Elliptic Curves - Homework 1

Francesco Minnocci

November 27, 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) If we take E to be the elliptic over $\mathbb{Q}_p$ with (clearly minimal) affine equation

$$y^2 = x^3 + p^4,$$

then $Q \coloneqq (0, p^2)$ is a lift of the point $(0, 0)$ on the reduction of E modulo p which 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, 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

$$\bigcup_{m=p^k q_1^{e_1} \cdots q_n^{e_n}} E(\mathbb{Q})[m] \hookrightarrow E(\mathbb{Q}_l)/E(\mathbb{Q}_l)^{(1)},$$

which concludes the proof.

6.

(a) By definition, the reduction $r(Q)$ of any point $Q \in E(\mathbb{Q}_p^{\mathrm{nr}})^{(0)}$ is a smooth point of $\overline{E}(\overline{\mathbb{F}}_p)$. In the case of bad reduction, we know that $\overline{E}(\overline{\mathbb{F}}_p)_{\mathrm{smooth}}$ is an abelian group isomorphic to either the additive or the multiplicative group of the field, and both $(\overline{\mathbb{F}}_p, +)$ as well as $(\overline{\mathbb{F}}_p^{\times}, \cdot)$ are m-divisible for all m prime to p (although the latter is far from being *uniquely* m-divisible). In the case of good reduction ($\overline{E}(\overline{\mathbb{F}}_p) = \overline{E}(\overline{\mathbb{F}}_p)_{\mathrm{smooth}}$), and have seen that for an elliptic curve over an algebraically closed field multiplication by m is a surjective morphism, so we get m-divisibility as well.

Therefore, there exists a point $\overline{P} \in \overline{E}(\overline{\mathbb{F}}_p)_{\mathrm{smooth}}$ such that $m\overline{P} = r(Q)$, and if $\overline{P}$ has coordinates in $\mathbb{F}_{p^l}$ for some l, 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

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

So, after choosing n so that $mP - Q$ lies in the (uniquely) m-divisible group $E(K_n)^{(1)}$, we find some $R \in E(K_n)^{(1)}$ such tat

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

and we are done.

(b) We give a counterexample for $m = 2$ which works for all p different from 2: as the kernel of multiplication by 2 on an elliptic curve is exactly the group of 2-torsion points, we can take the elliptic curve E over $\mathbb{Q}_p$ with (again, minimal) affine equation

$$y^2 = x^3 - 4x,$$

whose 2-torsion points are the roots $(0,0)$, $(2,0)$ and $(-2,0)$ of the polynomial $(x^3 - 4x)$, plus the point at infinity. This concludes because the curve has good reduction, so $E(\mathbb{Q}_p)^{(0)}$ coincides with $E(\mathbb{Q}_p)$ and multiplication by 2 is not injective by the above.

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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$. The existence of an isogeny between E and E' gives us an exact sequence

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

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

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & E'(\mathbb{Q}) & \xrightarrow{\alpha} & H^1(\mathbb{Q}, K) & \longrightarrow & H^1(\mathbb{Q}, E) & \longrightarrow & H^1(\mathbb{Q}, E') \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\cdots & \longrightarrow & \prod_v E'(\mathbb{Q}_v) & \xrightarrow{\beta} & \prod_v H^1(\mathbb{Q}_v, K) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, E) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, E')
\end{array}$$

Here, v ranges all prime numbers plus the archimedean place, and the vertical maps into the products are given by restriction maps. Modding out by the image of the first map in both rows and taking kernels vertically, we get another commutative diagram with exact rows

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K' & \longrightarrow & Ш(E) & \longrightarrow & Ш(E') & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1(\mathbb{Q}, K)/\mathrm{im}\,\alpha & \longrightarrow & H^1(\mathbb{Q}, E) & \longrightarrow & H^1(\mathbb{Q}, E') & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, K)/\mathrm{im}\,\beta & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, E) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, E') & &
\end{array}$$

Note that the kernel K' is a torsion group killed by the order m of the finite G-module K: indeed, it is a subquotient of $H^1(\mathbb{Q}, K)$, which is an inductive limit of torsion groups each killed by m. We have thus found an exact sequence of abelian groups

$$0 \to K' \to Ш(E) \to K'' \to 0,$$

where $K'' = \mathrm{im}\,(Ш(E) \to Ш(E'))$ is a finite group killed by the order n of $Ш(E')$.

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