DIVISION POLYNOMIALS FOR ARBITRARY ISOGENIES

KATHERINE E. STANGE

Abstract. Following work of Mazur-Tate and Satoh, we extend the definition of division polynomials to arbitrary isogenies of elliptic curves, including those whose kernels do not sum to the identity. In analogy to the classical case of division polynomials for multiplication-by-n, we demonstrate recurrence relations, identities relating to classical elliptic functions, the chain rule describing relationships between division polynomials on source and target curve, and generalizations to higher dimension (i.e., elliptic nets).

1. Introduction

Given an elliptic curve E with identity $\mathcal{O}$, and a positive integer n with associated multiplication-by-n map $[n] : E \to E$, the n-th division polynomial Ψ_n is an elliptic function on E with divisor

$$[n]^*(\mathcal{O}) - n^2(\mathcal{O}). \tag{1}$$

We typically set $\Psi_0 = 0$ and $\Psi_{-n} = -\Psi_n$. Sometimes these are called *Weber polynomials* [3]. These are furthermore normalized so that they satisfy a recurrence relation

$$\Psi_{p+q}\Psi_{p-q}\Psi_r^2 + \Psi_{q+r}\Psi_{q-r}\Psi_p^2 + \Psi_{r+p}\Psi_{r-p}\Psi_q^2 = 0, \tag{2}$$

or the more general

$$\Psi_{p+q+s}\Psi_{p-q}\Psi_{r+s}\Psi_r + \Psi_{q+r+s}\Psi_{q-r}\Psi_{p+s}\Psi_p + \Psi_{r+p+s}\Psi_{r-p}\Psi_{q+s}\Psi_q = 0, \tag{3}$$

for all $p, q, r, s \in \mathbb{Z}$. The first few division polynomials, in terms of a Weierstrass curve $y^2 = x^3 + ax + b$, are:

$$\Psi_1 = 1, \quad \Psi_2 = 2y, \quad \Psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,$$
$$\Psi_4 = 4y \cdot \left(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3\right).$$

from which the rest follow by (2) or (3).

The recurrence allows for efficient computation, with $O(\log n)$ applications of (3) to compute Ψ_n from the initial terms $\Psi_1, \Psi_2, \Psi_3, \Psi_4$. Ward [15] showed in 1948 that integer sequences satisfying (2) are essentially those of the form $\Psi_n(P)$ for some point P on an elliptic curve E; the curve coefficients and point coordinates can be recovered from the integer sequence as polynomials in the initial terms. Such integer sequences are known as *elliptic divisibility sequences*.

There are three traditionally important properties of the division polynomials:

(1) **Chain rule**. The Ψ_n satisfy
$$\Psi_{nm} = (\Psi_n \circ [m])\, \Psi_m^{n^2}.$$

(2) **Relation to** x. Letting x be the x-coordinate in the Weierstrass form, the Ψ_n satisfy
$$\frac{\Psi_{n+m}\Psi_{n-m}}{\Psi_n^2\Psi_m^2} = x \circ [n] - x \circ [m].$$

(3) **Recurrence relations**. The Ψ_n satisfy (2) as a consequence of the relation to x, as well as the more general (3).

2020 *Mathematics Subject Classification.* Primary: 11G05 11B37 14H52 Secondary: 11B39 11R37 14K02.

Key words and phrases. elliptic curves, division polynomials, kernel polynomials, elliptic divisibility sequence, isogenies, elliptic functions.

Stange was supported by NSF DMS-2401580.

In 1991, in an appendix to their work on the p-adic sigma function, Mazur and Tate defined division polynomials more generally [7, Appendix I] as follows. For any isogeny $\phi : E \to E'$ for which the sum of the points in the kernel $E[\phi]$, with multiplicity, is trivial, the divisor

$$\phi^*(\mathcal{O}) - \deg \phi(\mathcal{O})$$

is principal, hence the divisor of some function Ψ_ϕ, which we will call the division polynomial for ϕ. To set the scalar normalization, let t and t' be uniformizers at the identities $\mathcal{O}$ and $\mathcal{O}'$ for E and E' respectively, and let ω and ω' be invariant differentials. One requires

$$\frac{t^{\deg \phi}\Psi_\phi}{t' \circ \phi}(\mathcal{O}) = \left(\frac{dt}{\omega}(\mathcal{O})\right)^{\deg \phi} \left(\frac{dt'}{\omega'}(\mathcal{O}')\right)^{-1}.$$

This is independent of the choice of t and t' but depends on ω, ω'. The requirement on the sum of points in the kernel being trivial is restrictive: the isogenies for which the sum of points is non-zero are exactly those which are cyclic of even degree, with odd inseparable degree. For example, the endomorphisms $1+i$, $1+\sqrt{-5}$, $\sqrt{-2}$ etc. do not have well-defined division polynomials (see also [8, Lemma 2.2]).

They show that for Ψ_ϕ which are defined, we obtain the three usual properties: a recurrence relation, the chain rule, and the relation to the x-coordinate.

In the case that ϕ has odd degree, these polynomials are exactly the *kernel polynomials* of Schoof [9] (sometimes themselves referred to as division polynomials [3]); for even degree they are closely related. The kernel polynomials are polynomials in x having roots exactly the x-coordinates of the kernel of ϕ, with multiplicity. Schoof shows how to compute these from knowledge of the image curve, the degree, and the sum of the x-coordinates of the kernel points (which specifies the second coefficient of the polynomial), by means of Taylor series expansions of Weierstrass functions. The kernel polynomial can be used to compute the isogeny itself, by a method of Kohel [5]. The roots can be used to the same purpose with Vélu's formulas [14]. The kernel polynomial can be computed by an algorithm of Stark based on continued fraction expansions [12]. For more background on the isogeny computation problem, see [3]. Evaluations of kernel polynomials can be used to compute the values of isogenies [1]. In the theory of complex multiplication, ray class fields can be generated over Hilbert class fields by kernel polynomials. More recently in 2015, Küçüksakalli studied kernel polynomials (calling them generalized division polynomials), and gave a method to compute them using Newton identities and Hurwitz numbers [6]. None of these methods approach the problem using recurrence relations like (2).

In 2004, Satoh independently defined generalized division polynomials for endomorphisms, and studied their computational properties [8]. Again, one is restricted to the case that the kernel sums to zero; Satoh called such endomorphisms *unbiased*. In this case, the normalization condition is given in terms of the uniformizer $T = -x/y$ at $\mathcal{O}$ by specifying the leading coefficient of a formal series expansion:

$$\Psi_\alpha = (-1)^{N(\alpha)-1}\alpha T^{-N(\alpha)+1} + \cdots.$$

Again, Satoh recovers the three basic properties of recurrence, chain rule and relation to x.

Over $\mathbb{Q}$, a closely related (but not exactly equivalent) definition of an elliptic divisibility sequence is as the sequence of denominators of $[n]P$, $n \geq 0$. In 2008, Streng [13] generalized this definition to curves with complex multiplication, in order to prove a generalization of a property due to Silverman [10] for elliptic divisibility sequences: that every term has a primitive divisor, that is, a prime divisor not appearing earlier in the sequence. Streng's definition generalizes terms from numbers to ideals.

In 2008, the author generalized elliptic divisibility sequences and division polynomials to elliptic nets [11]. Net polynomials are polynomials in the coefficients of E and *several* points P_i: the net polynomial $\Psi_{a_1,\ldots,a_n}$ will vanish when $\sum a_i P_i = \mathcal{O}$.

The purpose of this note is to show that the restriction that the sum of points in the kernel be trivial can be circumvented. We can define division polynomials Ψ_ϕ attached to arbitrary isogenies ϕ, and they satisfy analogues of the three main properties: chain rule, relation to x, and recurrence relation. Some adjustments to the statements are needed.

The fundamental idea is to replace the Mazur-Tate divisor with

$$D_\phi = \phi^*(\mathcal{O}') - \deg \phi(\mathcal{O}) + (P_\phi) - (\mathcal{O}),$$

where $P_\phi \in E[2]$ is the sum of the kernel of ϕ. This necessitates a great deal of wrangling of two-torsion points and isogenies of degree 2. In particular, the normalization of division polynomials is delicate (the

recurrences depend on it), and our case is no exception. The normalization in the general case is taken with respect to a fixed collection of isogenies of degree 2.

One of the interesting waypoints appears in the form of Lemma 3, which turns on the fact that kernel sums play well with the cube law of quadratic forms. To facilitate all this wrangling, we consider some generalities about *kernel divisors* formed as linear combinations of divisors of the form $\phi^*(\mathcal{O}')$, and, for principal kernel divisors, appropriately normalized *kernel functions*. We do only what is needed here, but there may be a more general theory available.

Since the recurrence relations necessitate new factors in our setting, the Ψ_ϕ themselves do not form an elliptic net. However, we demonstrate that specializations to a point $\Psi_\phi(P)$ can recover elliptic nets on the target curve.

Finally, we generalize such generalized division polynomials – perhaps 'kernel polynomials' is a better name – to higher dimension. That is, we define such things on products of E, in analogy to elliptic nets.

Acknowledgements. Thank you to Joseph Macula for helpful feedback on an earlier draft.

2. Definitions

Throughout the paper, we will assume the characteristic is not two.

2.1. **Biased and unbiased isogenies.** Generalizing Satoh, we call an isogeny *unbiased* if its kernel elements sum to the identity with multiplicity [8, Section 2]. In other words, the map $\sum_i n_i(P_i) \mapsto \sum_i n_i P_i$ taking $\mathrm{Div}(E)$ to E takes $\phi^*(\mathcal{O}')$ to $\mathcal{O}$. Equivalently, (1) is principal. An isogeny is *biased* if its kernel sum is non-trivial; in this case, it must sum to a non-trivial two-torsion point (all points of higher order are distinct from their inverses and will cancel one another).

2.2. **Three isogenies of degree two.** Write $P_0 = \mathcal{O}, P_1, P_2, P_3$ for the points in $E[2]$. For each $i = 1, 2, 3$, let $g_i : E \to E_i$ denote a fixed isogeny of degree 2 with kernel $\{\mathcal{O}, P_i\}$. Let g_0 denote the identity isogeny on $E_0 := E$. Let t and t_i be uniformizers on E and E_i respectively. Let ω and ω_i be invariant differentials on E and E_i respectively. And finally, write $\mathcal{O}$ for the identity on E and $\mathcal{O}_i$ for the identity on E_i.

Let $\phi : E \to E'$ be an isogeny. Let $P_\phi \in E[2]$ be the kernel sum of ϕ. Write $\iota(\phi)$ for the i such that $P_\phi = P_i$. Then we have or define

$$P_\phi = P_{\iota(\phi)}, \quad g_\phi := g_{\iota(\phi)}, \quad t_\phi := t_{\iota(\phi)}, \quad \omega_\phi := \omega_{\iota(\phi)}, \quad \mathcal{O}_\phi := \mathcal{O}_{\iota(\phi)}.$$

Observe that $\iota(\phi)$ depends only on $\phi|_{E[2]}$, since $P_\phi = \sum_{P \in E[\phi]} P = \sum_{P \in E[\phi] \cap E[2]} P$.

2.3. **The elliptic function Ψ_ϕ.** We now extend the definition of division polynomials to arbitrary (possibly biased) isogenies. Let $\phi : E \to E'$, let t' be a uniformizer and ω' an invariant differential for E'. Let $\mathcal{O}'$ be the identity of E'. In analogy to Mazur and Tate, define an elliptic function Ψ_ϕ with the principal divisor

$$D_\phi = \phi^*(\mathcal{O}') - \deg \phi(\mathcal{O}) + (P_\phi) - (\mathcal{O}),$$

where we require, as a means of normalization, that

$$\frac{t^{\deg \phi + \deg g_\phi} \Psi_\phi}{(t_\phi \circ g_\phi)(t' \circ \phi)}(\mathcal{O}) = \left(\frac{dt}{\omega}(\mathcal{O})\right)^{\deg \phi + \deg g_\phi} \left(\frac{dt'}{\omega'}(\mathcal{O}')\right)^{-1} \left(\frac{dt_\phi}{\omega_\phi}(\mathcal{O}_\phi)\right)^{-1}. \tag{4}$$

One observes that this is independent of t, t', t_ϕ but depends on $\omega, \omega', \omega_\phi$. As an example, for $E : y^2 = x^3 + x$ with complex multiplication by $\mathbb{Z}[i]$, $\Psi_{1+i} = 2ix$ has divisor $2(0,0) - 2(\mathcal{O})$ (examples are given in Section 5).

2.4. **Kernel functions.** Besides Ψ_ϕ, one needs a few auxiliary functions to formulate the generalization of division polynomials. It is useful to define a larger class of carefully normalized elliptic functions called *kernel functions*. Given an isogeny $\phi : E \to E'$, define the divisor

$$K_\phi := \phi^*(\mathcal{O}').$$

We can define the group of formal $\mathbb{Z}$-sums of kernel symbols (K_ϕ),

$$\mathrm{Ker}(E) := \left\{ \sum_\phi n_\phi(K_\phi) : \phi \text{ is an isogeny with source } E \text{ and all but finitely many } n_\phi \in \mathbb{Z} \text{ are zero.} \right\}.$$

Its elements will be called *kernel symbol sums*. There is a map from $\mathrm{Ker}(E)$ to $\mathrm{Div}(E)$ by substituting the kernel divisor K_ϕ for each symbol (K_ϕ).

Given a kernel symbol sum whose image in $\mathrm{Div}(E)$ is principal, we can associate an elliptic function with that divisor, up to scalar normalization. The choice of normalization is more delicate, depending on the kernel symbol sum and not just the image divisor. Fix a uniformizer t_ϕ and differential ω_ϕ on the target curve for each ϕ. For now, for the greatest generality, we do this independently for each ϕ, even if some target curves coincide. To a principal kernel symbol sum $\sum_\phi n_\phi(K_\phi)$, the associated elliptic function h can be normalized by requiring

$$\frac{h}{\left(\prod_\phi (t_\phi \circ \phi)^{n_\phi}\right)}(\mathcal{O}) = \prod_\phi \left(\frac{dt_\phi}{\omega_\phi}(\mathcal{O}_\phi)\right)^{-n_\phi},$$

where by design both sides have a non-zero value. This is independent of the choice of uniformizers but depends on the choice of invariant differentials. Any elliptic function h of this form and normalized in this way is called the *kernel function* for the associated kernel symbol sum.

This normalization is consistent in the sense that the product of two kernel functions is again a kernel function (for the sum of the kernel symbol sums).

It has the following convenient property.

Lemma 1. *Suppose $\omega := \omega_\phi$ are chosen to agree for all $\phi \in \mathrm{Hom}(E, E')$. Then a kernel function derived from kernel symbol sum $\sum_{\phi\in I} n_\phi(K_\phi)$ is independent of the choice of invariant differential ω' on E' whenever $\sum_{\phi\in I\cap \mathrm{Hom}(E,E')} n_\phi = 0$.*

Returning to Ψ_ϕ, observe that we have defined it by kernel symbol sum

$$D_\phi = (K_\phi) + (K_{g_\phi}) - (\deg\phi + \deg g_\phi)(K_1),$$

and the associated normalization; it is therefore a kernel function with respect to the given kernel symbol sum.

2.5. **The elliptic function $\widehat{\Psi}_\phi$.** To account for biased isogenies, we need auxiliary functions associated to the isogenies of degree two. For each $i = 0, 1, 2, 3$, define a kernel function $\widehat{\Psi}_i$ on E with the principal divisor

$$\mathrm{div}(\widehat{\Psi}_i) = \widehat{D}_i := 2(P_i) - 2(\mathcal{O}) = 2(K_{g_i} - \deg g_i K_1),$$

normalized so that

$$\frac{t^{2\deg g_i}\widehat{\Psi}_i}{(t_i \circ g_i)^2}(\mathcal{O}) = \left(\frac{dt}{\omega}(\mathcal{O})\right)^{2\deg g_i}\left(\frac{dt_i}{\omega_i}(\mathcal{O}_i)\right)^{-2}.$$

This is independent of t, t_i but depends on the invariant differentials. Observe that $\widehat{\Psi}_0 = 1$. Finally, for a general isogeny, define

$$\widehat{\Psi}_\phi := \widehat{\Psi}_{\iota(\phi)}.$$

2.6. **The elliptic function $\widetilde{\Psi}_\phi$.** Finally, define one more auxiliary kernel function $\widetilde{\Psi}_\phi$ with the principal divisor

$$\widetilde{D}_\phi = 2\phi^*(\mathcal{O}') - 2\deg\phi(\mathcal{O}) = 2(K_\phi - \deg\phi K_1),$$

where we require, as a means of normalization, that

$$\frac{t^{2\deg\phi}\widetilde{\Psi}_\phi}{(t' \circ \phi)^2}(\mathcal{O}) = \left(\frac{dt}{\omega}(\mathcal{O})\right)^{2\deg\phi}\left(\frac{dt'}{\omega'}(\mathcal{O}')\right)^{-2}$$

Observe that

$$\widetilde{\Psi}_\phi\widehat{\Psi}_\phi = \Psi_\phi^2.$$

The notations $\widetilde{\Psi}_\phi$ and Ψ_ϕ agree with Satoh for unbiased endomorphisms, up to a factor of ± 1.

2.7. **Kernel functions revisited.** Because of the importance of the isogenies of degree two, we will make a further convention on the choice of invariant differentials, i.e., we choose ω_1, ω_2, ω_3 and ω so that the kernel function associated to the kernel symbol sum

$$(K_{g_1}) + (K_{g_2}) + (K_{g_3}) - (K_{[2]}) - 2(K_1) \tag{5}$$

is 1. Namely,

$$\frac{(t \circ [2])t^2}{(t_1 \circ g_1)(t_2 \circ g_2)(t_3 \circ g_3)}(\mathcal{O}) = \left(\frac{dt_1}{\omega_1}(\mathcal{O})\right)^{-1}\left(\frac{dt_2}{\omega_2}(\mathcal{O})\right)^{-1}\left(\frac{dt_3}{\omega_3}(\mathcal{O})\right)^{-1}\left(\frac{dt}{\omega}(\mathcal{O})\right)^{3} \tag{6}$$

In other words, we accomplish this by scaling the ω_i, ω relative to one another. This convention allows us to consider kernel symbol sums equivalent modulo the expression (5) when normalizing kernel functions.

Lemma 2. *Under the convention above, any kernel function all of whose kernel divisors are supported only on $E[2]$ is independent of the particular kernel symbol sum generating it.*

Proof. It suffices to verify that the elements of the kernel of the map $\mathrm{Ker}(E) \to \mathrm{Div}(E)$ whose kernels are supported on $E[2]$ are only those generated by (5). □

It would be interesting to describe the kernel of $\mathrm{Ker}(E) \to \mathrm{Div}(E)$ more generally; for related literature, see [2].

This allows us to define a final auxiliary function with divisor supported on $E[2]$. When we write $\sum_\phi$ we will take this as an abbreviation for $\sum_{\phi \in \mathrm{Hom}(E,E')}$ for a fixed E and E'. We also define a *finite integral quadratic identity* to be any identity of the form $\sum_{i \in I} a_i q(i) = 0$, having finitely many terms, indexed over a $\mathbb{Z}$-module I with coefficients $a_i \in \mathbb{Z}$, which is a combination of finitely many instances of the cube identity:

$$q(\alpha+\beta+\gamma) - q(\alpha+\beta) - q(\beta+\gamma) - q(\gamma+\alpha) + q(\alpha) + q(\beta) + q(\gamma) - q(0) = 0,$$

One example is the better-known parallelogram rule,

$$q(\alpha+\beta) + q(\alpha-\beta) - 2q(\alpha) - 2q(\beta) = 0.$$

Such identities are true for all quadratic functions.

Lemma 3. *Fix E and E'. Suppose that*

$$\sum_\phi e_\phi q(\phi) = 0$$

is a finite integral quadratic identity on $\phi \in \mathrm{Hom}(E, E')$. Then there is a unique kernel function supported on $E[2]$ whose square is

$$\prod_\phi \widehat{\Psi}_\phi^{e_\phi}.$$

We will denote this by

$$\sqrt{\prod_\phi \widehat{\Psi}_\phi^{e_\phi}}.$$

Proof. We have

$$\mathrm{div}\left(\prod_\phi \widehat{\Psi}_\phi^{e_\phi}\right) = 2\left(\sum_\phi e_\phi K_{g_\phi}\right) - 2\left(\sum_\phi e_\phi \deg\phi\right) K_1 = 2\left(\sum_\phi e_\phi K_{g_\phi}\right).$$

It suffices to show that $\sum_\phi e_\phi K_{g_\phi}$ is a principal divisor, for then by Lemma 2, the associated kernel function must square to the kernel function indicated.

We may assume without loss of generality that we are in the case of the cube identity

$$q(\alpha+\beta+\gamma) - q(\alpha+\beta) - q(\beta+\gamma) - q(\gamma+\alpha) + q(\alpha) + q(\beta) + q(\gamma) = 0.$$

To determine how many of the points P_ϕ are equal to P_i, it suffices to examine the action of $\phi \in \mathrm{Hom}(E, E')$ on the 2-torsion, as a map $E[2] \to E'[2]$. Denote this by $\rho(\phi) \in \mathrm{Hom}_{\mathbb{F}_2}(E[2], E'[2])$. The map $\kappa_i : \mathrm{Hom}_{\mathbb{F}_2}(E[2], E'[2]) \to E'[2]$ taking $\rho(\phi)$ to $\rho(\phi)(P_i)$ is a linear transformation of vector spaces over $\mathbb{F}_2$ from dimension 4 to dimension 2. We have $P_\phi = P_i$ if and only if $\rho(\phi) \in \ker\kappa_i \setminus \{0\}$. The 'cube' of elements

$$0, \alpha, \beta, \gamma, \alpha+\beta, \beta+\gamma, \gamma+\alpha, \alpha+\gamma+\beta$$

is the subspace generated by α, β, γ. If it is of dimension 3, then we conclude from linearity that the fibres are of even size, and so the number of elements in the cube having $P_\phi = P_i$ is odd.

On the other hand, if it is of lower dimension, then each element in the cube has even multiplicity in the list of cube elements. Therefore $P_\phi = P_i$ occurs an even number of times for ϕ in the list.

Write $\sum_\phi e_\phi K_{g_\phi} = \sum_{i=0}^3 a_i K_i$. We have shown that the parity of a_1, a_2, a_3 agree. This guarantees the divisor is principal. □

Lemma 4. *If*

$$\sum_\phi e_\phi q(\phi) = 0$$

is a finite integral quadratic identity, then

$$\prod_\phi \Psi_\phi^{e_\phi} \sqrt{\prod_\phi \widehat{\Psi}_\phi^{-e_\phi}}$$

is a well-defined kernel function, with divisor

$$\sum_\phi e_\phi (\phi P = \mathcal{O}).$$

Proof. That it is well-defined follows from Lemma 3; that it has the given divisor is a calculation using the fact that $\sqrt{\prod_\phi \widehat{\Psi}_\phi^{e_\phi}}$ has divisor $\sum_\phi e_\phi K_{g_\phi}$ (from the proof of Lemma 3). □

2.8. **Normalization in terms of formal groups.** If we choose the normalizer $T := -x/y$ for the Weierstrass form $E : y^2 = f(x)$, and similarly T' for E' and T_i for E_i, then we can specify the normalizations of Ψ_ϕ etc. in terms of the formal groups. We have expansions for the normalized invariant differential, formal group law and x and y coordinates:

(7)
$$\omega = \frac{dT}{f(T)} := \frac{dT}{1 + O(T)}, \quad F(T_1, T_2) = T_1 + T_2 + \cdots, \quad x(T) = T^{-2} + O(T^{-1}), \quad y(T) = -T^{-3} + O(T^{-2}).$$

We also have that there are constants a_ϕ and $a_i := a_{g_i}$ so that

$$\phi T = a_\phi T^{\deg_{in} \phi} + O(T^{2 \deg_{in} \phi}), \quad g_i T = a_i T^{\deg_{in} g_i} + O(T^{2 \deg_{in} g_i}),$$

where $\deg_{in}$ represents the inseparable degree. So the normalization (4), taking the normalized differential as above, becomes

(8)
$$\begin{aligned} \Psi_\phi(T) &= T^{-\deg \phi - \deg g_{\iota(\phi)}} (\phi T)(g_{\iota(\phi)} T) \\ &= a_{\iota(\phi)} a_\phi T^{-\deg \phi - \deg g_{\iota(\phi)} + \deg_{in} \phi + \deg_{in} g_{\iota(\phi)}} + \cdots. \end{aligned}$$

In the case that ϕ is a separable endomorphism with $\iota(\phi) = 0$, Satoh's generalization is defined and the normalization agrees up to a sign of the form $(-1)^{\deg \phi - 1}$. Observe that including this sign does not affect (2) or (3), nor does it affect the relation to x or the chain rule. It is just a convention.

3. Properties

For everything that follows, we will now fix five invariant differentials: ω on E, ω' on E', ω_i on E_i (regardless of whether some of these curves coincide). We will simultaneously fix Weierstrass equations for E, E', E_i for which these are the normalized invariant differentials as in Section 2.8. These are used for normalization consistently as described for Ψ, $\widehat{\Psi}$ and $\widetilde{\Psi}$ above, subject to the constraint (6). Finally, we will use the expressions x', y' for the coordinate functions associated to the Weierstrass equation for E'.

Theorem 5 (Relation to x)**.** *Let α and β be isogenies from E to E'. Then*

(9)
$$\frac{\Psi_{\alpha+\beta} \Psi_{\alpha-\beta} \widehat{\Psi}_\alpha \widehat{\Psi}_\beta}{\Psi_\alpha^2 \Psi_\beta^2 \widehat{\Psi}_{\alpha+\beta}} = x' \circ \alpha - x' \circ \beta.$$

Proof. Any quadratic function f satisfies the parallelogram law

$$f(\alpha+\beta)+f(\alpha-\beta)-2f(\alpha)-2f(\beta)=0.$$

Thus from Lemma 4 (observe that $\widehat{\Psi}_{\alpha+\beta}=\widehat{\Psi}_{\alpha-\beta}$), the left side has divisor

$$K_{\alpha+\beta}+K_{\alpha-\beta}-2K_\alpha-2K_\beta,$$

which is also the divisor of the right hand side.

For the scaling on both sides of (9), we can compute the formal group expansions around $\mathcal{O}$. For the right side,

$$(x'\circ\alpha-x'\circ\beta)(T)=(a_\beta T)^{-2}-(a_\alpha T)^{-2}+\cdots=\frac{(a_\alpha T)^2-(a_\beta T)^2}{(a_\alpha T)^2(a_\beta T)^2}+\cdots.$$

For the other side, we have, using (8),

$$\frac{\Psi_{\alpha+\beta}\Psi_{\alpha-\beta}\widehat{\Psi}_\alpha\widehat{\Psi}_\beta}{\Psi_\alpha^2\Psi_\beta^2\widehat{\Psi}_{\alpha+\beta}}(T)=\frac{(a_\alpha T-a_\beta T)(a_\alpha T+a_\beta T)}{(a_\alpha T)^2(a_\beta T)^2}+\cdots$$

Thus, we obtain (9). □

Observe that

$$\frac{\widehat{\Psi}_\alpha\widehat{\Psi}_\beta}{\widehat{\Psi}_{\alpha+\beta}}=\sqrt{\frac{\widehat{\Psi}_\alpha^2\widehat{\Psi}_\beta^2}{\widehat{\Psi}_{\alpha+\beta}\widehat{\Psi}_{\alpha-\beta}}}.$$

Corollary 6 (First recurrence relation)**.** *We have the recurrence*

$$\frac{\Psi_{\alpha+\beta}\Psi_{\alpha-\beta}\widehat{\Psi}_\alpha\widehat{\Psi}_\beta}{\Psi_\alpha^2\Psi_\beta^2\widehat{\Psi}_{\alpha+\beta}}+\frac{\Psi_{\beta+\gamma}\Psi_{\beta-\gamma}\widehat{\Psi}_\beta\widehat{\Psi}_\gamma}{\Psi_\beta^2\Psi_\gamma^2\widehat{\Psi}_{\beta+\gamma}}+\frac{\Psi_{\gamma+\alpha}\Psi_{\gamma-\alpha}\widehat{\Psi}_\gamma\widehat{\Psi}_\alpha}{\Psi_\gamma^2\Psi_\alpha^2\widehat{\Psi}_{\gamma+\alpha}}=0 \tag{10}$$

In the case of endomorphisms for which all sums and differences of α,β,γ are unbiased, Satoh obtains the special case

$$\frac{\Psi_{\alpha+\beta}\Psi_{\alpha-\beta}}{\widetilde{\Psi}_\alpha\widetilde{\Psi}_\beta}+\frac{\Psi_{\beta+\gamma}\Psi_{\beta-\gamma}}{\widetilde{\Psi}_\beta\widetilde{\Psi}_\gamma}+\frac{\Psi_{\gamma+\alpha}\Psi_{\gamma-\alpha}}{\widetilde{\Psi}_\gamma\widetilde{\Psi}_\alpha}=0.$$

Recall that $\widetilde{\Psi}_\alpha=\Psi_\alpha^2$ when α is unbiased, and $\widetilde{\Psi}_\alpha\widehat{\Psi}_\alpha=\Psi_\alpha^2$ in general; if all subscripts are unbiased this recovers the usual form (2).

We now give the second, more general recurrence relation.

Theorem 7 (Second relation to x)**.** *Let α, β and σ be isogenies from E to E'. Then*

$$\frac{\Psi_{\alpha+\beta+\sigma}\Psi_{\alpha-\beta}\Psi_\sigma}{\Psi_{\alpha+\sigma}\Psi_{\beta+\sigma}\Psi_\alpha\Psi_\beta}\sqrt{\frac{\widehat{\Psi}_{\alpha+\sigma}\widehat{\Psi}_{\beta+\sigma}\widehat{\Psi}_\alpha\widehat{\Psi}_\beta}{\widehat{\Psi}_{\alpha+\beta+\sigma}\widehat{\Psi}_{\alpha-\beta}\widehat{\Psi}_\sigma}}=\frac{y'\circ\alpha-y'\circ\sigma}{x'\circ\alpha-x'\circ\sigma}-\frac{y'\circ\beta-y'\circ\sigma}{x'\circ\beta-x'\circ\sigma}.$$

Proof. The left side is an instance of the cube law, so that from Lemma 4, the left side has divisor

$$K_{\alpha+\beta+\sigma}+K_{\alpha-\beta}-K_{\alpha+\sigma}-K_\alpha-K_{\beta+\sigma}-K_\beta+K_\sigma,$$

which is also the divisor of the right hand side.

Next, we check the constant. There is an algebraic identity in abstract variables a, b, s:

$$\frac{b^{-3}-s^{-3}}{b^{-2}-s^{-2}}-\frac{a^{-3}-s^{-3}}{a^{-2}-s^{-2}}=\frac{(a+b+s)(a-b)s}{(a+s)(b+s)ab}.$$

We consider the leading coefficients of the formal expansions around the origin, using (7):

$$\frac{y'\circ\alpha-y'\circ\sigma}{x'\circ\alpha-x'\circ\sigma}-\frac{y'\circ\beta-y'\circ\sigma}{x'\circ\beta-x'\circ\sigma}=\frac{(a_\beta T)^{-3}-(a_\sigma T)^{-3}}{(a_\beta T)^{-2}-(a_\sigma T)^{-2}}-\frac{(a_\alpha T)^{-3}-(a_\sigma T)^{-3}}{(a_\alpha T)^{-2}-(a_\sigma T)^{-2}}+\cdots$$

On the other hand, using the fact that the quotient at hand is an example of a cube identity, we have

$$\deg(\alpha+\beta+\sigma)+\deg(\alpha-\beta)+\deg(\sigma)-\deg(\alpha+\sigma)-\deg(\beta+\sigma)-\deg\alpha-\deg\beta=0.$$

Applying that fact, together with (8) and its analogue for $\widehat{\Psi}$, we have

$$\frac{\Psi_{\alpha+\beta+\sigma}\Psi_{\alpha-\beta}\Psi_\sigma}{\Psi_{\alpha+\sigma}\Psi_{\beta+\sigma}\Psi_\alpha\Psi_\beta}\sqrt{\frac{\widehat{\Psi}_{\alpha+\sigma}\widehat{\Psi}_{\beta+\sigma}\widehat{\Psi}_\alpha\widehat{\Psi}_\beta}{\widehat{\Psi}_{\alpha+\beta+\sigma}\widehat{\Psi}_{\alpha-\beta}\widehat{\Psi}_\sigma}} = \frac{(a_\alpha T + a_\beta T + a_\sigma T)(a_\alpha T - a_\beta T)(a_\sigma T)}{(a_\alpha T + a_\sigma T)(a_\beta T + a_\sigma T)(a_\alpha T)(a_\beta T)} + \cdots$$

These agree in leading coefficient by the abstract identity. □

The following is an immediate consequence.

Corollary 8 (Second recurrence relation)**.** *The division polynomials Ψ_ϕ satisfy the more general recurrence relation*

$$\begin{aligned}\frac{\Psi_{\alpha+\beta+\sigma}\Psi_{\alpha-\beta}}{\Psi_{\alpha+\sigma}\Psi_{\beta+\sigma}\Psi_\alpha\Psi_\beta}\sqrt{\frac{\widehat{\Psi}_{\alpha+\sigma}\widehat{\Psi}_{\beta+\sigma}\widehat{\Psi}_\alpha\widehat{\Psi}_\beta}{\widehat{\Psi}_{\alpha+\beta+\sigma}\widehat{\Psi}_{\alpha-\beta}}} + \frac{\Psi_{\beta+\gamma+\sigma}\Psi_{\beta-\gamma}}{\Psi_{\beta+\sigma}\Psi_{\gamma+\sigma}\Psi_\beta\Psi_\gamma}\sqrt{\frac{\widehat{\Psi}_{\beta+\sigma}\widehat{\Psi}_{\gamma+\sigma}\widehat{\Psi}_\beta\widehat{\Psi}_\gamma}{\widehat{\Psi}_{\beta+\gamma+\sigma}\widehat{\Psi}_{\beta-\gamma}}}\\ + \frac{\Psi_{\gamma+\alpha+\sigma}\Psi_{\gamma-\alpha}}{\Psi_{\gamma+\sigma}\Psi_{\alpha+\sigma}\Psi_\gamma\Psi_\alpha}\sqrt{\frac{\widehat{\Psi}_{\gamma+\sigma}\widehat{\Psi}_{\alpha+\sigma}\widehat{\Psi}_\gamma\widehat{\Psi}_\alpha}{\widehat{\Psi}_{\gamma+\alpha+\sigma}\widehat{\Psi}_{\gamma-\alpha}}} = 0.\end{aligned} \tag{11}$$

In particular, if all the indices represent unbiased isogenies, then the Ψ_ϕ satisfy (3).

Finally, we consider the chain rule. There is a natural notion of pullback on kernel symbol sums, namely, when $\beta : E'' \to E$,

$$\beta^* \sum_{\gamma\in\mathrm{Hom}(E,E')} (K_\gamma) = \sum_{\gamma\in\mathrm{Hom}(E,E')} (K_{\gamma\beta}).$$

This commutes with pullback on divisors.

Lemma 9. *Suppose f and g are kernel functions associated to sums $\sum_{\gamma\in\mathrm{Hom}(E,E')}(K_\gamma)$ and $\sum_{\delta\in\mathrm{Hom}(E'',E')}(K_\delta)$, respectively. Suppose $\beta : E'' \to E$. Suppose that $\sum_\delta(K_\delta) = \beta^*\sum_\gamma(K_\gamma)$. Then $f \circ \beta = g$.*

That is, the pullback of a kernel function is a kernel function for the pullback of its kernel symbol sum.

Proof. The assumptions imply $\beta^* \operatorname{div} f = \operatorname{div} g$. Now we consider the normalization. Since f and g are kernel functions,

$$\frac{g}{\prod_\gamma(t'\circ\gamma\beta)}(\mathcal{O}'') = \left(\frac{dt'}{\omega'}(\mathcal{O}')\right)^{-\sum_\gamma 1}.$$

and

$$\frac{f\circ\beta}{\prod_\gamma(t'\circ\gamma\circ\beta)}(\mathcal{O}'') = \frac{f}{\prod_\gamma(t'\circ\gamma)}(\mathcal{O}) = \left(\frac{dt'}{\omega'}(\mathcal{O}')\right)^{-\sum_\gamma 1}.$$

Therefore, the normalizations agree. □

Theorem 10 (First chain rule)**.** *If α and β are unbiased, then*

$$\Psi_{\alpha\beta} = (\Psi_\alpha\circ\beta)\,\Psi_\beta^{\deg\alpha}$$

Otherwise, we have

$$\left(\frac{\Psi_{\alpha\beta}}{(\Psi_\alpha\circ\beta)\,\Psi_\beta^{\deg\alpha}}\right)^2 = \frac{\widehat{\Psi}_{\alpha\beta}}{(\widehat{\Psi}_\alpha\circ\beta)\widehat{\Psi}_\beta^{\deg\alpha}}.$$

Proof. We begin with the second equation. Using Lemma 9, the left side is a kernel function with kernel symbol sum

$$\begin{aligned}&2((K_{\alpha\beta}) + (K_{g_{\alpha\beta}}) - \beta^*(K_\alpha) - \beta^*(K_{g_\alpha}) - \deg\alpha(K_\beta) - \deg\alpha(K_{g_\beta})\\ &+ \beta^*(\deg\alpha + \deg g_\alpha)(K_1) - (\deg g_{\alpha\beta} - \deg\alpha\deg g_\beta)(K_1))\\ &= 2((K_{g_{\alpha\beta}}) - \beta^*(K_{g_\alpha}) - \deg\alpha(K_{g_\beta}) + \beta^*\deg g_\alpha(K_1) - (\deg g_{\alpha\beta} - \deg\alpha\deg g_\beta)(K_1))\\ &+ 2(K_{\alpha\beta}) - 2\deg\alpha(K_\beta) - 2\beta^*(K_\alpha) + 2\beta^*\deg\alpha(K_1)\\ &= 2((K_{g_{\alpha\beta}}) - \beta^*(K_{g_\alpha}) - \deg\alpha(K_{g_\beta}) + \beta^*\deg g_\alpha(K_1) - (\deg g_{\alpha\beta} - \deg\alpha\deg g_\beta)(K_1)).\end{aligned}$$

The right side is a kernel function whose kernel symbol sum is this same quantity. Therefore the two sides have the same divisor and normalization. The first equation is calculated similarly (but more simply). □

The preceding result in the biased case is somewhat unsatisfying. However, in certain cases the relationship simplifies. The following follows immediately from Lemma 4, Lemma 9 and Lemma 1.

Theorem 11 (Second chain rule)**.** *Suppose* $\sum_{\alpha\in\mathrm{Hom}(E'',E')} e_\alpha q(\alpha) = 0$ *is a finite integral quadratic identity. Let* $\beta : E'' \to E$ *be non-zero, such that* $e_\alpha = 0$ *for* α *not factoring through* β*. Then*

$$\left(\prod_{\gamma\in\mathrm{Hom}(E,E')} \Psi_\gamma^{e_{\gamma\beta}} \sqrt{\prod_{\gamma\in\mathrm{Hom}(E,E')} \widehat{\Psi}_\gamma^{e_{\gamma\beta}}}\right)\circ\beta = \prod_{\gamma\in\mathrm{Hom}(E,E')} \Psi_{\gamma\beta}^{e_{\gamma\beta}} \sqrt{\prod_{\gamma\in\mathrm{Hom}(E,E')} \widehat{\Psi}_{\gamma\beta}^{e_{\gamma\beta}}}.$$

The quantity is independent of the choice of invariant differential on E *and* E''*. If, in addition,* $\sum_\gamma e_{\gamma\beta} = 0$*, then the quantity in question is independent of the choice of invariant differential on* E'*.*

4. Specialization and elliptic nets

Specializing (evaluating) Ψ_ϕ at a specific point $P \in E$, we obtain a sequence of values of the field satisfying the recurrence relations (10) and (11). Observe that we have a choice of ω_i. Fix a particular point $P \in E$. We can choose ω_i, $i = 1, 2, 3$ so that $\widehat{\Psi}_i(P) = 1$; by our convention (6), this dictates the choice of $\omega = \omega_0$. In this case, the extra factors of $\widehat{\Psi}$ disappear and we recover the usual recurrences (2) and (3) for that value of P. We cannot, however, choose such a normalization globally (that is, simultaneously for all P).

Definition 12. *The collection* $\Psi_\phi(P)$ *is called* consonant *if the* ω_i *are chosen so that* $\widehat{\Psi}_i(P) = 1$ *for all* $i = 1, 2, 3$*.*

Lemma 13. *A consonant collection* $\Psi_\phi(P)$ *satisfies* (2) *and* (3)*.*

Next we recall some general results classifying collections satisfying (3).

Net polynomials [11] generalize dvision polynomials. Define for any vector $\vec{a} = (a_1, \ldots, a_k) \in \mathbb{Z}^k$, an elliptic function $\Psi_{\vec{a}}$ on E^k with divisor

$$\left(\sum a_i P_i = \mathbf{0}\right) - \sum_i a_i^2 (P_i = \mathcal{O}) - \sum_{i<j} a_i a_j \left((P_i + P_j = \mathcal{O}) - (P_i = \mathcal{O}) - (P_j = \mathcal{O})\right), \tag{12}$$

and normalized in a manner similar to the previous cases, namely, where we denote by σ the summation function $(P_1, \ldots, P_k) \mapsto P_1 + \cdots + P_k$, and by π_i the projection onto the i-th component, and require

$$\frac{\Psi_{\vec{a}} \prod_i (t^{a_i^2 - \sum_{j\neq i} a_i a_j} \circ \pi_i) \prod_{i<j} t^{a_i a_j} \circ (\sigma \circ (\pi_i \times \pi_j))}{t \circ \sigma \circ (a_1 \times \cdots \times a_k)}(\mathcal{O}) = \left(\frac{dt}{\omega}(\mathcal{O})\right)^{\sum_i a_i^2 - \sum_{i<j} a_i a_j - 1}. \tag{13}$$

The means of normalizing in [11] differs, but amounts to the same thing: in both means of normalizing, the dependence on ω is the same [11, Proposition 7.1], and $\Psi_{\mathbf{e}_i}(P) = 1$ for the standard basis vectors $\mathbf{e}_i$.

Interpreting the indices of (2) and (3) as elements of $\mathbb{Z}^k$, the $\Psi_{\vec{a}}$ satisfy both recurrences [11, Theorem 4.1]. More generally, we call any k-dimensional array which satisfies (3) an *elliptic net* [11, Definition 1.1].

The $\psi_{\vec{a}}$ also satisfy the usual relationship to x [11, Lemma 4.2], and a version of the chain rule [11, Proposition 4.3], namely, for a $k \times k$ linear transformation T, and standard basis vectors $\mathbf{e}_i$,

$$(\Psi_{\vec{a}} \circ T) \prod_{i=1}^k \Psi_{T^{tr}(\mathbf{e}_i)}^{a_i^2 - \sum_{j\neq i} a_i a_j} \prod_{i<j} \Psi_{T^{tr}(\mathbf{e}_i + \mathbf{e}_j)}^{a_i a_j} = \Psi_{T^{tr}(\vec{a})}.$$

Ward's theorem classifying elliptic divisibility sequences extends to elliptic nets [11, Theorem 7.4]. This result states that, up to appropriate equivalences and normalizations and degenerate cases, n-dimensional arrays satisfying (3) are in bijection with tuples $(E, P_1, \ldots, P_n)$. In particular, since for a fixed point P, the $\Psi_{\phi_i}(P)$ satisfy (3) (after suitable normalization), we can conclude that they form an elliptic net of the form $\Psi_{\vec{a}}(P_1, \ldots, P_k)$ for some choice of curve E and points $P_i \in E$. The following theorem verifies this constructively.

Theorem 14. *Let* $\phi_1, \ldots, \phi_n \in \mathrm{Hom}(E, E')$*. Let* $P \in E$*. Suppose that* $\phi_i(P) \notin E'[2]$ *and* $(\phi_i \pm \phi_j)(P) \neq 0$ *for all* i, j*. Choose the* ω_i *so that the resulting division polynomials* $W(\vec{a}) := \Psi_{\sum a_i \phi_i}(P)$ *form a consonant collection. Then they form an elliptic net associated to* E' *and the points* $\phi_i(P)$*.*

Proof. This is an application of the chain rule. In particular, since the collection is consonant, it forms an elliptic net in the sense that it satisfies (3), where the indices $\vec{a}$ are interpreted as $\sum_i a_i\phi_i$. To apply [11, Theorem 7.4], we require that the elliptic net be non-degenerate. That is, we require $\Psi_{\phi_i}(P)$, $\Psi_{2\phi_i}(P)$, $\Psi_{\phi_i+\phi_j}(P)$ and $\Psi_{\phi_i-\phi_j}(P)$ to be non-zero. This is guaranteed by the hypotheses.

To figure out which curve and points this elliptic net represents, we can look at elliptic divisibility sequences $\Psi_{n\phi_i}(P)$, $n \in \mathbb{Z}$ for each i. Fixing i, by the chain rule (Theorem 10), using the assumption the collection is consonant,

$$\Psi_{n\phi_i}(P) = \Psi_n(\phi_i(P))\Psi_{\phi_i}(P)^{n^2}.$$

Thus, up to normalization, the associated curve and point are E' and $\phi_i(P)$. From this we conclude that the elliptic net is that associated to $(E', \phi_1(P), \ldots, \phi_n(P))$. □

This shows that the collection of division polynomials Ψ_α for $\alpha \in \mathrm{End}(E)$ (differentials suitably normalized) form an elliptic net whose rank is equal to the rank of the endomorphism ring $\mathrm{End}(E)$. In particular, by the classification theorem for the endomorphism ring of an elliptic curve, these are equivalent to an elliptic net associated to a single, pair or quadruple of points.

The term *magnified* has been applied to elliptic divisibility sequences associated to image points of rational isogenies; see for example [4].

5. Example

Let $E : y^2 = x^3 - x$, which is an elliptic curve with complex multiplication by $\mathbb{Z}[i]$. In particular, $[i] : (x, y) \mapsto (-x, yi)$ and $E[2] = \{(0,0), (1,0), (-1,0)\}$. We also have

$$\begin{aligned}
&\Psi_1 = 1, \quad \Psi_2 = 2y, \quad \Psi_3 = 3\left(x^4 - 2x^2 - \frac{1}{3}\right),\\
&\Psi_4 = 4y(x+i)(x-i)(x^2-2x-1)(x^2+2x+1),\\
&\Psi_5 = 5\left(x^2 - \frac{2}{5}i - \frac{1}{5}\right)\left(x^2 + \frac{2}{5}i - \frac{1}{5}\right)\left(x^8 - 12x^6 - 26x^4 + 52x^2 + 1\right).
\end{aligned}$$

Now, Ψ_i is constant, and to determine the constant, we have the requirement that

$$\frac{t\Psi_i}{t \circ [i]}(\mathcal{O}) = 1,$$

which implies that $\Psi_i = i$. Similarly, we can compute

$$\begin{aligned}
&\Psi_i = i, \quad \Psi_{1+i} = 2ix, \quad \Psi_{1-i} = -2ix,\\
&\Psi_{1+2i} = (1+2i)\left(x^2 + \frac{2}{5}i - \frac{1}{5}\right), \quad \Psi_{1-2i} = (1-2i)\left(x^2 - \frac{2}{5}i - \frac{1}{5}\right),\\
&\Psi_{2+i} = (2+i)\left(x^2 - \frac{2}{5}i - \frac{1}{5}\right), \quad \Psi_{2-i} = (2-i)\left(x^2 + \frac{2}{5}i - \frac{1}{5}\right),\\
&\Psi_{2+2i} = 4iy(x-i)(x+i).
\end{aligned}$$

Regarding the last, the kernel of $2+2i$ is $\{\mathcal{O}, (0,0), (1,0), (-1,0), \pm(-i, i+1), \pm(i, i-1)\}$. Observe that both Ψ_{1+i} and Ψ_2 divide Ψ_{2+2i}.

Let $\alpha = 1+i$, $\beta = i$, $\gamma = 1$. Then we have

$$\begin{aligned}
\frac{\Psi_{\alpha+\beta}\Psi_{\alpha-\beta}\widehat{\Psi}_\alpha\widehat{\Psi}_\beta}{\Psi_\alpha^2\Psi_\beta^2\widehat{\Psi}_{\alpha+\beta}} &= \frac{\Psi_{1+2i}\Psi_1\widehat{\Psi}_{1+i}\widehat{\Psi}_i}{\Psi_{1+i}^2\Psi_i^2\widehat{\Psi}_{1+2i}} = \frac{(1+2i)\left(x^2 + \frac{2}{5}i - \frac{1}{5}\right)2ixi}{(2i)^2x^2}\\
\frac{\Psi_{\beta+\gamma}\Psi_{\beta-\gamma}\widehat{\Psi}_\beta\widehat{\Psi}_\gamma}{\Psi_\beta^2\Psi_\gamma^2\widehat{\Psi}_{\beta+\gamma}} &= \frac{\Psi_{1+i}\Psi_{i-1}\widehat{\Psi}_i\widehat{\Psi}_1}{\Psi_i^2\Psi_1^2\widehat{\Psi}_{1+i}} = \frac{(2i)x(-2i)xi}{i^2(2i)x}\\
\frac{\Psi_{\gamma+\alpha}\Psi_{\gamma-\alpha}\widehat{\Psi}_\gamma\widehat{\Psi}_\alpha}{\Psi_\gamma^2\Psi_\alpha^2\widehat{\Psi}_{\gamma+\alpha}} &= \frac{\Psi_{2+i}\Psi_{-i}\widehat{\Psi}_1\widehat{\Psi}_{1+i}}{\Psi_1^2\Psi_{1+i}^2\widehat{\Psi}_{2+i}} = \frac{(2+i)\left(x^2 - \frac{2}{5}i - \frac{1}{5}\right)(-i)(2i)x}{(2i)^2x^2i}
\end{aligned}$$

Plugging these in verifies (10) in this example.

There is a rational isogeny from E to $E' : y^2 = x^3 - 11x - 14$ given by

$$\phi_{(1,0)} : (x, y) \mapsto \left(\frac{x^2 - x + 2}{x - 1}, \frac{y(x^2 - 2x - 1)}{x^2 - 2x + 1} \right)$$

with kernel $\{(1, 0), \mathcal{O}\}$. To compute the associated division polynomial, observe that $x - 1$ has the correct divisor. To set the normalization, choose the normalized invariant differential on the target curve and compute

$$\phi T = -\frac{x'}{y'} = -\frac{(x^2 - x + 2)(x^2 - 2x + 1)}{y(x - 1)(x^2 - 2x - 1)} = -\frac{x}{y}\frac{T^{-6} + \cdots}{T^{-6} + \cdots} = T + \cdots .$$

So we obtain

$$\Psi_\phi = x - 1.$$

The kernel of $\phi \circ (1 + i)$ is cyclic of order 4:

$$\{\mathcal{O}, (i, i - 1), (i, -i - 1), (0, 0)\}.$$

This has trivial kernel sum. Therefore, up to a scalar, the kernel polynomial is

$$x(x - i).$$

Combining the known scalars for ϕ and $1 + i$, we have

$$\Psi_{\phi\circ(1+i)} = 2ix(x - i).$$

We also have

$$\widehat{\Psi}_\phi \circ (1 + i) = \frac{(x - i)^2}{2ix}, \quad \widehat{\Psi}_{\phi\circ(1+i)} = \widehat{\Psi}_{1+i} = 2ix$$

We verify the chain rule by checking

$$\left(\frac{\Psi_{\phi\circ(1+i)}}{\Psi_\phi \circ (1 + i))\Psi_{1+i}^2} \right)^2 = \frac{1}{(x - i)^2} = \frac{\widehat{\Psi}_{\phi\circ(1+i)}}{\widehat{\Psi}_\phi \circ (1 + i))\widehat{\Psi}_{1+i}^2}.$$

6. Higher dimension

The definitions and result for Ψ_ϕ can be extended to higher dimension, in the same fashion as for elliptic nets. Let $\langle \phi, \phi' \rangle = \frac{1}{2}(\deg(\phi + \phi') - \deg \phi - \deg \phi')$. Define for any vector $\vec{\phi} = (\phi_1, \ldots, \phi_k)$ whose entries are isogenies $\phi_i : E \to E'$, an elliptic function $\Psi_{\vec{\phi}}$ on E^k with divisor

(14)
$$(\vec{\phi} \cdot \mathbf{P} = \mathbf{0}) + \sum_i (P_i = P_{\phi_i}) - \sum_i (\deg \phi_i + 1)(P_i = \mathcal{O}) - \sum_{i<j} \langle \phi_i, \phi_j \rangle \left((P_i + P_j = \mathcal{O}) - (P_i = \mathcal{O}) - (P_j = \mathcal{O}) \right),$$

and normalized in a manner similar, namely, where we denote by σ the summation function $(P_1, \ldots, P_k) \mapsto P_1 + \cdots + P_k$, and by π_i the projection onto the i-th component, and require

(15)
$$\begin{aligned} &\frac{\Psi_{\vec{\phi}} \prod_i (t^{\deg \phi_i + \deg g_{\phi_i} - \sum_{j \neq i} \langle \phi_i, \phi_j \rangle} \circ \pi_i) \prod_{i<j} t^{\langle \phi_i, \phi_j \rangle} \circ (\sigma \circ (\pi_i \times \pi_j))}{(t' \circ \sigma \circ (\phi_1 \times \cdots \times \phi_k)) \prod_i (t_{\phi_i} \circ g_{\phi_i} \circ \pi_i)}(\mathcal{O}) \\ &= \left(\frac{dt}{\omega}(\mathcal{O}) \right)^{\sum_i (\deg \phi_i + \deg g_{\phi_i}) - \sum_{i<j} \langle \phi_i, \phi_j \rangle} \left(\frac{dt'}{\omega'}(\mathcal{O}') \right)^{-1} \prod_i \left(\frac{dt_{\phi_i}}{\omega_{\phi_i}}(\mathcal{O}_{\phi_i}) \right)^{-1}. \end{aligned}$$

One can verify that, in each individual copy of E, the function above is an elliptic function. One can define

$$\widehat{\Psi}_{\vec{\phi}} = \prod_i \widehat{\Psi}_{\phi_i},$$

and $\tilde{\Psi}_{\vec{\phi}}$ so $\widehat{\Psi}_{\vec{\phi}} \tilde{\Psi}_{\vec{\phi}} = \Psi_{\vec{\phi}}$. The formal group expansion becomes

$$\Psi_{\vec{\phi}}(T) = \left(\prod_i a_{\phi_i} a_{\iota(\phi_i)} \right) T^{-\sum_i (\deg \phi_i + \deg g_{\phi_i} - \deg_{in} \phi_i - \deg_{in} g_{\phi_i}) + \sum_{i<j} \langle \phi_i, \phi_j \rangle} + \cdots .$$

Lemma 4 holds where the α are interpreted as vectors, and the relation to x can be given as

$$\frac{\Psi_{\vec{\alpha}+\vec{\beta}}\Psi_{\vec{\alpha}-\vec{\beta}}\widehat{\Psi}_{\vec{\alpha}}\widehat{\Psi}_{\vec{\beta}}}{\Psi_{\vec{\alpha}}^2\Psi_{\vec{\beta}}^2\widehat{\Psi}_{\vec{\alpha}+\vec{\beta}}} = x' \circ \sigma \circ \prod_i \alpha_i - x' \circ \sigma \circ \prod_i \beta_i.$$

The first and second recurrence relations (Corollaries 6 and 8) work out the same, where we interpret the indices as vectors of endomorphisms.

The final consideration is the chain rule, and one can show a version of the elliptic net chain rule for isogenies. Let $T : E''^k \to E^k$ be a linear transformation. Then we have $T^{tr} : \mathrm{Hom}(E, E')^k \to \mathrm{Hom}(E'', E')^k$.

Theorem 15 (First chain rule in higher dimension)**.** *Let T be as above. Let $\vec{\phi} \in \mathrm{Hom}(E, E')^k$, i.e. $\phi_i : E \to E'$. Then whenever all coordinate isogenies in the subscripts are unbiased, we have*

$$(\Psi_{\vec{\phi}} \circ T) \prod_{i=1}^{k} \Psi_{T^{tr}(\mathbf{e}_i)}^{\deg \phi_i - \sum_{j\neq i}\langle \phi_i, \phi_j\rangle} \prod_{i<j} \Psi_{T^{tr}(\mathbf{e}_i+\mathbf{e}_j)}^{\langle \phi_i, \phi_j\rangle} = \Psi_{T^{tr}(\vec{\phi})}.$$

In general, we have

$$\left(\frac{(\Psi_{\vec{\phi}} \circ T) \prod_{i=1}^{k} \Psi_{T^{tr}(\mathbf{e}_i)}^{\deg \phi_i - \sum_{j\neq i}\langle \phi_i, \phi_j\rangle} \prod_{i<j} \Psi_{T^{tr}(\mathbf{e}_i+\mathbf{e}_j)}^{\langle \phi_i, \phi_j\rangle}}{\Psi_{T^{tr}(\vec{\phi})}} \right)^2 = \frac{(\widehat{\Psi}_{\vec{\phi}} \circ T) \prod_{i=1}^{k} \widehat{\Psi}_{T^{tr}(\mathbf{e}_i)}^{\deg \phi_i - \sum_{j\neq i}\langle \phi_i, \phi_j\rangle} \prod_{i<j} \widehat{\Psi}_{T^{tr}(\mathbf{e}_i+\mathbf{e}_j)}^{\langle \phi_i, \phi_j\rangle}}{\widehat{\Psi}_{T^{tr}(\vec{\phi})}}.$$

Theorem 16 (Second chain rule in higher dimension)**.** *Let T be as above. Suppose $\sum_{\vec{\alpha}\in \mathrm{Hom}(E'',E')^k} e_{\vec{\alpha}} q(\vec{\alpha}) = 0$ is a finite integral quadratic identity. Suppose $e_{\vec{\alpha}} = 0$ whenever α is not in the image of T^{tr}. Then*

$$\left(\prod_{\vec{\gamma}\in \mathrm{Hom}(E,E')^k} \Psi_{\vec{\gamma}}^{e_{T^{tr}(\vec{\gamma})}} \sqrt{\prod_{\vec{\gamma}\in \mathrm{Hom}(E,E')^k} \widehat{\Psi}_{\vec{\gamma}}^{e_{T^{tr}(\vec{\gamma})}}} \right) \circ T = \prod_{\vec{\gamma}\in \mathrm{Hom}(E,E')^k} \Psi_{T^{tr}(\vec{\gamma})}^{e_{T^{tr}(\vec{\gamma})}} \sqrt{\prod_{\vec{\gamma}\in \mathrm{Hom}(E,E')^k} \widehat{\Psi}_{T^{tr}(\vec{\gamma})}^{e_{T^{tr}(\vec{\gamma})}}}.$$

References

[1] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. In *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *Open Book Ser.*, pages 39–55. Math. Sci. Publ., Berkeley, CA, 2020.

[2] K. P. S. Bhaskara Rao and J. D. Reid. Abelian groups that are unions of proper subgroups. *Bull. Austral. Math. Soc.*, 45(1):1–7, 1992.

[3] A. Bostan, F. Morain, B. Salvy, and É. Schost. Fast algorithms for computing isogenies between elliptic curves. *Math. Comp.*, 77(263):1755–1778, 2008.

[4] Graham Everest, Patrick Ingram, Valéry Mahé, and Shaun Stevens. The uniform primality conjecture for elliptic curves. *Acta Arith.*, 134(2):157–181, 2008.

[5] David Russel Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkeley, 1996.

[6] Ömer Küçüksakallı. On the computation of generalized division polynomials. *Turkish J. Math.*, 39(4):547–555, 2015.

[7] B. Mazur and J. Tate. The p-adic sigma function. *Duke Math. J.*, 62(3):663–688, 1991.

[8] Takakazu Satoh. Generalized division polynomials. *Math. Scand.*, 94(2):161–184, 2004.

[9] René Schoof. Counting points on elliptic curves over finite fields. volume 7, pages 219–254. 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[10] Joseph H. Silverman. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory*, 30(2):226–237, 1988.

[11] Katherine Stange. Elliptic nets and elliptic curves. *Algebra Number Theory*, 5(2):197–229, 2011.

[12] H. M. Stark. Class-numbers of complex quadratic fields. In *Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, volume Vol. 320 of *Lecture Notes in Math.*, pages 153–174. Springer, Berlin-New York, 1973.

[13] Marco Streng. Divisibility sequences for elliptic curves with complex multiplication. *Algebra Number Theory*, 2(2):183–208, 2008.

[14] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[15] Morgan Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.

University of Colorado Boulder, Boulder, Colorado, USA
Email address: kstange@math.colorado.edu
URL: https://math.katestange.net/