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 $\alpha : E_1 \to E_2$ between elliptic curves in short Weierstrass form $y^2 = x^3 + Ax + B$ can be written as

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

where $u \perp v$ and $s \perp t$ are pairs of relatively prime polynomials in $\bar{k}[x]$. 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 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 $\alpha$ to be $\max\{\deg u, \deg v\}$, and said that $\alpha$ 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 $\alpha$. 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 $\alpha$ 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 $\alpha : E_1 \to E_2$ be a nonzero isogeny. Then $\alpha$ 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 $\alpha$.

**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

---

1The 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 \(\alpha\) (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 \(\alpha\) and is equal to \(\alpha(P_2)\) for some \(P_2 \in E_1(\bar{k})\). But then

\[
\alpha(P_1 - P_2) = -(a, b) = (a, -b) \quad \text{and} \quad \alpha(P_2 - P_1) = (a, b),
\]

so \((a, b)\) and \((a, -b)\) are both in the image of \(\alpha\). Therefore \(\alpha\) is surjective. \(\square\)

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 inseparable isogeny \(\alpha\) can be uniquely decomposed as \(\alpha = \alpha_{\text{sep}} \circ \pi^n\), where \(\alpha_{\text{sep}}\) 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 \(\alpha\) is defined to be \(\deg \alpha_{\text{sep}}\), or simply \(\deg \alpha\) when \(\alpha\) is separable.

**Theorem 6.2.** Let \(\alpha: E_1 \to E_2\) be a nonzero isogeny. The cardinality of \(\ker \alpha\) is equal to the separable degree of \(\alpha\).

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

Let \(\alpha\) 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 \(\alpha\) 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 \(\alpha\) 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 \(\alpha\) is a group homomorphism, \(\#S(a, b) = \# \ker \alpha\).

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

\[
\frac{u(x_0)}{v(x_0)} = a, \quad \frac{s(x_0)}{t(x_0)}y_0 = b.
\]

We must have \(t(x_0) \neq 0\), since \(\alpha\) 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

\[
u'(x_0)v(x_0) = v'(x_0)u(x_0).
\]
If $\alpha$ 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. \hfill $\Box$

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 do 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

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

We will instead work with the equivalence relation

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

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

$$y^2 + a_1 xyz + a_3 yz^3 = x^3 + a_2 x^2 z + a_4 xz^4 + a_6 z^6 ,$$

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

$$x_3 \frac{z_3^2}{z_1^2} = \left( \frac{y_1/z_1^3 - y_2/z_2^3}{x_1/z_1^2 - x_2/z_2^2} \right)^2 - \left( \frac{x_1/z_1^2 + x_2/z_2^2}{z_1^2/z_2^2} \right) = \frac{(y_1/z_1^3 - y_2/z_2^3)^2 - (x_1/z_1^2 + x_2/z_2^2)(x_1/z_1^2 - x_2/z_2^2)^2}{(x_1/z_1^2 - x_2/z_2^2)^2 z_1^2 z_2^2} .$$
This formula can be simplified by using $y_1^2 - x_1^3 = Ax_1z_1^4 + Bz_1^6$ to get rid of the terms in the numerator containing $y_1^4$ or $x_1^3$. This makes the numerator divisible by $z_1z_2$ allowing us to cancel this with the corresponding factor in the denominator. We have

$$
x_3 \div z_3 = \frac{(y_1^2z_2^6 - x_1^3z_2^6) + (y_2^2z_1^6 - x_2^3z_1^6) + x_1^2x_2z_2^2z_1^2 + x_1x_2^2z_1^2z_2^2 - 2y_1y_2z_1^3z_2^3}{(x_1z_2^2 - x_2z_1^2)^2z_1^2z_2^2} = \frac{(Ax_1z_1^4 + Bz_1^6)z_2^6 + (Ax_2^4 + Bz_2^6)z_1^6 + x_1^2x_2z_2^2z_1^2 + x_1x_2^2z_1^2z_2^2 - 2y_1y_2z_1^3z_2^3}{(x_1z_2^2 - x_2z_1^2)^2z_1^2z_2^2} = \frac{(Az_1^2z_2^2 + x_1x_2)(x_1z_2^2 + x_2z_1^2) + 2Bz_1^4z_2^4 - 2y_1y_2z_1z_2}{(x_1z_2^2 - x_2z_1^2)^2}
$$

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

$$
y_3 \div z_3 = \frac{(y_1/z_1^3 - y_2/z_2^3)(2x_1z_2^3 + x_2z_1^3)(x_1z_2^2 + x_2z_1^2)^2 - (y_1z_2^3 - y_2z_1^3)^3}{(x_1z_2^2 - x_2z_1^2)^3z_1^3z_2^3} = \frac{(A_{x_2z_2} + B_{z_2}^6)yz_1^3 - (Ax_1^4 + B_{z_1}^6)y_1z_2^3 + 2(y_2^4z_1^2 - x_1^4y_2^2z_2^2) + 3x_1x_2z_2z_2(x_1y_2z_1 - x_2y_1z_2) + 3y_1z_2(y_1z_2^3 - y_2z_1^3)}{(x_1z_2^2 - x_2z_1^2)^3}
$$

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

$$z_3 = x_1z_1^2 - x_2z_1^2, \quad (2)
$$

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

$$
x_3 \div z_3 = \left\{\frac{3(x_1/z_1^3)^2 + A}{2y_1/z_1^3}\right\}^2 - 2x_1z_1^2 = \frac{(3x_1^2 + A_{z_1}^4)^2 - 8x_1^4z_1^2}{(2y_1z_1)^2} = \frac{x_3^4 - 2Ax_1^2z_1^4 - 8Bx_1z_1^6 + A_{z_1}^8}{(2y_1z_1)^2}
$$

and for the $y$-coordinate we get

$$
y_3 \div z_3 = \frac{3(x_1/z_1^3)^2 + A}{2y_1/z_1^3}z_1 - \left\{\frac{3(x_1/z_1^3)^2 + A}{2y_1/z_1^3}\right\}^3 - y_1/z_1^3 = \frac{3x_1^3 + A_{z_1}^4}{2y_1z_1^3} - \frac{(3x_1^2 + A_{z_1}^4)^3}{(2y_1z_1)^3} - y_1/z_1^3 = \frac{12x_1^3y_1^3(3x_1^2 + A_{z_1}^4) - (3x_1^2 + A_{z_1}^4)^3}{(2y_1z_1)^3} - 8y_1^4 = \frac{x_1^6 + 5Ax_1^4z_1^4 + 20Bx_1^3z_1^6 - 5A_{z_1}^2x_1^2z_1^8 - 4ABx_1z_1^{10} - (A_{z_1}^3 + 8B_{z_1}^2)z_1^{12}}{(2y_1z_1)^3}.
$$

Thus we have

$$z_3 = 2y_1z_1. \quad (3)$$

4
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 \( \phi_n, \omega_n, \) and \( \psi_n \) 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 \( \psi_n \) is known as the \( n \)th division polynomial. So far we have really only defined the ratios \( \phi_n/\psi_n^2 \) and \( \omega_n/\psi_n^3 \), since we have been working in projective coordinates. In order to nail down \( \phi_n, \omega_n \) and \( \psi_n \) 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):

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

We then define the division polynomials \( \psi_n \) via the recurrences

\[
\psi_{2m+1} = \psi_m + 2\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,
\]

\[
\psi_{2m} = \frac{1}{2y}\psi_m(\psi_m + 2\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2),
\]

where we reduce the result modulo the curve equation so that \( \psi_n \) 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 \( \psi_{2m} \) 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 \( \phi_n \) and \( \omega_n \) via

\[
\begin{align*}
\phi_n &= x\psi_n^2 - \psi_n+1\psi_{n-1}, \\
\omega_n &= \frac{1}{4y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2).
\end{align*}
\]

These equations hold for all integers \( n \), and we have \( \phi_n = \phi_{-n} \) and \( \omega_n = \omega_{-n} \). As above, we always reduce \( \phi_n \) and \( \omega_n \) modulo the curve equation to make them at most linear in \( y \).

**Lemma 6.5.** For every integer \( n \),

\[
\begin{align*}
\psi_n &\text{ lies in } \begin{cases} \mathbb{Z}[x,A,B] & n \text{ odd} \\ 2y\mathbb{Z}[x,A,B] & n \text{ even} \end{cases} \\
\phi_n &\text{ lies in } \mathbb{Z}[x,A,B] \quad \text{for all } n, \\
\omega_n &\text{ lies in } \begin{cases} \mathbb{Z}[x,A,B] & n \text{ even} \\ y\mathbb{Z}[x,A,B] & n \text{ odd}. \end{cases}
\end{align*}
\]
\textit{Proof.} These are easy inductions; see Lemmas 3.3 and 3.4 in Washington \[2\]. \hfill \Box

It follows from the lemma that \( \psi_n^2 \) lies in \( \mathbb{Z}[x, A, B] \) for all positive \( n \), so we think of \( \phi_n \) and \( \psi_n^2 \) as a polynomial in \( x \) alone, whereas there is always exactly one of \( \omega_n \) and \( \psi_n^3 \) that depends on \( y \).

### 6.5 Multiplication-by-\( n \) maps

At this point it is not at all obvious that the polynomials \( \phi_n \), \( \omega_n \), and \( \psi_n \) 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

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

so it suffices to consider positive \( n \). The proof given by Washington \[2, \text{Thm. 9.33}\] 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 \[1, \text{Ex. 3.7}\]). 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 \( \psi_n \) are correct.

For \( 1 \leq n \leq 4 \) the formulas given for \( \psi_n \), match our computations in Sage using the group law. To verify the formula for \( \psi_n \) 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 \( \phi_m \) for \( x_1 \), \( \psi_m \) for \( z_1 \), \( \phi_{m+1} \) for \( x_2 \), and \( \psi_{m+1} \) for \( z_2 \) yields

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

which we wish to show is equal to \( \psi_{2m+1} \). Applying the formulas for \( \phi_m \) and \( \phi_{m+1} \) gives

\[
\phi_m\psi_{m+1}^2 - \phi_{m+1}\psi_m^2 = (x\psi_m^2 - \psi_{m+1}\psi_m - \psi_{m+2}\psi_m)\psi_{m+1} - (x\psi_{m+1}^2 - \psi_{m+2}\psi_m)\psi_m^2
\]

\[
= \psi_{m+2}\psi_m - \psi_{m+1}\psi_m - \psi_{m+1}\psi_m
\]

\[
= \psi_{2m+1},
\]

as desired.

To verify the formula for \( \psi_n \) 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

\[
2\omega_m\psi_m = 2 \cdot \frac{1}{4y}(\psi_{m+2}\psi_{m-1} - \psi_{m-2}\psi_{m+1})\psi_m
\]

\[
= \psi_{2m},
\]

as desired. This completes the verification for \( \psi_n \). To complete the proof one performs a similar verification for \( \phi_n \) and \( \omega_n \) using the group law formulas for \( x_3 \) and \( y_3 \). \hfill \Box
Theorem 6.7. For every positive integer \( n \) the polynomials \( \phi_n \) and \( \psi_n \) satisfy

\[
\phi_n(x) = x^n + \cdots,
\]

\[
\psi_n(x) = \begin{cases} nx^{n+1} + \cdots, & n \text{ odd} \\ y \left( nx^{n+1} + \cdots \right), & n \text{ even.} \end{cases}
\]

where each ellipsis hides terms of lower degree in \( x \).

Proof. We first prove the formula for \( \psi_n \) 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 \( \text{lt}_x f \) denote the leading term of \( f \) as a polynomial in \( x \).

Case 0: \( n \equiv 0 \mod 4 \).
Let \( n = 2m \), with \( m \) even. We have

\[
\text{lt}_x \psi_{2m} = \text{lt}_x \left( \frac{1}{2y} \psi_m (\psi_{m+2} \psi_{m-1}^2 - \psi_{m-2} \psi_{m+1}^2) \right) = \frac{1}{2y} \cdot y m x^{m^2-4} \left( y(m+2)x^{(m+2)^2-4} \left( m - 1 \right) x^{2(m-1)^2-2} - y(m-2)x^{(m-2)^2-4} \left( m + 1 \right) x^{2(m+1)^2-2} \right)
\]

\[
= \frac{ym}{2} \left( \left( m - 1 \right)^2 (m + 2)x^{m^2-4+4m+4} - (m - 2)(m + 1) x^{m^2-4+4m}ight)
\]

\[
= \frac{ym}{2} \left( \left( m - 1 \right)^2 (m + 2) - (m - 2)(m + 1) \right) x^{m^2-4}
\]

\[
= y(2m)x^{m^2-4} = ynx^{n^2-4}
\]

Case 1: \( n \equiv 1 \mod 4 \).
Let \( n = 2m + 1 \), with \( m \) even. We have

\[
\text{lt}_x \psi_{2m+1} = \text{lt}_x \left( \psi_{m+2} \psi_m - \psi_{m-1} \psi_{m+1} \right) = \text{lt}_x \left( y(m+2)x^{(m+2)^2-4} y^3 m^3 x^{3m^2+12} - (m - 1)x^{(m-1)^2-1} (m + 1) x^{3(m+1)^2-3} \right)
\]

\[
= (m + 2)m^3 x^6 x^{m^2+4m+3m^2+12-} - (m - 1)(m + 1) x^{m^2-2m+3m^2+6m}
\]

\[
= (2m + 1)x^{m^2+4m} = n x^{n^2-1}
\]

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

Case 2: \( n \equiv 2 \mod 4 \).
Let \( n = 2m \), with \( m \) odd. We have

\[
\text{lt}_x \psi_{2m} = \text{lt}_x \left( \frac{1}{2y} \psi_m (\psi_{m+2} \psi_{m-1}^2 - \psi_{m-2} \psi_{m+1}^2) \right) = \frac{1}{2y} m x^{m^2-1} \left( (m + 2)x^{(m+2)^2-1} y^2 (m - 1) x^{2(m-1)^2-8} - (m - 2)x^{(m-2)^2-1} y^2 (m + 1) x^{2(m+1)^2-8} \right)
\]

\[
= \frac{ym}{2} \left( (m + 2)(m - 1)^2 x^{m^2-1+(m+2)^2-1+2(m-1)^2-8} - (m - 2)(m + 1)^2 x^{m^2-1+(m-2)^2+2(m+1)^2-8} \right)
\]

\[
= \frac{ym}{2} \left( (m + 2)(m - 1)^2 - (m - 2)(m + 1)^2 \right) x^{4m^2-4}
\]

\[
= y(2m)x^{4m^2-4} = ynx^{n^2-4}
\]
Case 3: $n \equiv 3 \mod 4$.
Let $n = 2m + 1$, with $m$ odd. We have

$$\text{lt}_x \psi_{2m+1} = \text{lt}_x \left( \psi_{m+2} \psi_m^3 - \psi_m \psi_{m+1}^3 \right)$$

$$= \text{lt}_x \left( (m+2)x^{(m+2)^2-1} - m^3x^{m^2-3} - y(m-1)x^{(m-1)^2-4} - y^3(m+1)x^{3(m+1)^2-12} \right)$$

$$= (2m+1)x^{4m^2+4m}$$

$$= nx^{\frac{n^2+1}{2}}$$

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

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

$$\text{lt}_x \phi_n = \text{lt}_x \left( x \psi_n^2 - \psi_{n+1} \psi_{n-1} \right)$$

$$= \text{lt}_x \left( x^2 \psi_n^2 - n^2x^{(n+1)^2-8} - (n+1)x^{(n+1)^2-1} \right)$$

$$= n^2x^{n^2} - (n^2-1)x^{n^2}$$

$$= x^{n^2},$$

and if $n$ is odd we have

$$\text{lt}_x \phi_n = \text{lt}_x \left( x \psi_n^2 - \psi_{n+1} \psi_{n-1} \right)$$

$$= \text{lt}_x \left( x^2 \psi_n^2 - n^2x^{(n-1)^2-8} - (n-1)x^{(n-1)^2-1} \right)$$

$$= n^2x^{n^2} - (n^2-1)x^{n^2}$$

$$= x^{n^2},$$

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 $\overline{k}[x]$.

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

$$\phi_n(x_0) = x_0 \psi_n^2(x_0) - \psi_{n+1}(x_0, y_0) \psi_{n-1}(x_0, y_0)$$

$$0 = 0 - \psi_{n+1}(x_0, y_0) \psi_{n-1}(x_0, y_0),$$

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 $[n]: E \to E$ is an endomorphism of degree $n^2$. It is separable if and only if it $n$ is not divisible by the characteristic of $k$.  

8
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 $\left( \frac{\phi_n(x)}{\psi_n(x)} \right)' \neq 0$ 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


18.783 Elliptic Curves
Spring 2013

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.