Elliptic curves exercise sheet 6

David Holmes

Abstract

Giulio is away this week, so all solutions must be emailed to him at ellipticcurvesleiden@gmail.com (either latex or a scan).

Questions 3 and 4 will be graded, the others not. However, you are very strongly recommended to do the other questions, if you are not already very familiar with Hensel's lemma.

This is due in on 16/3/2015 before the start of the lecture (13:45). **Giulio is away this week, so all solutions must be emailed to him at ellipticcurvesleiden@gmail.com (either latex or a scan)**. 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 ??? of the online lecture notes (this is approximately what was covered in the lecture, but contains some extra details).

1. Let $f(x) = x^2 + 2x + 2 \in \mathbb{Z}[x]$. How many roots does f have in

   (a) $\mathbb{Z}_2$;

   (b) $\mathbb{Z}_3$;

   (c) $\mathbb{Z}_5$.

2. Let p and q be distinct prime numbers. Show that $\mathbb{Z}_p$ contains a primitive q-th root of unity if and only if $\mathbb{F}_p$ contains a primitive q-th root of unity. [A primitive q-th root of unity is an element ζ such that $\zeta^q = 1$ and $\zeta^d \neq 1$ for all $1 \leq d < q$].

3. (a) What is the cardinality of $\mathbb{Q}_p$?

   (b) What is the cardinality of $\mathbb{Z}_p$?

   (c) Let (E, O) be an elliptic curve over $\mathbb{Q}_p$. What is the cardinality of $E(\mathbb{Q}_p)$? [Warning: be careful when the reduction is singular, especially if $p = 2$].

4. Define a metric on $\mathbb{Q}_p$ by $\mathrm{d}(x, y) = |x - y|_p$. Two weeks ago, you checked this really is a metric. We endow $\mathbb{Q}_p$ with the topology induced by this metric, and we give $\mathbb{Z}_p$ the subspace topology.

In this question, you may use without proof that the 'reduction modulo p^n' maps

$$\mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p = \mathbb{Z}/p^n\mathbb{Z}$$

are continuous, when the right hand side is given the discrete topology. While you do not need to prove this, please try to convince yourself that it is true, at least if $n = 1$.

(a) Is $\mathbb{Q}_p$ compact?

(b) Is $\mathbb{Z}_p$ compact?

(c) Is $\mathbb{Z}_p^\times$ compact?

(d) Is $\mathbb{Z}_p$ closed in $\mathbb{Q}_p$?

(e) Is $\mathbb{Z}_p$ open in $\mathbb{Q}_p$?

(f) Is $\mathbb{Q}_p$ connected?

(g) Is $\mathbb{Z}_p$ connected?