Elliptic curves exercise sheet 12

David Holmes

Abstract

Questions 1 and 2 will be graded, the others not.

This is due in on 18/5/2015 at 13:45 (though note the lecture will be earlier than usual). 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 `LATEX`).

0. Read to the end of the online lecture notes (covers to the end of the proof of MW, but not the factoring stuff, sorry.).

1. Though we only proved it in class for $n = 1$, the following theorem holds for all n with a similar proof:

   Theorem 0.1. *Let $n \geq 0$ and $d > 1$. Let $f_0, \cdots, f_n \in \mathbb{Q}[x_0, \cdots, x_n]$ be homogeneous polynomials of degree d such that the intersection $\bigcap_i V_{f_i}^P$ is empty. Define*

   $$f \colon \mathbb{P}^n(\mathbb{Q}) \to \mathbb{P}^n(\mathbb{Q}) \tag{1}$$

   by the formula $f(p) = (f_0(p) : f_1(p) : \cdots : f_n(p))$. Then there exists a constant $c \geq 0$ such that for all $p \in \mathbb{P}^n(\mathbb{Q})$, we have

   $$|\mathrm{h}(f(p)) - d\,\mathrm{h}(p)| \leq c. \tag{2}$$

   In the remainder of this question, you may assume this theorem. In the following questions, we use the notation of the theorem.

   (a) Write $f^{[0]}(p) \stackrel{\text{def}}{=} p$, and $f^{[r+1]}(p) \stackrel{\text{def}}{=} f(f^{[r]}(p))$. Show that the limit

   $$\hat{h}(p) \stackrel{\text{def}}{=} \lim_{r \to \infty} \frac{h(f^{[r]}(p))}{d^r}$$

   exists, and that there exists a constant b such that for all $p \in \mathbb{P}^n(\mathbb{Q})$, we have

   $$|h(p) - \hat{h}(p)| \leq b.$$

(b) We say that a point $p \in \mathbb{P}^n(\mathbb{Q})$ is preperiodic if there exists $M, N > 0$ such that for all $i > N$, we have

$$f^{[i]}(p) = f^{[i+M]}(p).$$

Show that for any $p \in \mathbb{P}^n(\mathbb{Q})$, p is preperiodic if and only if $\hat{h}(p) = 0$.

(c) Define a map $f : \mathbb{P}^2(\mathbb{Q}) \setminus \{(0 : 1 : 0)\} \to \mathbb{P}^2(\mathbb{Q})$ by $f((x : y : z)) = (x^2 : xy : z^2)$. Show that there are infinitely many distinct points $p \in \mathbb{P}^2(\mathbb{Q})$ such that $h(p) = h(f(p))$. Why does this not contradict the theorem?

2. Use Pollard's algorithm to find a prime factor of the integer 11861. At each step 2, please choose $a = 19$ (to avoid any 'cheating'). For this question, you can use the online MAGMA calculator at `http://magma.maths.usyd.edu.au/calc/`. Some helpful commands include GCD(x,y) for the greatest common divisor, and 'x mod y' for reducing an integer modulo another integer.

   Please don't just hand in the factor! You are expected to show your working to some extent. Please include a copy of whatever code you ran in MAGMA (or whatever software you prefer).

   Note that you may need to think a bit to compute a^l in step 4.