Elliptic curves exercise sheet 11

David Holmes

Abstract

Questions 2 and 3 will be graded, the others not.

This is due in on 11/5/2015 before the start of the lecture (13:45). Please email your solutions to Giulio at ellipticcurvesleiden@gmail.com, or put them in his 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 $\mathtt{LATEX}$).

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. We define the height of a rational number $a \in \mathbb{Q}$ to be the height of the point $(a : 1) \in \mathbb{P}^1(\mathbb{Q})$. Prove that for all $x_1, \ldots x_n \in \mathbb{Q}$, we have $H(x_1 + x_2 + \cdots + x_n) \leq n \cdot H(x_1) \cdots H(x_n)$.

2. Let $p = (p_0 : \cdots : p_n) \in \mathbb{P}^n(\mathbb{Q})$, and $q = (q_0 : \cdots : q_m) \in \mathbb{P}^m(\mathbb{Q})$. Define

$$p \star q = (p_0 q_0 : p_0 q_1 : \cdots : p_n q_m) \in \mathbb{P}^{(m+1)(n+1)-1}(\mathbb{Q}).$$

   Prove that $H(p \star q) = H(p)H(q)$.

3. Define the Veronese map

$$\mathscr{V} : \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1 2(\mathbb{Q})$$

   by

$$\mathscr{V}((a : b), (c : d)) = (ac : ad + bc : bd).$$

   (a) Show this map is well-defined (independent of choice of representatives a, b, c, d).

   (b) Let $P, Q \in \mathbb{P}^1(\mathbb{Q})$, and write $R = \mathscr{V}(P, Q)$. Show that

$$\frac{1}{2} \leq \frac{H(R)}{(H(P), H(Q))} \leq 2.$$