6 Isogeny kernels and division polynomials

In this lecture we continue our study of isogenies of elliptic curves. Recall that an isogeny is a surjective morphism that is also a group homomorphism, equivalently, a non-constant rational map that fixed the identity. In the previous lecture we showed that every nonzero isogeny $\alpha\colon E_1 \to E_2$ between elliptic curves in short Weierstrass form $y^2 = x^3 + Ax + B$ can be written in the standard affine form

$$\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right),$$

where $u \perp v$ and $s \perp t$ are pairs of relatively prime polynomials in $k[x]$.[1] For any affine point $(x_0, y_0) \in E_1(\bar{k})$, we have $\alpha(x_0, y_0) = 0$ if and only if $v(x_0) = 0$ (equivalently, $t(x_0) = 0$, by Lemma 5.22); this follows from the fact that $\ker\alpha$ is a subgroup, so if $P = (x_0, y_0) \in \ker\alpha$ then so is $-P = (x_0, -y_0)$, and this accounts for every point in $E(\bar{k})$ with x-coordinate x_0. It follows that

$$\ker\alpha = \{(x_0, y_0) \in E_1(\bar{k})\colon v(x_0) = 0\} \cup \{0\}$$

is completely determined by the polynomial $v(x)$ (here $0 = (0 : 1 : 0)$ is the point at infinity).

When α is the multiplication-by-n map $P \mapsto nP = P + \cdots + P$ (which is an isogeny because it is a group homomorphism defined by a non-constant rational map), the kernel of α is the *n-torsion subgroup*

$$E[n] := \{P \in E(\bar{k}) : nP = 0\}.$$

Torsion subgroups play a key role in the theory of elliptic curves. In particular, when $k = \mathbb{F}_q$ is a finite field, the finite abelian group $E(\mathbb{F}_q)$ is completely determined by its intersection with the n-torsion subgroups $E[n]$ (in fact, its intersections with $E[\ell^e]$ for the prime powers ℓ^e that divide $\#E(\mathbb{F}_q)$). Understanding the structure of $E[n]$ will allow us to understand the structure of $E(\mathbb{F}_q)$, and will also turn out to be the key to efficiently computing $\#E(\mathbb{F}_q)$.

6.1 Kernels of isogenies

Recall that we defined the *degree* of an isogeny α in standard form to be $\max\{\deg u, \deg v\}$, and said that α is *separable* whenever $\left(\frac{u}{v}\right)' \neq 0$. We are going to prove that for separable isogenies, the order of the kernel of α is equal to its degree. But first let us dispose of the inseparable case by showing that every isogeny can be decomposed into the composition of a separable isogeny and a power of the p-power Frobenius π (which has trivial kernel).

Lemma 6.1. *Let u and v be relatively prime polynomials in $k[x]$.*

$$\left(\frac{u}{v}\right)' = 0 \iff u' = v' = 0 \iff u = f(x^p) \text{ and } v = g(x^p),$$

where f and g are polynomials in $k[x]$ and p is the characteristic of k (which may be zero).

[1] The assumption that E_1 and E_2 are in short Weierstrass form implies that we are not in characteristic 2 (and rules out some curves in characteristic 3). Most of the results we will prove can be extended to curves in general Weierstrass form and therefore apply to any elliptic curve. Where this is true we will state our theorems generally, but our proofs will use elliptic curves in short Weierstrass form.

Proof. Suppose $\left(\frac{u}{v}\right)' = \frac{u'v - v'u}{v^2} = 0$. Then

$$u'v = v'u.$$

The polynomials u and v have no common roots in $\bar{k}$, therefore every root of u in $\bar{k}$ must also be a root of u', with at least the same multiplicity. But $\deg u' < \deg u$, so this is possible only if $u' = 0$, and by the same argument we must also have $v' = 0$. Conversely, if $u' = v' = 0$ then $u'v = v'u$. This proves the first equivalence.

Now let $u(x) = \sum_n a_n x^n$. If $u'(x) = \sum n a_n x^{n-1} = 0$, then $n a_n = 0$ for every n, which means that n must be a multiple of p for every nonzero a_n (if $p = 0$ this means $u' = 0$). In this case we can write u as

$$u(x) = \sum_m a_{pm} x^{pm} = f(x^p),$$

where $f = \sum_m a_m x^m$. Similarly, if $v'(x) = 0$ then $v(x) = g(x^p)$ for some $g \in k[x]$. Conversely, if $u(x) = f(x^p)$ then $u'(x) = p x^{p-1} f'(x^p) = 0$, and similarly for $v(x)$. □

Corollary 6.2. *Over a field of characteristic zero, every isogeny is separable.*

We now show that every inseparable isogeny arises as the composition of a separable isogeny with some power of the p-power Frobenius map $\pi\colon (x, y, z) \mapsto (x^p, y^p, z^p)$.

Lemma 6.3. *Let $\alpha\colon E_1 \to E_2$ be an inseparable isogeny of elliptic curves*

$$E_1\colon y^2 = x^3 + A_1 x + B_1 \qquad E_2\colon y^2 = x^3 + A_2 x + B_2$$

defined over a field k of characteristic $p > 0$, Then α can be written in the form

$$\alpha = (r_1(x^p), r_2(x^p) y^p)$$

for some rational functions $r_1, r_2 \in k(x)$.

Proof. Let $\alpha(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)} y\right)$ be in standard form. It follows from Lemma 6.1 that $\frac{u(x)}{v(x)} = r_1(x^p)$ for some $r_1 \in k(x)$; we only need to show that $\frac{s(x)}{t(x)} y$ can be put in the form $r_2(x^p) y^p$. As in the proof of Lemma 5.22, substituting u/v and s/t into the equation for E_2 and using the equation for E_1 to eliminate y^2 yields the equality

$$v^3 s^2 f = t^2 w,$$

where $f(x) = x^3 + A_1 x + B_1$ and $w = u^3 + A_2 u v^2 + B_2 v^3$. Since α is inseparable, we have $u' = v' = 0$, hence $w' = 0$, and therefore $\left(\frac{w}{v^3}\right)' = \left(\frac{s^2 f}{t^2}\right)' = 0$. Thus $s(x)^2 f(x) = g(x^p)$ and $t(x)^2 = h(x^p)$, for some polynomials g and h. Every root of $g(x^p)$ in $\bar{k}$ has multiplicity p and the roots of f in $\bar{k}$ are distinct, thus we may write $s^2 f = s_1^2 f^p$, where $s_1 = g_1(x^p)$ for some polynomial g_1 (here we have used the fact that p is odd). We then have

$$(s(x)y)^2 \equiv s(x)^2 f(x) = g_1(x^p)^2 f(x)^p \equiv g_1(x^p)^2 y^p,$$

where the equivalences are modulo the curve equation for E_1. Thus

$$\left(\frac{s(x)}{t(x)} y\right)^2 \equiv \left(\frac{g_1(x^p)}{h(x^p)} y^p\right)^2 = (r(x^p) y^p)^2,$$

where $r(x) = g_1(x)/h(x)$. It follows that $\frac{s(x)}{t(x)} y \equiv r_2(x^p) y^p$ with $r_2 = \pm r$, since two rational functions that agree up to sign at infinitely many points can differ only in sign. □

Corollary 6.4. *Let α be an isogeny over a field k of characteristic $p > 0$. Then*

$$\alpha = \alpha_{\text{sep}} \circ \pi^n$$

for some separable isogeny α_{sep} and integers $n \geq 0$, where π is the p-power Frobenius morphism $(x, y, z) \mapsto (x^p, y^p, z^p)$. We then have $\deg \alpha = p^n \deg \alpha_{\text{sep}}$.

Proof. This holds in general, but we will only prove it for $p > 3$. If α is separable then $\alpha_{\text{sep}} = \alpha$ and $n = 0$, so we now assume α is inseparable. By the lemma, we may write $\alpha = (r_1(x^p), r_2(x^p)y^p)$ for some $r_1, r_2 \in k(x)$. We then have $\alpha = \alpha_1 \circ \pi$, where $\alpha_1 = (r_1(x), r_2(x)y)$. If α_1 is inseparable we apply the same procedure to α_1 (recursively) and eventually obtain $\alpha = \alpha_n \circ \pi^n$ where α_n is a separable isogeny (this process must terminate, since $\deg \alpha$ is finite and the each step reduces the degree by a factor of p). We may then take $\alpha_{\text{sep}} = \alpha_n$. □

Remark 6.5. Note that the isogeny α_{sep} does not necessarily have the same domain as $\alpha \colon E_1 \to E_2$, since the image of π^n is not necessarily E_1 (but π^n will map E_1 to E_1 whenever E_1 is defined over $\mathbb{F}_{p^n}$). Alternatively we could decompose α as

$$\alpha = \pi^n \circ \tilde{\alpha}_{\text{sep}},$$

where the rational functions defining $\tilde{\alpha}_{\text{sep}}$ are obtained from the rational functions defining α_{sep} by taking p^nth roots of each coefficient (note that $x \mapsto x^{p^n}$ is a field automorphism of k, so it has an inverse $x \mapsto x^{1/p^n}$). In the case that α, E_1,E_2 are all defined over $\mathbb{F}_{p^n}$ we will have $\tilde{\alpha}_{\text{sep}} = \alpha_{\text{sep}}$, but not in general.

With $\alpha = \alpha_{\text{sep}} \circ \pi^n$ as in the corollary above, the degree of α_{sep} is called the *separable degree* of α, denoted $\deg_s \alpha$; the *inseparable degree* of α is p^n, and is denoted $\deg_i \alpha$. It follows from the corollary that the degree of α is always the product of its separable and inseparable degrees:

$$\deg \alpha = (\deg_s \alpha)(\deg_i \alpha).$$

The inseparable isogeny π^n has separable degree 1; such isogenies are said to be *purely inseparable.* The degree of a purely inseparable isogeny is always a power of p, but the converse does not hold (as we shall see in the next lecture).

Remark 6.6. Not every purely inseparable isogeny is inseparable; in particular every isogeny of degree 1 is both separable and purely inseparable (this includes all isomorphisms of elliptic curves). The terminology is slightly unfortunate but we are stuck with it. We will generally only be interested in purely inseparable isogenies of degree greater than 1.

We can now prove our first main result.

Theorem 6.7. *The order of the kernel of an isogeny is equal to its separable degree.*

Proof. Let $\alpha = \alpha_{\text{sep}} \circ \pi^n$. Then $\# \ker \alpha = \# \ker \alpha_{\text{sep}}$, since the kernel of π (and hence π^n) is trivial. Thus it suffices to consider the case $\alpha = \alpha_{\text{sep}}$, which we now assume.

Let $\alpha(x, y) = (\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$ be in standard form and pick a point (a, b) in $\alpha(E_1(\bar{k}))$ with $a, b \neq 0$ and such that a is not equal to the ratio of the leading coefficients of u and v (this is possible because $\alpha(E_1(\bar{k})$ is infinite). We now consider the set

$$S(a, b) = \{(x_0, y_0) \in E_1(\bar{k}) : \alpha(x_0, y_0) = (a, b)\}$$

of points in the pre-image of (a,b). Since α is a group homomorphism, $\#S(a,b) = \#\ker\alpha$.

If $(x_0,y_0) \in S(a,b)$ then

$$\frac{u(x_0)}{v(x_0)} = a, \qquad \frac{s(x_0)}{t(x_0)}y_0 = b.$$

We must have $t(x_0) \neq 0$, since α is defined at (x_0,y_0), and $b \neq 0$ implies $s(x_0) \neq 0$. It follows that $y_0 = \frac{t(x_0)}{s(x_0)}b$ is uniquely determined by x_0. Thus to compute $\#S(a,b)$ it suffices to count the number of distinct values of x_0 that occur among the points in $S(a,b)$.

We now let let $g = u - av$ so that $\alpha(x_0,y_0) = (a,b)$ if and only if $g(x_0) = 0$. We must have $\deg g = \deg\alpha$, since a is not equal to the ratio of the leading coefficients of u and v (so their leading terms do not cancel). The cardinality of $S(a,b)$ is then equal to the number of *distinct* roots of g.

Any $x_0 \in \bar{k}$ is a multiple root of g if and only if $g(x_0) = g'(x_0) = 0$, equivalently, if and only if $av(x_0) = u(x_0)$ and $av'(x_0) = u'(x_0)$. If we multiply opposite sides of these equations and cancel the a's we get

$$u'(x_0)v(x_0) = v'(x_0)u(x_0). \tag{1}$$

Now α is separable, so $u'v - v'u \neq 0$ has only a finite number of roots. Since $\alpha(E_1(\bar{k}))$ is infinite and $\#S(a,b) = \#\ker\alpha$ is finite, we may assume that (a,b) was chosen so that (1) is not satisfied for any (x_0,y_0) in $S(a,b)$. Then every root x_0 of g is distinct and we have

$$\#\ker\alpha = \#S(a,b) = \deg g = \deg\alpha,$$

as desired. □

6.2 Isogenies from kernels

We have seen that associated to each isogeny $\alpha\colon E_1 \to E_2$ is a finite subgroup of $E_1(\bar{k})$ whose order is equal to the separable degree of α. It is reasonable to ask whether the converse holds, that is, given a finite subgroup G of $E_1(\bar{k})$ does their exist an isogeny α from E_1 to some elliptic curve E_2 with G as its kernel?

The answer is yes. Moreover, if we restrict our attention to separable isogenies (which we should, since if $\alpha = \alpha_{\text{sep}} \circ \pi^n$ then the purely inseparable isogeny π^n has trivial kernel), the isogeny α and the elliptic curve E_2 are determined up to isomorphism by G.

We have not developed quite enough theory at this point to give a self-contained proof of this result, but it is so striking and so useful that we will take a moment to sketch the proof and give explicit formulas for constructing α and E_2 from G that are due to Velú [2].

Theorem 6.8. *Let E/k be an elliptic curve and let G be a finite subgroup of $E(\bar{k})$. There exists an elliptic curve E' and a separable isogeny $\phi\colon E \to E'$ with $\ker\phi = G$. The curve E' and the isogeny ϕ are defined over a finite extension of k are are unique up to isomorphism.*

We can actually be more precise about the field over which E' and ϕ are defined, it is the minimal extension L/k for which G is invariant under the action of $\mathrm{Gal}(\bar{k}/L)$ (each field automorphism in $\mathrm{Gal}(\bar{k}/k)$ acts on points $P \in E(\bar{k})$ via its action on the coordinates of P); we then say that G is *defined* over L. To say that G is invariant under this action simply means that the image of G under each $\sigma \in \mathrm{Gal}(\bar{k}/L)$ is G; it does *not* mean that every point in G is necessarily fixed by $\mathrm{Gal}(\bar{k}/L)$, which is a stronger condition (so G might be defined over k even though it contains points that are not).

Proof sketch. Given any smooth projective curve C and a finite group G of automorphisms of the curve (invertible morphisms from the curve to itself), there is a smooth projective curve C/G and a surjective morphism $\phi\colon C \to C/G$ that maps each G-orbit $\{\sigma(P) : \sigma \in G\}$ of points $P \in C(\bar{k})$ to a distinct point in C/G. The curve C/G is called the *quotient* of C by G. The standard way to prove this is to use the categorical equivalence of smooth projective curves and their function fields to derive C/G and ϕ from the field embedding

$$k(C)^{G^*} \hookrightarrow k(C),$$

where $k(C)^{G^*}$ denotes the subfield of $k(C)$ fixed by the automorphisms $\sigma^*\colon k(C) \to k(C))$ induced by the automorphisms $\sigma\colon C \to C$ in G (so $\sigma^*(f) = f \circ \sigma$). The map ϕ is separable because $k(C)/k(C)^{G^*}$ is separable, and provided that the group G is defined over k, both ϕ and C/G are defined over k (otherwise base change E to the field of definition of G).

In our situation the curve C is an elliptic curve, and we can associate to each point $P \in E(\bar{k})$ the automorphism $\tau_P\colon Q \mapsto Q + P$, the *translation-by-$P$ map.* Note that τ_P is not an isogeny because it does not fix the point 0 (unless $P = 0$), but it is a morphism $E \to E$, and it has an inverse τ_{-P}, so it is an automorphism. Thus we can associate a group of automorphisms G to any finite subgroup of $E(\bar{k})$ and we then obtain a morphism $\phi\colon E \mapsto E/G$ from E to its quotient by G.

Now from what we have said so far, it's not immediately clear that E/G is actually an elliptic curve, but this is indeed the case. The fact that ϕ is surjective implies that the genus of E/G is at most 1, and the fact that ϕ is unramified (because the G-orbits of $E(\bar{k})$ all have the same size) implies that its genus is equal to 1; this follows from the Hurwitz genus formula [1, II.2.7]. Assuming G is defined over k, the point $\phi(0)$ will be rational and we can take it as our distinguished rational point (and in any case $\phi(0)$ will be defined over the field of definition of E/G). So E/G is an elliptic curve, and $\phi\colon E \to E/G$ is a surjective morphism that fixes the identity and is therefore an isogeny; as noted above, it is separable. The kernel of ϕ is just the G-orbit of 0 in $E(\bar{k})$, which is precisely the subgroup of $E(\bar{k})$ that we started with.

Moreover, if we have another separable isogeny $\phi'\colon E \to E'$ with the same kernel, then we can view $k(E')$ as a subfield of $k(E)$ via the induced embedding $\phi^*\colon k(E') \to k(E)$, and then $k(E')$ is fixed by every automorphism in G. And since ϕ' is separable, we have $[k(E) : k(E')] = \#G$, so $k(E')$ must be (isomorphic to) the fixed field $k(E)^G$. It follows that there exists an isomorphism $\iota\colon E/G \xrightarrow{\sim} E'$ for which $\phi' = \iota \circ \phi$, and the curve E/G and the isogeny ϕ are unique up to such an isomorphism. □

Corollary 6.9. *An isogeny of composite degree can always be decomposed into a sequence of isogenies of prime degree.*

Proof. Let $\alpha\colon E_1 \to E_2$ be an isogeny. If we are working in a field of characteristic $p > 0$, by writing α as $\alpha = \alpha_{\text{sep}} \circ \pi^n$, we can decompose $\pi^n = \pi \circ \cdots \circ \pi$ as a sequence of isogenies of prime degree p. Thus it suffices to consider the case where α is separable. As a nontrivial abelian group, $G = \ker \alpha$ contains a subgroup H of prime order. By the theorem, there exists a separable isogeny $\alpha_1\colon E_1 \to E_3$ with H as its kernel. Then $\alpha_1(G)$ is a finite subgroup of $E_3(\bar{k})$ isomorphic to G/H, and there is a separable isogeny $\alpha_2\colon E_3 \to E_4$ with $\alpha_1(G)$ as its kernel. The kernel of the composition $\alpha_2 \circ \alpha_1$ is $G = \ker \alpha$, so there exists an isomorphism $\iota\colon E_4 \to E_2$ such that $\alpha = \iota \circ \alpha_2 \circ \alpha_1$.

We now proceed by induction and apply the same decomposition to $\iota \circ \alpha_2$, which has smaller degree than α. We eventually obtain a sequence of separable isogenies of prime degree whose composition is equal to α. □

This is all very nice from an abstract point of view, but it is not immediately useful for practical applications. We would really like to have an explicit description of the elliptic curve E/G and the isogeny ϕ. So let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve and let G be a finite subgroup of $E(\bar{k})$. Let $G_{\neq 0}$ denote the set of nonzero points in G, all of which are affine points $Q = (x_Q, y_Q)$, and for each point $P = (x_P, y_P)$ in $E(\bar{k})$ that is not in G, let us define

$$\phi(P) := \left(x_P + \sum_{Q \in G_{\neq 0}} (x_{P+Q} - x_Q)\,,\ y_P + \sum_{Q \in G_{\neq 0}} (y_{P+Q} - y_Q) \right).$$

Here x_P and y_P are variables, x_Q and y_Q are fixed elements of $\bar{k}$, and x_{P+Q} and y_{P+Q} are the affine coordinates of $P + Q$, which we can view as rational functions of x_P and y_P by plugging the coordinates of P and Q into the formulas for the group law.

It's not immediately obvious what the image of this map is, but it is clearly a nonconstant rational map, so it defines a morphism from E to some smooth projective curve E'. Moreover, we can see that the group law on E induces a group law on E' that is defined by rational maps, thus E' is an abelian variety (of dimension one), hence an elliptic curve. For any $P \notin G$ we have $\phi(P) = \phi(P + Q)$ if and only if $Q \in G$, so the kernel of ϕ must be G.

Thus, assuming it is separable, ϕ is the isogeny we are looking for (up to isomorphism). By using the group law to write x_{P+Q} and y_{P+Q} as rational functions in terms of x_P and y_P (and the coordinates of the points in G, which we regard as constants), we can get explicit equations for ϕ and determine an equation for its image E'. The details are somewhat involved (see [3, Thm. 12.16]), so we will just give the formulas. To simplify the expressions we will assume that the order of G is either 2 or odd; this covers all isogenies of prime degree, and by the corollary above, this is sufficient to handle every case.

Theorem 6.10 (Vélu)**.** *Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over k and let $x_0 \in \bar{k}$ be a root of $x^3 + Ax + B$. Define $t := 3x_0^2 + A$ and $w := x_0 t$. The rational map*

$$\phi(x, y) := \left(\frac{x^2 - x_0 x + t}{x - x_0},\ \frac{(x - x_0)^2 - t}{(x - x_0)^2} y \right)$$

is a separable isogeny from E to $E'\colon y^2 = x^3 + A'x + B'$, where $A' := A - 5t$ and $B' := B - 7w$. The kernel of ϕ is the group of order 2 generated by $(x_0, 0)$.

Proof. It is clear that ϕ is a separable isogeny of degree 2 with $(x_0, 0)$ in its kernel. the only thing to check is that E' is it's image, which is an easy verification (just plug the formulas for $\phi(x, y)$ into the equation for E'). □

Remark 6.11. If $x_0 \in k$ then ϕ and E' will both be defined over k, but in general they will be defined over the extension field $k(x_0)$ which contains A' and B'.

Theorem 6.12 (Vélu)**.** *Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over k and let G be a finite subgroup of $E(\bar{k})$ of odd order. For each nonzero $Q = (x_Q, y_Q)$ in G define*

$$t_Q := 3x_Q^2 + A, \qquad u_Q := 2y_Q^2, \qquad w_Q := u_Q + t_Q x_Q,$$

and let

$$t := \sum_{Q \in G_{\neq 0}} t_Q, \qquad w := \sum_{Q \in G_{\neq 0}} w_Q, \qquad r(x) := x + \sum_{Q \in G_{\neq 0}} \left(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right).$$

The rational map

$$\phi(x,y) := \bigl(r(x),\, r'(x)y\bigr)$$

is a separable isogeny from E *to* $E'\colon y^2 = x^3 + A'x + B'$*, where* $A' := A - 5t$ *and* $B' := B - 7w$*, with* $\ker\phi = G$.

Proof. This is a special case of [3, Thm. 12.16]. □

Remark 6.13. The formulas for $t, w, r(x)$ sum over all the nonzero points in G but effectively depend only on the x-coordinates x_Q. Since $|G|$ is odd and $Q = (x_Q, y_Q) \in G$ if and only if $-Q = (x_Q, -y_Q) \in G$, one can sum over half the points in $G_{\neq 0}$ and double the result. The elliptic curve E' and ϕ are defined over any extension L/k where G is defined ($\mathrm{Gal}(\bar{k}/L)$-invariant).

Remark 6.14. Theorem 6.12 implies that (possibly after composing with an isomorphism) we can put any separable isogeny α of odd degree in the form

$$\alpha(x,y) = \left(\frac{u}{w^2}, \left(\frac{u}{w^2}\right)' y\right) = \left(\frac{u}{w^2}, \frac{u'w - 2w'u}{w^3} y\right),$$

for some relatively prime polynomials u and w in $k[x]$.

6.3 Jacobian coordinates

We now turn to the multiplication-by-n map $P \mapsto nP$, which we will denote by $[n]$. We want to write the isogeny $[n]$ in standard form. To do this, it turns out to be more convenient to work with *Jacobian coordinates*, which we now define.

Recall that points in standard projective coordinates are nonzero triples $(x : y : z)$ subject to the equivalence relation

$$(x : y : z) = (\lambda x : \lambda y : \lambda z),$$

for any $\lambda \in k^\times$. We will instead work with the equivalence relation

$$(x : y : z) = (\lambda^2 x : \lambda^3 y : \lambda z),$$

which corresponds to assigning *weights* 2 and 3 to the variables x and y (and leaving z with weight 1). Projective coordinates with these weights are called *Jacobian coordinates*. The homogeneous curve equation for E in Jacobian coordinates then has the form

$$y^2 = x^3 + Axz^4 + Bz^6,$$

which explains the motivation for giving x weight 2 and y weight 3: the leading terms for x and y do not involve z. In Jacobian coordinates, each point $(x : y : z)$ with $z \neq 0$ corresponds to the affine point $(x/z^2, y/z^3)$, and the point at infinity is still $(0 : 1 : 0)$.

Remark 6.15. As an aside, the general Weierstrass form of an elliptic curve in Jacobian coordinates is

$$y^2 + a_1xyz + a_3yz^3 = x^3 + a_2x^2z^2 + a_4xz^4 + a_6z^6,$$

which is a weighted homogeneous equation of degree 6. Each a_i is the coefficient of a term with degree i in z. This explains the otherwise mysterious fact that there is no Weierstrass coefficient a_5.

6.4 The group law in Jacobian coordinates

We now compute formulas for the elliptic curve group law in Jacobian coordinates, beginning with addition. Recall that in affine coordinates, to compute the sum $P_3 = (x_3, y_3)$ of two affine points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ with $P_1 \neq \pm P_2$ we use the formulas

$$x_3 = m^2 - (x_1 + x_2) \quad \text{and} \quad y_3 = m(x_1 - x_3) - y_1,$$

where $m = \frac{y_1 - y_2}{x_1 - x_2}$ is the slope of the line through P_1 and P_2. In Jacobian coordinates we have $P_i = (x_i/z_i^2, y_i/z_i^3)$ and the formula for the x-coordinate becomes

$$\frac{x_3}{z_3^2} = \left(\frac{y_1/z_1^3 - y_2/z_2^3}{x_1/z_1^2 - x_2/z_2^2}\right)^2 - \left(\frac{x_1}{z_1^2} + \frac{x_2}{z_2^2}\right) = \frac{(y_1z_2^3 - y_2z_1^3)^2 - (x_1z_2^2 + x_2z_1^2)(x_1z_2^2 - x_2z_1^2)^2}{(x_1z_2^2 - x_2z_1^2)^2 z_1^2 z_2^2}.$$

This formula can be simplified by using $y_i^2 - x_i^3 = Ax_iz_i^4 + Bz_i^6$ to get rid of the terms in the numerator containing y_i^2 or x_i^3. This makes the numerator divisible by $z_1^2z_2^2$ allowing us to cancel this with the corresponding factor in the denominator. We have

$$\begin{aligned}
\frac{x_3}{z_3^2} &= \frac{(y_1^2z_2^6 - x_1^3z_2^6) + (y_2^2z_1^6 - x_2^3z_1^6) + x_1^2x_2z_1^2z_2^4 + x_1x_2^2z_1^4z_2^2 - 2y_1y_2z_1^3z_2^3}{(x_1z_2^2 - x_2z_1^2)^2z_1^2z_2^2} \\
&= \frac{(Ax_1z_1^4 + Bz_1^6)z_2^6 + (Ax_2z_2^4 + Bz_2^6)z_1^6 + x_1^2x_2z_1^2z_2^4 + x_1x_2^2z_1^4z_2^2 - 2y_1y_2z_1^3z_2^3}{(x_1z_2^2 - x_2z_1^2)^2z_1^2z_2^2} \\
&= \frac{A(x_1z_2^2 + x_2z_1^2)z_1^2z_2^2 + 2Bz_1^4z_2^4 - 2y_1y_2z_1z_2}{(x_1z_2^2 - x_2z_1^2)^2}.
\end{aligned}$$

For the y-coordinate, using $y_3 = m(x_1 - x_3) - y_1 = m(2x_1 + x_2) - m^3 - y_1$ we have

$$\begin{aligned}
\frac{y_3}{z_3^3} &= \left(\frac{y_1/z_1^3 - y_2/z_2^3}{x_1/z_1^2 - x_2/z_2^2}\right)\left(\frac{2x_1}{z_1^2} + \frac{x_2}{z_2^2}\right) - \left(\frac{y_1/z_1^3 - y_2/z_2^3}{x_1/z_1^2 - x_2/z_2^2}\right)^3 - \frac{y_1}{z_1^3} \\
&= \frac{(y_1z_2^3 - y_2z_1^3)(2x_1z_2^2 + x_2z_1^2)(x_1z_2^2 - x_2z_1^2)^2 - (y_1z_2^3 - y_2z_1^3)^3 - y_1z_2^3(x_1z_2^2 - x_2z_1^2)^3}{(x_1z_2^2 - x_2z_1^2)^3z_1^3z_2^3} \\
&= \frac{\cdots}{(x_1z_2^2 - x^2z_1^2)^3}
\end{aligned}$$

Where the missing numerator is some complicated polynomial in $x_1, y_1, z_1, x_2, y_2, z_2, A, B$. These formulas look horrible, but the key point is in Jacobian coordinates we now have

$$z_3 = x_1z_1^2 - x_2z_1^2, \tag{2}$$

which is actually a lot simpler than it would have otherwise been; note that the z-coordinate is the most interesting to us, because it will determine the kernel we are interested in.

The doubling formulas are simpler. In affine coordinates the slope of the tangent line is $m = (3x_1^2 + A)/(2y_1)$. For the x-coordinate we have

$$\frac{x_3}{z_3^2} = \left(\frac{3(x_1/z_1^2)^2 + A}{2y_1/z_1^3}\right)^2 - 2\frac{x_1}{z_1^2} = \frac{(3x_1^2 + Az_1^4)^2 - 8x_1y_1^2}{(2y_1z_1)^2} = \frac{x_1^4 - 2Ax_1^2z_1^4 - 8Bx_1z_1^6 + A^2z_1^8}{(2y_1z_1)^2}$$

and for the y-coordinate we get

$$\begin{aligned}\frac{y_3}{z_3^3} &= \left(\frac{3(x_1/z_1^2)^2 + A}{2y_1/z_1^3}\right)\frac{3x_1}{z_1^2} - \left(\frac{3(x_1/z_1^2)^2 + A}{2y_1/z_1^3}\right)^3 - \frac{y_1}{z_1^3}\\ &= \frac{12x_1y_1^2(3x_1^2 + Az_1^4) - (3x_1^2 + Az_1^4)^3 - 8y_1^4}{(2y_1z_1)^3}\\ &= \frac{x_1^6 + 5Ax_1^4z_1^4 + 20Bx_1^3z_1^6 - 5A^2x_1^2z_1^8 - 4ABx_1z_1^{10} - (A^3 + 8B^2)z_1^{12}}{(2y_1z_1)^3}.\end{aligned}$$

Thus

$$z_3 = 2y_1z_1. \tag{3}$$

6.5 Division polynomials

We now wish to apply our addition formulas to a "generic" point $P = (x : y : 1)$ on the elliptic curve E defined by $y^2 = x^3 + Ax + B$, and use them to compute $2P, 3P, 4P, \ldots, nP$. In Jacobian coordinates, the point nP has the form $(\phi_n : \omega_n : \psi_n)$, where ϕ_n, ω_n, and ψ_n are integer polynomials in x, y, A, B that we reduce modulo the curve equation so that the degree in y is at most 1. In affine coordinates we then have

$$nP = \left(\frac{\phi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3}\right). \tag{4}$$

We will see that ϕ_n and ψ_n^2 do not depend on y, so for fixed A and B they are univariate polynomials in x, and exactly one of ω_n and ψ_n^3 depends on an odd power of y, so this will give us $[n]$ in standard form. The Sage worksheet 18.783 Lecture 6: Division polynomials.sws computes the polynomials ϕ_n, ω_n, ψ_n for the first several values of n.

Remark 6.16. Another way to think of this is to view E as an elliptic curve over $k(E)$. In concrete terms, let F be the fraction field of the ring $k[x, y]/(y^2 - x^3 - Ax - B)$, and let $P = (x, y) \in E(F)$.

The polynomial ψ_n is known as the nth *division polynomial.* So far we have really only defined the ratios ϕ_n/ψ_n^2 and ω_n/ψ_n^3, since we have been working in projective coordinates. In order to nail down ϕ_n ω_n and ψ_n precisely, we make the following recursive definition. Let $\psi_0 = 0$, and define $\psi_1, \psi_2, \psi_3, \psi_4$ to be:

$$\begin{aligned}&\psi_1 = 1,\\ &\psi_2 = 2y,\\ &\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,\\ &\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2).\end{aligned}$$

Note that these are the same polynomials we computed in Sage (up to a sign). We then define the division polynomials ψ_n for integers $n > 4$ via the recurrences

$$\begin{aligned}\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3,\\ \psi_{2n} &= \frac{1}{2y}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2),\end{aligned}$$

where we reduce the result modulo the curve equation so that ψ_n is at most linear in y. It is not difficult to show that $\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$ is always divisible by $2y$, so that ψ_{2n} is in fact a polynomial; see Lemma 6.17 below. If we define $\psi_{-n} := -\psi_n$, one can check that these recurrences hold for all integers n.

We then define ϕ_n and ω_n via

$$\begin{aligned}\phi_n &:= x\psi_n^2 - \psi_{n+1}\psi_{n-1},\\ \omega_n &:= \frac{1}{4y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2).\end{aligned}$$

These equations hold for all integers n, and one finds that $\phi_n = \phi_{-n}$ and $\omega_n = \omega_{-n}$. As above, we reduce ϕ_n and ω_n modulo the curve equation to make them at most linear in y, as noted above.

Lemma 6.17. *For every integer n,*

$$\begin{aligned}&\psi_n \text{ lies in } \begin{cases}\mathbb{Z}[x,A,B] & n \text{ odd}\\ 2y\mathbb{Z}[x,A,B] & n \text{ even},\end{cases}\\ &\phi_n \text{ lies in } \quad \mathbb{Z}[x,A,B] \qquad\qquad \text{for all } n,\\ &\omega_n \text{ lies in } \begin{cases}\mathbb{Z}[x,A,B] & n \text{ even}\\ y\mathbb{Z}[x,A,B] & n \text{ odd}.\end{cases}\end{aligned}$$

Proof. These are easy inductions; see Lemmas 3.3 and 3.4 in Washington [3]. □

It follows from the lemma that, after replacing y^2 with $x^3 + Ax + B$ if necessary, ψ_n^2 lies in $\mathbb{Z}[x,A,B]$ for all positive n, so we think of ϕ_n and ψ_n^2 as a polynomial in x alone, while exactly one of ω_n and ψ_n^3 depends on y. In the latter case we can multiply the numerator and denominator of ω_n/ψ_n^3 by y and then replace y^2 in the denominator with $x^3 + Ax + B$ so that $\omega_n/\psi_n \in y\mathbb{Z}(x,A,B)$. With this understanding, we can view

$$\left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\right)$$

as an isogeny in standard form provided that the numerators and denominators are relatively prime (which we will verify below).

6.6 Multiplication-by-n maps

At this point it is not at all obvious that the polynomials ϕ_n, ω_n,ψ_n defined by our recursive equations actually satisfy equation (4) for nP, but this is indeed the case.

Theorem 6.18. *Let E/k be an elliptic curve defined by the equation $y^2 = x^3 + Ax + B$ and let n be a nonzero integer. The rational map*

$$[n](x,y) = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\right)$$

sends each point $P \in E(\bar{k})$ to nP.

Proof. We have

$$[-n](x,y) = \left(\frac{\phi_{-n}(x)}{\psi_{-n}^2(x)}, \frac{\omega_{-n}(x,y)}{\psi_{-n}^3(x,y)}\right) = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{-\psi_n^3(x,y)}\right) = -\left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\right),$$

so it suffices to consider positive n. The proof given in [3, Thm. 9.33] uses complex analysis and the Weierstrass $\wp$-function, which we will see later in the course. However, as noted in [1, Ex. 3.7], one can give a purely algebraic proof by induction, using the formulas for the group law. This approach has the virtue of being completely elementary and works over any field, but it is computationally intensive (and really should be done with a computer algebra system).[2] Here we will just verify that the formulas for ψ_n are correct.

For $1 \le n \le 4$ the formulas given for ψ_n match our computations in Sage using the group law. To verify the formula for ψ_n when $n = 2m+1 > 4$ is odd, we let P_m be the point $(\phi_m, \omega_m, \psi_m)$ in Jacobian coordinates and compute $P_m + P_{m+1}$ using the group law. The z-coordinate of the sum is given by the formula $z_3 = x_1z_2^2 - x_2z_1^2$ from (2). Substituting ϕ_m for x_1, ψ_m for z_1, ϕ_{m+1} for x_2, and ψ_{m+1} for z_2 yields

$$\phi_m\psi_{m+1}^2 - \phi_{m+1}\psi_m^2,$$

which we wish to show is equal to ψ_{2m+1}. Applying the formulas for ϕ_m and ϕ_{m+1} gives

$$\begin{aligned}\phi_m\psi_{m+1}^2 - \phi_{m+1}\psi_m^2 &= (x\psi_m^2 - \psi_{m+1}\psi_{m-1})\psi_{m+1}^2 - (x\psi_{m+1}^2 - \psi_{m+2}\psi_m)\psi_m^2\\ &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3\\ &= \psi_{2m+1},\end{aligned}$$

To verify the formula for ψ_n when $n = 2m > 4$ is even, we now compute $P_m + P_m$. The z-coordinate of the sum is given by the formula $z_3 = 2y_1z_1$ from (3). We then have

$$\begin{aligned}2\omega_m\psi_m &= 2\cdot\frac{1}{4y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m\\ &= \psi_{2m}.\end{aligned}$$

as desired. This completes the verification for ψ_n. To complete the proof one performs a similar verification for ϕ_n and ω_n using the group law formulas for x_3 and y_3 in Jacobian coordinates that we derived earlier. □

To compute the degree of $[n]\colon E \to E$, we need to know the degrees of the polynomials $\phi_n(x)$ and $\psi_n^2(x)$, and we need to verify that they are relatively prime.

Lemma 6.19. *For every positive integer n the polynomials ϕ_n and ψ_n satisfy*

$$\phi_n(x) = x^{n^2} + \cdots,$$
$$\psi_n(x) = \begin{cases} nx^{\frac{n^2-1}{2}} + \cdots, & n \text{ odd}\\ y\left(nx^{\frac{n^2-4}{2}} + \cdots\right), & n \text{ even.}\end{cases}$$

where each ellipsis hides terms of lower degree in x.

[2] If k has characteristic 2 or 3 one needs to modify the formulas to use a general Weierstrass equation; this changes ψ_2, ψ_3, ψ_4 and the recurrence for ω_n, but the recurrences for ϕ_n and ψ_n are unaffected. Be aware that there are a few typos in the formulas given in [1, Ex. 3.7] on page 105 that are corrected in the errata.

Proof. We first prove the formula for ψ_n by induction on n. By inspection, the formulas hold for $n = 1, 2, 3, 4$. There are then four cases to consider, depending on the value of $n \bmod 4$. For any polynomial $f(x, y)$ we let $\mathrm{lt}_x f$ denote the leading term of f as a polynomial in x.

Case 0: $n \equiv 0 \bmod 4$. Let $n = 2m$, with m even. We have

$$\begin{aligned}
\mathrm{lt}_x \psi_{2m} &= \mathrm{lt}_x \left(\frac{1}{2y} \psi_m (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \right) \\
&= \frac{1}{2y} \cdot ymx^{\frac{m^2-4}{2}} \left(y(m+2)x^{\frac{(m+2)^2-4}{2}} (m-1)^2 x^{\frac{2(m-1)^2-2}{2}} - y(m-2)x^{\frac{(m-2)^2-4}{2}} (m+1)^2 x^{\frac{2(m+1)^2-2}{2}} \right) \\
&= \frac{ym}{2} \left((m-1)^2(m+2)x^{\frac{m^2-4+m^2+4m+4-4+2m^2-4m}{2}} - (m-2)(m+1)^2 x^{\frac{m^2-4+m^2-4m+4-4+2m^2+4m}{2}} \right) \\
&= \frac{ym}{2} \left((m-1)^2(m+2) - (m-2)(m+1)^2 \right) x^{\frac{4m^2-4}{2}} \\
&= y(2m)x^{\frac{4m^2-4}{2}} = ynx^{\frac{n^2-4}{2}}.
\end{aligned}$$

Case 1: $n \equiv 1 \bmod 4$. Let $n = 2m + 1$, with m even. We have

$$\begin{aligned}
\mathrm{lt}_x \psi_{2m+1} &= \mathrm{lt}_x \left(\psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \right) \\
&= \mathrm{lt}_x \left(y(m+2)x^{\frac{(m+2)^2-4}{2}} y^3 m^3 x^{\frac{3m^2-12}{2}} - (m-1)x^{\frac{(m-1)^2-1}{2}} (m+1)^3 x^{\frac{3(m+1)^2-3}{2}} \right) \\
&= (m+2)m^3x^6x^{\frac{m^2+4m+3m^2-12}{2}} - (m-1)(m+1)^3 x^{\frac{m^2-2m+3m^2+6m}{2}} \\
&= (2m+1)x^{\frac{4m^2+4m}{2}} = nx^{\frac{n^2-1}{2}}.
\end{aligned}$$

Here we used the curve equation to replace y^4 with x^6, the leading term of $(x^3 + Ax + B)^2$.

Case 2: $n \equiv 2 \bmod 4$. Let $n = 2m$, with m odd. We have

$$\begin{aligned}
\mathrm{lt}_x \psi_{2m} &= \mathrm{lt}_x \left(\frac{1}{2y} \psi_m (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \right) \\
&= \frac{1}{2y} mx^{\frac{m^2-1}{2}} \left((m+2)x^{\frac{(m+2)^2-1}{2}} y^2 (m-1)^2 x^{\frac{2(m-1)^2-8}{2}} - (m-2)x^{\frac{(m-2)^2-1}{2}} y^2 (m+1)^2 x^{\frac{2(m+1)^2-8}{2}} \right) \\
&= \frac{y}{2} m \left((m+2)(m-1)^2 x^{\frac{m^2-1+(m+2)^2-1+2(m-1)^2-8}{2}} - (m-2)(m+1)^2 x^{\frac{m^2-1+(m-2)^2-1+2(m+1)^2-8}{2}} \right) \\
&= \frac{y}{2} m \left((m+2)(m-1)^2 - (m-2)(m+1)^2 \right) x^{\frac{4m^2-4}{2}} \\
&= y(2m)x^{\frac{4m^2-4}{2}} = ynx^{\frac{n^2-4}{2}}.
\end{aligned}$$

Case 3: $n \equiv 3 \bmod 4$. Let $n = 2m + 1$, with m odd. We have

$$\begin{aligned}
\mathrm{lt}_x \psi_{2m+1} &= \mathrm{lt}_x \left(\psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \right) \\
&= \mathrm{lt}_x \left((m+2)x^{\frac{(m+2)^2-1}{2}} m^3 x^{\frac{3m^2-3}{2}} - y(m-1)x^{\frac{(m-1)^2-4}{2}} y^3 (m+1)^3 x^{\frac{3(m+1)^2-12}{2}} \right) \\
&= (2m+1)x^{\frac{4m^2+4m}{2}} \\
&= nx^{\frac{n^2-1}{2}}.
\end{aligned}$$

Here we have again used the curve equation to replace y^4 with x^6.

Now that we have verified the formulas for ψ_n, we need to check ϕ_n. There are two cases, depending on the parity of n. If n is even we have

$$\begin{aligned}
\mathrm{lt}_x\phi_n &= \mathrm{lt}_x\left(x\psi_n^2 - \psi_{n+1}\psi_{n-1}\right)\\
&= \mathrm{lt}_x\left(xy^2n^2x^{\frac{2n^2-8}{2}} - (n+1)x^{\frac{(n+1)^2-1}{2}}(n-1)x^{\frac{(n-1)^2-1}{2}}\right)\\
&= n^2x^{n^2} - (n^2-1)x^{n^2}\\
&= x^{n^2},
\end{aligned}$$

and if n is odd we have

$$\begin{aligned}
\mathrm{lt}_x\phi_n &= \mathrm{lt}_x\left(x\psi_n^2 - \psi_{n+1}\psi_{n-1}\right)\\
&= \mathrm{lt}_x\left(xn^2x^{n^2-1} - y(n+1)x^{\frac{(n+1)^2-4}{2}}y(n-1)x^{\frac{(n-1)^2-4}{2}}\right)\\
&= n^2x^{n^2} - (n^2-1)x^{n^2}\\
&= x^{n^2},
\end{aligned}$$

where we have used the curve equation to replace y^2 with x^3. □

Corollary 6.20. *For all positive integers n, we have $\psi_n^2(x) = n^2x^{n-1} + \cdots$, where the ellipsis denotes terms of degree less than $n-1$.*

Lemma 6.21. *Let E/k be an elliptic curve defined by $y^2 = x^3 + Ax + B$. The polynomials $\phi_n(x)$ and $\psi_n^2(x)$ are relatively prime.*

Proof. Suppose not. Let $x_0 \in \bar{k}$ be a common root of $\phi_n(x)$ and $\psi_n^2(x)$, and let $P = (x_0, y_0)$ be a nonzero point in $E(\bar{k})$. Then $nP = 0$, since $\psi_n^2(x_0) = 0$, and we also have

$$\begin{aligned}
\phi_n(x_0) &= x_0\psi_n^2(x_0) - \psi_{n+1}(x_0,y_0)\psi_{n-1}(x_0,y_0)\\
0 &= 0 - \psi_{n+1}(x_0,y_0)\psi_{n-1}(x_0,y_0),
\end{aligned}$$

so at least one of $\psi_{n+1}(x_0,y_0)$ and $\psi_{n-1}(x_0,y_0)$ is zero. But then either $(n-1)P = 0$ or $(n+1)P = 0$, and after subtracting $nP = 0$ we see that either $-P = 0$ or $P = 0$, which is a contradiction. □

Theorem 6.22. *Let E/k be an elliptic curve. The multiplication-by-n map $[n]\colon E \to E$ has degree n^2. It is separable if and only it n is not divisible by the characteristic of k.*

Proof. From Lemma 6.19, we have $\deg\phi_n = n^2$ and $\deg\psi_n^2 \le n-1$, and from Lemma 6.21 we know that $\phi_n \perp \psi_n^2$. It follows that $\deg[n] = n^2$. If n is not divisible by the characteristic p of k, then the leading term $n^2x^{n^2-1}$ of $\phi_n'(x)$ is nonzero and therefore

$$\left(\frac{\phi_n(x)}{\psi_n^2(x)}\right)' \neq 0$$

and $[n]$ is separable. If n is divisible by the characteristic of k then the x^{n-1} term in ψ_n^2 vanishes and $\deg\psi_n^2$ is less than n^2-1. This implies that the kernel of $[n]$ is smaller than its degree n^2, and therefore $[n]$ is inseparable. □

References

[1] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, second edition, Springer 2009.

[2] J. Vélu, *Isogénies entre courbe elliptiques*, C. R. Acad. Sci. Paris Séries A **273** (1971), 238–241.

[3] Lawrence C. Washington, *Elliptic Curves: Number Theory and Cryptography*, second edition, Chapman and Hall/CRC, 2008.