Elliptic Curves - Homework 1

Francesco Minnocci

November 25, 2024

4.

(a) We proceed by contradiction: suppose that some $(a, b) \in (\mathbb{Q}_p)^2$ is a lift of $(0, 0)$ and lies on $E(\mathbb{Q}_p)$, that is

$$\begin{cases} a^2 = b^3 + p \\ a \equiv b \equiv 0 \pmod{p} \end{cases}$$

Then, the second condition implies $v_p(a), v_p(b) \geq 1$, but then by the first condition we find a contradiction:

$$1 = v_p(p) = v_p(a^2 - b^3) \geq \min\{2v_p(a), 3v_p(b)\} \geq 2.$$

(b) Let $n \geq 1$, and take E to be the elliptic over $\mathbb{Q}_p$ with affine equation

$$y^2 = x^3 + p^{2n}$$

Then, $Q \coloneqq (0, p^n)$ is a lift of the point $(0, 0)$ on the reduction of E modulo p and it lies on $E(\mathbb{Q}_p)$. Moreover, E has additive reduction as $\overline{E}$ has affine equation $y^2 = x^3$.

5. (in collaboration with Antonio di Nunzio)

The fact that $E(\mathbb{Q}_p)^{(1)}$ is uniquely m-divisible for all m prime to p implies that, for such m, multiplication by m is injective on $E(\mathbb{Q}_p)^{(1)}$. In other words, the following composition is injective for any m prime to p

$$E(\mathbb{Q}_p)[m] \hookrightarrow E(\mathbb{Q}_p) \twoheadrightarrow E(\mathbb{Q}_p)/E(\mathbb{Q}_p)^{(1)},$$

and the last term is finite by the filtration of $E(\mathbb{Q}_p)$ analysed in class. Thus, we get that

$$\bigcup_{(m,p)=1} E(\mathbb{Q})[m] \subset \bigcup_{(m,p)=1} E(\mathbb{Q}_p)[m] \hookrightarrow E(\mathbb{Q}_p)/E(\mathbb{Q}_p)^{(1)}$$

is finite as well. But then, the set S of prime numbers q different from p such that $E(\mathbb{Q})[q]$ is non-trivial must be finite (since all such q are prime to p), say

$$S = \{q_1, \dots, q_n\}.$$

Therefore, if m is not divisible by any of the q_i, for any point $Q \in E(\mathbb{Q})$ we have

$$mp^kQ = 0 \implies p^kQ = 0$$

for any $k \geq 1$, which means that $E(\mathbb{Q})[mp^k] \subset E(\mathbb{Q})[p^k]$.

We are thus left to show that the m-torsion is finite for all m of the form

$$m = p^k q_1^{e_1} \cdots q_n^{e_n},$$

where $k \geq 1$ and $e_i \geq 0$ for all i. For this, it's enough to take a prime number l different from p and from the q_i. Then, by the same argument as before we get an injection in a finite quotient

$$E(\mathbb{Q})[m] \hookrightarrow E(\mathbb{Q})/E(\mathbb{Q})[l],$$

which concludes the proof.

6.

(a) Take any point Q in $E(\mathbb{Q}_p^{nr})^{(0)}$. Then, by definition its reduction $r(Q)$ is a smooth point of $\overline{E}(\overline{\mathbb{F}}_p)$. We know that, for an algebraically closed field, these smooth points form an abelian group which is isomorphic to either the additive or the multiplicative group of the field, and that both $(\overline{\mathbb{F}}_p, +)$ as well as $(\overline{\mathbb{F}}_p^{\times}, \cdot)$ are m-divisible for all m prime to p.

Thus, there exists a point $\overline{P} \in \overline{E}(\overline{\mathbb{F}}_p)_{\text{smooth}}$ such that $m\overline{P} = r(Q)$, and if $\overline{P}$ has coordinates in $\mathbb{F}_{p^l}$ for some k, we can use Hensel's lemma to lift $\overline{P}$ to a point $P \in E(K_l)$. Now, since the reduction map r is a group homomorphism, we have

$$r(mP) = mr(P) = r(Q) \implies mP - Q \in E(\mathbb{Q}_p^{nr})^{(1)}.$$

If we choose n so that $mP - Q$ lies in the (uniquely) m-divisible group $E(K_n)^{(1)}$, we find some $P' \in E(K_n)^{(1)}$ such tat

$$mP' = mP - Q \iff m(P - P') = Q,$$

and we are done.

(b)

7.

(a) The implication $\Rightarrow$ is trivial, since if $Ш(E)$ is finite group then it is killed by $N = \#Ш(E)$. Conversely, suppose that $NШ(E) = 0$ for some $N > 0$; this implies that

$$Ш(E) = Ш(E)[N],$$

and we have seen in class that $Ш(E)[m]$ is finite for all $m \geq 1$. Thus, $Ш(E)$ is finite.

(b) Let G be the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$. The existence of an isogeny between E and E' gives us an exact sequence

$$0 \to K \to E \to E' \to E$$

of G-modules, where K is the finite kernel of the isogeny. Then, the associated long exact sequence in cohomology yields a commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & K' & \longrightarrow & Ш(E) & \longrightarrow & Ш(E') \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
E'(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, K) & \longrightarrow & H^1(\mathbb{Q}, E) & \longrightarrow & H^1(\mathbb{Q}, E') \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\prod_v E'(\mathbb{Q}_v) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, K) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, E) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, E')
\end{array}$$

Here, v ranges all prime numbers plus the archimedean place, and the vertical maps into the products are given by restriction maps. We can place a zero in the top left because restriction on the H^0 is given by inclusion of the $\mathbb{Q}$-points into the $\mathbb{Q}_v$-points.

Note that the kernel K' is a torsion group killed by the order m of the finite G-module K: indeed, it is a subgroup of $H^1(\mathbb{Q}, K)$, which is an inductive limit of torsion groups each killed by m. Setting K'' to be the cokernel of $Ш(E) \to Ш(E')$, we find an exact sequence of abelian groups

$$0 \to K' \to Ш(E) \to K'' \to 0$$

where K'' is a finite group killed by the order n of $Ш(E')$.

But then $Ш(E)$ must be killed by m times n, and thus point (a) implies the finiteness of $Ш(E)$.