Elliptic curves exercise sheet 3

David Holmes

Abstract

Questions 2 and 3 will be graded, the others not. However, you are very strongly recommended to do question 1, as this kind of computation is really important to be familiar with.

This is due in on 23/2/2015 before the start of the lecture (13:45), either by email to ellipticcurvesleiden@gmail.com (with subject line EC2) or a physical copy in Giulio Orecchia's mailbox. Please include your student number on your answer sheet.

Attempt all questions unless otherwise noted. 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 16 of the online lecture notes (this is approximately what was covered in the lecture, but contains some extra details). This will not be graded.

1. This question is about intersection numbers. If you are not used to working with localisations, please have a look at the 'localisations' handout on the homepage - it will hopefully clarify things, and should make this question much easier.

   We work over $k = \mathbb{Q}$. Consider the plane curves $C = V_y^P$, $D = V_{yz-x^2}^P$, and $E = V_{zy^2-x^3+z^3}^P$. For the pairs (C, D) and (C, E), compute the naive intersections, and also the intersection numbers at each point in the naive intersection over $\bar{\mathbb{Q}}$.

   Now compute all the pairwise intersection numbers of these two pairs curves - please don't use Bezoult's theorem (if we reached this, or if you have read to there in the notes).

   *Slightly harder, optional: do the same for (D, E).

2. In this question we show that the group law sends rational points to rational points. Let k be a field and $\bar{k}$ an algebraic closure. Let (E, O) be an elliptic curve over k. Let L be a line in $\mathbb{P}_k^2$. By Bezoult we know that the intersection number of L and E is three. Write $L \cdot E = [p] + [q] + [r]$, where p, q and r are (not necessarily distinct) points of $\mathbb{P}_k^2(\bar{k})$. Show that, if any two of p, q and r lie in k then the same holds for the third point.

   [For this question, you may use without proof that the intersection pairing is invariant under linear automorphisms of $\mathbb{P}_k^2$ (see last week's homework).]

3. Let E be the elliptic curve over $\mathbb{F}_3$ given by the equation

$$y^2 = x^3 + x + 1.$$

Let p denote the point $(1 : 0 : 1)$. Define $2p = p + p, \cdots, np = p + (n-1)p$.

(a) Compute $2p$;

(b) Compute $3p$;

(c) Compute $4p$;

(d) List all the points of $E(\mathbb{F}_3)$.

4. * This question is optional, and assumes more knowledge of algebraic geometry. Let k be a field, and let (C, O) be a pair of a smooth projective geometrically connected curve C of genus 1 over k and a point $O \in C(k)$. Use the Riemann-Roch theorem to construct a canonical bijection from $C(k)$ to the set of divisors on C modulo linear equivalence. This makes $C(k)$ into a group. Show that this group law coincides with the one defined in the course. This is the slick way to prove associativity of the group law we gave.