Elliptic Curves - Assignment 6

Matteo Durante, s2303760, Leiden University

30th April 2019

Exercise 1

Proof. (a) Since $\Gamma(\mathbb{C}) = 0$, by [1, cor. 6.4] for any $m \in \mathbb{Z}_{>0}$ we have that $E[n] = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Consider the subset of E_{tors} given by $H = \bigcup_{n\in\mathbb{N}} E[2n+1]$. This defines a subgroup since, given any elements $e_{2m+1} \in E[2m+1]$, $e_{2n+1} \in E[2n+1]$, we have that $e_{2m+1} - e_{2n+1} \in E[2(2mn+m+n)+1]$. Also, it is a torsion group.

Since each $E[n]$ is finite but strictly increasing in size with $n \in \mathbb{N}$ and the countably infinite union of finite sets is countably infinite, $E_{tors} = \bigcup_{n\in\mathbb{N}} E[n+1]$ is countably infinite and the same goes for $H \subset E_{tors}$.

Let now $e \in H$. We know that there exists a $n \in \mathbb{N}$ s.t. $e \in E[2n+1]$. Since $2k + (2n+1)m = 1$ for some $k, m \neq 0$, we may set $e' = ke$. By construction, $2e' = e$, hence $H \subset 2H$. □

Proof. (b) By the fundamental theorem of algebra, we know that for any $x \in \mathbb{C}$ we may find a $y \in \mathbb{C}$ s.t. $(x, y) \in E$. Since $\mathbb{C}$ is uncountably infinite, E has uncountably many points. By a previous argument, $E_{tors} = \bigcup_{n\in\mathbb{N}} E[n+1]$ is countably infinite, hence $E \setminus E_{tors}$ is uncountably infinite, which implies that there are infinitely many points with infinite order. Let $e_0 \in E$ be one of these.

Remember that the isogeny $E \xrightarrow{[2]} E$ is surjective, hence there is a point $e_1 \in E$ s.t. $2e_1 = e_0$. Iterating, we get for any $e_n \in E$ a point $e_{n+1} \in E$ s.t. $2e_{n+1} = e_n$.

Consider $h \in H =< e_n \mid n \in \mathbb{N} >$, where $h = \sum_n k_n e_n \neq 0$ can be written s.t. $2 \nmid k_n$ for every $k_n \neq 0$, $n > 0$, as, given $k_n = 2k'_{n-1}$, $k_n e_n = k'_{n-1} e_{n-1}$.

Let m be the maximal n with $k_n \neq 0$. If $m = 0$, $h \in H$ has trivially infinite order, hence we consider $m > 0$. We then see that $2^m h = (\sum_n 2^{m-n} k_n) e_0$ and, since $2^{m-m} k_m = k_m$ is odd while $2 | 2^{m-n} k_n$ for all of the other n, $\sum_n 2^{m-n} k_n \neq 0$ and again h has infinite order.

We have H is a torsion-free group. Also, it is countably infinite because it has a countably infinite system of generators. Since for any $n \in \mathbb{N}$ we have that $2e_{n+1} = e_n$, $e_n \in 2H$, which implies that $H \subset 2H$. □

Proof. (c) Remember that $S = E \setminus E_{tors}$ is uncountably infinite.

Suppose that $(e_i)_{i=0}^n \subset S$ is a finite set of independent elements. Such a set exists, for we may just pick a single element. We will show that we can pick an element $e_{n+1} \in S$ s.t. $(e_i)_{i=0}^{n+1}$ is still a system of independent elements.

Indeed, let $G_n =< e_i \mid i = 0, \dots, n >$. Since it is finitely generated, it is countable, hence for any $m \in \mathbb{Z} \setminus \{0\}$ we have that $[m]^{-1}(G_n)$ is countable and the same goes for $\bigcup_{m\in\mathbb{Z}\setminus\{0\}} [m]^{-1}(G_n)$. Notice that this is the set of elements $e \in E$ s.t. $me \in G_n$, hence $\bigcup_{m\in\mathbb{Z}\setminus\{0\}} [m]^{-1}(G_n)$ is the set of elements of E related to the e_i. By a previous argument, this implies that there exists an element $e_{n+1} \in S \setminus G_n$, hence we may extend our system of independent elements.

Consider now the system of generators of $H = \bigcup_{n\in\mathbb{N}} G_n$ given by $(e_n)_{n\in\mathbb{N}}$. If these elements were not independent, then we would have some relation $\sum k_n e_n = 0$, which is not possible because then, given the maximal index appearing in this equation $m \in \mathbb{N}$, $(e_i)_{i=0}^m$ would not be a system of independent elements.

This implies that $H \cong \bigoplus_{n\in\mathbb{N}} \mathbb{Z}$, which is clearly torsion-free and s.t. $H/2H \cong \bigoplus_{n\in\mathbb{N}} \mathbb{Z}/2\mathbb{Z}$ is infinite. □

Exercise 2

Proof. Observe that the elliptic curve E given by $y^2 = x(x^2+13)$ has a 2-torsion point at $(0,0)$, $a = 0$, $b = 13 \neq 0$, $a^2 - 4b \neq 0$. Referring to [2, lemma 4], we have another elliptic curve E' given by $v^2 = u(u^2 - 52)$, $a' = 0$, $b' = -52$. Also, referring to [2, lemma 4,5], we have two 2-isogenies $E \xrightarrow{\phi} E'$, $E' \xrightarrow{\hat{\phi}} E$ s.t. $[2] = \hat{\phi} \circ \phi$.

Referring to [2, lemma 6,7], to compute $\mathrm{im}(q) \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$ we have to look at the square-free integers r dividing $b' = -52$, i.e. $r \in \{\pm1, \pm2, -4, \pm13, \pm26\}$, and check for which values the diophantine equation given by $r^2 l^4 - 52m^4 = rn^2$ has non-trivial solutions.

First of all, $q((0,0)) = [-52] = [-13]$. Also, for $r = -1$, we find the solution $(2,1,6)$.

Setting $r = \pm2$, the equation becomes $4l^4 - 52m^4 = \pm 2n^2$, whence $2l^4 - 26m^4 = \pm n^2$. It follows that $n = 2k$ for some $k \in \mathbb{Z}$, which gives us $l^4 - 13m^4 = \pm 2k^2$.

We may now assume $\gcd(k,l,m) = d = 1$, for otherwise if $d > 1$ we would have that $d^2|k$ and therefore $(k/d^2, l/d, m/d)$ would be another solution with $\gcd(k/d^2, l/d, m/d) = 1$. Looking at the equation $\mod 8$, since the square residues are $\{0, \pm1\}$, we have that $l^4 \equiv 0, 1 \mod 8$, $-13n^4 \equiv 0, 3 \mod 8$, $\pm 2k^2 \equiv 0, \pm 2 \mod 8$. Checking every combination, we see that there is a solution if and only if they are all $\equiv 0 \mod 8$, which implies that $2|k, l, m$, a contradiction.

It follows that $\mathrm{im}(q) = \{[\pm1], [\pm13]\}$, for $[1] = [-1]^2$, $[13] = [-1][-13]$ and if there were $[\pm26]$ there would also be $[\pm2] = [13][\pm26]$, which is absurd.

We get that $E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \cong \mathrm{im}(q)$ is a group of order 4 generated by the elements corresponding to $[-1]$ and $[-13]$, which are respectively the classes of $(-4, 12)$ and $(0,0)$.

To compute $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$ we have refer again to [2, lemma 6,7] and look at the square-free integers r dividing $b = 13$, that is $r \in \{\pm1, \pm13\}$. We see that that $q((0,0)) = [-13]$ and, setting $r = -1$, the diophantine equation $l^4 + 13m^4 = -n^2$ has a no non-trivial solutions because the left side is always positive, the right one negative. It follows, by a previous reasoning, that $\mathrm{im}(q) = \{[1], [-13]\}$.

We get that $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \cong \mathrm{im}(q)$ has order 2 and it is generated by the class of the point corresponding to $[-13]$, that is $(0,0)$.

Applying [2, lemma 9], we see that a system of generators for $E(\mathbb{Q})/2E(\mathbb{Q})$ is given by the images of $[(0,0)], [(-4,12)] \in E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ and an element which is mapped to $[(0,0)] \in E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$. The former correspond to $[\hat{\phi}(0,0)] = [O]$, which does not contribute, and $[\hat{\phi}(-4,12)] = [(9/4, 51/8)]$, while for the latter we may choose $[(0,0)] \in E(\mathbb{Q})/2E(\mathbb{Q})$ itself.

This implies that $E(\mathbb{Q})/2E(\mathbb{Q})$ is a group of rank 2 and order 4 generated by $\{[(0,0)], [(9/4, 51/8)]\}$. □

References

[1] Silverman James Harris. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.

[2] Bright Martin. *Descent by 2-Isogeny*. 2018.