Elliptic curves exercise sheet 5

David Holmes

Abstract

Questions 1 and 2 will be graded, the others not. However, you are very strongly recommended to do the other questions.

This is due in on 9/3/2015 before the start of the lecture (13:45), either by email to ellipticcurvesleiden@gmail.com (with subject line EC5) or a physical copy in Giulio Orecchia's mailbox. Please include your student number on your answer sheet.

You may work together on the problems, but please write up your answers separately.

The grade for this work is out of 25. Of this, 20 points are for the content, and 5 points are for clarity and style. This is about mathematical style, not handwriting (though the latter must be legible - if you have terrible handwriting, it may help to use `LATEX`).

0. Read up to page 31 of the online lecture notes (this is approximately what was covered in the lecture, but contains some extra details).

1. Let p be an odd prime and let D be an integer. Consider the curve E_D over $\mathbb{F}_p$ given by $E_D : Y^2Z = X^3 - D^2XZ^2$.

   (a) Show that $(E_D, (0 : 1 : 0))$ is an elliptic curve over $\mathbb{F}_p$ if and only if $p \nmid D$.

   (b) Now suppose that $p \nmid D$. Show that

   $$\#(E_D(\mathbb{F}_p)) = 1 + \sum_{x \in \mathbb{F}_p} \left(\left(\frac{f(x)}{p} \right) + 1 \right)$$

   where $f(x) = x^3 - D^2x$ and $\left(\frac{a}{p}\right)$ denotes the Legendre symbol of a modulo p.

   $$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a nonzero square modulo } p \\ -1 & \text{if } a \text{ is not a square modulo } p \\ 0 & \text{if } a \text{ is zero modulo } p. \end{cases}$$

   The Legendre symbol is multiplicative in its top argument. In other words, for all a, b in $\mathbb{F}_p$,

   $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(c) Now suppose in addition that $p \equiv 3 \pmod 4$. Show that $\left(\frac{f(-x)}{p}\right) = -\left(\frac{f(x)}{p}\right)$. Use this to calculate $\#(E_D(\mathbb{F}_p))$.

2. Consider the sequence 1, 11, 111, 1111, $\cdots$ in $\mathbb{Q}$.

   (a) Show that this sequence converges with respect to $|-|_5$;

   (b) Find the limit of the sequence in $\mathbb{Q}_5$. Hint: the limit lies in $\mathbb{Q} \subseteq \mathbb{Q}_5$.

3. Often, p-adic analysis is much easier than real analysis. Show that a series $\sum_{n=0}^{\infty} a_n$ converges in $\mathbb{Q}_p$ if and only if the sequence $(a_n)_n$ tends to 0 as n tend to ∞.

4. Let $E : y^2 = x^3 + 3x + 5$. an elliptic curve over $\mathbb{Q}$. Let $p = (1 : 3 : 1)$

   (a) Compute $p + p$.

   (b) Compute the images of p, $2p$ and $5p$ in $\overline{E}(\mathbb{F}_5)$. You may use without proof that $5p = (-11/25, 237/125)$.