ALGEBRAIC PROOFS FOR ELLIPTIC DIVISIBILITY SEQUENCES AND DIVISION POLYNOMIALS OF ELLIPTIC CURVES

JUNYAN XU

ABSTRACT. We give a purely algebraic proof of the formula $nP = (\phi_n(x,y) : \omega_n(x,y) : \psi_n(x,y))$ in Jacobian coordinates where $P = (x,y) = (x : y : 1)$ is a nonsingular point on the curve given by a long Weierstrass equation $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$, and ϕ_n, ω_n, ψ_n are explicit polynomials in $a_1, a_2, a_3, a_4, a_6, X, Y$ with integer coefficients, with ψ_n the well-known division polynomials. As a prerequisite, we give purely algebraic proofs that the even-odd recurrence used to define ψ_n and a particular Somos 4 recurrence both give rise to elliptic divisibility sequences.

1. NOTATIONS AND THE STATEMENT

This note is aimed at proving in a purely algebraic way a well-known explicit formula for scalar product nP for $n \in \mathbb{Z}$ and $P \neq O$ a nonsingular point on a curve in long Weierstrass form. To state the formula, we introduce the following notations:

- Let $J(X,Y,Z) := Y^2 + a_1XYZ + a_3YZ^3 - (X^3 + a_2X^2Z^2 + a_4XZ^4 + a_6Z^6)$ denote the (2,3,1)-homogeneous Weierstrass polynomial, so that $J(X,Y,Z) = 0$ is the equation in Jacobian coordinates of the curve. a_i $(i = 1,2,3,4,6)$ can be explicit elements in a field, or indeterminates in a polynomial ring.
- Let $J_X(X,Y,Z) := 3X^2 + 2a_2XZ^2 + a_4Z^4 - a_1YZ$ denote the negation of the partial derivative of J w.r.t. X.
- Let $J_Y(X,Y,Z) := 2Y + a_1XZ + a_3Z^3$ denote the partial derivative of J w.r.t. Y.
- Given a field K and $a_1, \ldots, a_6 \in K$, a point $P = (x : y : z)$ on the curve J over K (a K-point of J) is an equivalence class of triples $(x,y,z) \neq (0,0,0)$ satisfying $J(x,y,z) = 0$ under the equivalence relation $(x,y,z) \sim (u^2x, u^3y, uz)$ $(u \in K \setminus \{0\})$.

If $z \neq 0$, P corresponds to the point $(x/z^2, y/z^3)$ on the affine curve $J(X, Y, 1) = 0$, and if $z = 0$, then both x and y are nonzero, and P is the unique point at infinity $((y/x)^2 : (y/x)^3 : 0) = (1 : 1 : 0)$.

- A point $(x : y : z)$ of J over a field is nonsingular if $J_X(x, y, z) \neq 0$ or $J_Y(x, y, z) \neq 0$. The set of nonsingular K-points of J is denoted $J(K)$ and is an abelian group by transferring the well-known group law in affine coordinates (cf. [1]). We will discuss the group law in Jacobian coordinates in Section 2.
- Define

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2 \\ b_4 &:= 2a_4 + a_1a_3 \\ b_6 &:= a_3^2 + 4a_6 \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

  Notice that if we assign weight i to a_i, then b_i also has weight i.
- ([2], Exercise 3.7) Define **division polynomials** $\{\psi_n\}_{n\in\mathbb{Z}} \subseteq \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, X, Y]$ by the recurrence*

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \qquad \text{for } n \geq 2 \tag{1a}$$

$$\psi_2\psi_{2n} = \psi_n(\psi_{n-1}^2\psi_{n+2} - \psi_{n-2}\psi_{n+1}^2) \qquad \text{for } n \geq 3 \tag{1b}$$

$$\psi_n = -\psi_{-n} \qquad \text{for } n < 0 \tag{1c}$$

*Since ψ_2 is a nonzero element in the polynomial ring over $\mathbb{Z}$ (which is an integral domain), it is not a zero divisor, so ψ_{2n} is a well-defined polynomial provided that the right-hand side of the second equation is divisible by ψ_2, which can be proven by induction: either n is even and $\psi_n\psi_{n+2}$ and $\psi_n\psi_{n-2}$ are divisible by ψ_2^2, or n is odd and ψ_{n-1}^2 and ψ_{n+1}^2 are divisible by ψ_2^2.

Alternatively, it is also possible to define an auxiliary sequence $\{\tilde{\psi}_n\}_{n\in\mathbb{Z}}$ in a division-free way such that $\psi_n = \tilde{\psi}_n$ for n odd and $\psi_n = \psi_2\tilde{\psi}_n$ for n even. See `normEDS` in mathlib, [9], or Section 5.

and initial values*

$$\psi_0 = 0, \psi_1 = 1$$

$$\psi_2 = 2Y + a_1X + a_3 = J_Y(X, Y, 1)$$

$$\psi_3 = 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8$$

$$\psi_4 = \psi_2(2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + b_4b_8 - b_6^2)$$

We also define

$$\psi_n^c = (\psi_{n-1}^2\psi_{n+2} - \psi_{n-2}\psi_{n+1}^2)/\psi_2, \tag{1d}$$

so that

$$\psi_{2n} = \psi_n\psi_n^c, \tag{1e}$$

and

$$\psi_2^{2(1)} = 4X^3 + b_2X^2 + 2b_4X + b_6 = \psi_2^2 - 4J(X, Y, 1) \tag{1f}$$

which is a polynomial in a single variable that evaluates to ψ_2^2 when applied to a point on J.

- If we assign weight 2 to X, 3 to Y, and i to a_i, we can check that ψ_n is weighted homogeneous of degree $n^2 - 1$ for $n = 1, 2, 3, 4$ and by induction for all n, and that ψ_n^c has degree $3n^2$.

  In general, for a weighted homogeneous polynomial f in $\mathbb{Z}[a_1, \ldots, a_6, X, Y]$ of degree $d(f)$, we can consider its homogenization w.r.t. a new variable Z:

$$f^h := Z^{d(f)}f(X/Z^2, Y/Z^3) \tag{2}$$

*Exercise 3.7 in [2] does not cover the $n \leq 0$ cases, even though e.g. the definition of ω_1 depends on ψ_{-1} and ϕ_1 depends on ψ_0.

which can be obtained by replacing each term cX^iY^j by $cX^iY^jZ^{d(c)}$, where $d(c)$ is the degree of the coefficient c, a homogeneous polynomial in indeterminates $a_1, \ldots, a_6$. The resulting f^h is homogeneous of the same degree $d(f)$ if we assign weight 2 to X, 3 to Y, 1 to Z, and 0 to a_i.

If we substitute a homogeneous polynomial of degree $2k$ into X, one of degree $3k$ into Y and one of degree $k-1$ into Z in f^h, we again get a homogeneous polynomial, of degree $d(f)k$. ϕ_n and ω_n defined below form such a valid triple with ψ_n, with $k = n^2$.

As examples, we have $\psi_2^h = J_Y$ and $\psi_3^h = 3X^4+b_2X^3Z^2+3b_4X^2Z^4+3b_6XZ^6+b_8Z^8$.

- Define two more sequences of polynomials $\{\phi_n\}_{n\in\mathbb{Z}}, \{\omega_n\}_{n\in\mathbb{Z}}$ by the equations

$$\phi_n = X\psi_n^2 - \psi_{n-1}\psi_{n+1} \tag{3a}$$

$$\psi_n^c = J_Y(\phi_n, \omega_n, \psi_n) \tag{3b}$$

Solving for ω_n we obtain

$$\omega_n = (\psi_n^c - a_1\phi_n\psi_n - a_3\psi_n^3)/2, \tag{3c}$$ [†]

which does not obviously have coefficients in $\mathbb{Z}$, but we will assume this for now and prove it later in Section 3. An easy computations shows ϕ_n has degree $2n^2$ and ω_n has degree $3n^2$.

For convenience, we shall use P_n to denote the triple of polynomials $(\phi_n, \omega_n, \psi_n)$, so for a polynomial f in X, Y, Z, $f(P_n)$ means $f(\phi_n, \omega_n, \psi_n)$, and for a polynomial f in $X_1, Y_1, Z_1, X_2, Y_2, Z_2$, $f(P_m, P_n)$ means $f(\phi_m, \omega_m, \psi_m, \phi_n, \omega_n, \psi_n)$. If f is a polynomial in X, Y only, we take $f(P_n)$ to mean $f(\phi_n/\psi_n^2, \omega_n/\psi_n^3)$. For homogeneous $f \in \mathbb{Z}[a_1, \ldots, a_6, X, Y]$ we therefore have $f^h(P_n) = \psi_n^{d(f)} f(P_n)$ according to (2). An important

[†]Exercise 3.7 in [2] neglects the a_1 and a_3 terms; [8] gives the correct definition.

example is

$$2\frac{\omega_n}{\psi_n^3} + \frac{\phi_n}{\psi_n^2} + a_3 = \psi_2(P_n) = \frac{\psi_2^h(P_n)}{\psi_n^3} = \frac{J_Y(P_n)}{\psi_n^3} = \frac{\psi_n^c}{\psi_n^3} = \frac{\psi_{2n}}{\psi_n^4}. \tag{3d}$$

The main theorem we will prove is

Theorem 1. *Let K be a field, $a_1, a_2, a_3, a_4, a_6 \in K$, and $P = (x, y) = (x : y : 1) \in J(K)$. Then we have*

$$nP = (\phi_n(x, y) : \omega_n(x, y) : \psi_n(x, y)) \tag{4}$$

for every $n \in \mathbb{Z}$.

This is Exercise 3.7(d) in [2], but without assuming J is nonsingular everywhere. It is easy to verify that

$$\begin{aligned} \psi_0^c &= 2, & (\phi_0 : \omega_0 : \psi_0) &= (1 : 1 : 0) = O \\ \psi_1^c &= \psi_2, & (\phi_1 : \omega_1 : \psi_1) &= (X : Y : 1) = P \\ \psi_{-n}^c &= \psi_n^c, & (\phi_{-n} : \omega_{-n} : \psi_{-n}) &= (\phi_n : J_Y(\phi_n, \omega_n, \psi_n) - \omega_n : -\psi_n) = -P \end{aligned}$$

so we only need to deal with $n \geq 2$. (For the last equality in each row, we need to plug in $X = x$ and $Y = y$, or else consider the universal point $P = (X, Y)$ on the universal curve.) It turns out (see Section 2) that there exists "doubling polynomials" $D_X, D_Y, D_Z \in \mathbb{Z}[a_1, \ldots, a_6, X, Y, Z]$ and "addition polynomials" $A_X, A_Y, A_Z \in \mathbb{Z}[a_1, \ldots, a_6, X_1, Y_1, Z_1, X_2, Y_2, Z_2]$ such that for any field K and $P := (x : y : z) = (x_1 : y_1 : z_1), Q := (x_2 : y_2 : z_2) \in J(K)$, we have

$$P + Q = (A_X(x_1, y_1, z_1, x_2, y_2, z_2) : A_Y(x_1, y_1, z_1, x_2, y_2, z_2) : A_Z(x_1, y_1, z_1, x_2, y_2, z_2)) \text{ if } P \neq Q$$

$$P + P = (D_X(x, y, z) : D_Y(x, y, z) : D_Z(x, y, z))$$

This is a particularly nice property of the Jacobian coordinates, which e.g. the projective coordinates do not enjoy (and in affine coordinates it is definitely necesary to special-case $P = O$, $Q = O$ and $P + Q = O$). In fact we have $A_Z = X_1 Z_2^2 - X_2 Z_1^2$ (independent of Y_1, Y_2) and $D_Z = Z J_Y$, both weighted homogeneous of degree 4, which forces A_X and D_X to have degree 8 and A_Y and D_Y to have degree 12.

Now assume Formula (4) is true for all positive $m < n$, and split into two cases ($n = 2m + 1$ and $n = 2m$) following the proof of Theorem 5.21 in [3]. In the first case we know $mP = (\phi_m(x, y) : \omega_m(x, y) : \psi_m(x, y))$ and $(m+1)P = (\phi_{m+1}(x, y) : \omega_{m+1}(x, y) : \psi_{m+1}(x, y))$ by induction hypothesis, and we have $mP \neq (m + 1)P$ because $P \neq O$. Therefore we just need to verify the following identities, either for specialized $a_1, \ldots, a_6, x, y \in K$ satisfying $J(x, y, 1) = 0$, or as identities between polynomials in $\mathbb{Z}[a_1, \ldots, a_6, X, Y]$ modulo $J(X, Y, 1)$, i.e. in the universal ring $U := \mathbb{Z}[a_1, \ldots, a_6, X, Y]/\langle J(X, Y, 1)\rangle$:

$$\phi_{2m+1} \equiv A_X(P_m, P_{m+1}) \tag{5a}$$

$$\omega_{2m+1} \equiv A_Y(P_m, P_{m+1}) \tag{5b}$$

$$\psi_{2m+1} \equiv A_Z(P_m, P_{m+1}) \tag{5c}$$

where we use the standard notation $\equiv$ to denote congruence (modulo $J(X, Y, 1)$ by default, and the same convention applies throughout the paper if the modulus is not specified). In the second case we know $mP = (\phi_m(x, y) : \omega_m(x, y) : \psi_m(x, y))$ so we just need to verify

$$\phi_{2m} \equiv D_X(P_m) \tag{6a}$$

$$\omega_{2m} \equiv D_Y(P_m) \tag{6b}$$

$$\psi_{2m} \equiv D_Z(P_m). \tag{6c}$$

It is interesting to note that my proofs of (6a), (6b) and (5a) also invoke $mP = (\phi_m : \omega_m : \psi_m)$ (and $(m + 1)P$ for (5a)), and not just for the specific (x, y), but the universal (X, Y) on the universal curve.

It is often convenient to work in the field of fractions $\mathrm{Frac}(U)$: $J(\mathrm{Frac}(U))$ is an abelian group with (X, Y) a nonsingular point on it (of infinite order because of (4) and $J(X, Y, 1) \nmid \psi_n$ for $n \neq 0$), so we can use group axioms (e.g. associativity) to identify rational functions in X, Y modulo $J(X, Y, 1)$.

It is easy to verify that (5c) and (6c) actually hold exactly (without modding out $J(X, Y, 1)$), as was already done in [3]: (6c) is simply the equation $\psi_{2n} = \psi_n \psi_n^c$ given (3b), and for (5c), just plug in the definition (3a) of ϕ_n:

$$\begin{aligned} A_Z(P_m, P_n) &= \phi_m \psi_n^2 - \phi_n \psi_m^2 \\ &= (X\psi_m^2 - \psi_{m+1}\psi_{m-1})\psi_n^2 - (X\psi_n^2 - \psi_{n+1}\psi_{n-1})\psi_m^2 \\ &= \psi_{n+1}\psi_{n-1}\psi_m^2 - \psi_{m+1}\psi_{m-1}\psi_n^2 = \psi_{n+m}\psi_{n-m} \end{aligned} \tag{7a}$$

where the last identity is justified by the defining equation (1a) when $n = m + 1$ and by the elliptic relation $E(n, m, 1, 0)$ (12) in general. If $n, m \neq 0$, this could also be written in the form

$$\frac{\phi_m}{\psi_m^2} - \frac{\phi_n}{\psi_n^2} = \frac{\psi_{n+m}\psi_{n-m}}{\psi_m^2 \psi_n^2}. \tag{7b}$$

At this stage, it suffices to prove Formula (4) for *elliptic* curves (i.e. nonsingular everywhere) over the complex numbers (for which one can use a complex analytic proof using the Weierstrass $\wp$ function[‡]), because the universal ring U embeds as a subring of the complex numbers[§] say via some $e : U \hookrightarrow \mathbb{C}$. Apply Formula (4) to the point $(e(X), e(Y))$ on the elliptic curve with coefficients $e(a_1), \ldots, e(a_6)$ over $\mathbb{C}$ and $n = m, m+1$ and $2m+1$: these together with (5c) and $mP + (m+1)P = (2m+1)P$ forces (5a) and (5b) to hold because $\psi_{2m+1} \neq 0$

[‡]See e.g. Theorem II.2.1 of [4], but some coordinate change will be required to derive division polynomials for curves with a_1, a_2, a_3 terms.

[§]For example, we can choose six algebraically independent complex numbers and map a_1, a_2, a_3, a_4, a_6 and X to them, and map Y to a solution of the quadratic equation $J(X, Y, 1) = 0$ in $\mathbb{C}$, which exists because $\mathbb{C}$ is algebraically closed; this defines an injective ring homomorphism because the discriminant of the quadratic equation is a polynomial of degree 3 in X and therefore cannot be a perfect square.

in U, and similarly (4) for $n = m$ and $2m$ together with (6c) and $mP + mP = (2m)P$ forces (6a) and (6b) to hold because $\psi_{2m} \neq 0$ in U for $m > 0$ (Exercise 3.7(b) of [2] shows that ψ_n^2 lies in the subring $\mathbb{Z}[a_1, \ldots, a_6, X] \subseteq U$ and has leading term $n^2 X^{n^2-1}$ as a polynomial in the single variable X). We nonetheless continue to pursue a purely algebraic proof by verifying the four remaining identities (5a, 5b, 6a, 6b).

2. Group law in Jacobian coordinates

In this section we derive formulas for A_X, A_Y, D_X and D_Y and show they indeed have coefficients in $\mathbb{Z}$. First suppose $P = (x, y) = (x_1, y_1)$ and $Q = (x_2, y_2)$ are points of J on the affine plane. If P and Q has different x-coordinates, the slope of the secant line through P and Q is

$$k = (y_1 - y_2)/(x_1 - x_2), \tag{8a}$$

so the x-coordinate of $P + Q$ is

$$x_3 = k(k + a_1) - (a_2 + x_1 + x_2), \tag{8b}$$

the y-coordinate of $-(P + Q)$ is

$$y_3^- = k(x_3 - x_1) + y_1 = kx_3 + \frac{x_1 y_2 - y_1 x_2}{x_1 - x_2}, \tag{8c}$$

and the y-coordinate of $P + Q$ is

$$y_3 = -(y_3^- + a_1 x_3 + a_3) = -\left((k + a_1)x_3 + \frac{x_1 y_2 - y_1 x_2}{x_1 - x_2} + a_3\right). \tag{8d}$$

If $P = Q$, we consider the slope of the tangent line at P instead, which is

$$k = J_X(x, y, 1)/J_Y(x, y, 1). \tag{8e}$$

If we work with Jacobian coordinates $P = (x : y : z) = (x_1 : y_1 : z_1)$ and $Q = (x_2 : y_2 : z_2)$, (8a) becomes

$$k = \frac{y_1/z_1^3 - y_2/z_2^3}{x_1/z_1^2 - x_2/z_2^2} = \frac{y_1 z_2^3 - y_2 z_1^3}{z_1 z_2 (x_1 z_2^2 - x_2 z_1^2)}, \tag{8f}$$

and (8b) becomes

$$\frac{x_3}{z_3^2} = k(k + a_1) - \left(a_2 + \frac{x_1}{z_1^2} + \frac{x_2}{z_2^2} \right), \tag{8g}$$

and it looks like that z_3 needs to be $z_1 z_2 (x_1 z_2^2 - x_2 z_1^2)$ to account for the denominator. But by some magic, $z_3 = x_1 z_2^2 - x_2 z_1^2$ is in fact enough. This can be seen by multiplying the right-hand side of (8g) by z_3^2 and replacing the x_1^3 term in $x_1 z_3^2 = x_1 (x_1 z_2^2 - x_2 z_1^2)^2$ by $x_1^3 - J(x_1, y_1, z_1)$ and similarly for the x_2^3 in $x_2 z_3^2$. This parsimonious choice of z_3 makes the formula more broadly applicable and in fact cover all cases with $P \neq Q$, including the cases $P \neq Q = O$, $Q \neq P = O$, and $P = -Q \neq Q$. A similar magic happens for y_3 (no need to substitute x^3 this time), and we arrive at the formulas

$$\begin{aligned} A_X &= -Z_1 Z_2 (2 Y_1 Y_2 + a_1 (X_1 Y_2 Z_1 + X_2 Y_1 Z_2) + a_3 (Y_1 Z_2^3 + Y_2 Z_1^3)) \\ &\quad + Z_1^2 Z_2^2 (2 a_2 X_1 X_2 + a_4 (X_1 Z_2^2 + X_2 Z_1^2)) + 2 a_6 Z_1^4 Z_2^4 + X_1 X_2 (X_1 Z_2^2 + X_2 Z_1^2) \end{aligned} \tag{9a}$$

$$A_Z = X_1 Z_2^2 - X_2 Z_1^2 \tag{9b}$$

$$A_{YZ} = Y_1 Z_2^3 - Y_2 Z_1^3 \tag{9c}$$

$$A_{XY} = X_1 Y_2 Z_1 - X_2 Y_1 Z_2 \tag{9d}$$

$$\begin{aligned} A_Y^- &= (X_1^3 Y_2 Z_2^3 - X_2^3 Y_1 Z_1^3) + a_1 (X_1 Y_2^2 Z_1^4 - X_2 Y_1^2 Z_2^4) + a_4 Z_1 Z_2 (X_1 Y_1 Z_2^5 - X_2 Y_2 Z_1^5) \\ &\quad - (2 Y_1 Y_2 - 2 a_2 X_1 X_2 Z_1 Z_2 + a_3 (Y_2 Z_1^3 + Y_1 Z_2^3) - 2 a_6 Z_1^3 Z_2^3) A_{YZ} \\ &\quad - (3 X_1 X_2 Z_1 Z_2 + a_4 Z_1^3 Z_2^3) A_{XY} - a_1 Y_1 Y_2 Z_1 Z_2 A_Z \end{aligned} \tag{9e}$$

$$A_Y = -(A_Y^- + a_1 A_X A_Z + a_3 A_Z^3) \tag{9f}$$

If we define

$$A'_X = A_{YZ}^2 + a_1 Z_1 Z_2 A_{YZ} A_Z - (a_2 Z_1^2 Z_2^2 + X_1 Z_2^2 + X_2 Z_1^2) A_Z^2 \tag{9g}$$

$$A_Y^{-\prime} = A_{YZ} A_X + A_{XY} A_Z^2 \tag{9h}$$

following (8b) and (8c), we can verify

$$Z_1^2 Z_2^2 A_X = A'_X + Z_1^6 J(X_2, Y_2, Z_2) + Z_2^6 J(X_1, Y_1, Z_1) \tag{9i}$$

$$Z_1 Z_2 A_Y^- = A_Y^{-\prime} \tag{9j}$$

The formulas (9a - 9f) have been verified by David Angdinata in Lean (A_X, A_Y). No similar magics happen for the projective coordinates, and in fact one has to take $z_3 = z_1 z_2 (x_1 z_2 - x_2 z_1)^3$; due to the presence of the factor $z_1 z_2$, there is no hope the formula can apply to $P + O$ or $O + P$ with $P \neq O$. The cube is necessary for y_3, not for x_3, so there is some inefficiency going on here, which is not present for the Jacobian coordinates, because the weighting there is exactly 2:3 for x:y.

We check that the formulas continue to work in the nontrivial case $P = -Q \neq Q$. By weighted homogeneity of A_X, we assume $z_1 = z_2 = 1$, so $x_1 = x_2 = x$ and $y \neq y_2 = -(y + a_1 x + a_3)$, i.e. $J_Y(x, y, 1) \neq 0$. We compute

$$\begin{aligned}
A_Z(x, y, 1, x, y_2, 1) &= x - x = 0 \\
A_X(x, y, 1, x, y_2, 1) &= -(-2y(y + a_1 x + a_3) - a_1 x(a_1 x + a_3) - a_3(a_1 x + a_3)) \\
&\quad + (2a_2 x^2 + 2a_4 x) + 2a_6 + 2x^3 \\
&= 2(y^2 + x^3 + a_2 x^2 + a_4 x + a_6) + (2y + a_1 x + a_3)(a_1 x + a_3) \\
&= 2(y^2 + y^2 + a_1 xy + a_3 y) + (2y + a_1 x + a_3)(a_1 x + a_3) \\
&= 2y(2y + a_1 x + a_3) + (2y + a_1 x + a_3)(a_1 x + a_3) \\
&= (2y + a_1 x + a_3)^2 = J_Y(x, y, 1)^2 \neq 0
\end{aligned}$$

where the third identity uses $J(x,y,1)=0$, and

$$\begin{aligned} A_Y(x,y,1,x,y_2,1) &= J_Y(x,y,1)(-x^3+a_1x(a_1x+a_3)+a_4x \\ &\qquad -(-2y(y+a_1x+a_3)-2a_2x^2-a_3(a_1x+a_3)-2a_6)+(3x^2+a_4)x) \\ &= J_Y(x,y,1)(2(y^2+x^3+a_2x^2+a_4x+a_6)+(2y+a_1x+a_3)(a_1x+a_3)) \\ &= J_Y(x,y,1)^3 \neq 0 \end{aligned}$$

For $Q \neq P = O$, we check $(A_X : A_Y : A_Z)$ evaluated at $(1,1,0,x,y,1)$ is $(x : y : 1)$; for $P \neq Q = O$, we check that evaluation at $(x,y,1,1,1,0)$ gives $(x : y : -1)$. If $P = Q$ it is easy to check the formulas produce $(0:0:0)$ and therefore do not work.

Next we deal with the doubling formulas. In Jacobian coordinates, (8e) becomes

$$k = \frac{J_X(x/z^2, y/z^3, 1)}{J_Y(x/z^2, y/z^3, 1)} = \frac{z^{-4}J_X(x,y,z)}{z^{-3}J_Y(x,y,z)} = \frac{J_X(x,y,z)}{zJ_Y(x,y,z)} \tag{10}$$

and it is therefore natural to take $D_Z = ZJ_Y$, and (8b) and (8d) become

$$D_X = J_X^2 + a_1ZJ_XJ_Y - (a_2Z^2+2X)J_Y^2 \tag{11a}$$

$$D_Y^- = J_X(D_X - XJ_Y^2) + YJ_Y^3 \tag{11b}$$

$$D_Y = -(D_Y^- + a_1D_XD_Z + a_3D_Z^3) \tag{11c}$$

The formulas continue to hold when $P = Q = O$, since $J_X(1,1,0) = 3$, $J_Y(1,1,0) = 2$, $D_X(1,1,0) = 3^2 - 2\cdot 1\cdot 2^2 = 1$, $D_Y^-(1,1,0) = 3(1-1\cdot 2^2)+1\cdot 2^3 = -1$, $D_Z(1,1,0) = 0$, and $D_Y(1,1,0) = 1$. It also holds when $P = -P = Q$, in which case we have $J_Y(x,y,z) = 0$, so $D_X(x,y,z) = J_X(x,y,z)^2 \neq 0$ (since $(x:y:z)$ is nonsingular), $D_Y^-(x,y,z) = J_X(x,y,z)^3$, $D_Z(x,y,z) = 0$, and $D_Y(x,y,z) = -J_X(x,y,z)^3$.

Now, bring to mind that $(\phi_2 : \omega_2 : \psi_2)$ is also supposed to give doubling formulas. Since $D_Z = Z^4\psi_2(X/Z^2, Y/Z^3)$, we should expect $D_X = Z^8\phi_2(X/Z^2, Y/Z^3)$ and $D_Y =$

$Z^{12}\omega_2(X/Z^2, Y/Z^3)$ modulo J, and indeed if we take

$$D_X = XJ_Y^2 - \psi_3^h \tag{11d}$$

$$D_Y = (\psi_2^{ch} - a_1 D_X D_Z - a_3 D_Z^3)/2 \tag{11e}$$

(where ϕ_3^h and ψ_2^{ch} are the homogenization according to (2) of ψ_3 and ψ_2^c respectively), then we can verify that (11d) − (11a) $= (12X + b_2Z^2)J$ and (11e) − (11c) $= (8Y^2 - 4a_1XYZ - (a_1b_2 - 8a_3)YZ^3 - 28X^3 - (7b_2 + 4a_1^2)X^2Z^2 - (b_2(b_2 - 2a_2) + 4(b_4 - a_4))XZ^4 - (b_2(b_4 - a_4) - 4(b_6 - 2a_6))Z^6)J$.

3. Elliptic relations and Somos recurrence

The defining recurrence (1a - 1b) of ϕ_n are special cases of the more general elliptic relation

$$E(a,b,c,d): \quad \psi_{a+b}\psi_{a-b}\psi_{c+d}\psi_{c-d} = \psi_{a+c}\psi_{a-c}\psi_{b+d}\psi_{b-d} - \psi_{b+c}\psi_{b-c}\psi_{a+d}\psi_{a-d}, \tag{12}$$

where $a, b, c, d \in \mathbb{Z}$ or a, b, c, d are all half-integers[¶]. More precisely, (1a) is $E(n+1, n, 1, 0)$ and (1b) is $E(n+1, n-1, 1, 0)$. If $\psi_0 = 0$ and $\psi_{-n} = -\psi_n$, we can check that arbitrarily permuting a, b, c, d and/or negating any number of a, b, c, d yield equivalent relations. The collection of all $E(a, b, c, d)$ is equivalent to the axiom for elliptic nets introduced in [7]. [6] and Exercise 3.7(g) and 3.34 in [2] concern the specialized relations $E(m, n, r, 0)$.

It is a surprising fact that (1a - 1b) is sufficient to imply all other elliptic relations, which is traditionally proven using elliptic functions [7, 6][‖], but we'll also give a purely algebraic proof. An especially useful family of elliptic relations is the Somos 4 recurrence

$$E(n,2,1,0): \quad \psi_{n+2}\psi_{n-2} = \psi_2^2\psi_{n+1}\psi_{n-1} - \psi_3\psi_n^2 \tag{13a}$$

[¶]Allowing the half-integer case does not make the relation more general, because the four subscripts in each term still add up to an even number, and there is at least one way to break the four subscripts into two pairs, each adding up to an even number. However, allowing half-integers is necessary to carry out certain inductive proofs about these relations.

[‖]See also Silverman's comment in [9].

which determines one term (ψ_{n+2}) of the sequence ψ from the previous four terms plus the constants ψ_2 and ψ_3, provided ψ_{n-2} is not a zero divisor. This is highlighted in Section 4.3-4.4 (page 51) in [5] and attributed to [6].

Given a sequence satisfying a Somos recurrence of the form

$$\psi_{n+2}\psi_{n-2} = A\psi_{n+1}\psi_{n-1} - B\psi_n^2, \tag{13b}$$

we show that $(\psi_{n+2}\psi_{n-1}^2 + \psi_{n+1}^2\psi_{n-2} + A\psi_n^3)/\psi_{n+1}\psi_n\psi_{n-1}$ is an invariant independent of n. Indeed, multiplying a relation of the form

$$C(\psi_{n+2}\psi_{n-1}^2 + \psi_{n+1}^2\psi_{n-2} + A\psi_n^3) = D\psi_{n+1}\psi_n\psi_{n-1} \tag{13c}$$

by ψ_{n+2}, we obtain

$$\begin{aligned} D\psi_{n+2}\psi_{n+1}\psi_n\psi_{n-1} &= C(\psi_{n+2}^2\psi_{n-1}^2 + \psi_{n+2}\psi_{n-2}\psi_{n+1}^2 + A\psi_{n+2}\psi_n^3) \\ &= C(\psi_{n+2}^2\psi_{n-1}^2 + (A\psi_{n+1}\psi_{n-1} - B\psi_n^2)\psi_{n+1}^2 + (\psi_{n+3}\psi_{n-1} + B\psi_{n+1}^2)\psi_n^2) \\ &= C(\psi_{n+3}\psi_n^2 + \psi_{n+2}^2\psi_{n-1} + A\psi_{n+1}^3)\psi_{n-1}, \end{aligned}$$

where the second identity uses the Somos recurrence (13b) twice, at n and $n+1$. If ψ_{n-1} is not a zero divisor, we can cancel it from both sides and arrive at (13c) with n replaced by $n+1$. In general, if $k < n$ and $\psi_{k-1}, \psi_k, \ldots, \psi_{n-2}$ are not zero divisors, we can prove by induction

$$\psi_{k+1}\psi_k\psi_{k-1}(\psi_{n+2}\psi_{n-1}^2 + \psi_{n+1}^2\psi_{n-2} + A\psi_n^3) = (\psi_{k+2}\psi_{k-1}^2 + \psi_{k+1}^2\psi_{k-2} + A\psi_k^3)\psi_{n+1}\psi_n\psi_{n-1}.$$

Specializing to division polynomials (or more generally an elliptic divisibility sequence) and $k = 2$, and cancelling ψ_2 from both sides, we obtain

$$\psi_3(\psi_{n+2}\psi_{n-1}^2 + \psi_{n+1}^2\psi_{n-2} + \psi_2^2\psi_n^3) = (\psi_2^c + \psi_2^4)\psi_{n+1}\psi_n\psi_{n-1}. \tag{13d}$$

We have $\psi_3 \mid \psi_{n+1}\psi_n\psi_{n-1}$ (or even $\psi_3\psi_2 \mid \psi_{n+1}\psi_n\psi_{n-1}$) because ψ is a divisibility sequence. However, ψ_3 only divides the other factor $\psi_2^c + \psi_2^4$ modulo $8J(X,Y,1)$:

$$\psi_2^c + \psi_2^4 = (6X^2 + b_2X + b_4)\psi_3 + 8J(X,Y,1)(2J(X,Y,1) + \psi_2^{2(1)}). \tag{13e}$$

This is a more precise version of formula 2.5 in [8], and when plugged into the right-hand side of (13d), it gives

$$8J(X,Y,1) \mid \psi_3(\psi_{n+2}\psi_{n-1}^2 + \psi_{n+1}^2\psi_{n-2} + \psi_2^2\psi_n^3 - (6X^2 + b_2X + b_4)\psi_{n+1}\psi_n\psi_{n-1}).$$

Since both 2 and $J(X,Y,1)$ are prime elements in the polynomial ring (a UFD) and does not divide ψ_3, we conclude

$$\psi_{n+2}\psi_{n-1}^2 + \psi_{n+1}^2\psi_{n-2} + \psi_2^2\psi_n^3 \equiv (6X^2 + b_2X + b_4)\psi_{n+1}\psi_n\psi_{n-1} \pmod{8J(X,Y,1)}. \tag{13f}$$

Another application of the Somos recurrence is to prove the integrality of ω_n. It suffices to show that $2\psi_2\omega_n$ has even coefficients, because 2 is coprime to ψ_2. We have

$$\begin{aligned}
2\psi_2\omega_n &= \psi_2(\psi_n^c - a_1\phi_n\psi_n - a_3\psi_n^3) \\
&= \psi_{n-1}^2\psi_{n+2} - \psi_{n-2}\psi_{n+1}^2 - \psi_2(a_1(X\psi_n^2 - \psi_{n+1}\psi_{n-1})\psi_n + a_3\psi_n^3) \\
&\equiv \psi_2^2\psi_n^3 + (b_2X + b_4)\psi_{n+1}\psi_n\psi_{n-1} + \psi_2((a_1X + a_3)\psi_n^3 + a_1\psi_{n+1}\psi_n\psi_{n-1}) \pmod 2 \\
&= \psi_2(\psi_2 + a_1X + a_3)\psi_n^3 + (a_1\psi_2 + b_2X + b_4)\psi_{n+1}\psi_n\psi_{n-1} \\
&= 2\psi_2(Y + a_1X + a_3)\psi_n^3 + 2(a_1Y + (a_1^2 + 2a_2)X + a_4 + a_1a_3)\psi_{n+1}\psi_n\psi_{n-1} \\
&\equiv 0 \pmod 2,
\end{aligned}$$

where the first congruence is by (13f).

4. Verification of identities

In this section, we verify the four identities (5a, 5b, 6a, 6b), and we switch from m to n in the subscripts. These are just one sentence in [3] ("one performs a similar verification for ϕ_n

and ω_n"), and it is surprising that the four proofs I worked out are of quite different flavor from each other. I would be curious to learn about alternative, especially simpler, proofs.

We first verify the two doubling identities (6a) and (6b). Since $J_Y = \psi_2^h$ is the (weighted) homogenization of ψ_2 and $P_n = (\phi_n, \omega_n, \psi_n)$ lies on J by inductive hypothesis, we can replace $J_Y(P_n)^2$ by $\underline{\psi_2^{2(1)h}(P_n)} = \psi_2^h(P_n)^2 - 4J(P_n)$. On the other hand, we also have $J_Y(P_n) = \underline{\psi_n^c}$ by (3b). The right-hand side of (6a) is

$$\begin{aligned}
&\phi_n J_Y(P_n)^2 - \psi_3^h(P_n) \\
&\equiv X\psi_n^2(\underline{\psi_n^c})^2 - \psi_{n+1}\psi_{n-1}\underline{\psi_2^{2(1)h}(P_n)} - \psi_3^h(P_n) \pmod{J(X,Y,1)} \\
&= X\psi_{2n}^2 - \psi_{n+1}\psi_{n-1}(4\phi_n^3 + b_2\phi_n^2\psi_n^2 + 2b_4\phi_n\psi_n^4 + b_6\psi_n^6) - (3\phi_n^4 + b_2\phi_n^3\psi_n^2 + 3b_4\phi_n^2\psi_n^4 + 3b_6\phi_n\psi_n^6 + b_8\psi_n^8) \\
&= X\psi_{2n}^2 + \psi_3\psi_n^8 - 2\psi_2^{2(1)}\psi_n^6\psi_{n+1}\psi_{n-1} + (6X^2 + b_2X + b_4)\psi_n^4(\psi_{n+1}\psi_{n-1})^2 - (\psi_{n+1}\psi_{n-1})^4
\end{aligned}$$

where the last identity is by substituting $\phi_n = X\psi_n^2 - \psi_{n+1}\psi_{n-1}$ plus brute force, while the left-hand side is

$$\begin{aligned}
\phi_{2n} &= X\psi_{2n}^2 - \psi_{2n+1}\psi_{2n-1} \\
&= X\psi_{2n}^2 - (\psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3)(\psi_{n+1}\psi_{n-1}^3 - \psi_{n-2}\psi_n^3) \\
&= X\psi_{2n}^2 - \psi_n^6\psi_{n+2}\psi_{n-2} + \psi_n^3\psi_{n+1}\psi_{n-1}(\psi_{n+2}\psi_{n-1}^2 + \psi_{n-2}\psi_{n+1}^2) - (\psi_{n+1}\psi_{n-1})^4 \\
&\equiv X\psi_{2n}^2 - \psi_n^6(\psi_2^2\psi_{n+1}\psi_{n-1} - \psi_3\psi_n^2) \\
&\qquad + \psi_n^3\psi_{n+1}\psi_{n-1}((6X^2 + b_2X + b_4)\psi_{n+1}\psi_n\psi_{n-1} - \psi_2^2\psi_n^3) - (\psi_{n+1}\psi_{n-1})^4 \pmod{J(X,Y,1)} \\
&= X\psi_{2n}^2 + \psi_3\psi_n^8 - 2\psi_2^2\psi_n^6\psi_{n+1}\psi_{n-1} + (6x^2 + b_2X + b_4)\psi_n^4(\psi_{n+1}\psi_{n-1})^2 - (\psi_{n+1}\psi_{n-1})^4
\end{aligned}$$

(where the congruence (fourth line) uses both (13a) and (13f)), which only differ from the left-hand side by ψ_2^2 vs. $\psi_2^{2(1)}$.

We can also directly show $J(P_n) = 0$ in the universal ring U. For this calculations it is most convenient to work in $\mathrm{Frac}(U)$, where we are free to replace denominators by expressions

congruent modulo $J(X,Y,1)$. We have

$$\begin{aligned}
J(P_n) &= \omega_n(\omega_n + a_1\phi_n\psi_n + a_3\psi_n^3) - (\phi_n^3 + a_2\phi_n^2\psi_n^2 + a_4\phi_n\psi_n^4 + a_6\psi_n^6) \\
&= \frac{\psi_n^c - a_1\phi_n\psi_n - a_3\psi_n^3}{2} \cdot \frac{\psi_n^c + a_1\phi_n\psi_n + a_3\psi_n^3}{2} - \cdots \\
&= \frac{(\psi_n^c)^2 - (a_1\phi_n\psi_n + a_3\psi_n^3)^2}{4} - \cdots \\
&= \frac{(\psi_{n-1}^2\psi_{n+2} - \psi_{n-2}\psi_{n+1}^2)^2/\psi_2^2 - \cdots}{4} - \cdots \\
&= \frac{((\psi_{n-1}^2\psi_{n+2} + \psi_{n-2}\psi_{n+1}^2)^2 - 4\psi_{n+2}\psi_{n-2}(\psi_{n+1}\psi_{n-1})^2)/\psi_2^{2(1)} - \cdots}{4} - \cdots
\end{aligned}$$

Using (13a) and (13f) again to replace $\psi_{n+2}\psi_{n-2}$ and $\psi_{n-1}^2\psi_{n+2} + \psi_{n-2}\psi_{n+1}^2$ but changing any resulting ψ_2^2 to $\psi_2^{2(1)}$ and expand $\phi_n = X\psi_n^2 - \psi_{n+1}\psi_{n-1}$ by brute force, we get exactly zero.

We can in fact write (6a) in a very succinct equivalent form: multiplying both sides by ψ_n^2 (which is nonzero in U), the right-hand side becomes

$$\phi_n(\psi_n J_Y(P_n))^2 - \psi_n^2\psi_3^h(P_n) = \phi_n(\psi_n\psi_n^c)^2 - \psi_n^2\psi_3^h(P_n) = \phi_n\psi_{2n}^2 - \psi_n^2\psi_3^h(P_n),$$

so (6a) is equivalent to $\psi_n^2\psi_3^h(P_n) \equiv \phi_n\psi_{2n}^2 - \phi_{2n}\psi_n^2 = \psi_{3n}\psi_n$ using (7a), or $\psi_n\psi_3^h(P_n) \equiv \psi_{3n}$. This is the $m = 3$ case of the general formula

$$\psi_{mn} \equiv \psi_n\psi_m^h(P_n) \tag{14a}$$

which can also be writen as

$$\psi_{mn}/\psi_n \equiv \psi_m^h(P_n)$$

for $n \neq 0$ (notice that $\psi_n \mid \psi_{mn}$ for all m, n because ψ is a divisibility sequence). Since $\psi_m^h = \psi_n^{m^2-1}\psi_m(P_n)$, this is also equivalent to $\psi_{mn} \equiv \psi_n^{m^2}\psi_m(P_n)$, the last identity in (2.3) of [8]:

$$\psi_{mn}(P) = \psi_n^{m^2}(P)\psi_m(nP) \tag{14b}$$

(understood to hold modulo $J(X,Y,1)$). For $m = 2$, (14a) says $J_Y(P_n) = \psi_2^h(P_n) \equiv \psi_{2n}/\psi_n = \psi_n^c$, which holds exactly by definition (3b) (without modding out $J(X,Y,1)$) and the $m = 1$ and $m = 0$ cases are trivial.

For (6b), since we have already proven $D_X(P_n) = \phi_{2n}$ and $D_Z(P_n) = \psi_{2n}$, the right-hand side is simply $(\psi_2^{ch}(P_n) - a_1\phi_{2n}\psi_{2n} - a_3\psi_{2n}^3)/2$ according to (11e), while the left-hand side is $(\psi_{2n}^c - a_1\phi_{2n}\psi_{2n} - a_3\psi_{2n}^3)/2$, so it remains to prove $\psi_{2n}^c \equiv \psi_2^{ch}(P_n)$. Expanding the left-hand side using (1d) and (1a) leads to factors ranging from ψ_{n-3} to ψ_{n+3}, and many of the resulting terms I do not know how to deal with.

Instead, we notice that our goal $\psi_{2n}^c \equiv \psi_2^{ch}(P_n)$ is exactly equivalent to the $m = 4$ case of (14a): multiplying both sides by $\psi_{2n} = \psi_n\psi_n^c$ we get

$$\begin{aligned}\psi_{4n} &= \psi_{2n}\psi_{2n}^c \equiv \psi_n\psi_n^c\psi_2^{ch}(P_n) \\ &= \psi_n\psi_2^h(P_n)\psi_2^{ch}(P_n) = \psi_n(\psi_2\psi_2^c)^h(P_n) = \psi_n\psi_4^h(P_n).\end{aligned}$$

We first prove the special case of (14a) with $n = 2$: $\psi_{2m} \equiv \psi_2\psi_m^h(P_2)$, which we will use in the form

$$\psi_{2m} \equiv \psi_2^{m^2}\psi_m(P_2) \tag{14c}$$

to exploit self-similarity within the division polynomials using the fact that $4 = 2 \times 2$. We will in fact show that for fixed n, if (14a) holds for $m = 0, 1, 2, 3, 4$ then it holds for all $n \in \mathbb{Z}$; therefore the $m = 4$ case we are tackling now is the last obstruction to proving it in full generality. It is clear that switch from m to $-m$ does not affect validity of (14a), so we assume $m > 0$ and argue by induction: if $m = 2k + 1 > 4$, we can use the elliptic relation $E((k+1)n, kn, n, 0)$ to write

$$\begin{aligned}\psi_{mn}\psi_n^3 &= \psi_{(k+1)n+kn}\psi_{(k+1)n-kn}\psi_n^2 \\ &= \psi_{(k+1)n+n}\psi_{(k+1)n-n}\psi_{kn}^2 - \psi_{kn+n}\psi_{kn-n}\psi_{(k+1)n}^2\end{aligned}$$

$$\begin{aligned}
&= \psi_{(k+2)n}\psi_{kn}^3 - \psi_{(k-1)n}\psi_{(k+1)n}^3 \\
&\equiv \psi_n\psi_{k+1}^h(P_n)(\psi_n\psi_k^h(P_n))^3 - \psi_n\psi_{k-1}^h(P_n)(\psi_n\psi_{k+1}^h(P_n))^3 \\
&= \psi_n^4(\psi_{k+1}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3)^h(P_n) \\
&= \psi_n^4\psi_{2k+1}^h(P_n) = \psi_n^4\psi_m^h(P_n)
\end{aligned}$$

where the congruence is by induction hypothesis, since $k+2 < 2k+1$; we then cancel ψ_n^3 from both sides to conclude (14a). Basically we exploit homogeneity and scaling invariance of the elliptic relations, and the same argument applies for $m = 2k > 4$, where we use $E((k+1)n, (k-1)n, n, 0)$ and cancel $\psi_{2n}\psi_n^2$ from both sides instead.

Some digression to further showcase the power of this technique: if we look at only the first three rows of the above computation, we see that we can deduce $\psi_n \mid \psi_{mn}$ from induction hypotheses $\psi_n \mid \psi_{(k-1)n}$, …, $\psi_n \mid \psi_{(k+2)n}$, so to show $\psi_n \mid \psi_{mn}$ for all m, n we just need to verify it for $m = 1, 2, 3, 4$. The $m = 1$ case is trivial, and for $m = 2, 4$ we have $\psi_n \mid \psi_{2n} \mid \psi_{4n}$ because $\psi_{2n} = \psi_n\psi_n^c$. For $m = 3$, use $E(2n, n, 1, 0) : \psi_{3n}\psi_n = \psi_{2n+1}\psi_{2n-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_{2n}^2$.

We can also cancel ψ_n^2 from both sides of

$$\begin{aligned}
\phi_{mn}\psi_n^2 &= \phi_n\psi_{mn}^2 - \psi_{(m+1)n}\psi_{(m-1)n} \\
&\equiv \phi_1^h(P_n)(\psi_n\psi_m^h(P_n))^2 - \psi_n\psi_{m+1}^h(P_n)\psi_n\psi_{m-1}^h(P_n) \\
&= \psi_n^2(X\psi_m^2 - \psi_{m+1}\psi_{m-1})^h(P_n) = \psi_n^2\phi_m^h(P_n)
\end{aligned}$$

(where the first identity is by (7a)) to show $\phi_{mn} \equiv \phi_m^h(P_n)$, and easily show

$$\psi_{mn}^c = \psi_{2mn}/\psi_{mn} \equiv (\psi_n\psi_{2m}^h(P_n))/(\psi_n\psi_m^h(P_n)) = \psi_m^{ch}(P_n),$$

as well as

$$\begin{aligned}
\omega_{mn} &= (\psi_{mn}^c - a_1\phi_{mn}\psi_{mn} - a_3\psi_{mn}^3)/2 \\
&\equiv (\psi_m^{ch}(P_n) - a_1\phi_m^h(P_n)\psi_n\psi_m^h(P_n) - a_3\psi_n^3\psi_m^h(P_n)^3)/2
\end{aligned}$$

$$= (\psi_m^c - a_1\phi_m\psi_m - a_3\psi_m^3)^h(P_n)/2 = \omega_m^h(P_n)$$

noticing that the homogenization of a_i is a_iZ^i which evaluates to $a_i\psi_n^i$ at P_n. This establishes the remaining two identities in (2.3) of [8].

It remains to verify the identity $\psi_{2m} \equiv \psi_2\psi_m^h(P_2)$ for $m = 4$, which we have shown is equivalent to the more manageable goal $\psi_4^c \equiv \psi_2^{ch}(P_2)$. Even though Mathematica successfully verifies it, this is still a huge computation and may cause trouble in Lean: in fully expanded form (b_i replaced by a_i), ϕ_2 has 14 terms, ψ_2 has 3 terms (ω_2 has 58 terms but is not involved), and ψ_2^{ch} is a polynomial with 37 terms of degree 6 in X (ϕ_2) and degree 12 in Z (ψ_2), resulting in a total of 19,162 terms in $\psi_2^{ch}(P_2)$, compared to 17,747 terms in ψ_4^c. Their difference is $4J(X, Y, 1)$ times a sum of 10,303 terms.

A more practical way to verify the identity is to expand ψ_4^c using the defining recurrence, resulting in $3\psi_2^4\psi_3^3\psi_2^c - (\psi_2^8 + \psi_3^3)(\psi_2^c)^2 - 2\psi_3^6 \equiv 3\left(\psi_2^{2(1)}\right)^2\psi_3^3\psi_2^c - \left(\left(\psi_2^{2(1)}\right)^4 + \psi_3^3\right)(\psi_2^c)^2 - 2\psi_3^6$, a polynomial in X only, and to transform $\psi_2^{ch}(P_2) = \psi_2^{12}\psi_2^c(\phi_2/\psi_2^2) \equiv \left(\psi_2^{2(1)}\right)^6\psi_2^c\left(\phi_2^{(1)}/\psi_2^{2(1)}\right)$, where $\phi_2^{(1)} = X\psi_2^{2(1)} - \psi_3$ is the polynomial in X congruent to ϕ_2. Since both sides are polynomials in X and congruent modulo $J(X, Y, 1)$, they must in fact be equal, and this can be verified (both sides have 5,387 terms). Using this proof we won't need to manually input an expression of 10,303 terms into Lean.

Back to the proof of $\psi_{4n} \equiv \psi_n\psi_4^h(P_n)$, or equivalently $\psi_{4n} \equiv \psi_n^{16}\psi_4(P_n)$. We compute

$$\begin{aligned}
\frac{\psi_{4n}}{\psi_{2n}^4} &\equiv \frac{\psi_2^{(2n)^2}\psi_{2n}(P_2)}{(\psi_2^{n^2}\psi_n(P_2))^4} = \frac{\psi_{2n}(P_2)}{\psi_n(P_2)^4} \\
&= 2\frac{\omega_n(P_2)}{\psi_n(P_2)^3} + a_1\frac{\phi_n(P_2)}{\psi_n(P_2)^2} + a_3 \\
&\equiv 2\frac{\omega_2(P_n)}{\psi_2(P_n)^3} + a_1\frac{\phi_2(P_n)}{\psi_2(P_n)^2} + a_3 \\
&= \frac{\psi_4(P_n)}{\psi_2(P_n)^4} = \frac{\psi_4(P_n)}{(\psi_{2n}/\psi_n^4)^4} = \frac{\psi_n^{16}\psi_4(P_n)}{\psi_{2n}^4},
\end{aligned}$$

where the second, third, and fourth identities use (3d), and the second congruence is by computing $(2n)P$ in two different ways: as $n(2P) = nP_2$ or as $2(nP) = 2P_n$. Notice that $P_n = (\phi_n, \omega_n, \psi_n)$ gives a valid formula for nP by induction hypothesis, and $n(2P) = (2n)P = 2(nP)$ relies on associativity of the group law, which is a nontrivial fact but can also be proven algebraically [1].

This computation is best carried out in $\mathrm{Frac}(U)$, where all the Z-coordinates (ψ_{2n}, $\psi_n(P_2)$ and $\psi_n(P_2)$) never vanish, as the universal point (X, Y) has infinite order.

Having dealt with the doubling formulas, we proceed to the addition formulas (5a) and (5b). In general, given two points $Q = (x_1, y_1)$ and $R = (x_2, y_2)$ on J, we have $-Q = (x_1, -y_1 - a_1x_1 - a_3)$. If $x_1 \neq x_2$, let $-Q + R = (x, y)$ and $Q + R = (x_3, y_3)$, then (8a) and (8b) apply to both addition and yield

$$x_3 = k(k + a_1) - (a_2 + x_1 + x_2), \quad x = k'(k' + a_1) - (a_2 + x_1 + x_2),$$

where

$$k = \frac{y_1 - y_2}{x_1 - x_2}, \quad k' = \frac{(-y_1 - a_1x_1 - a_3) - y_2}{x_1 - x_2},$$

and we have

$$\begin{aligned} x_3 &= x + k(k + a_1) - k'(k' + a_1) \\ &= x + (k - k')(k + k' + a_1) \\ &= x + \frac{(2y_1 + a_1x_1 + a_3)}{x_1 - x_2} \cdot \frac{-(2y_2 + a_1x_2 + a_3)}{x_1 - x_2} \\ &= x - \frac{\psi_2(Q)\psi_2(R)}{(x_1 - x_2)^2}. \end{aligned}$$

Now consider the two points $P_n = (\phi_n/\psi_n^2, \omega_n/\psi_n^3)$ and $P_{n+1} = (\phi_{n+1}/\psi_{n+1}^2, \omega_{n+1}/\psi_{n+1}^3)$ over $\mathrm{Frac}(U)$, which indeed have distinct X-coordinates. We have $P_n = nP$ and $P_{n+1} = (n+1)P$ by induction hypothesis, so $P_n + P_{n+1} = (2n+1)P$ and $-P_n + P_{n+1} = P = (X, Y)$,

and the above formula becomes

$$\begin{aligned} x_3 &= X - \frac{\psi_2(P_n)\psi_2(P_{n+1})}{(\phi_n/\psi_n^2 - \phi_{n+1}/\psi_{n+1}^2)^2} \\ &= X - \frac{(\psi_{2n}/\psi_n^4)(\psi_{2(n+1)}/\psi_{n+1}^4)}{\left(\psi_{2n+1}/\psi_n^2\psi_{n+1}^2\right)^2} \\ &= X - \frac{\psi_{(2n+1)-1}\psi_{(2n+1)+1}}{\psi_{2n+1}^2} = \frac{\phi_{2n+1}}{\psi_{2n+1}^2}. \end{aligned}$$

where the second identity uses (7b) and (3d). Since $x_3 = A_X(P_n, P_{n+1})/A_Z(P_n, P_{n+1})^2$ in $\mathrm{Frac}(U)$ by the addition formulas in Jacobian coordinates and we already know $\psi_{2n+1} = A_Z(P_n, P_{n+1})$, we conclude that $\phi_{2n+1} \equiv A_X(P_n, P_{n+1})$, namely (5a). It might be possible to "homogenize" this argument to make it work within the polynomial ring $\mathbb{Z}[a_1, \ldots, a_6, X, Y]$, but that probably makes it more cumbersome and less insightful.

Given that we already showed $x_3 = \phi_{2n+1}/\psi_{2n+1}^2$, it suffices to show $y_3 = \omega_{2n+1}/\psi_{2n+1}^3 = (\psi_2(P_{2n+1}) - a_1x_3 - a_3)/2$ in $\mathrm{Frac}(U)$ to prove (5b), or $2y_3 + a_1x_3 + a_3 = \psi_2(P_{2n+1})$. Write

$$k = \frac{y_1 - y_2}{x_1 - x_2} = \frac{(\psi_2(P_n) - a_1x_1 - a_3)/2 - (\psi_2(P_{n+1}) - a_1x_2 - a_3)/2}{x_1 - x_2} = \frac{\psi_2(P_n) - \psi_2(P_{n+1})}{2(x_1 - x_2)} - \frac{a_1}{2}$$

and

$$\frac{x_1y_2 - x_2y_1}{x_1 - x_2} = \frac{x_1\psi_2(P_{n+1}) - x_2\psi_2(P_n)}{2(x_1 - x_2)} - \frac{a_3}{2}$$

we obtain from (8d)

$$2y_3 = -\left(\frac{\psi_2(P_n) - \psi_2(P_{n+1})}{x_1 - x_2} + a_1\right)x_3 - \frac{x_1\psi_2(P_{n+1}) - x_2\psi_2(P_n)}{x_1 - x_2} - a_3,$$

so

$$\begin{aligned} &(x_1 - x_2)(2y_3 + a_1x_3 + a_3) \\ =\ &-x_3(\psi_2(P_n) - \psi_2(P_{n+1})) - x_1\psi_2(P_{n+1}) + x_2\psi_2(P_n) \end{aligned}$$

$$= -\left(X - \frac{\psi_{2n+2}\psi_{2n}}{\psi_{2n+1}^2}\right)(\psi_2(P_n) - \psi_2(P_{n+1})) - \left(X - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2}\right)\psi_2(P_{n+1}) + \left(X - \frac{\psi_{n+2}\psi_n}{\psi_{n+1}^2}\right)\psi_2(P_n)$$
$$= \frac{\psi_{n+1}\psi_{n+1}^c\psi_n\psi_n^c}{\psi_{2n+1}^2}(\psi_2(P_n) - \psi_2(P_{n+1})) + \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2}\psi_2(P_{n+1}) - \frac{\psi_{n+2}\psi_n}{\psi_{n+1}^2}\psi_2(P_n).$$

Since $\psi_2(P_n) = \psi_n^c/\psi_n^3$ by (3d), all terms in the last expression are products of terms of the sequence ψ and are free of all variables $a_1, \ldots, a_6, X, Y$, and it suffices to show that it is equal to

$$(x_1 - x_2)\psi_2(P_{2n+1}) = \frac{\psi_{2n+1}}{\psi_{n+1}^2\psi_n^2} \cdot \frac{\psi_{2n+1}^c}{\psi_{2n+1}^3} = \frac{\psi_{2n+1}^c}{\psi_{2n+1}^2\psi_{n+1}^2\psi_n^2}$$

which has the same property. Computational experiments show that the identity holds for any elliptic divisibility sequence ψ, so we should be able to prove it in that generality. Multiplying by the denominator $\psi_{2n+1}^2\psi_{n+1}^2\psi_n^2$ and using $\psi_2(P_n) = \psi_n^c/\psi_n^3$, our goal becomes

$$\frac{\psi_{2n+3}\psi_{2n}^2 - \psi_{2n-1}\psi_{2n+2}^2}{\psi_2} = \psi_{2n+1}^c = \psi_{n+1}^c\psi_n^c(\psi_n^c\psi_{n+1}^3 - \psi_{n+1}^c\psi_n^3) + \psi_{2n+1}^2(\psi_{n-1}\psi_{n+1}^c - \psi_{n+2}\psi_n^c).$$

It turns out

$$\begin{aligned}
&\frac{\psi_{2n+3}\psi_{2n}^2 - \psi_{2n-1}\psi_{2n+2}^2}{\psi_2} - \psi_{n+1}^c\psi_n^c(\psi_n^c\psi_{n+1}^3 - \psi_{n+1}^c\psi_n^3) \\
= &\frac{(\psi_{n+3}\psi_{n+1}^3 - \psi_n\psi_{n+2}^3)\psi_n^2(\psi_n^c)^2 - (\psi_{n+1}\psi_{n-1}^3 - \psi_{n-2}\psi_n^3)\psi_{n+1}^2(\psi_{n+1}^c)^2}{\psi_2} \\
&- (\psi_n^c)^2\psi_{n+1}^3\frac{\psi_{n+3}\psi_n^2 - \psi_{n-1}\psi_{n+2}^2}{\psi_2} + (\psi_{n+1}^c)^2\psi_n^3\frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{\psi_2}.
\end{aligned}$$

There are a total of 8 terms if expanded out. Among these, the 1st term cancel with the 6th, and the 4th with the 7th, and the 2nd term pair up with the 5th, and the 3rd with the 8th, simplifying to $\left((\psi_{n-1}\psi_{n+1}^c)^2 - (\psi_{n+2}\psi_n^c)^2\right)\psi_{2n+1}$. Factoring the difference of squares, we see that our goal reduces to $\psi_2\psi_{2n+1} = \psi_{n-1}\psi_{n+1}^c + \psi_{n+2}\psi_n^c$. Expanding ψ^c we see that this is exactly equivalent to $E(n+1, n, 2, 0)$. (One can discover this factor by expanding everything to terms around ψ_n and factoring the resulting expression.)

5. Elliptic relations from the defining recurrence

See [9] for now.

6. Acknowledgements

I thank David Angdinata for raising the question to me and identifying the most difficult parts, for sharing his communications with experts, and for encouraging me to write this note.

References

[1] David K. Angdinata and Junyan Xu. An Elementary Formal Proof of the Group Law on Weierstrass Elliptic Curves in any Characteristic. 14th International Conference on Interactive Theorem Proving (ITP 2023), pp.6:1–6:19. https://drops.dagstuhl.de/storage/00lipics/lipics-vol268-itp2023/LIPIcs.ITP.2023.6/LIPIcs.ITP.2023.6.pdf

[2] Joseph H. Silverman. The Arithmetic of Elliptic Curves (2nd Edition), Graduate Texts in Mathematics 106, Springer.

[3] Andrew Sutherland. MIT 18.783 Elliptic Curves, Lecture #5, Fall 2023, 09/26/23. https://math.mit.edu/classes/18.783/2023/LectureNotes5.pdf

[4] Serge Lang. Elliptic Curves Diophantine Analysis, Springer-Verlag 1978.

[5] Christine S. Swart. Sequences related to elliptic curves. PhD thesis, Royal Holloway (University of London), 2003. http://www.isg.rhul.ac.uk/files/alumni/thesis/swart_c.pdf

[6] Morgan Ward. Memoir on Elliptic Divisibility Sequences. American Journal of Mathematics Vol. 70, No. 1 (Jan., 1948), pp. 31-74.

[7] Katherine Stange. Elliptic nets and elliptic curves. Algebra & Number Theory 5:2(2011). https://projecteuclid.org/journals/algebra-and-number-theory/volume-5/issue-2/Elliptic-nets-and-elliptic-curves/10.2140/ant.2011.5.197.pdf

[8] Mohamed Ayad. Points S-entiers des courbes elliptiques, Manuscripta Mathematica 76, 305-324 (1992), Springer-Verlag. https://eudml.org/doc/155756

[9] Junyan Xu. Answer to "Division polynomials of elliptic curves". https://math.stackexchange.com/a/4903422/12932