1.20 26/07/15 - Descent via Two-Isogeny

The following discussion has been adapted from [1, §14] and [2, §3.4].

We will now give another proof of 1.15.9 for elliptic curves E over $\mathbb{Q}$ under the additional hypothesis that there is at least one nontrivial rational 2-torsion point $T \in E[2](\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$. Up to an admissible change of coordinates, we can then assume that $T = (0,0)$ and E has the Weierstrass form

$$E_{a,b} : y^2 = x(x^2 + ax + b)$$

for some $a, b \in \mathbb{Z}$. The discriminant and j-invariant of $E_{a,b}$ are easily seen to be (c.f. 1.9.21)

$$\Delta(E_{a,b}) = 16b^2(a^2 - 4b) \text{ and } j(E_{a,b}) = 256\frac{(a^2 - 3b)^3}{b^2(a^2 - 4b)}.$$

so $E_{a,b}$ defines an elliptic curve iff $b \neq 0$ and $a^2 - 4b \neq 0$. Let us make some easy observations.

Observation 1.20.1. In the above setup,

(a) the point $T = (0,0) \in E_{a,b}(\mathbb{Q})$ is the only point on $E_{a,b}$ with x-coordinate 0, and
(b) the 2-torsion on $E_{a,b}$ is fully split (i.e., we have that $E_{a,b}[2](\mathbb{Q}) \cong_{\mathsf{Ab}} \mathbb{Z}/2 \oplus \mathbb{Z}/2$) iff $x^2 + ax + b \in \mathbb{Q}[x]$ has two rational roots, which happens iff $a^2 - 4b$ is a perfect square.

In fact, we didn't really use any properties of $K = \mathbb{Q}$ so far other than $\operatorname{ch} K \neq 2$.

We wish to study the duplication map $[2] : E \to E$ on E and say something about the cokernel $\operatorname{coker}([2] : E(\mathbb{Q}) \to E(\mathbb{Q}))$. To do this, we'll break up the map [2] into two simpler maps. Let's take a second to review some general algebra formalism that will enable us to do this.

1.20.A Quick Algebra Review

Let's take a second to review some basic terminology involving exact sequences.

Definition 1.20.2. Let $A \xrightarrow{f} B \xrightarrow{g} B$ be a sequence of homomorphisms of abelian groups.

(a) We say that this sequence is a *complex* iff $gf = 0$, which happens iff $\operatorname{Im} f \subset \ker g$.
(b) We say that this sequence is an *exact complex* or *exact at B* iff $\operatorname{Im} f = \ker g$.

A longer sequence of homomorphisms of abelian groups is said to be a complex if the composite of every consecutive pair of morphisms is zero, and it is said to be exact iff it is exact at each term. We will need two basic facts about these objects, which are summarized in

Proposition 1.20.3.

(a) Suppose that $A \xrightarrow{f} B \xrightarrow{g} C$ is an exact sequence. If A and C are finite, then so is B.
(b) Suppose that $A \xrightarrow{f} B \xrightarrow{g} C$ is a sequence of homomorphisms of abelian groups (not necessarily a complex). Then there is an exact sequence of the form

$$0 \to \ker(f) \to \ker(gf) \to \ker(g) \to \operatorname{coker}(f) \to \operatorname{coker}(gf) \to \operatorname{coker}(g) \to 0.$$

Proof. I will leave the proofs of both of these facts as an exercise (2.5.11), and only remark here that the proof of (a) uses nothing more than the First Isomorphism Theorem. ∎

The above proposition suggests a strategy for studying (co)kernels of complicated morphisms. Suppose that $h : A \to C$ is a homomorphism of abelian groups, and we are trying to show that $\ker(h)$ (resp. $\operatorname{coker}(h)$) is finite. One strategy for how we might do this involves breaking h up into two "simpler" maps $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ such that $h = gf$. If we can then show that $\ker(f)$ and $\ker(g)$ are finite (resp. $\operatorname{coker}(f)$ and $\operatorname{coker}(g)$ are finite), then 1.20.3 will be enough to conclude that $\ker(h)$ (resp. $\operatorname{coker}(h)$) is finite.

1.20.B Isogenies

Let's carry out the strategy of §1.20.A for the duplication map $h = [2] : E(\mathbb{Q}) \to E(\mathbb{Q})$. We will start by giving a definition.

Definition 1.20.4 (Isogenies)**.** Let K be a field, and let E_1 and E_2 be elliptic curves over K.

(a) An *isogeny defined over* K (also known as K*-isogeny*) from E_1 to E_2 is a morphism $\phi : E_1 \to E_2$ such that $\phi(\mathscr{O}_1) = \mathscr{O}_2$, where $\mathscr{O}_i$ denotes the origin in E_i for $i = 1, 2$.
(b) We say that E_1 and E_2 are *isogenous over* K (also known as K*-isogenous*) iff there is a nonconstant isogeny $E_1 \to E_2$.

Clearly, the composite of two isogenies is an isogeny. Here's an important

Remark 1.20.5. We haven't quite defined what a morphism of curves is in this course, but for our purposes it suffices to think of a morphism as being a map given by some polynomial functions (or rational functions, when defined).[8] The precise definition of a morphism can be found in, say, [8, Ch. I].

The above definition is slightly strange, but before we say anything more, let's give a few examples.

Example 1.20.6. Let K be a field and $E = E_1$ and E_2 be elliptic curves over K.

(a) The constant map $E_1 \to E_2$ with value $\mathscr{O}$ is always an isogeny, known as the 0-isogeny.
(b) The identity map $[1] : E \to E$ is an isogeny.
(c) The duplication map $[2] : E \to E$ is an isogeny. This is clear by the general form of the duplication formula (1.12.12). Indeed, for any integer $n \in \mathbb{Z}$, the multiplication-by-n morphism $[n] : E \to E$ is an isogeny, as is easily seen by a quick induction using the ideas of 1.12.D (see also 2.2.10). The cases $n = 0, 1$ correspond to (a) and (b) above.
(d) An admissible change of coordinates $\phi : E_1 \to E_2$ is an isogeny. In particular, automorphisms are isogenies. This already shows that there is a difference in general between isogenies defined over a field K and those defined over a bigger field (say $\overline{K}$) in general.

For an example of a map of elliptic curves that is *not* an isogeny, consider the example of translation $\tau_P : E \to E$ by a nontrivial point $P \in E(K) \smallsetminus \{\mathscr{O}\}$; this is a morphism, but it is not an isogeny because it doesn't preserve $\mathscr{O}$.

We'll give many more examples soon, but two can also be found on the exercise sheets (2.5.13 and 2.5.14). Let's now list some facts about isogenies (without proof).

Fact 1.20.7.

(a) An isogeny of elliptic curves $\phi : E_1 \to E_2$ is automatically a group homomorphism. More precisely, if $\phi : E_1 \to E_2$ is an isogeny over K, then for each extension L/K, the map $\phi(L) : E_1(L) \to E_2(L)$ induced by ϕ on the set of L-points is a group homomorphism. (This is very surprising–the fact that *any* polynomial map preserving $\mathscr{O}$ is automatically a homomorphism for the complicated group operation obtained from the chord-and-tangent process! This is part of some sort of "rigidity" package for elliptic curves.)
(b) The relation of being isogenous over K is an equivalence relation. Reflexivity and transitivity are basically clear (one has to argue that a composite of nonconstant isogenies is nonconstant, but this is not hard). What is more surprising is that this relationship is also symmetric; this is harder. Therefore, you should think of two isogenous curves as being "similar" to each other. This is ultimately where the name "isogeny" comes from (iso = same, genus = type).
(c) Associated to every isogeny $\phi : E_1 \to E_2$ is an integer called its *degree*; an isogeny of degree $n \in \mathbb{Z}_{\geq 0}$ is said to be an n*-isogeny*. Roughly speaking, the degree of an isogeny is the size of its kernel (as measured over an algebraic closure $\overline{K}$ of K), i.e., $\deg \phi = \# E_1[\phi](\overline{K})$. (This is not strictly correct; it is correct in characteristic zero, but not in positive characteristic

[8] It would be somewhat strange if in our algebraic theory of curves we somehow had the exponential function showing up!

due to the presence of purely inseparable field extensions.) This degree is multiplicative: if $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_3$ are isogenies, then so is $\psi \circ \phi$ and

$$\deg(\psi \circ \phi) = \deg(\psi) \cdot \deg(\phi).$$

We will not prove these facts, and hence we will also not use them in what follows. However, these results are good to know and will serve as important motivation for what we do below. The interested reader can find a proof of these facts in [8].

Now let $K = \mathbb{Q}$ (actually we will only use that $\operatorname{ch} K \neq 2$), let E/K be an elliptic curve, and consider the duplication map $[2] : E \to E$. By 1.20.6(c), this is an isogeny. By 1.20.7(c) and 1.12.7, we have that $\deg[2] = 4$. Therefore, if we can "break up" [2] into two steps, i.e., as a composite of two isogenies $\phi : E \to E'$ and $\phi' = \hat{\phi} : E' \to E$, each of degree 2, then we could hope to apply the strategy of §1.20.A to reduce the proof of 1.15.9 to showing that $\operatorname{coker} \phi(K)$ and $\operatorname{coker} \phi'(K)$ are finite. This procedure is known as "descent by two-isogeny", and this is exactly what we will do.

At this point, I might as well give you some explicit formulae. Let $a, b \in K$ with $b(a^2 - 4b) \neq 0$, and let $E_{a,b} : y^2 = x(x^2 + ax + b)$ as above, with 2-torsion point $T = (0,0) \in E[2](K) \smallsetminus \{\mathscr{O}\}$. We define $a', b' \in K$ by the formula

$$(a', b') := (-2a, a^2 - 4b), \tag{1.20.8}$$

and we let E' be the elliptic curve $E' = E_{a',b'} : y'^2 = (x')^3 + a'(x')^2 + b'x'$, which has its own two-torsion point $T' = (0,0) \in E'[2](K) \smallsetminus \{\mathscr{O}'\}$. Next, we let $\phi : E \to E'$ be defined by the formula

$$(x, y) \mapsto \left(x + a + \frac{b}{x}, y \cdot \left(1 - \frac{b}{x^2} \right) \right)$$

when $x \neq 0$ and by $\mathscr{O}, T \mapsto \mathscr{O}'$. Note that since the point (x, y) lies on E, we can also write the first coordinate of this map as

$$x + a + \frac{b}{x} = \frac{y^2}{x^2}.$$

Finally, we let $\phi' : E' \to E$ be defined by essentially the same formula except for a few powers of 2; more precisely, by the formula

$$(x', y') \mapsto \left(\frac{1}{4} \left(x' + a' + \frac{b'}{x'} \right), \frac{1}{8} \cdot y' \cdot \left(1 - \frac{b'}{(x')^2} \right) \right)$$

when $x' \neq 0$ and by $\mathscr{O}', T' \mapsto \mathscr{O}$. We will soon show that these formulae work and that $\phi' \circ \phi = [2]_E$, but before that, I should probably spend some time explaining *where* these formulae come from.

One quick note before we do that: if we iterate the map 1.20.8, then we get immediately that

$$(a'', b'') := (-2a', (a')^2 - 4b') = (4a, 16b).$$

Therefore, the resulting curve $E'' : (y'')^2 = (x'')^3 + a''(x'')^2 + b''$ is isomorphic to E via the map $(x'', y'') \mapsto (x''/4, y''/8)$. In other words, the map ϕ' is precisely the same kind of map out of E' that ϕ is out of E, just composed with the isomorphism $E'' \xrightarrow{\sim} E$ to take values in E. This means that ϕ and ϕ' play very symmetric roles. In particular, if we can show that $\operatorname{coker} \phi'(K) = E(K)/\phi'(E'(K))$ is finite, this would automatically mean by symmetry that $\operatorname{coker} \phi(K)$ is finite as well. If we can further prove that $\phi' \circ \phi = [2]_E$, then we have reduced the more difficult problem of showing that $\operatorname{coker}[2](K) = E(K)/2E(K)$ is finite to the simpler problem of showing that $\operatorname{coker} \phi'(K)$ is finite.

1.20.C Motivational Aside

It is now time to explain where the above formulae actually come from. Suppose now that we are working over $K = \mathbb{C}$, and that $E/\mathbb{C}$ is an elliptic curve, which by the discussion in 1.13.A looks like $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. Up to scaling Λ (i.e., homothety, which doesn't change the isomorphism type of the quotient $\mathbb{C}/\Lambda$), we might as well assume that it is generated by 1 and τ with $\operatorname{Im} \tau > 0$, so that

$\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau \subset \mathbb{C}$. As in 1.13.A, we can "visualize" the points of $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ as being the points of a fundamental parallelogram in the lattice Λ, e.g., the parallelogram generated by the vectors 1 and τ.

We are interested in studying the duplication map

$$[2] : E(\mathbb{C}) \to E(\mathbb{C}).$$

The first thing to note is that this map is surjective. This is clear in the plane-mod-lattice picture, since this map just maps each "quarter" of the fundamental parallelogram in the domain isomorphically to the fundamental parallelogram in the codomain. Algebraically, this is also a consequence of 1.19.3, since $K = \mathbb{C}$ is algebraically closed. Since the duplication map $[2] : E(\mathbb{C}) \to E(\mathbb{C})$ is a surjective group homomorphism, it is essentially given by the quotient by its kernel, which in this case is $E[2](\mathbb{C}) = \{\mathscr{O}, T_1, T_2, T_3\}$, where T_1, T_2, T_3 correspond to the points $1/2, \tau/2$, and $(1+\tau)/2$ in the fundamental parallelogram. This subgroup is evidently isomorphic to $\mathbb{Z}/2 \oplus \mathbb{Z}/2$.

But now, instead of directly taking the quotient by $E[2](\mathbb{C})$, we could break this operation up into two steps. We could first take the quotient by the subgroup $\{\mathscr{O}, T\}$ where $T = T_2$, and then take the quotient by the image of $E[2](\mathbb{C})$ in that. Geometrically, this amounts to considering the lattice $\Lambda' := \mathbb{Z} \oplus \mathbb{Z}\tau'$, where $\tau' := \tau/2$ and the "vertical slide" map $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$, which gives rise to a "degree 2" map of the corresponding elliptic curves $\phi : E(\mathbb{C}) \to E'(\mathbb{C})$, where $E'(\mathbb{C}) \cong \mathbb{C}/\Lambda'$. After having done this, we would then consider the lattice $\Lambda'' := (1/2)\mathbb{Z} \oplus \mathbb{Z}\tau'$ and the "horizontal slide" map $\psi : \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda''$, which would give rise to another "degree 2" map of the corresponding elliptic curves $\psi : E'(\mathbb{C}) \to E''(\mathbb{C})$, where $E''(\mathbb{C}) \cong \mathbb{C}/\Lambda''$. Finally, we would note that the lattices Λ'' and Λ are homothetic, and so a simple scaling by two gives us an isomorphism $\mathbb{C}/\Lambda'' \xrightarrow{\sim} \mathbb{C}/\Lambda$, which corresponds to the isomorphism $E''(\mathbb{C}) \to E(\mathbb{C})$ given essentially by $(x'', y'') \mapsto (x''/4, y''/8)$. The composite $\mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$ of ψ with this isomorphism is what we are calling ϕ', and this corresponds exactly to the map $\phi' : E'(\mathbb{C}) \to E(\mathbb{C})$. Geometrically, it is evident that the composition $\phi' \circ \phi$ is multiplication by 2 on $E(\mathbb{C})$, since that's what we designed this composite operation to be. See 1.20.9 for an illustration.

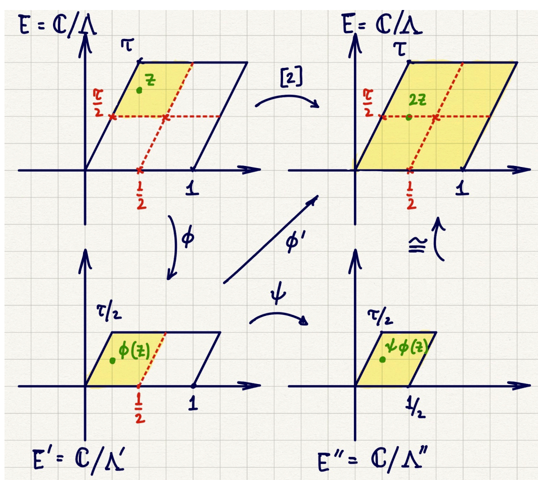

Figure 1.20.9: A diagrammatic representation of the two-isogenies ϕ and ϕ'.

Let's now reconcile this picture with the algebra, so again we have $a, b \in K$ with $b(a^2 - 4b) \neq 0$ and E/K is the elliptic curve $y^2 = x^3 + ax^2 + bx$. This has a 2-torsion point $T = (0,0) \in E[2](K) \smallsetminus \{\mathscr{O}\}$, we wish to take the "quotient" of E by the translation-by-T map $\tau_T : E \to E$. This warrants an exercise.

Exercise 1.20.10. In the above setup, show that the translation-by-T map $\tau_T : E(K) \to E(K)$ is given by the formula

$$P \mapsto P + T = \begin{cases} T & \text{if } P = \mathscr{O}, \\ \mathscr{O} & \text{if } P = T, \text{ and} \\ \left(\dfrac{b}{x}, -\dfrac{by}{x^2}\right) & \text{if } P = (x,y) \in E(K) \smallsetminus \{\mathscr{O}, T\}. \end{cases}$$

Since T is a 2-torsion point, τ_T is an involution, as is also clear from the formula.

If the quotient $\phi : E \to E'$ by $\{\mathscr{O}, T\}$ is given by the formula $\phi(x,y) = (\xi, \eta)$, where $\xi, \eta \in K(E)$, then we would certainly need ϕ to have the property that $\phi(P) = \phi(P+T)$ for all P. In particular, we would need ξ and η to be invariant under the operation τ_T. This suggests what we might take ξ and η to be, as functions of P: we could try, for instance,

$$\xi(P) := x(P) + x(P+T) + a \text{ and } \eta(P) := y(P) + y(P+T). \tag{1.20.11}$$

(The additional a in the formula for ξ is simply to make the formulae a little cleaner, and serves no essential function.) Rewriting these in terms of 1.20.10 gives us precisely the formulae

$$(\xi, \eta) = \left(x + \frac{b}{x} + a, y - \frac{by}{x^2} \right).$$

Now it is a simple check to see that these quantities satisfy the equation

$$\eta^2 = \xi^3 - 2a\xi^2 + (a^2 - 4b)\xi.$$

Exercise 1.20.12. Check this! You will need to use that $y^2 = x^3 + ax^2 + bx$.

This is where the formulae for the elliptic curve E' and the map ϕ come from. Again, it is clear from the geometric picture (1.20.9) that repeating this procedure should just return E up to a change of coordinates involving scaling by $u = 2$, and this is indeed the case, as can be checked easily algebraically.

All of the above discussion was by way of motivation; we will not use these ideas (especially those involving complex lattices) in any serious way. Let's now return to the algebraic formalism.

1.20.D Back to the Properties of Our Two-Isogenies

Let's summarize what we want in

Theorem 1.20.13. Let K be a field of characteristic other than 2, and let $a, b \in K$ with the property $b(a^2 - 4b) \neq 0$. Let $E = E_{a,b}$ be the elliptic curve over K given by $E : y^2 = x^3 + ax^2 + bx$. Let $T := (0,0) \in E[2](K) \smallsetminus \{\mathscr{O}\}$.

Let $a', b' \in K$ be defined by $(a', b') = (-2a, a^2 - 4b)$, and let E'/K be the elliptic curve $E' : y^2 = x^3 + a'x^2 + b'x$, and again let $T' := (0,0) \in E'[2](K) \smallsetminus \{\mathscr{O}'\}$.

Consider the map $\phi : E \to E'$ which on K-points is given by the formula

$$P \mapsto \phi(P) := \begin{cases} \mathscr{O}' & \text{if } P = \mathscr{O}, T, \text{ and} \\ \left(x + a + \frac{b}{x}, y\left(1 - \frac{b}{x^2}\right) \right) & \text{if } P = (x,y) \in E(K) \smallsetminus \{\mathscr{O}, T\}, \end{cases}$$

and indeed by the same formula for every field extension L/K. Similarly, consider the map $\phi' : E' \to E$ which on K-points is given by the formula

$$P' \mapsto \phi'(P') := \begin{cases} \mathscr{O} & \text{if } P' = \mathscr{O}', T', \text{ and} \\ \left(\frac{1}{4}\left(x' + a' + \frac{b'}{x} \right), \frac{1}{8} \cdot y' \left(1 - \frac{b'}{(x')^2}\right) \right) & \text{if } P' = (x', y') \in E'(K) \smallsetminus \{\mathscr{O}', T'\}, \end{cases}$$

and indeed by the same formula for every field extension L/K. Then:

(a) The maps ϕ and ϕ' are well-defined, i.e., the formula for ϕ above does take points on E to E', and similarly for ϕ'.
(b) The map $\phi(K) : E(K) \to E(K)$ induced by ϕ is a group homomorphism with kernel $\{\mathscr{O}, T\}$ (and the same is true for K replaced by any extension L/K). A similar result is true for ϕ'.
(c) We have that $\phi' \circ \phi = [2]_E$, and similarly $\phi \circ \phi' = [2]_{E'}$.

Proof. Note that the formulae for ϕ and ϕ' at least make sense thanks to 1.20.1(a).

(a) This is just a simple algebraic check which is left to the reader (1.20.12 and 1.20.14).

(b) This follows from 1.20.7(a), but since we haven't proven that, we will give a direct proof. Invoking 1.15.5 as in the proofs of 1.18.1 and 1.19.1, it suffices to show that if $P_1, P_2, P_3 \in E(K) \smallsetminus \{\mathscr{O}\}$ are collinear (with multiplicities), then so are $\phi(P_1), \phi(P_2), \phi(P_3)$. Suppose first that none of the P_i are T, and that the line ℓ containing the P_i (which is not vertical) has the equation $\ell : y = \lambda x + \nu$ for some $\lambda, \nu \in K$. Note that since $T \notin \ell(K)$, we must have $\nu \neq 0$. Our goal is to produce $\lambda', \nu' \in K$ such that if ℓ' is the line with equation $\ell' : y' = \lambda' x' + \nu'$, then $\phi(P_1), \phi(P_2)$, and $\phi(P_3)$ are precisely the intersection points of ℓ' with E'. We claim that it suffices to take

$$(\lambda', \nu') := \left(\lambda - \frac{b}{\nu}, \nu - a\lambda + b\frac{\lambda^2}{\nu}\right).$$

It is a straightforward algebraic check to see that this works, and this is left as an exercise (1.20.14); however, see also 1.20.15 below. Finally, it remains only to deal with the case in which exactly one of the P_is is T, say $P_1 = T$ and $P_2, P_3 \notin T$. We have to show in this case that $T + P_2 + P_3 = \mathscr{O}$ in $E(K)$ implies that $\phi(T) + \phi(P_2) + \phi(P_3) = \mathscr{O}'$ in $E'(K)$. Since $\phi(T) = \mathscr{O}'$ by definition, this is equivalent to showing that $\phi(P_2) = -\phi(P_3)$. But indeed, since ϕ obviously plays well with negatives, we have that

$$\phi(P_2) = \phi(-(P_3 + T)) = -\phi(P_3 + T) = -\phi(P_3),$$

where the last equality follows simply because evidently $\phi(P_3) = \phi(P_3 + T)$ (check; see 1.20.10 and 1.20.11).

(c) One can check easily using the results of §1.12.D (e.g., 1.12.12) that both the maps $\phi' \circ \phi$ and $[2]_E$ are given on K-points by the formulae

$$P \mapsto \begin{cases} \mathscr{O} & \text{if } P = \mathscr{O} \text{ or } y(P) = 0, \text{ and} \\ \left(\dfrac{(x^2-b)^2}{4y^2}, \dfrac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{8y^3}\right) & \text{if } P = (x,y) \in E(K) \smallsetminus E[2](K), \end{cases}$$

and indeed that this recipe works on L points for any extension L/K. The proof of the second fact is symmetric. We leave the details to the reader (1.20.14).

■

Exercise 1.20.14. Fill in the gaps in the above proof, i.e., perform all the algebraic checks left to the reader. (Hint: If you get stuck, it may help to look at [2, §3.4].)

Remark 1.20.15. The formulae for (λ', ν') in the proof of part (b) of 1.20.13 may seem to have come out of nowhere. Let me try to explain *how* one might come up with such formulae (which the authors of [2] do not do), so suppose we are in the setting there: $P_1, P_2, P_3 \in E(K) \smallsetminus \{\mathscr{O}\}$ are points which form the intersection of E with the line $\ell : y = \lambda x + \nu$. Let $P_i = (x_i, y_i)$ and $\phi(P_i) = (x_i', y_i')$ for $i = 1, 2, 3$, so that $x_1 x_2 x_3 \neq 0$ and for each i we have

$$x_i' = x_i + a + \frac{b}{x_i} \text{ and } y_i' = y_i\left(1 - \frac{b}{x_i^2}\right).$$

Then x_1, x_2, x_3 are roots of the polynomial

$$g(x) = f(x) - (\lambda x + \nu)^2 = x^3 - (\lambda^2 - a)x^2 + (b - 2\lambda\nu)x - \nu^2.$$

Our first goal is to find $\lambda', \nu' \in K$ so that x_1', x_2', x_3' are roots of the polynomial

$$g'(x) = f'(x) - (\lambda' x + \nu')^2 = x^3 - ((\lambda')^2 - a')x^2 + (b' - 2\lambda'\nu')x - (\nu)'^2,$$

which should exist if we believe 1.20.7(a).[9] From Vieta's formulae applied to $g(x)$, we note that

$$x_1 + x_2 + x_3 = \lambda^2 - a, \quad x_1x_2 + x_1x_3 + x_2x_3 = b - 2\lambda\nu, \text{ and } \quad x_1x_2x_3 = -\nu^2.$$

This allows us to conclude that

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = \frac{b - 2\lambda\nu}{\nu^2},$$

[9] The notation $f'(x)$ and $g'(x)$ here does *not* stand for the derivatives of $f(x)$ and $g(x)$ respectively; sorry about this overloaded notation!

since $\nu \neq 0$. If indeed x_i' are to be roots of $g'(x)$, then we should also have that

$$x_1' + x_2' + x_3' = (\lambda')^2 - a'.$$

But we know how to express the x_i' in terms of the x_i. Indeed, we get from this the equation

$$(\lambda')^2 - a' = \sum_{i=1}^{3} x_i' = \sum_{i=1}^{3} \left(x_i + a + \frac{b}{x_i} \right) = (\lambda^2 - a) + 3a + b\left(\frac{b - 2\lambda\nu}{\nu^2} \right),$$

which along with $a' = -2a$ suggests that we might take

$$\lambda' := \lambda - \frac{b}{\nu}$$

as above. Having obtained this formula for λ', we can easily obtain ν' by simply asking for

$$\nu' := y_i' - \lambda' x_i'$$

for any i and doing some simplification (1.20.14); miraculously, all choices of i give the same formula

$$\nu' = \nu - a\lambda + b\frac{\lambda^2}{\nu}.$$

This is one way one might derive a formula for λ' and ν'.

We have now reduced the proof of 1.15.9 in the case of a nontrivial two-torsion point to showing that the cokernel $\operatorname{coker} \phi(\mathbb{Q})$ is finite, for if we do this, by symmetry, the cokernel $\operatorname{coker} \phi'(\mathbb{Q})$ would also be finite, and hence so would be $\operatorname{coker}[2](\mathbb{Q}) = E(\mathbb{Q})/2E(\mathbb{Q})$ by 1.20.3(b). Of course, our strategy for this will be to produce a group homomorphism α out of $E(\mathbb{Q})$ with the property that $\ker \alpha = \phi'(E'(\mathbb{Q}))$ and that $\operatorname{Im} \alpha$ is finite. This is what we will start with next time.