compute the rank of an elliptic curve $Y^2 = X(X^2+aX+b)$ with $a, b \in \mathbb{Z}$ of your own choosing, but where b is divisible by at least three distinct primes. Also compute the rank of an example for which the rank is at least 2.

(iii) For an elliptic curve $Y^2 = X(X^2+aX+b)$, suppose that $b(a^2-4b)$ is divisible by precisely k distinct primes. Give an upper bound on the rank. Are there any conditions on the sign of a, b which allow this bound to be improved? Can you describe any other conditions on a, b which allow the bound to be improved?