In this lecture we continue our study of isogenies and introduce the division polynomials. Recall that an isogeny is a rational map that is also a group homomorphism. In the last 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 as

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

where $u \perp v$ and $s \perp t$ are pairs of relatively prime polynomials in $\bar{k}[x]$.[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 x_0 is a a root of $v(x)$ (recall that v and t always have the same set of roots), and of course $\alpha(0) = 0$. We defined the *degree* of α to be $\max\{\deg u, \deg v\}$, and said that α is *separable* whenever $\left(\frac{u}{v}\right)' \neq 0$.

6.1 The kernel of an isogeny

The polynomial $v(x)$ allows us to determine the points in $E(\bar{k})$ that lie in the kernel of α. Indeed, we have

$$\ker \alpha = \{(x_0, y_0) \in E(\bar{k}) : v(x_0) = 0\} \cup \{0\}.$$

If E_1 is defined by $y^2 = f(x) = x^3 + Ax + B$, then we get one point in $\ker \alpha$ for each root of v that is also a root of f (these are points $(x_0, 0)$ of order 2), two points for every other distinct root of v (since $\alpha(x_0, y_0) = 0$ implies $\alpha(x_0, -y_0) = -\alpha(x_0, y_0) = 0$), and the point 0 (the point at infinity). Thus the polynomial $v(x)$ completely determines $\ker \alpha$, and we will see later in the course that separable isogenies are effectively determined by their kernel.

We now wish to show that when α is separable, the number of points in its kernel is exactly equal to its degree. We first prove an important intermediate result: every nonzero isogeny is surjective.

Theorem 6.1. *Let $\alpha\colon E_1 \to E_2$ be a nonzero isogeny. Then α surjects onto $E_2(\bar{k})$.*

Proof. Let $\alpha = (\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$ be in standard form. Let (a, b) be any nonzero point in $E_2(\bar{k})$, and let f be the polynomial $u - av$. There are two cases:

Case 1: f has a root $x_0 \in \bar{k}$.
Pick $y_0 \in \bar{k}$ so that $(x_0, y_0) \in E_1(\bar{k})$ (this is possible, since $\bar{k}$ is algebraically closed). We have $f(x_0) = u(x_0) - av(x_0) = 0$ with $v(x_0) \neq 0$, since $u \perp v$ implies $f \perp v$. Thus $a = u(x_0)/v(x_0)$, so $\alpha(x_0, y_0) = (a, b') \in E_2(\bar{k})$ for some $b' \in \bar{k}$. If E_2 is defined by the equation $y^2 = x^3 + Ax + B$, then we have

$$b'^2 = a^3 + Aa + B = b^2.$$

Thus $b' = \pm b$ and $(a, b) = \alpha(x_0, \pm y_0)$, so (a, b) lies in the image of α.

Case 2: f has no roots in $\bar{k}$.
This means that f is constant (since $\bar{k}$ is algebraically closed). But u and v cannot both

[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.

be constant, otherwise there would be a point $(u/v, y_0) \in E_2(\bar{k})$ with infinite pre-image in $E_1(\bar{k})$, which is impossible since the kernel of any nonzero isogeny is finite. It follows that a is uniquely determined as the ratio of the leading coefficients of u and v.

Since a is unique, at most two points $(a, \pm b)$ do not lie in the image of α (all others fall into Case 1). Choose $(a', b') = \alpha(P_1)$ so that $(a, b) + (a', b') \neq (a, \pm b)$; this is possible since $E_1(\bar{k})$ and $E_2(\bar{k})$ are infinite. Then $(a, b) + (a', b')$ lies in the image of α and is equal to $\alpha(P_2)$ for some $P_2 \in E_1(\bar{k})$. But then

$$\alpha(P_1 - P_2) = -(a, b) = (a, -b) \qquad \text{and} \qquad \alpha(P_2 - P_1) = (a, b),$$

so (a, b) and $(a, -b)$ are both in the image of α. Therefore α is surjective. □

We now show that the degree of a nonzero separable isogeny is equal to the size of its kernel. More generally, we will prove that the *separable degree* of any nonzero isogeny is equal to the size of its kernel. Recall that every inseprable isogeny α can be uniquely decomposed as $\alpha = \alpha_{\text{sep}} \circ \pi^n$, where α_{sep} is a separable isogeny and $\pi(x, y) = (x^p, y^p)$ is the p-power Frobenius map and p is the characteristic of k. The separable degree of α is defined to be $\deg \alpha_{\text{sep}}$, or simply $\deg \alpha$ when α is separable.

Theorem 6.2. *Let $\alpha\colon E_1 \to E_2$ be a nonzero isogeny. The cardinality of $\ker \alpha$ is equal to the separable degree of α.*

Proof. If $\alpha = \alpha_{\text{sep}} \circ \pi^n$ is inseparable, then $\#\ker \alpha = \#\ker \alpha_{\text{sep}}$, since the kernel of π^n is trivial (if we put π^n in standard form $(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$, then $v(x) = 1$ has no roots), and π^n is surjective, by the previous theorem. Thus it is enough to consider the case where α is separable, which we now assume.

Let α be in standard form $(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$. Let (a, b) be a point in the image of α 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 since the image of α is infinite). We now consider the set

$$S(a, b) = \{(x, y) \in E_1 : \alpha(x, y) = (a, b)\}$$

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 $S(a, b)$.

As in the proof of Theorem 6.1, we let $f = u - av$ so that $\alpha(x_0, y_0) = (a, b)$ if and only if $f(x_0) = 0$. We must have $\deg f = \deg \alpha$, 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 f.

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

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

If α is separable, then $u'v - v'u$ is not the zero polynomial and has only finitely many roots. Thus 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 of f is distinct and $\#S(a, b) = \deg f = \deg \alpha$, as desired. □

For a given elliptic curve E/k, we use $[n]$ to denote the map that sends each point P to the scalar multiple $nP = P + \cdots + P$. This is clearly a group homomorphism, and, since the group operation is defined by rational functions, it is also a rational map and therefore an isogeny. It is an isogeny from E to itself (and therefore an endomorphism). We wish to put the isogeny $[n]$ into standard form. In order to to this it turns out to be more convenient to work with weighted projective coordinates.

6.2 Jacobian coordinates

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

$$(x : y : z) \sim (\lambda x : \lambda y : \lambda z) \qquad (\text{for } \lambda \in \bar{k}^*).$$

We will instead work with the equivalence relation

$$(x : y : z) \sim (\lambda^2 x : \lambda^3 y : \lambda z) \qquad (\text{for } \lambda \in \bar{k}^*),$$

which corresponds to assigning *weights* 2 and 3 to the variables x and y. Projective coordinates with these weights are also 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 6.3. As an aside, the general Weierstrass form of an elliptic curve in Jacobian coordinates is

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

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

6.3 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

$$\begin{aligned}\frac{x_3}{z_3^2} &= \frac{(y_1^2z_2^6 - x_1^3z_2^6) + (y_2^2z_1^6 - x_2^3z_1^6) + x_1^2x_2z_1^2z_2^4 + x_1x_2^2z_1^4z_2^2 - 2y_1y_2z_1^3z_2^3}{(x_1z_2^2 - x_2z_1^2)^2z_1^2z_2^2}\\ &= \frac{(Ax_1z_1^4 + Bz_1^6)z_2^6 + (Ax_2z_2^4 + Bz_2^6)z_1^6 + x_1^2x_2z_1^2z_2^4 + x_1x_2^2z_1^4z_2^2 - 2y_1y_2z_1^3z_2^3}{(x_1z_2^2 - x_2z_1^2)^2z_1^2z_2^2}\\ &= \frac{(Az_1^2z_2^2 + x_1x_2)(x_1z_2^2 + x_2z_1^2) + 2Bz_1^4z_2^4 - 2y_1y_2z_1z_2}{(x_1z_2^2 - x_2z_1^2)^2}.\end{aligned}$$

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

$$\begin{aligned}\frac{y_3}{z_3^3} &= \left(\frac{y_1/z_1^3 - y_2/z_2^3}{x_1/z_1^2 - x_2/z_2^2}\right)\left(\frac{2x_1}{z_1^2} + \frac{x_2}{z_2^2}\right) - \left(\frac{y_1/z_1^3 - y_2/z_2^3}{x_1/z_1^2 - x_2/z_2^2}\right)^3 - \frac{y_1}{z_1^3}\\ &= \frac{(y_1z_2^3 - y_2z_1^3)(2x_1z_2^2 + x_2z_1^2)(x_1z_2^2 - x_2z_1^2)^2 - (y_1z_2^3 - y_2z_1^3)^3 - y_1z_2^3(x_1z_2^2 - x_2z_1^2)^3}{(x_1z_2^2 - x_2z_1^2)^3z_1^3z_2^3}\\ &= \frac{(y_2^3z_1^9 - x_2^3y_2z_1^9) - (y_1^3z_2^9 - x_1^3y_1z_2^9)}{(x_1z_2^2 - x_2z_1^2)^3z_1^3z_2^3} + \frac{2(x_2^3y_1z_1^3 - x_1^3y_2z_2^3) + 3x_1x_2z_1z_2(x_1y_2z_1 - x_2y_1z_2) + 3y_1y_2(y_1z_2^3 - y_2z_1^3)}{(x_1z_2^2 - x_2z_1^2)^3}\\ &= \frac{(Ax_2z_2^4 + Bz_2^6)y_2z_1^9 - (Ax_1z_1^4 + Bz_1^6)y_1z_2^9}{(x_1z_2^2 - x_2z_1^2)^3z_1^3z_2^3} + \frac{2(x_2^3y_1z_1^3 - x_1^3y_2z_2^3) + 3x_1x_2z_1z_2(x_1y_2z_1 - x_2y_1z_2) + 3y_1y_2(y_1z_2^3 - y_2z_1^3)}{(x_1z_2^2 - x_2z_1^2)^3}\\ &= \frac{(Ax_2z_2 + Bz_2^3)y_2z_1^6 - (Ax_1z_1 + Bz_1^3)y_1z_2^6 + 2(x_2^3y_1z_1^3 - x_1^3y_2z_2^3) + 3x_1x_2z_1z_2(x_1y_2z_1 - x_2y_1z_2) + 3y_1y_2(y_1z_2^3 - y_2z_1^3)}{(x_1z_2^2 - x_2z_1^2)^3}\end{aligned}$$

These formulas look quite complicated, but the key point is that we have

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

which is simpler than it would have otherwise been.

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

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

Thus we have

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

6.4 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, and B that we reduce modulo the curve equation so that the degree in y is at most 1. In affine coordinates we then have

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

The sage worksheet 18.783 Lecture 6: Division polynomials.sws computes nP for the first several values of n.

Remark 6.4. Another way to think of this is to view E as an elliptic curve over its function field. In concrete terms, let k be the field $\mathbb{Q}(A, B)$, let F be the fraction field of the ring $k[x, y]/(y^2 - x^3 - Ax - B)$, and consider the point $P = (x, y) \in E(F)$.

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 let $\psi_1, \psi_2, \psi_3, \psi_4$ be as computed in Sage (up to a sign):

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

We then define the division polynomials ψ_n via the recurrences

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

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 $\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$ is always divisible by $2y$, so that ψ_{2m} is a polynomial; see Lemma 6.5 below. The recurrences above hold for all integers m, and one finds that $\psi_{-n} = -\psi_n$ for all 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 we have $\phi_n = \phi_{-n}$ and $\omega_n = \omega_{-n}$. As above, we always reduce ϕ_n and ω_n modulo the curve equation to make them at most linear in y.

Lemma 6.5. *For every integer n,*

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

Proof. These are easy inductions; see Lemmas 3.3 and 3.4 in Washington [2]. □

It follows from the lemma that 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, whereas there is always exactly one of ω_n and ψ_n^3 that depends on y.

6.5 Multiplication-by-n maps

At this point it is not at all obvious that the polynomials ϕ_n, ω_n, and ψ_n actually satisfy equation (4) for nP. But this is indeed the case.

Theorem 6.6. *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 by Washington [2, Thm. 9.33] uses complex analysis and the Weierstrass $\wp$-function, which we will see later in the course However, one can give a purely algebraic proof by induction, using the formulas for the group law (as noted by Silverman [1, Ex. 3.7]). This approach has the virtue of being completely elementary, but it is computationally intensive (and really should be done with a computer algebra system). 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 $z_3 = x_1 z_2^2 - x_2 z_1^2$ 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

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

as desired.

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 $z_3 = 2y_1 z_1$ 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. □

Theorem 6.7. *For every postive 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.

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 mod 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

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

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

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

and if n is odd we have

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

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

Lemma 6.8. *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 in $\bar{k}[x]$.*

Proof. Suppose not. Let x_0 be a common root, 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 $P = 0$. Thus $P = 0$, which is a contradiction. □

Theorem 6.9. *Let E/k be an elliptic curve. The multiplication-by-n map $[n]\colon E \to E$ is an endomorphism of degree n^2. It is separable if and only it n is not divisible by the characteristic of k.*

Proof. The fact that deg $[n] = n^2$ follows immediately from the previous lemma and its corollary. If n is not divisible by the characteristic of p then the leading term $n^2 x^{n^2-1}$ 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 degree of $\psi_n^2(x)$ is strictly smaller than $n^2 - 1$, which implies that the kernel of $[n]$ is smaller than its degree n^2, and therefore $[n]$ is inseparable. □

References

[1] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, second edition, Springer 2009.

[2] L. Washington, *Elliptic curves: number theory and cryptography*, second edition, Chapman & Hall/CRC, 2008 **50**, 50–59.

18.783 Elliptic Curves
Spring 2013