Elliptic curves exercise sheet 4

David Holmes

Abstract

Questions 1 and 2 will be graded, the others not. However, you are very strongly recommended to do question 3 if you haven't already seen p-adic numbers, as these p-adic absolute values will be used extensively in the course. Question 3 should not be hard, though there are several parts.

This is due in on 2/3/2015 before the start of the lecture (13:45), either by email to ellipticcurvesleiden@gmail.com (with subject line EC4) 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 22 of the online lecture notes (this is approximately what was covered in the lecture, but contains some extra details).

1. Let E be the elliptic curve over $\mathbb{Q}$ given by the equation

$$y^2 = x^3 - 43x + 166.$$

Let p be the point $(3 : 8 : 1)$. Compute

(a) $2 * p$ (i.e. $p + p$);

(b) $4 * p$;

(c) $9 * p$.

2. In the lectures we looked at the 2- (respectively 3-) torsion points on an elliptic curve over a field of characteristic not 2 (respectively not 3). In this question you will do the analogous calculation for the 3-torsion in characteristic 3. Let k be an *algebraically closed* field of characteristic 3, and let

$$E : y^2 = x^3 + ax^2 + bx + c$$

be an elliptic curve over k.

(a) Show that

$$E(k)[3] \cong \mathbb{Z}/3\mathbb{Z} \text{ or } 0;$$

(b) For which values of a, b and c do we have $E(k)[3] \cong 0$?

3. Fix a prime number p. We define a function

$$\operatorname{ord}_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

as follows: First, set $\operatorname{ord}_p(0) = \infty$. Given a non-zero element $r \in \mathbb{Q}$, write $r = p^v a/b$ for integers a, b and v with $p \nmid a$ and $p \nmid b$. Set $\operatorname{ord}_p(r) = v$.

   (a) Show that for all r_1, $r_2 \in \mathbb{Q}$, we have

$$\operatorname{ord}_p(r_1 r_2) = \operatorname{ord}_p(r_1) + \operatorname{ord}_p(r_2)$$

   (here $\infty + x = \infty$ for all x);

   (b) Show that for all r_1, $r_2 \in \mathbb{Q}$, we have

$$\operatorname{ord}_p(r_1 + r_2) \geq \min\left(\operatorname{ord}_p(r_1), \operatorname{ord}_p(r_2)\right).$$

   (here $\infty \geq x$ for all x, with equality iff $x = \infty$). Show that, if $\operatorname{ord}_p(r_1) \neq \operatorname{ord}_p(r_2)$, then this inequality is actually an equality.

Now define

$$||-||_p\colon \mathbb{Q} \to \mathbb{R}$$

by $||r||_p = 1/p^{\operatorname{ord}_p(r)}$. Show that

   (a) $||r||_p \geq 0$, with equality iff $r = 0$;

   (b) $||r_1 r_2||_p = ||r_1||_p ||r_2||_p$;

   (c) $||r_1 + r_2||_p \leq \max\left(||r_1||_p, ||r_2||_p\right)$.

You have just shown that $||-||_p$ is an *absolute value* (see eg. Wikipedia). We call an absolute value that satisfies the 'strong triangle inequality'

$$||r_1 + r_2||_p \leq \max\left(||r_1||_p, ||r_2||_p\right) \qquad (1)$$

a *non-Archimedean absolute value.*