# Getting to the right root: radical isogenies of every degree

Thomas Decru
COSIC, KU Leuven

**Abstract**

Class group actions on supersingular elliptic curves over $\mathbb{F}_p$ as in CSIDH are typically evaluated as long chains of isogenies of small prime degree. Radical isogeny formulae compute such chains using a single $N$th root per step, without sampling torsion points. Compact formulae of linear size had been conjectured for all odd $N$. We prove a corrected version of these formulae for every $N \geq 4$, odd and even, over every field of characteristic coprime to $2N$. In our formulation, every building block is a twisted sum of a discrete Kronecker function over $\mathbb{Z}/N\mathbb{Z}$, and the formulae follow from a distribution relation for the Kronecker theta function.

For even $N$, the $N$th root is only determined up to sign over $\mathbb{F}_p$, and the sign decides whether the walk stays on the surface of the 2-isogeny volcano. We show that the radical times a 2-torsion coordinate of the next curve is a square, which yields the horizontal choice for all even $N$; previously this was only known for $N \leq 14$. Algorithmically, one radical step costs about $12.5N$ multiplications and one exponentiation, without inversions. For horizontal 2-isogeny walks, radical $2^m$-isogenies with $m \in \{5, 6, 7\}$ are optimal for primes of 512 to 4096 bits. Finally, we show how to evaluate radical isogenies on points. As a consequence, a class group action can be computed from two given points, one on the curve and one on its quadratic twist, without ever sampling torsion points.

## 1 Introduction

Let $p$ be a prime and let $\mathcal{O}$ be an order in $\mathbb{Q}(\sqrt{-p})$ containing the Frobenius $\pi$. The class group $\mathrm{Cl}(\mathcal{O})$ acts freely and transitively on the set of supersingular elliptic curves over $\mathbb{F}_p$ whose $\mathbb{F}_p$-rational endomorphism ring is $\mathcal{O}$. This action underlies CSIDH [CLM+18] and a growing family of related constructions. Examples are CSURF [CD20], constant-time variants such as CTIDH [BBC+21], signatures with a known class group structure such as CSI-FiSh [BKV19], actions on oriented curves [CK20, DFFK+23] and on curves with level structure [DFFP24], and verifiable delay functions [DFMPS19]. In all of them, the action of an ideal class $\prod_i \mathfrak{l}_i^{e_i}$ with $\mathfrak{l}_i = (\ell_i, \pi - 1)$ is evaluated as a chain of $\ell_i$-isogenies for small primes $\ell_i \mid p + 1$. The standard way to compute an $\ell$-isogeny needs a point of order $\ell$ as input, which is obtained by sampling a random point and multiplying it by a large cofactor. This sampling is costly and has to be repeated many times, with a failure probability complicating constant-time implementations.

Radical isogenies [CDV20] avoid this sampling. Starting from an elliptic curve in Tate normal form with a point $P$ of order $N$, they produce the codomain of $E \to E/\langle P \rangle$ together with a new point $P'$ of order $N$ that extends the isogeny cyclically. The only expensive operation is the extraction of one $N$th root, so iterating yields a cyclic $N^k$-isogeny at the cost of $k$ exponentiations. Explicit formulae were first obtained from models of the modular curve $X_1(N)$, for small $N$ in [CDV20] and for $N \leq 37$ in [CDHV22]; see also [OM22] for radical 4-isogenies on Montgomery curves, and [CD22] for a generalisation to abelian varieties, called

multiradical isogenies. In [Dec24], compact formulae of size $O(N)$ were conjectured for all odd $N$, without using any model of $X_1(N)$. In a variable-time implementation, they sped up the CSIDH-512 action by 35% compared to [CDHV22].

Three questions remained open. First, the erstwhile conjecture of [Dec24] was supported by experiments only, and no analogue for even $N$ was known. Second, for even $N$ the radical has two $\mathbb{F}_p$-rational roots $\pm\beta$, and only one of them keeps a walk on the surface of the 2-isogeny volcano. A rule for this choice was conjectured in [CDHV22] and proved there for $N \leq 14$. Third, radical formulae so far only returned the codomain curve, so applications that transport points along the walk, such as actions on oriented curves [CK20, DFFK$^+$23] or with level structure [DFFP24], could not benefit from them, and every chain still started from a freshly sampled point.

**Class group actions with radicals.** We address these questions with a view towards evaluating class group actions. Our formulae describe the full isomorphism between the next Tate normal form and the Vélu codomain, such that points can be pushed through every radical step inversion-free and at a cost linear in $N$. With an inversion-free conversion between Tate normal forms of coprime orders, the whole action can then be evaluated from two fixed points of full order, one on the starting curve and one on its twist, and the same machinery transports the torsion points that represent an orientation or a level structure. For horizontal 2-isogeny walks, as in CSURF or in the $\mathbb{F}_p$-instance of the delay function of [DFMPS19], the root choice for even $N$ allows radical $2^m$-isogenies of arbitrary size.

**Contributions.**

- We prove the radical isogeny formulae for every $N \geq 4$, over any field of characteristic coprime to $2N$ (Theorem 3.1). The formulae are expressed in the elliptic divisibility sequence of $P$. They include a closed formula for the $x$-coordinate of the new kernel generator, and hence the full isomorphism onto the Vélu codomain. The $N$ choices of the root correspond bijectively to the $N$ cyclic extensions of the isogeny.

- For even $N$, we determine the class of the radical modulo squares (Theorem 4.1). Over $\mathbb{F}_p$ this gives the horizontal root choice for all even $N$ (Corollary 4.10): take the root that is a square if and only if $P$ is halvable in $E(\mathbb{F}_p)$.

- We give an inversion-free, constant-time radical step of about $12.5N$ multiplications plus one exponentiation (Algorithm 5.2). For horizontal 2-isogeny walks, radical $2^m$-isogenies with $m \in \{5, 6, 7\}$ are optimal for 512- to 4096-bit primes (Section 5.3).

- We show how to push points through radical steps at about $3N$ multiplications per point, and how to change the degree without inversions (Sections 5.4 and 5.5). In a cost model for constant-time actions with dummy steps and inversions by exponentiation, actions with radical chains of the size used in [Dec24] become 1.44–1.56 times faster for 512- to 4096-bit primes (Section 5.6).

**Outline.** The remainder of this section gives a technical overview. Section 2 recalls the necessary background. Section 3 proves the radical isogeny formulae and Section 4 determines the root choice for even $N$. Section 5 discusses algorithms and costs. We conclude with some open questions in Section 6. Appendix A compares our formulation with the one from [Dec24].

**Conventions.** Throughout, $N \geq 4$ is an integer and $K$ is a field with $\operatorname{char} K \nmid 2N$; we write $\overline{K}$ for an algebraic closure. Elliptic curves are given by Weierstrass equations

$$E:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and for a point $Q = (x_0, y_0) \in E$ we write $x(Q) = x_0$ and $y(Q) = y_0$. All isogenies are considered separable unless specified otherwise. For an elliptic curve $E_{b,c}$ in Tate normal form (Section 2.3) we always write $P = (0, 0)$, which is assumed to have exact order $N$. We let $\varphi\colon E_{b,c} \to E'$ denote the isogeny with kernel $\langle P \rangle$ given by Vélu's formulae (Section 2.4) and $\hat{\varphi}$ its dual. A point $P' \in E'(\overline{K})$ is called *$P$-distinguished* if $\hat{\varphi}(P') = P$, following [CDV20].

## Technical overview

**Radical isogenies.** Every pair $(E, Q)$ of an elliptic curve and a point of order $N \geq 4$ is isomorphic to a unique pair $(E_{b,c}, (0, 0))$ with $E_{b,c} : y^2 + (1 - c)xy - by = x^3 - bx^2$, which is called the *Tate normal form*. Let $P = (0, 0) \in E_{b,c}$ have order $N$ and let $\varphi\colon E_{b,c} \to E'$ be the isogeny with kernel $\langle P \rangle$. A radical isogeny formula computes the Tate normal form $(b', c')$ of $(E', P')$, where $P'$ is $P$-distinguished. Iterating these formulae then walks along a cyclic $N^k$-isogeny. The $N$ choices of $P'$ correspond to the $N$th roots of a *radical* $\rho_N \in K$.

**The formulae.** Let $W_n = \psi_n(P)$ be the *elliptic divisibility sequence* of $P$, i.e. the values of the division polynomials at $P$. The radical is $\rho_N = -W_{N-2}/(bW_{N-1})$. For an $N$th root $\beta$ of $\rho_N$ we form twisted sums

$$\mathcal{S}_k = \sum_{i=1}^{N-1} \beta^{ki}\, \frac{W_{i+k}}{W_iW_k}, \qquad \mathcal{S}_{j,k} = \sum_{i=1}^{N-1} \beta^{(j+k)i}\, \frac{W_{i+j}W_{i+k}}{W_i^2W_jW_k}.$$

Theorem 3.1 states that the isomorphism from $E_{b',c'}$ onto the Vélu codomain is $x = u^2x^* + r$, $y = u^3y^* + su^2x^* + t$ with

$$u = 1 + 3\mathcal{S}_1 - \mathcal{S}_3, \qquad s = 2\mathcal{S}_1 - \mathcal{S}_2, \qquad r = (\mathcal{S}_1 + \mathcal{S}_2)(1 - \mathcal{S}_3) + \tfrac{3}{2}\big(\mathcal{S}_1^2 - \mathcal{S}_{1,1}\big) - \mathcal{S}_{1,2},$$

and $t$ determined by $u, r, s$. In particular $P' = (r, t)$. The radical $\rho_N$ is the unique value of $\beta^N$ for which all summands are $N$-periodic in $i$.

**The proof.** Over $\mathbb{C}$, write $E_{b,c} \cong \mathbb{C}/\Lambda$ with $P$ corresponding to $z_0$, and $E' \cong \mathbb{C}/\Lambda'$ with $\Lambda' = \Lambda + \mathbb{Z}z_0$. The Weierstrass $\sigma$-function of $\Lambda$ gives $W_n$ up to elementary factors: $W_n = (-1)^{n+1}\kappa^{n^2-1}\sigma(nz_0)/\sigma(z_0)^{n^2}$ for a scaling constant $\kappa$. Hence each summand above is, up to a constant, a value of the *Kronecker function* $\mathcal{K}_\Lambda(z, w) = \sigma(z + w)/(\sigma(z)\sigma(w))$, twisted by the powers $\varepsilon^{ki}$ of a constant $\varepsilon$. Here $\varepsilon$ is an exponential in the quasi-periods of $\Lambda$ that encodes the choice of $\beta$, and hence of a point $w_0 \in \mathbb{C}/\Lambda'$ with $Nw_0 \equiv z_0$, i.e. of a $P$-distinguished point. The key identity is a *distribution relation* (Proposition 3.11):

$$\sum_{i=0}^{N-1} \varepsilon^{ki}\, \mathcal{K}_\Lambda(z + iz_0, kz_0) = e^{-kTz}\, \mathcal{K}_{\Lambda'}(z, kw_0)$$

for a constant $T$. Comparing Laurent expansions at $z = 0$ expresses $\mathcal{S}_k$ and $\mathcal{S}_{j,k}$ through $\zeta$- and $\wp$-values at $z_0$ on $\Lambda$ and at $w_0$ on $\Lambda'$. These are exactly the data of the Tate normal forms of $(E, P)$ and $(E', P')$, the constant $T$ cancels, and the formulae reduce to simple identities. Positive characteristic follows by a specialisation argument on the modular curve $Y_1(N)$ over $\mathbb{Z}[1/2N]$.

**The root choice for even $N$.** Replacing $\beta$ by $-\beta$ replaces $P'$ by $P'+T$, where $T$ is the point of order 2 in $\ker\hat{\varphi}$. Let $T_3 = [N/2]P' + T$, and let $\theta = -x(T_3)$, computed on $E_{b',c'}$. Theorem 4.1 states that $\beta\theta$ is a square. Over $\mathbb{C}$ we write down an explicit square root $\Omega$ of $\beta\theta$, built from $\sigma$-values on $\Lambda$ and $\Lambda'$, an exponential in the quasi-periods, and a sign that depends on the class of the lattice point $Nw_0 - z_0$ modulo $2\Lambda$. The main work is to show that $\Omega$ does not depend on the choice of representatives in $\mathbb{C}$; the sign, a quadratic refinement of the Weil pairing on $\Lambda/2\Lambda$, is needed exactly for this. Then $\Omega$ is a holomorphic function on the modular curve parametrising $(E, P, P')$, so $\beta\theta$ is a square up to a rational constant. An expansion at the Tate curve shows that this constant is 1. Over $\mathbb{F}_p$, the class of $\theta$ modulo squares is the 2-Tate pairing of $T_3$ and $P'$. On the surface of the volcano, $E(\mathbb{F}_p) \cong \mathcal{O}/(\pi - 1)$ as $\mathcal{O}$-modules, which makes this pairing explicit and yields the halvability criterion.

**Algorithms.** We scale the Tate normal form so that its coefficients are polynomials in a projective representative $(B : C : Z)$ of $(b, c)$. The $x$-coordinates of the multiples of $P$ satisfy a three-term recursion, and the radical, the root and the twisted sums are computed with one common denominator using prefix products. This gives about $12.5N$ multiplications per step, without inversions or branches. Points are pushed with Kohel's form of Vélu's formulae followed by the isomorphism of Theorem 3.1. Changing the degree uses an $x$-only formula for the Tate normal form.


### Acknowledgements

Thomas Decru is funded by Fonds voor Wetenschappelijk Onderzoek (FWO) with reference number 1245025N, by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement ISOCRYPT – No. 101020788), by the Research Council KU Leuven grant C14/24/099 and by CyberSecurity Research Flanders with reference number VOEWICS02.


## 2 Preliminaries

### 2.1 Changes of Weierstrass coordinates

For $(u, r, s, t) \in \overline{K}^\times \times \overline{K}^3$ and a Weierstrass curve $E$ with coefficients $a_1, a_2, a_3, a_4, a_6$, we write $E^{(u,r,s,t)}$ for the curve obtained by the substitution

$$x = u^2x^* + r, \qquad y = u^3y^* + su^2x^* + t, \tag{1}$$

where $(x, y)$ are coordinates on $E$ and $(x^*, y^*)$ coordinates on $E^{(u,r,s,t)}$. Its coefficients are given by [Sil09, Table 3.1]:

$$\begin{aligned} ua_1^* &= a_1 + 2s, \qquad u^2a_2^* = a_2 - sa_1 + 3r - s^2, \qquad u^3a_3^* = a_3 + ra_1 + 2t, \\ u^4a_4^* &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st, \\ u^6a_6^* &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1. \end{aligned} \tag{2}$$

The map $(x^*, y^*) \mapsto (x, y)$ in (1) is an isomorphism $E^{(u,r,s,t)} \to E$, which we call the isomorphism *attached to* $(u, r, s, t)$. Every isomorphism between Weierstrass curves is of this form [Sil09, Proposition III.3.1(b)].

We will often compose such isomorphisms. Let

$$E_A = E^{(u_A,r_A,s_A,t_A)}, \qquad E_B = E^{(u_B,r_B,s_B,t_B)}.$$

Then $E_B = E_A^{(u,r,s,t)}$ and the isomorphism attached to $(u_B, r_B, s_B, t_B)$ is the composition of the ones attached to $(u, r, s, t)$ and to $(u_A, r_A, s_A, t_A)$, where

$$u = \frac{u_B}{u_A}, \qquad r = \frac{r_B - r_A}{u_A^2}, \qquad s = \frac{s_B - s_A}{u_A}, \qquad t = \frac{t_B - t_A - s_A(r_B - r_A)}{u_A^3}. \tag{3}$$

Indeed, substituting $x' = u^2x^* + r$ and $y' = u^3y^* + su^2x^* + t$ into $x = u_A^2x' + r_A$ and $y = u_A^3y' + s_Au_A^2x' + t_A$ gives

$$x = (u_Au)^2x^* + r_A + u_A^2r, \qquad y = (u_Au)^3y^* + (s_A + u_As)(u_Au)^2x^* + t_A + u_A^2s_Ar + u_A^3t,$$

so the composition is attached to $(u_Au,\ r_A + u_A^2r,\ s_A + u_As,\ t_A + u_A^2s_Ar + u_A^3t)$. Solving for $(u, r, s, t)$ gives (3).

## 2.2 Division polynomials and elliptic divisibility sequences

Let $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$ and $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$ be the usual $b$-invariants of $E$. The *division polynomials* $\psi_n \in \mathbb{Z}[a_1, \dots, a_6][x, y]$ are defined by $\psi_0 = 0$, $\psi_1 = 1$,

$$\psi_2 = 2y + a_1x + a_3, \qquad \psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,$$
$$\psi_4 = \psi_2\big(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2\big),$$

the recursions

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \qquad (m \geq 2),$$
$$\psi_2\psi_{2m} = \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2 \qquad (m \geq 3),$$

and $\psi_{-n} = -\psi_n$ [Sil09, Exercise 3.7]. We regard them as functions on $E$. For $Q \in E$, the values $W_n = \psi_n(Q)$ are called the *elliptic divisibility sequence* of $Q$ [War48]. We use the following standard facts [Sil09, Exercise 3.7].

(D1) If $Q \in E$ and $kQ \neq \mathcal{O}$, then $x(kQ) = x(Q) - \psi_{k-1}\psi_{k+1}(Q)/\psi_k(Q)^2$.

(D2) For all $m, n \in \mathbb{Z}$ one has $\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2$.

(D3) For $\operatorname{char} K \nmid n$, the function $\psi_n$ has simple zeros exactly at the points of $E[n] \setminus \{\mathcal{O}\}$ and a pole of order $n^2 - 1$ at $\mathcal{O}$. Near $\mathcal{O}$, in terms of the uniformiser $\tau = -x/y$, one has $\psi_n = (-1)^{n+1}n\,\tau^{1-n^2}(1 + O(\tau))$.

For (D3), the leading terms $\psi_n = nx^{(n^2-1)/2} + \cdots$ ($n$ odd) and $\psi_n = \psi_2(\frac{n}{2}x^{(n^2-4)/2} + \cdots)$ ($n$ even), together with $x = \tau^{-2} + \cdots$ and $y = -\tau^{-3} + \cdots$ [Sil09, §IV.1], give the pole; the $n^2 - 1$ zeros [Sil09, Corollary III.6.4] are then simple since the divisor has degree zero.

**Lemma 2.1.** *Let $E^* = E^{(u,r,s,t)}$, let $Q^* \in E^*$ and let $Q \in E$ be its image under the attached isomorphism. Then $\psi_n^{E^*}(Q^*) = u^{1-n^2}\,\psi_n^E(Q)$ for all $n \in \mathbb{Z}$.*

*Proof.* Pull back $\psi_n^E$ along the attached isomorphism $E^* \to E$. Since the isomorphism preserves the group law, it maps $E^*[n]$ onto $E[n]$, so by (D3) the pulled-back function has the same divisor as $\psi_n^{E^*}$. Hence $\psi_n^E/\psi_n^{E^*}$ is a non-zero constant. To compute it, note that by (1) the uniformisers satisfy $\tau = -x/y = u^{-1}\tau^*(1 + O(\tau^*))$. Comparing the leading terms in (D3) on both sides shows that the constant equals $u^{n^2-1}$. □

### 2.3 Tate normal form

For $b, c \in K$ we let

$$E_{b,c}:\ y^2 + (1-c)xy - by = x^3 - bx^2,$$

so that $a_1 = 1-c$, $a_2 = a_3 = -b$ and $a_4 = a_6 = 0$. Every pair $(E, Q)$ with $Q$ of order at least 4 is isomorphic to $(E_{b,c}, (0,0))$ for a unique pair $(b, c)$ [Hus04, Ch. 4, §4]. Moreover the isomorphism is unique since an automorphism of $E$ that fixes a point of order at least 4 is the identity. This follows from the description of $\mathrm{Aut}(E)$ in [Sil09, Theorem III.10.1]: the fixed points of a non-trivial automorphism have order at most 3. The isomorphism is given explicitly by the following lemma.

**Lemma 2.2.** *Let $Q = (x_0, y_0) \in E$ be a point of order at least 4 and define*

$$\lambda = \frac{3x_0^2 + 2a_2x_0 + a_4 - a_1y_0}{\psi_2(Q)}, \qquad u_Q = \frac{\psi_2(Q)}{x(Q) - x(2Q)}.$$

*Then*

$$E^{(u_Q, x_0, \lambda, y_0)} = E_{b,c} \qquad \text{with} \qquad b = \frac{x(2Q) - x(Q)}{u_Q^2}, \quad c = 1 - \frac{a_1 + 2\lambda}{u_Q},$$

*and the attached isomorphism maps $(0,0)$ to $Q$.*

*Proof.* Note that $\lambda$ is the slope of the tangent at $Q$ and both denominators are non-zero. Indeed, $\psi_2(Q) = 0$ would mean $2Q = \mathcal{O}$, and $x(Q) = x(2Q)$ would mean $2Q = \pm Q$. We apply three changes of variables.

- By (2) with $(u, r, s, t) = (1, x_0, 0, y_0)$, the point $Q$ is moved to $(0,0)$. This gives $a_6^* = 0$ (as $Q \in E$), $a_3^* = \psi_2(Q)$, $a_4^* = 3x_0^2 + 2a_2x_0 + a_4 - a_1y_0$ and $a_2^* = a_2 + 3x_0$.
- Next, $(1, 0, \lambda, 0)$ makes the tangent at $(0,0)$ horizontal, i.e. $a_4^* = 0$. It turns $a_2^*$ into $a_2 + 3x_0 - \lambda a_1 - \lambda^2 = x(Q) - x(2Q)$; here we used the duplication formula $x(2Q) = \lambda^2 + a_1\lambda - a_2 - 2x_0$ [Sil09, Algorithm III.2.3].
- Finally, scaling by $u_Q$ makes $a_2^* = a_3^*$.

By (3), the three steps compose to $(u_Q, x_0, \lambda, y_0)$. □

### 2.4 Vélu's formulae

Let $G \subset E(\overline{K})$ be a finite subgroup that is stable under $\mathrm{Gal}(\overline{K}/K)$ and whose order is coprime to $\mathrm{char}\, K$. Vélu [Vél71] gave an explicit separable isogeny $\varphi\colon E \to E'$ over $K$ with kernel $G$, normalised so that it pulls back the invariant differential $dx/(2y + a_1x + a_3)$ of $E'$ to that of $E$. For $R \notin G$ it is given by

$$\begin{aligned} x(\varphi(R)) &= x(R) + \sum_{Q \in G \setminus \{\mathcal{O}\}} \big(x(R+Q) - x(Q)\big), \\ y(\varphi(R)) &= y(R) + \sum_{Q \in G \setminus \{\mathcal{O}\}} \big(y(R+Q) - y(Q)\big), \end{aligned} \tag{4}$$

and $\varphi(R) = \mathcal{O}$ for $R \in G$. The codomain $E'$ has the same coefficients $a_1, a_2, a_3$ as $E$. To describe the others, put, for $Q = (x_Q, y_Q) \in G \setminus \{\mathcal{O}\}$,

$$g_Q^x = 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q, \qquad g_Q^y = -2y_Q - a_1x_Q - a_3,$$

and let $v_Q = g_Q^x$ if $2Q = \mathcal{O}$ and $v_Q = 2g_Q^x - a_1g_Q^y$ otherwise. Let $\mathcal{Q}$ consist of the points of order 2 in $G$ together with one point of each pair $\{Q, -Q\}$ of the remaining points of $G \setminus \{\mathcal{O}\}$, and put $v = \sum_{Q \in \mathcal{Q}} v_Q$ and $w = \sum_{Q \in \mathcal{Q}} \big((g_Q^y)^2 + x_Q v_Q\big)$. Then $E'$ has coefficients $a_4 - 5v$ and $a_6 - b_2v - 7w$ in place of $a_4$ and $a_6$ [Vél71]; see also [Dec24, Theorem 1]. When $G = \langle P \rangle$ we call $\varphi$ the *Vélu isogeny* with kernel $\langle P \rangle$ and $E'$ the *Vélu codomain*.

## 2.5 Complex uniformisation

Let $\Lambda \subset \mathbb{C}$ be a lattice with Weierstrass functions $\sigma_\Lambda$, $\zeta_\Lambda$, $\wp_\Lambda$, normalised by $\partial_z\sigma/\sigma = \zeta$ and $\partial_z\zeta = -\wp$. Throughout the paper, derivatives are written $\partial_z$; a prime on a function never denotes a derivative. The function $\sigma$ is entire and odd, with simple zeros exactly at the points of $\Lambda$. The function $\zeta$ is odd and quasi-periodic, and $\wp$ is even and $\Lambda$-periodic [Sil09, §VI.3]. We use the following facts. For (C1) and (C2), see [Lan87, Ch. 18] and [Sil09, Exercise 6.4]; (C4) follows by integrating the Laurent expansion of $\wp$ [Sil09, Theorem VI.3.5].

(C1) There is a $\mathbb{Z}$-linear map $\eta\colon \Lambda \to \mathbb{C}$ (the quasi-periods) with $\zeta(z+\omega) = \zeta(z) + \eta(\omega)$, and
$$\sigma(z+\omega) = \chi(\omega)\, e^{\eta(\omega)(z+\omega/2)}\sigma(z),$$
where $\chi(\omega) = 1$ if $\omega \in 2\Lambda$ and $\chi(\omega) = -1$ otherwise.

(C2) (Legendre relation) The *Legendre pairing* $\mathcal{E}(\lambda,\mu) := \eta(\lambda)\mu - \eta(\mu)\lambda$ takes values in $2\pi i\mathbb{Z}$. More precisely, $\mathcal{E}(\lambda,\mu)/2\pi i = \pm\det(\lambda,\mu)$ in coordinates with respect to any basis of $\Lambda$, so it is a perfect alternating pairing $\Lambda\times\Lambda \to \mathbb{Z}$.

(C3) (Addition formula) $\zeta(a+b) - \zeta(a) - \zeta(b) = \dfrac{1}{2}\dfrac{\partial_z\wp(a) - \partial_z\wp(b)}{\wp(a)-\wp(b)}$, and, letting $b \to a$,
$\zeta(2a) - 2\zeta(a) = \dfrac{\partial_z^2\wp(a)}{2\,\partial_z\wp(a)}$.

(C4) $\sigma(z) = z + O(z^5)$ and $\zeta(z) = z^{-1} + O(z^3)$.

We also use the following facts about elliptic functions [Sil09, §VI.2]:

(E1) an elliptic function without poles is constant;

(E2) a non-constant elliptic function has at least two poles modulo $\Lambda$, counted with multiplicity.

Let $G_{2k}(\Lambda) = \sum_{\omega\in\Lambda\setminus\{0\}}\omega^{-2k}$ for $k \geq 2$ be the Eisenstein series of $\Lambda$, and put $g_2 = 60G_4(\Lambda)$ and $g_3 = 140G_6(\Lambda)$. Then $\wp$ satisfies $(\partial_z\wp)^2 = 4\wp^3 - g_2\wp - g_3$ [Sil09, Theorem VI.3.5]. Hence, on the curve $E_\Lambda : y^2 = x^3 - \frac{g_2}{4}x - \frac{g_3}{4}$, the map $z \mapsto [\wp(z) : \frac{1}{2}\partial_z\wp(z) : 1]$ (sending $\Lambda$ to $\mathcal{O}$) is a complex analytic group isomorphism $\mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C})$ [Sil09, Proposition VI.3.6]. Every elliptic curve over $\mathbb{C}$ arises in this way [Sil09, Theorem VI.5.1]. The invariant differential $dx/2y$ pulls back to $dz$, and the uniformiser $-x/y$ equals $z + O(z^5)$. Isogenies $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ are of the form $z \mapsto \gamma z$ with $\gamma\Lambda_1 \subset \Lambda_2$ [Sil09, Theorem VI.4.1].

Finally, the *Kronecker function* of $\Lambda$ is
$$\mathcal{K}_\Lambda(z,w) = \frac{\sigma(z+w)}{\sigma(z)\sigma(w)}.$$
Up to an elementary exponential factor and normalisation, it is the Kronecker theta function $(\partial_z\theta)(0)\,\theta(z+w)/(\theta(z)\theta(w))$ studied in [Zag91].

## 2.6 Class group actions and isogeny volcanoes

Let $p > 3$ be a prime with $p \equiv 3 \pmod 4$, and let $E/\mathbb{F}_p$ be supersingular. Its Frobenius $\pi$ satisfies $\pi^2 = -p$ and the ring $\mathrm{End}_{\mathbb{F}_p}(E)$ of $\mathbb{F}_p$-rational endomorphisms is either $\mathbb{Z}[\pi]$ or $\mathbb{Z}[(1+\pi)/2]$ [DG16]. Following the volcano terminology, we say that $E$ lies on the *floor* or on the *surface*, respectively. For an order $\mathcal{O} \in \{\mathbb{Z}[\pi], \mathbb{Z}[(1+\pi)/2]\}$ let $\mathcal{E}\ell\ell_p(\mathcal{O})$ be the set of $\mathbb{F}_p$-isomorphism classes of such curves with $\mathrm{End}_{\mathbb{F}_p}(E) = \mathcal{O}$. The class group acts freely and

transitively on it via $[\mathfrak{a}]\star E = E/E[\mathfrak{a}]$, where $E[\mathfrak{a}]$ is the common kernel of all endomorphisms in $\mathfrak{a}$ [CLM+18, DG16].

For a prime $\ell \mid p+1$ with $\ell \neq 2$, the ideal $\mathfrak{l} = (\ell, \pi - 1)$ satisfies $E[\mathfrak{l}] = E(\mathbb{F}_p)[\ell]$. So the action of $[\mathfrak{l}]$ is the $\ell$-isogeny whose kernel is generated by a rational point of order $\ell$, and $[\bar{\mathfrak{l}}] = [\mathfrak{l}]^{-1}$, with $\bar{\mathfrak{l}} = (\ell, \pi + 1)$, is obtained in the same way on the quadratic twist. Iterating, $[\mathfrak{l}]^k$ acts by a cyclic $\ell^k$-isogeny with successive kernels generated by rational points, which is what radical isogenies compute.

An isogeny between two curves with the same endomorphism ring $\mathcal{O}$ is called *horizontal*; this holds if and only if its kernel is $E[\mathfrak{a}]$ for an invertible ideal $\mathfrak{a}$ of $\mathcal{O}$, i.e. is $\mathcal{O}$-stable [Koh96]. For odd $\ell$, both orders are maximal at $\ell$, so every $\ell$-isogeny is horizontal. For $\ell = 2$ the situation is that of a volcano [DG16]. If $p \equiv 3 \pmod 8$, then 2 is inert in $\mathbb{Z}[(1+\pi)/2]$, and the three 2-isogenies of a surface curve all descend to the floor. If $p \equiv 7 \pmod 8$, then $2\mathcal{O} = \mathfrak{l}\bar{\mathfrak{l}}$ splits in $\mathcal{O} = \mathbb{Z}[(1+\pi)/2]$. A surface curve then has full rational 2-torsion, two horizontal 2-isogenies with kernels $E[\mathfrak{l}]$ and $E[\bar{\mathfrak{l}}]$, and one descending 2-isogeny. Horizontal 2-isogeny walks, as in CSURF [CD20] and [DFMPS19], therefore take place on the surface with $p \equiv 7 \pmod 8$. Finally, by [Len96, Theorem 1],

$$E(\mathbb{F}_p) \cong \mathcal{O}/(\pi - 1)\mathcal{O} \qquad \text{as } \mathcal{O}\text{-modules, where } \mathcal{O} = \mathrm{End}_{\mathbb{F}_p}(E). \tag{5}$$

# 3 Radical isogeny formulae for all $N$

In this section we prove the following theorem.

**Theorem 3.1.** *Let $N \geq 4$ and let $K$ be a field with $\operatorname{char} K \nmid 2N$. Let $b, c \in K$ be such that $P = (0,0) \in E_{b,c}$ has exact order $N$. Let $\varphi\colon E_{b,c} \to E'$ be the Vélu isogeny with kernel $\langle P \rangle$. Let $W_n = \psi_n(P)$, so that $W_i \neq 0$ for $N \nmid i$, since $\psi_i(P) = 0$ would force $[i]P = \mathcal{O}$ [Sil09, Exercise 3.7], and fix $\beta \in \overline{K}$ with*

$$\beta^N = \rho_N := -\frac{W_{N-2}}{b\,W_{N-1}}. \tag{6}$$

*For $j, k \geq 1$ define*

$$\mathcal{S}_k = \sum_{i=1}^{N-1} \beta^{ki}\,\frac{W_{i+k}}{W_i\,W_k}, \qquad \mathcal{S}_{j,k} = \sum_{i=1}^{N-1} \beta^{(j+k)i}\,\frac{W_{i+j}\,W_{i+k}}{W_i^2\,W_j\,W_k} \tag{7}$$

*and put*

$$\begin{aligned} u &= 1 + 3\mathcal{S}_1 - \mathcal{S}_3, \qquad s = 2\mathcal{S}_1 - \mathcal{S}_2, \\ r &= (\mathcal{S}_1 + \mathcal{S}_2)(1 - \mathcal{S}_3) + \tfrac{3}{2}\big(\mathcal{S}_1^2 - \mathcal{S}_{1,1}\big) - \mathcal{S}_{1,2}, \\ t &= \tfrac{1}{2}\big(u(3r - b - (1-c)s - s^2) + b - (1-c)r\big). \end{aligned} \tag{8}$$

*Then the following hold.*

1. *$u \neq 0$. Moreover $E'^{(u,r,s,t)} = E_{b',c'}$, where*

$$b' = \frac{b + (1-c)s + s^2 - 3r}{u^2}, \qquad c' = 1 - \frac{1 - c + 2s}{u}. \tag{9}$$

   *Thus the isomorphism $\iota\colon E_{b',c'} \to E'$ attached to $(u,r,s,t)$ is defined over $K(\beta)$.*

2. *$P' := \iota(0,0) = (r,t)$ is $P$-distinguished and has exact order $N$. If $\varphi'$ denotes the Vélu isogeny with kernel $\langle (0,0) \rangle$ on $E_{b',c'}$, then $\varphi' \circ \iota^{-1} \circ \varphi$ is cyclic of degree $N^2$.*

3. *The map $\beta \mapsto P'$ is a bijection from the $N$ roots of $X^N - \rho_N$ to the $N$ points of $E'(\overline{K})$ that are $P$-distinguished.*

Since $(0,0) \in E_{b',c'}$ again has exact order $N$, Theorem 3.1 can be applied to $(b', c')$ again, and iterating yields a cyclic $N^k$-isogeny without sampling any further point.

For computations, it is convenient to rewrite the sums in terms of the $x$-coordinates $x_k = x([k]P)$, $2 \le k \le N-2$, and of $\alpha = -\beta$. Put

$$h_i = \alpha^i \prod_{k=2}^{i} x_k \qquad (1 \le i \le N-2), \tag{10}$$

so that $h_1 = \alpha$.

**Proposition 3.2.** *In the setting of Theorem 3.1, we have $\alpha^N = -\big(b^2 \prod_{k=2}^{N-2} x_k\big)^{-1}$ and*

$$\mathcal{S}_1 = b \sum_{i=1}^{N-2} h_i, \qquad \mathcal{S}_2 = \frac{b}{\alpha} \sum_{i=1}^{N-3} h_i h_{i+1} - b\, h_{N-2},$$

$$\mathcal{S}_{1,1} = b^2 \sum_{i=1}^{N-2} h_i^2, \qquad \mathcal{S}_3 = \frac{1}{\alpha^3} \sum_{i=1}^{N-4} h_i h_{i+1} h_{i+2} - \frac{h_{N-2}^2}{\alpha^2} - \frac{h_{N-2}}{\alpha},$$

$$\mathcal{S}_{1,2} = \frac{b^2}{\alpha} \sum_{i=1}^{N-3} h_i^2 h_{i+1}.$$

*In particular, $u$, $s$ and $r$ are Laurent polynomials in $\alpha$ whose coefficients are polynomials in $\frac{1}{2}$, $b$ and $x_2, \dots, x_{N-2}$.*

We prove Proposition 3.2 at the end of the next subsection.

## 3.1 Algebraic lemmata

The next lemma describes $W_n$ for $n$ just outside the range $0 \le n \le N$. It is the only place where we need (D2).

**Lemma 3.3** (Reflection)**.** *In the setting of Theorem 3.1, for $-N < m < N$ one has*

$$W_{N+m} = -W_{N-1}\, \rho_N^{-m-1}\, W_m.$$

*Proof.* For $m = 0$ both sides vanish. The idea for the other cases is that $x([n]P)$ only depends on $n$ modulo $N$ and up to sign. By (D1), this forces the ratios between $W$-values at reflected or shifted indices to form geometric progressions. Note that $W_2 = -b$ and $W_3 = b_8 = -b^3$, by evaluating $\psi_2$ and $\psi_3$ at $(0,0)$.

*Case $m = -j$ with $1 \le j \le N-1$.* The claim reads $W_{N-j} = W_{N-1}\rho_N^{j-1} W_j$. Put $V_j = W_{N-j}/W_j$. Since $[N-j]P = -[j]P$, we have $x([N-j]P) = x([j]P)$, and by (D1) this gives

$$\frac{W_{N-j-1}W_{N-j+1}}{W_{N-j}^2} = \frac{W_{j-1}W_{j+1}}{W_j^2} \qquad (2 \le j \le N-2),$$

that is, $V_{j-1}V_{j+1} = V_j^2$. Hence $(V_j)$ is a geometric progression, so $V_j = V_1(V_2/V_1)^{j-1}$ for $1 \le j \le N-1$. Here $V_1 = W_{N-1}$ and $V_2/V_1 = W_{N-2}/(W_2 W_{N-1}) = \rho_N$.

*Case $1 \le m \le N-1$.* Put $U_m = W_{N+m}/W_m$. Since $x([N+m]P) = x([m]P)$, (D1) gives $U_{m-1}U_{m+1} = U_m^2$ for $2 \le m \le N-2$, so again it suffices to determine $U_1$ and $U_2$. Relation (D2) with $(m,n) = (N-1, 2)$ gives

$$W_{N+1}W_{N-3} = W_N W_{N-2} W_2^2 - W_3 W_1 W_{N-1}^2 = b^3 W_{N-1}^2.$$

By the first case, $W_{N-3} = W_{N-1}\rho_N^2 W_3 = -b^3 W_{N-1}\rho_N^2$, so

$$U_1 = W_{N+1} = -W_{N-1}\rho_N^{-2}.$$

Relation (D2) with $(m,n) = (N,2)$ gives $W_{N+2}W_{N-2} = b^2 W_{N+1}W_{N-1}$. Combined with $W_{N-2} = -b\rho_N W_{N-1}$ (first case, $j=2$), this yields

$$W_{N+2} = bW_{N-1}\rho_N^{-3}, \qquad \text{i.e.} \qquad U_2 = -W_{N-1}\rho_N^{-3}.$$

Therefore $U_2/U_1 = \rho_N^{-1}$, and $U_m = -W_{N-1}\rho_N^{-m-1}$ for all $1 \le m \le N-1$. □

Lemma 3.3 implies that every summand $\beta^{ki}W_{i+k}/W_i$ is $N$-periodic in $i$, as long as the indices stay in $(-N, 2N)$.[1] This characterises $\rho_N$: it is the unique value of $\beta^N$ for which the summands of $\mathcal{S}_k$ are periodic. It also means that the sums $\mathcal{S}_k$ and $\mathcal{S}_{j,k}$ are naturally sums over $\mathbb{Z}/N\mathbb{Z} \setminus \{0\}$.

**Lemma 3.4.** *We have*

$$\beta^i \frac{W_{i+1}}{W_i} = b\,h_i \quad (1 \le i \le N-2), \qquad \rho_N = (-1)^{N+1}\Big(b^2 \prod_{k=2}^{N-2} x_k\Big)^{-1}.$$

*Proof.* By (D1) with $x(P) = 0$, we have $x_k = -W_{k-1}W_{k+1}/W_k^2$ for $2 \le k \le N-2$. The product over $2 \le k \le i$ telescopes:

$$\prod_{k=2}^{i} x_k = (-1)^{i-1} \prod_{k=2}^{i} \frac{W_{k+1}/W_k}{W_k/W_{k-1}} = (-1)^{i-1}\frac{W_1}{W_2}\cdot\frac{W_{i+1}}{W_i} = (-1)^i \frac{W_{i+1}}{bW_i}.$$

Multiplying by $\alpha^i = (-1)^i\beta^i$ gives the first claim; it also holds for $i=1$. For $i = N-2$ it gives $b^2\prod_{k=2}^{N-2} x_k = (-1)^N bW_{N-1}/W_{N-2}$, and the second claim follows from (6). □

*Proof of Proposition 3.2.* The formula for $\alpha^N$ follows from Lemma 3.4, since $\alpha^N = (-1)^N\rho_N$. By Lemma 3.4, the summands of $\mathcal{S}_1$ are $\beta^i W_{i+1}/W_i = b\,h_i$ for $1 \le i \le N-2$, and the summand with $i = N-1$ vanishes because $W_N = 0$. This gives $\mathcal{S}_1$ and, squaring, $\mathcal{S}_{1,1}$.

$\mathcal{S}_2$. For $i \le N-3$, the $i$th summand equals $(bh_i)(bh_{i+1})\beta^{-1}/W_2 = b\,h_ih_{i+1}/\alpha$. The summand with $i = N-2$ vanishes. For $i = N-1$, Lemma 3.3 gives $W_{N+1} = -W_{N-1}\rho_N^{-2}$, so the summand equals

$$\beta^{2N-2}\frac{-W_{N-1}\rho_N^{-2}}{W_{N-1}(-b)} = \frac{\beta^{-2}}{b} = \frac{1}{b\alpha^2} = -b\,h_{N-2},$$

where the last step uses $h_{N-2} = \alpha^{N-2}\prod_k x_k = -(b^2\alpha^2)^{-1}$.

$\mathcal{S}_3$. For $i \le N-4$, the $i$th summand equals $(bh_i)(bh_{i+1})(bh_{i+2})\beta^{-3}/W_3 = h_ih_{i+1}h_{i+2}/\alpha^3$. The summand with $i = N-3$ vanishes. Using $W_{N+1} = -W_{N-1}\rho_N^{-2}$, $W_{N+2} = bW_{N-1}\rho_N^{-3}$ and $W_{N-1}/W_{N-2} = -1/(b\rho_N)$, the summands with $i = N-2$ and $i = N-1$ become, respectively,

$$-\frac{\beta^{-6}}{b^4} = -\frac{h_{N-2}^2}{\alpha^2} \qquad \text{and} \qquad -\frac{\beta^{-3}}{b^2} = -\frac{h_{N-2}}{\alpha}.$$

$\mathcal{S}_{1,2}$. The summands are the products of those of $\mathcal{S}_1$ and $\mathcal{S}_2$, and they vanish for $i \in \{N-2, N-1\}$. □

[1] In fact the identity of Lemma 3.3 holds for all $m \in \mathbb{Z}$, by Lemma 3.6 and (C1) over $\mathbb{C}$ and the argument of Section 3.4 in general. We only need $-N < m < N$ however.

### 3.2 Analytic lemmata

In this subsection $K = \mathbb{C}$. Let $\Lambda$ be a lattice and $z_0 \in \mathbb{C}$ a point of exact order $N$ in $\mathbb{C}/\Lambda$. Put $\omega = Nz_0 \in \Lambda$ and $\Lambda' = \Lambda + \mathbb{Z}z_0$. We write $\sigma, \zeta, \wp, \eta$ for the functions of $\Lambda$ and $\sigma', \zeta', \wp', \eta'$ for those of $\Lambda'$. (Recall that primes never denote derivatives.) For a lattice $L$ and a point $v$ of order at least 4 in $\mathbb{C}/L$ set

$$m_L(v) = \zeta_L(2v) - 2\zeta_L(v), \qquad q_L(v) = \zeta_L(3v) - 3\zeta_L(v), \qquad \kappa_L(v) = q_L(v)^{-1}.$$

The first lemma identifies these quantities with the data of the Tate normal form of $(\mathbb{C}/L, v)$.

**Lemma 3.5.** *Let $v$ have order at least 4 in $\mathbb{C}/L$, and write $m = m_L(v)$ and $q = q_L(v)$. Then:*

1. *$m$ is the slope of the tangent to $E_L$ at $v$, and $q = u_v$ is the scaling parameter of Lemma 2.2. In particular $q \neq 0$, and with $\kappa = \kappa_L(v)$ the Tate normal form of $(\mathbb{C}/L, v)$ is*
$$E_L^{(1/\kappa,\ \wp_L(v),\ m,\ \frac{1}{2}\partial_z \wp_L(v))}.$$
2. *$\wp_L(2v) = m^2 - 2\wp_L(v)$ and $\wp_L(3v) = q^2 - 2qm + \wp_L(v)$.*

*Proof.* Write $x_j = \wp_L(jv)$ and $y_j = \frac{1}{2}\partial_z \wp_L(jv)$, so that $jv \mapsto (x_j, y_j)$ is a point of $E_L$. The curve $E_L$ has $a_1 = a_2 = a_3 = 0$ and $a_4 = -g_2/4$.

By (C3) and $\partial_z^2 \wp = 6\wp^2 - g_2/2$, we get $m = \frac{\partial_z^2 \wp(v)}{2\,\partial_z \wp(v)} = \frac{3x_1^2 - g_2/4}{2y_1}$, which is the tangent slope at $v$.

By (C3), $\mu := \zeta(3v) - \zeta(2v) - \zeta(v)$ is the slope of the chord through $v$ and $2v$. The duplication formula [Sil09, Algorithm III.2.3] gives $x_2 = m^2 - 2x_1$ and $y_2 = -y_1 - m(x_2 - x_1)$. Hence

$$q = m + \mu = m + \frac{y_2 - y_1}{x_2 - x_1} = \frac{-2y_1}{x_2 - x_1} = \frac{\psi_2(v)}{x(v) - x(2v)} = u_v,$$

using $\psi_2 = 2y$ on $E_L$. Part (1) now follows from Lemma 2.2.

For part (2), the formula for $\wp_L(2v) = x_2$ was just used, and the addition formula for the chord through $v$ and $2v$ gives $x_3 = \mu^2 - x_1 - x_2 = (q-m)^2 - x_1 - m^2 + 2x_1 = q^2 - 2qm + x_1$. □

The next lemma expresses the elliptic divisibility sequence of $P$ in terms of $\sigma$; this is the bridge between the algebraic formulae and theta functions. This is a known result, but we include a proof to fix the signs and the normalisation.

**Lemma 3.6.** *Let $E_{b,c}$ be the Tate normal form of $(\mathbb{C}/\Lambda, z_0)$ and put $\kappa = \kappa_\Lambda(z_0)$. Then for all $n \in \mathbb{Z}$,*

$$W_n = (-1)^{n+1} \kappa^{n^2-1} \frac{\sigma(nz_0)}{\sigma(z_0)^{n^2}}.$$

*Proof.* We first show that on $E_\Lambda$, as functions of $z \in \mathbb{C}$,

$$\psi_n(z) = (-1)^{n+1} \frac{\sigma(nz)}{\sigma(z)^{n^2}}. \tag{11}$$

Call the right-hand side $f_n(z)$. For $n = 0$ both sides vanish, as $\psi_0 = 0$ and $\sigma(0) = 0$. Both sides are odd in $n$, since $\psi_{-n} = -\psi_n$, $\sigma$ is odd and $(-1)^{-n+1} = (-1)^{n+1}$. So we may assume $n \geq 1$.

- *$f_n$ is $\Lambda$-periodic.* By (C1), shifting $z$ by $\omega \in \Lambda$ multiplies $\sigma(nz)$ and $\sigma(z)^{n^2}$ by
$$\chi(n\omega)e^{\eta(n\omega)(nz+n\omega/2)} = \chi(\omega)^n e^{n^2\eta(\omega)(z+\omega/2)} \quad \text{and} \quad \chi(\omega)^{n^2} e^{n^2\eta(\omega)(z+\omega/2)},$$
respectively. These agree because $n \equiv n^2 \pmod 2$.
- *Divisor.* Since $\sigma$ has simple zeros exactly at $\Lambda$, the function $\sigma(nz)$ has simple zeros at $\frac{1}{n}\Lambda$. Hence $f_n$ has simple zeros at the non-zero $n$-torsion points of $\mathbb{C}/\Lambda$ and a pole of order $n^2-1$ at 0. By (D3), $\psi_n$ has the same divisor.
- *Leading term.* By (C4), $f_n(z) = (-1)^{n+1} n z^{1-n^2}(1+O(z))$. Since the uniformiser $-x/y$ equals $z + O(z^5)$, (D3) gives the same leading term for $\psi_n$.

So $\psi_n/f_n$ is an elliptic function without zeros or poles, hence constant by (E1), and the constant is 1. This proves (11).

By Lemma 3.5, $E_{b,c} = E_\Lambda^{(1/\kappa,\dots)}$ with $(0,0)$ corresponding to $z_0$. Lemma 2.1 with $u = 1/\kappa$ gives $W_n = \kappa^{n^2-1}\psi_n(z_0)$, and the claim follows from (11). □

**Lemma 3.7** (Vélu and $\Lambda'$)**.** *Let $E_{b,c} = E_\Lambda^{T_A}$ with $T_A = (1/\kappa_0, \wp(z_0), m_\Lambda(z_0), \frac{1}{2}\partial_z\wp(z_0))$ and $\kappa_0 = \kappa_\Lambda(z_0)$, as in Lemma 3.5. Then the Vélu codomain is $E' = E_{\Lambda'}^{T_A}$. Under the uniformisations $\mathbb{C}/\Lambda \cong E_{b,c}$ and $\mathbb{C}/\Lambda' \cong E'$, the isogeny $\varphi$ is $z \mapsto z$ and $\hat\varphi$ is $z \mapsto Nz$.*

*Proof.* We first show
$$\wp'(z) = \wp(z) + \sum_{j=1}^{N-1} \big(\wp(z+jz_0) - \wp(jz_0)\big). \tag{12}$$
The right-hand side is $\Lambda'$-periodic, since shifting $z$ by $z_0$ permutes the terms $\wp(z+jz_0)$, $0 \le j \le N-1$, cyclically. It is even, by the substitution $j \mapsto N-j$. Its only poles are double poles at the points $\gamma \in \Lambda'$, with principal part $(z-\gamma)^{-2}$, and its constant term at $z=0$ vanishes. Hence it differs from $\wp'$ by an elliptic function without poles that vanishes at 0, which is zero by (E1).

Write $T_A = (u_0, r_0, s_0, t_0)$. By (1), the point $z \in \mathbb{C}/\Lambda$ has coordinates
$$x = \frac{\wp(z) - r_0}{u_0^2}, \qquad y = \frac{\frac{1}{2}\partial_z\wp(z) - s_0(\wp(z) - r_0) - t_0}{u_0^3}$$
on $E_{b,c}$. We now evaluate Vélu's formulae (4) with $G = \langle P \rangle$, $R = z$ and $Q = jz_0$ for $1 \le j \le N-1$. In each difference, the constants of the change of variables cancel: $r_0$ in the $x$-coordinates, and $t_0$ and $s_0 r_0$ in the $y$-coordinates. This leaves
$$x(R+Q) - x(Q) = \frac{\wp(z+jz_0) - \wp(jz_0)}{u_0^2},$$
$$y(R+Q) - y(Q) = \frac{\frac{1}{2}\big(\partial_z\wp(z+jz_0) - \partial_z\wp(jz_0)\big) - s_0\big(\wp(z+jz_0) - \wp(jz_0)\big)}{u_0^3}.$$
Summing over $j$ and adding $x(R)$ and $y(R)$, we use three facts: the identity (12); its derivative $\partial_z\wp'(z) = \partial_z\wp(z) + \sum_j \partial_z\wp(z+jz_0)$; and $\sum_j \partial_z\wp(jz_0) = 0$, which holds because $\partial_z\wp$ is odd and $j \mapsto N-j$ permutes the terms. This gives
$$x(\varphi(z)) = \frac{\wp'(z) - r_0}{u_0^2}, \qquad y(\varphi(z)) = \frac{\frac{1}{2}\partial_z\wp'(z) - s_0(\wp'(z) - r_0) - t_0}{u_0^3}.$$
These are exactly the coordinates of $z \in \mathbb{C}/\Lambda'$ on $E_{\Lambda'}^{T_A}$. Hence $E'$ and $E_{\Lambda'}^{T_A}$ share infinitely many points, so the two Weierstrass equations coincide, and $\varphi$ is $z \mapsto z$.

Finally, $z \mapsto Nz$ maps $\Lambda'$ into $\Lambda$, and its composition with $\varphi$ is $[N]$. By uniqueness of the dual isogeny [Sil09, Theorem III.6.1], it equals $\hat\varphi$. □

**Lemma 3.8.** *Put $S = \sum_{j=1}^{N-1} \wp(jz_0)$. Then:*

1. $\zeta'(z) = \zeta(z) + \sum_{j=1}^{N-1}\big(\zeta(z+jz_0) - \zeta(jz_0) + \wp(jz_0)z\big)$;
2. $\eta'(\lambda) = N\eta(\lambda) + S\lambda$ *for* $\lambda \in \Lambda$, *and* $\eta'(z_0) = \eta(\omega) + Sz_0$.

*Proof.* (1) By (12), both sides have derivative $-\wp'(z)$, so they differ by a constant. Both sides are odd: for the right-hand side, substitute $j \mapsto N-j$ and use $\zeta(-z+(N-j)z_0) = -\zeta(z+jz_0) + \eta(\omega)$ and $\zeta((N-j)z_0) = -\zeta(jz_0) + \eta(\omega)$, by (C1). Hence the constant is 0.

(2) Shifting $z$ by $\lambda \in \Lambda$ in (1) adds $\eta(\lambda)$ to each of the $N$ zeta terms and $S\lambda$ to the linear terms. Shifting by $z_0$, the zeta terms telescope to $\zeta(z+\omega) - \zeta(z) = \eta(\omega)$, and the linear terms contribute $Sz_0$. □

The following lemma shows that choosing the $N$th root $\beta$ amounts to choosing a point $P'$ with $\hat{\varphi}(P') = P$.

**Lemma 3.9.** *Let $E_{b,c}$ be the Tate normal form of $(\mathbb{C}/\Lambda, z_0)$ and $\kappa_0 = \kappa_\Lambda(z_0)$. For $\beta \in \mathbb{C}$ put $\varepsilon = \beta\kappa_0^2/\sigma(z_0)^2$.*

1. $\beta^N = \rho_N$ *if and only if* $\varepsilon^N = e^{-\eta(\omega)z_0}$.
2. *The $P$-distinguished points of $E' = \mathbb{C}/\Lambda'$ are the classes modulo $\Lambda'$ of the points $w_0$ with $Nw_0 \in z_0 + \Lambda$. There are exactly $N$ of them. Writing $Nw_0 = z_0 + \lambda_0$ with $\lambda_0 \in \Lambda$, the assignment*
$$w_0 \longmapsto \varepsilon(w_0) := \exp\big(\eta(\lambda_0)z_0 - \eta(\omega)w_0\big)$$
*is a well-defined bijection onto the $N$th roots of $e^{-\eta(\omega)z_0}$.*

*Proof.* (1) By (C1) with the shift $\omega$, for $1 \le a \le N-1$ we have
$$\sigma((N-a)z_0) = \sigma(\omega - az_0) = -\chi(\omega)\, e^{-\eta(\omega)(az_0 - \omega/2)}\sigma(az_0).$$
In particular $\sigma((N-2)z_0)/\sigma((N-1)z_0) = e^{-\eta(\omega)z_0}\sigma(2z_0)/\sigma(z_0)$. Insert Lemma 3.6 into $\rho_N = -W_{N-2}/(bW_{N-1})$, where $b = -W_2 = \kappa_0^3\sigma(2z_0)/\sigma(z_0)^4$. The signs cancel, the powers of $\kappa_0$ add up to $(N-2)^2-(N-1)^2-3 = -2N$, and the powers of $\sigma(z_0)$ to $(N-1)^2-(N-2)^2+4 = 2N+1$. This gives
$$\rho_N = \kappa_0^{-2N}\sigma(z_0)^{2N+1}\frac{\sigma((N-2)z_0)}{\sigma(2z_0)\,\sigma((N-1)z_0)} = \kappa_0^{-2N}\sigma(z_0)^{2N}e^{-\eta(\omega)z_0},$$
which is equivalent to the claim.

(2) By Lemma 3.7, $\hat{\varphi}(w_0) = Nw_0$, which proves the description of the $P$-distinguished points. Their set is a coset of $\ker\hat{\varphi}$, which has order $N$.

Next, using $Nw_0 = z_0 + \lambda_0$ and $Nz_0 = \omega$,
$$\varepsilon(w_0)^N = \exp\big(\eta(\lambda_0)\omega - \eta(\omega)z_0 - \eta(\omega)\lambda_0\big) = e^{-\eta(\omega)z_0}e^{\mathcal{E}(\lambda_0,\omega)} = e^{-\eta(\omega)z_0}$$
by (C2).

It remains to show that $\varepsilon$ is well defined on classes modulo $\Lambda'$ and injective. Two solutions differ by $\lambda/N$ with $\lambda \in \Lambda$. If $w_0' = w_0 + \lambda/N$, then $\lambda_0' = \lambda_0 + \lambda$ and
$$\frac{\varepsilon(w_0')}{\varepsilon(w_0)} = \exp\Big(\eta(\lambda)z_0 - \eta(\omega)\frac{\lambda}{N}\Big) = e^{\mathcal{E}(\lambda,\omega)/N},$$
which equals 1 if and only if $N \mid \mathcal{E}(\lambda,\omega)/2\pi i$. Since $z_0$ has exact order $N$, we can write $\omega = g\omega^*$ with $\omega^*$ primitive in $\Lambda$ and $\gcd(g,N) = 1$. By (C2) there is $\nu \in \Lambda$ with $\mathcal{E}(\nu,\omega^*) = 2\pi i$, and then $\Lambda = \mathbb{Z}\omega^* \oplus \mathbb{Z}\nu$. Write $\lambda = a\omega^* + c\nu$. Then $\mathcal{E}(\lambda,\omega)/2\pi i = cg$, so $N \mid \mathcal{E}(\lambda,\omega)/2\pi i$ if and only if $N \mid c$. Since $\mathbb{Z}g + \mathbb{Z}N = \mathbb{Z}$, this holds if and only if $\lambda \in N\Lambda + \mathbb{Z}\omega$, i.e. if and only if $\lambda/N \in \Lambda'$, i.e. if and only if $w_0' \equiv w_0 \pmod{\Lambda'}$. So $\varepsilon$ is well defined and injective on the $N$ classes, and therefore bijective onto the $N$ roots. □

**Lemma 3.10.** *Let $L$ be a lattice and $a, b, w \notin L$ with $a + b \notin L$. Then:*

1. $\mathcal{K}_L(z+\gamma, w) = e^{\eta_L(\gamma)w}\mathcal{K}_L(z,w)$ *for* $\gamma \in L$, *and* $\partial_z \mathcal{K}_L(z,w) = \mathcal{K}_L(z,w)\big(\zeta_L(z+w) - \zeta_L(z)\big)$;
2. $\mathcal{K}_L(z,w) = z^{-1} + \zeta_L(w) + \frac{1}{2}\big(\zeta_L(w)^2 - \wp_L(w)\big)z + O(z^2)$;
3. $\mathcal{K}_L(z,a)\mathcal{K}_L(z,b) = \big(\zeta_L(a) + \zeta_L(b)\big)\mathcal{K}_L(z,a+b) - \partial_z \mathcal{K}_L(z,a+b)$.

*Proof.* (1) The first claim follows from (C1), since the factors $\chi(\gamma)e^{\eta(\gamma)\gamma/2}$ cancel between $\sigma(z+w)$ and $\sigma(z)$. The second claim is the logarithmic derivative of $\mathcal{K}_L$ with respect to $z$.

(2) By (C4), $\sigma(z)^{-1} = z^{-1} + O(z^3)$. Taylor expanding $\log\sigma$ around $w$ gives $\sigma(z+w)/\sigma(w) = \exp\big(\zeta(w)z - \frac{1}{2}\wp(w)z^2 + O(z^3)\big)$. Multiplying the two expansions gives the claim.

(3) By (1), the right-hand side equals $\mathcal{K}(z, a+b)\, g(z)$ with $g(z) = \zeta(a) + \zeta(b) + \zeta(z) - \zeta(z+a+b)$. Consider $f(z) = \mathcal{K}(z,a)\mathcal{K}(z,b)/\mathcal{K}(z,a+b)$.

- Both $f$ and $g$ are $L$-periodic: for $f$ by (1), since the multipliers $e^{\eta(\gamma)a}e^{\eta(\gamma)b}$ and $e^{\eta(\gamma)(a+b)}$ cancel; for $g$ by (C1).
- Both have at most simple poles, located at $z \in L$ and $z \in -a-b+L$.
- By (2), both equal $z^{-1} + \zeta(a) + \zeta(b) - \zeta(a+b) + O(z)$ near 0.

Hence $f - g$ is elliptic, holomorphic at 0, and has at most one simple pole modulo $L$. By (E2) it is constant, and the constant is 0 because $f - g = O(z)$ at 0. □

The key ingredient of the proof is the following distribution relation. It evaluates a twisted sum of Kronecker functions over the cyclic subgroup $\langle z_0\rangle$ as a single Kronecker function of the isogenous lattice $\Lambda'$.

**Proposition 3.11** (Distribution relation)**.** *Let $w_0$ be as in Lemma 3.9, let $\varepsilon = \varepsilon(w_0)$, and put $T = \eta(\lambda_0) + Sw_0$. Then for $1 \le k \le N-1$,*

$$\Phi_k(z) := \sum_{i=0}^{N-1} \varepsilon^{ki}\, \mathcal{K}_\Lambda(z + iz_0,\, kz_0) \;=\; e^{-kTz}\, \mathcal{K}_{\Lambda'}(z,\, kw_0) =: \Psi_k(z).$$

*Proof.* Both sides are meromorphic in $z$: we have $kz_0 \notin \Lambda$, and $kw_0 \notin \Lambda'$ because the class of $w_0$ has order $N$ in $\mathbb{C}/\Lambda'$ (Lemma 3.13 below).

The strategy is the usual one for theta function identities: we show that both sides transform in the same way under $\Lambda'$ and have the same poles. Then their ratio is an elliptic function with at most one simple pole, and hence constant.

*Transformation under* $\Lambda$. Let $\lambda \in \Lambda$. By Lemma 3.10(1), $\Phi_k(z+\lambda) = e^{k\eta(\lambda)z_0}\Phi_k(z)$. By Lemma 3.10(1) for $\Lambda'$ and Lemma 3.8(2),

$$\Psi_k(z+\lambda) = e^{-kT\lambda + \eta'(\lambda)kw_0}\Psi_k(z) = e^{k(N\eta(\lambda)w_0 - \eta(\lambda_0)\lambda)}\Psi_k(z).$$

Since $Nw_0 = z_0 + \lambda_0$, the exponent equals $k\eta(\lambda)z_0 + k\mathcal{E}(\lambda,\lambda_0)$, and $e^{k\mathcal{E}(\lambda,\lambda_0)} = 1$ by (C2).

*Transformation under* $z_0$. Replacing $z$ by $z + z_0$ in $\Phi_k$ shifts the summation index by one, which gives

$$\Phi_k(z+z_0) = \varepsilon^{-k}\sum_{i=1}^{N}\varepsilon^{ki}\mathcal{K}_\Lambda(z+iz_0, kz_0).$$

The term with $i = N$ equals $\varepsilon^{kN}e^{k\eta(\omega)z_0}\mathcal{K}_\Lambda(z, kz_0) = \mathcal{K}_\Lambda(z, kz_0)$ by Lemma 3.10(1) and Lemma 3.9. Hence $\Phi_k(z+z_0) = \varepsilon^{-k}\Phi_k(z)$. On the other side, Lemma 3.8(2) gives

$$\Psi_k(z+z_0) = e^{-kTz_0 + \eta'(z_0)kw_0}\Psi_k(z) = e^{k(\eta(\omega)w_0 - \eta(\lambda_0)z_0)}\Psi_k(z) = \varepsilon^{-k}\Psi_k(z).$$

*Conclusion.* The function $F := (\Phi_k - \Psi_k)/\Psi_k$ is therefore $\Lambda'$-periodic. Both $\Phi_k$ and $\Psi_k$ have at most simple poles, located at the points of $\Lambda'$, with residue 1 at $z = 0$. Hence $\Phi_k - \Psi_k$ is holomorphic at 0, and, since it transforms by non-vanishing factors under $\Lambda'$, it is entire. The only possible poles of $F$ are thus the zeros of $\Psi_k$, which are simple and lie in $-kw_0 + \Lambda'$. By (E2), $F$ is constant. Since $\Psi_k$ has a pole at 0 while $\Phi_k - \Psi_k$ does not, $F(0) = 0$, and hence $F = 0$. □

**Corollary 3.12.** *With notation as above, put*

$$\zeta_k = \zeta(kz_0), \quad \wp_k = \wp(kz_0), \quad \tilde{\zeta}_k = \zeta'(kw_0) - kT, \quad \tilde{\wp}_k = \wp'(kw_0),$$

*and*

$$X_k = \tilde{\zeta}_k - \zeta_k, \qquad \Delta_k = \tfrac{1}{2}(\tilde{\zeta}_k^2 - \tilde{\wp}_k) - \tfrac{1}{2}(\zeta_k^2 - \wp_k).$$

*Then for* $1 \le k \le N-1$,

$$\sum_{i=1}^{N-1} \varepsilon^{ki} \mathcal{K}_\Lambda(iz_0, kz_0) = X_k, \qquad \sum_{i=1}^{N-1} \varepsilon^{ki}\, \partial_z \mathcal{K}_\Lambda(iz_0, kz_0) = \Delta_k.$$

*Moreover, for* $j, k \ge 1$ *with* $j + k \le N-1$,

$$\sum_{i=1}^{N-1} \varepsilon^{(j+k)i} \mathcal{K}_\Lambda(iz_0, jz_0)\mathcal{K}_\Lambda(iz_0, kz_0) = (\zeta_j + \zeta_k)X_{j+k} - \Delta_{j+k}.$$

*Proof.* By Proposition 3.11, the function

$$\Psi_k(z) - \mathcal{K}_\Lambda(z, kz_0) = \sum_{i=1}^{N-1} \varepsilon^{ki} \mathcal{K}_\Lambda(z + iz_0, kz_0)$$

is holomorphic at 0. The first two identities are its value and derivative at $z = 0$. To compute them, expand $\Psi_k(z) = e^{-kTz}\mathcal{K}_{\Lambda'}(z, kw_0)$ and $\mathcal{K}_\Lambda(z, kz_0)$ using Lemma 3.10(2) and $e^{-kTz} = 1 - kTz + \frac{1}{2}k^2T^2z^2 + O(z^3)$. One finds

$$\Psi_k(z) = z^{-1} + \tilde{\zeta}_k + \tfrac{1}{2}(\tilde{\zeta}_k^2 - \tilde{\wp}_k)z + O(z^2),$$

and subtracting the expansion of $\mathcal{K}_\Lambda(z, kz_0)$ gives the claim. The last identity follows by evaluating Lemma 3.10(3) with $(a, b) = (jz_0, kz_0)$ at $z = iz_0$ and summing. □

## 3.3 Proof of Theorem 3.1 over $\mathbb{C}$

Let $E_{b,c}/\mathbb{C}$ with $P$ of exact order $N$. By the uniformisation theorem [Sil09, Theorem VI.5.1], we can choose $(\Lambda, z_0)$ with $(\mathbb{C}/\Lambda, z_0) \cong (E_{b,c}, P)$. By uniqueness of the Tate normal form, $E_{b,c} = E_\Lambda^{T_A}$ as in Lemma 3.7. Let $\beta^N = \rho_N$. By Lemma 3.9, $\varepsilon = \beta\kappa_0^2/\sigma(z_0)^2$ equals $\varepsilon(w_0)$ for a unique $P$-distinguished class $w_0$. This proves part (3) once parts (1) and (2) are established with $P' = w_0$.

**Translation into Kronecker functions.** By Lemma 3.6,

$$\beta^{ki}\frac{W_{i+k}}{W_iW_k} = -\kappa_0^{2ik+1}\sigma(z_0)^{-2ik}\beta^{ik}\,\frac{\sigma((i+k)z_0)}{\sigma(iz_0)\sigma(kz_0)} = -\kappa_0\,\varepsilon^{ki}\,\mathcal{K}_\Lambda(iz_0, kz_0).$$

(The signs combine to $(-1)^{(i+k+1)-(i+1)-(k+1)} = -1$.) Multiplying two such expressions, the summands of $\mathcal{S}_{j,k}$ equal $\kappa_0^2\varepsilon^{(j+k)i}\mathcal{K}_\Lambda(iz_0, jz_0)\mathcal{K}_\Lambda(iz_0, kz_0)$. Corollary 3.12 therefore gives

$$\mathcal{S}_k = -\kappa_0 X_k, \qquad \mathcal{S}_{1,1} = \kappa_0^2\big(2\zeta_1X_2 - \Delta_2\big), \qquad \mathcal{S}_{1,2} = \kappa_0^2\big((\zeta_1 + \zeta_2)X_3 - \Delta_3\big).$$

**The geometric parameters.** Let $T_B = (1/\kappa_1, \wp'(w_0), m_1, \frac{1}{2}\partial_z\wp'(w_0))$ be the Tate normalisation of $(\mathbb{C}/\Lambda', w_0)$ (Lemma 3.5), so that $E_{b',c'} := E_{\Lambda'}^{T_B}$. By Lemma 3.7, $E' = E_{\Lambda'}^{T_A}$. By (3), the isomorphism $\iota\colon E_{b',c'} \to E'$ that corresponds to the identity on $\mathbb{C}/\Lambda'$ is attached to

$$u_{\mathrm{geo}} = \frac{\kappa_0}{\kappa_1}, \qquad s_{\mathrm{geo}} = \kappa_0(m_1 - m_0), \qquad r_{\mathrm{geo}} = \kappa_0^2(\tilde\wp_1 - \wp_1), \tag{13}$$

where $m_0 = m_\Lambda(z_0)$ and $m_1 = m_{\Lambda'}(w_0)$, and $\wp_1 = \wp(z_0)$ and $\tilde\wp_1 = \wp'(w_0)$ are as in Corollary 3.12. In particular $\iota(0,0) = w_0 = P'$.

**Comparison.** It remains to show $(u, r, s) = (u_{\mathrm{geo}}, r_{\mathrm{geo}}, s_{\mathrm{geo}})$. Put $q_j = 1/\kappa_j$ and $d = \tilde\zeta_1 - \zeta_1$. By the definitions of $m$ and $q$,

$$\zeta_2 = 2\zeta_1 + m_0, \quad \zeta_3 = 3\zeta_1 + q_0, \quad \tilde\zeta_2 = 2\tilde\zeta_1 + m_1, \quad \tilde\zeta_3 = 3\tilde\zeta_1 + q_1,$$

where in the last two identities the shifts by $kT$ cancel. Hence

$$X_1 = d, \qquad X_2 = 2d + m_1 - m_0, \qquad X_3 = 3d + q_1 - q_0.$$

The transcendental constant $T$ only enters through $d$, and we will see that $d$ drops out.

For $u$ and $s$ this is immediate:

$$\begin{aligned} 1 + 3\mathcal{S}_1 - \mathcal{S}_3 &= 1 - \kappa_0(3X_1 - X_3) = 1 - \kappa_0(q_0 - q_1) = \kappa_0/\kappa_1 = u_{\mathrm{geo}}, \\ 2\mathcal{S}_1 - \mathcal{S}_2 &= -\kappa_0(2X_1 - X_2) = \kappa_0(m_1 - m_0) = s_{\mathrm{geo}}. \end{aligned}$$

For $r$, apply Lemma 3.5(2) to $(\Lambda, z_0)$ and to $(\Lambda', w_0)$:

$$\wp_2 = m_0^2 - 2\wp_1, \quad \wp_3 = q_0^2 - 2q_0m_0 + \wp_1, \quad \tilde\wp_2 = m_1^2 - 2\tilde\wp_1, \quad \tilde\wp_3 = q_1^2 - 2q_1m_1 + \tilde\wp_1.$$

Write $\Delta_k = \frac{1}{2}X_k(\tilde\zeta_k + \zeta_k) - \frac{1}{2}(\tilde\wp_k - \wp_k)$ and substitute. For $Q_2 := \kappa_0^{-2}\mathcal{S}_{1,1}$ this gives

$$\begin{aligned} Q_2 &= 2\zeta_1X_2 - \tfrac{1}{2}X_2(4\zeta_1 + 2d + m_0 + m_1) + \tfrac{1}{2}(\tilde\wp_2 - \wp_2) \\ &= -\tfrac{1}{2}\big((2d + m_1)^2 - m_0^2\big) + \tfrac{1}{2}(m_1^2 - m_0^2) - (\tilde\wp_1 - \wp_1), \end{aligned}$$

that is, $Q_2 = -2d^2 - 2dm_1 - (\tilde\wp_1 - \wp_1)$. Similarly, for $Q_3 := \kappa_0^{-2}\mathcal{S}_{1,2}$,

$$Q_3 = X_3\Big(m_0 - \tfrac{1}{2}(3d + q_0 + q_1)\Big) + \tfrac{1}{2}(\tilde\wp_3 - \wp_3) = -\tfrac{9}{2}d^2 + 3d(m_0 - q_1) + q_1(m_0 - m_1) + \tfrac{1}{2}(\tilde\wp_1 - \wp_1).$$

In both cases $\zeta_1$ cancels. Finally,

$$\begin{aligned} q_0^2\, r &= -q_0(X_1 + X_2) - (X_1 + X_2)X_3 + \tfrac{3}{2}(X_1^2 - Q_2) - Q_3 \\ &= -q_0(3d + m_1 - m_0) - (3d + m_1 - m_0)(3d + q_1 - q_0) \\ &\qquad + \tfrac{3}{2}\big(3d^2 + 2dm_1 + (\tilde\wp_1 - \wp_1)\big) + \tfrac{9}{2}d^2 - 3d(m_0 - q_1) - q_1(m_0 - m_1) - \tfrac{1}{2}(\tilde\wp_1 - \wp_1) \\ &= \tilde\wp_1 - \wp_1. \end{aligned}$$

In the last step, the terms in $d^2$ and in $d$ cancel. So does $-q_0(m_1 - m_0) - (m_1 - m_0)(q_1 - q_0) - q_1(m_0 - m_1)$. Hence $r = r_{\mathrm{geo}}$.

**Conclusion.** Since $(u, r, s) = (u_{\mathrm{geo}}, r_{\mathrm{geo}}, s_{\mathrm{geo}})$ and $E_{b',c'}$ is a Tate normal form, the value of $t$ is forced by $a_2^* = a_3^*$ in (2); this is the formula for $t$ in Theorem 3.1. The formulae for $b' = -a_2^*$ and $c' = 1 - a_1^*$ are read off from the first line of (2). Moreover $u = \kappa_0/\kappa_1 \neq 0$. This proves part (1).

For part (2), $\hat{\varphi}(w_0) = Nw_0 \equiv z_0$ by Lemma 3.7, so $P'$ is $P$-distinguished. The remaining claims follow from Lemma 3.13 below. Part (3) was shown above. □

**Lemma 3.13.** *Let $Q \in E'(\overline{K})$ be $P$-distinguished. Then $Q$ has exact order $N$. Moreover, if $\iota_Q \colon E_Q \to E'$ is any isomorphism with $\iota_Q(0,0) = Q$ and $\varphi_Q$ is an isogeny with kernel $\langle (0,0) \rangle$ on $E_Q$, then $\varphi_Q \circ \iota_Q^{-1} \circ \varphi$ is cyclic of degree $N^2$.*

*Proof.* Choose $R \in E(\overline{K})$ with $\varphi(R) = Q$. Then $[N]R = \hat{\varphi}(\varphi(R)) = \hat{\varphi}(Q) = P$, so $[N]Q = \varphi([N]R) = \varphi(P) = \mathcal{O}$. On the other hand, the order of $Q$ is at least that of $\hat{\varphi}(Q) = P$, which is $N$. Hence $Q$ has exact order $N$.

The kernel of the composition is $\varphi^{-1}(\langle Q \rangle)$, which has order $\deg \varphi \cdot N = N^2$ and contains $R$. Since $[N]R = P$ has order $N$, the point $R$ has order $N^2$. So the kernel is generated by $R$, and in particular it is cyclic. □

### 3.4 Arbitrary characteristic coprime to $2N$

We now deduce the theorem in positive characteristic from the complex case. The idea is to view all quantities as regular functions on a model of the moduli space over $\mathbb{Z}[1/2N]$. There, an identity that holds at all complex points holds identically, and therefore also at all points of characteristic $p \nmid 2N$.

Let $Y_1(N) = \operatorname{Spec} R$ be the fine moduli scheme of pairs $(E, P)$ with $P$ of exact order $N$ over $\mathbb{Z}[1/N]$. For $N \geq 4$ it exists and is smooth of relative dimension one over $\mathbb{Z}[1/N]$ [KM85, Ch. 2 and 5]. Over $R$, the point $P$ has exact order $N \geq 4$ in every geometric fibre, so $\psi_2(P)$ and $x(P) - x(2P)$ are units. Hence Lemma 2.2 applies over $R$, and the universal pair is isomorphic to $(E_{b,c}, (0,0))$ with $b, c \in R$. For the same reason $W_i \in R^\times$ for $N \nmid i$, since $\psi_i(P) = 0$ would force $[i]P = \mathcal{O}$, in any characteristic [Sil09, Exercise 3.7]; therefore $\rho_N \in R^\times$.

*Proof of Theorem 3.1 in general. Step 1: the parameter space.* Put $R' = R \otimes \mathbb{Z}[1/2]$ and $Y = \operatorname{Spec} R_Y$ with $R_Y = R'[\beta]/(\beta^N - \rho_N)$. Since $N$ and $\rho_N$ are units, $Y$ is finite étale of degree $N$ over $Y_1(N)_{\mathbb{Z}[1/2N]}$, so it is smooth over $\mathbb{Z}[1/2N]$. Consequently $R_Y$ is flat over $\mathbb{Z}[1/2N]$ (hence torsion-free) and reduced.

*Step 2: a density argument.* Let $f \in R_Y$ vanish at all $\mathbb{C}$-points of $Y$. Then $f$ lies in every maximal ideal of the finitely generated $\mathbb{Q}$-algebra $R_Y \otimes \mathbb{Q}$, so it is nilpotent by the Nullstellensatz, hence 0 in $R_Y \otimes \mathbb{Q}$ since this ring is reduced. As $R_Y$ is torsion-free, $f = 0$.

*Step 3: the point $(r, t)$.* The elements $u, r, s, t$ of Theorem 3.1 are defined in $R_Y$: they only involve $\beta$, the units $W_i$ ($N \nmid i$) and $1/2$. Let $E'$ and $\hat{\varphi}$ be the Vélu codomain and the dual isogeny over $R'$, and let $Y' = \hat{\varphi}^{-1}(P) \subset E'$. Then $Y'$ is a torsor under the finite étale group scheme $\ker \hat{\varphi}$ of order $N$, hence finite étale of degree $N$ over $Y_1(N)_{\mathbb{Z}[1/2N]}$. The pair $(r, t)$ defines a morphism $F \colon Y \to \mathbb{A}^2_{Y_1(N)}$. The ideal of the closed subscheme $F^{-1}(Y')$ consists of functions that vanish at all $\mathbb{C}$-points, by the theorem over $\mathbb{C}$. By Step 2 this ideal is zero, so $F$ factors through $Y'$.

*Step 4: parts (1) and (2).* On $Y'$, Lemma 2.2 gives regular functions $u_{\mathrm{true}}$ and $\lambda_{\mathrm{true}}$ describing the Tate normalisation of $(E', Q)$, and $u_{\mathrm{true}}$ is a unit. By the theorem over $\mathbb{C}$ and the uniqueness of the Tate normalisation, $u - u_{\mathrm{true}} \circ F$ and $s - \lambda_{\mathrm{true}} \circ F$ vanish at all $\mathbb{C}$-points, hence vanish identically by Step 2. So $u \in R_Y^\times$, and at every geometric point of characteristic $p \nmid 2N$ the tuple $(u, r, s, t)$ is the Tate normalisation of $(E', F(\beta))$ given by Lemma 2.2. This is part (1), with $b', c'$ read off from (2). Part (2) follows from $F(\beta) \in Y'$ and Lemma 3.13.

*Step 5: part (3).* The morphism $F\colon Y \to Y'$ is a morphism between finite étale covers of $Y_1(N)_{\mathbb{Z}[1/2N]}$ of the same degree, so it is finite étale, of locally constant degree. Since $Y'$ is flat over $\mathbb{Z}[1/2N]$, every connected component of $Y'$ meets the characteristic-0 fibre, and there $F$ is bijective by the theorem over $\mathbb{C}$. Hence $F$ has degree 1 everywhere. So $F$ is an isomorphism, and part (3) follows. □

# 4 Choosing the root for even $N$

Let $N \geq 4$ be even. By Theorem 3.1(3), replacing $\beta$ by $-\beta$ replaces $P'$ by $P' + T$, where $T$ is the point of order 2 in $\ker\hat{\varphi}$. Over $\mathbb{F}_p$ with $p \equiv 3 \pmod 4$ there are at most two rational roots $\pm\beta$, and an implementation has to pick one. In this section we determine the class of $\beta$ modulo squares in terms of $P'$, and deduce which root keeps a walk on the surface of the 2-isogeny volcano. We prove the following theorem.

**Theorem 4.1.** *Let $N \geq 4$ be even and let $K$, $b$, $c$, $\beta$, $\varphi\colon E_{b,c} \to E'$, $P'$ and $\iota\colon E_{b',c'} \to E'$ be as in Theorem 3.1. Let $T$ be the unique point of order 2 in the cyclic group $\ker\hat{\varphi}$, let $T_3 = [N/2]P' + T$, and put*

$$\theta = -x\big(\iota^{-1}(T_3)\big),$$

*the negated $x$-coordinate of $T_3$ on $E_{b',c'}$. Then $\theta \neq 0$ and $\beta\theta$ is a square in $K(\beta)$. More precisely, with $Y = \operatorname{Spec} R'[\beta]/(\beta^N - \rho_N)$ as in Section 3.4, there is a unit $g \in R_Y^\times$ with $g^2 = \beta\theta$.*

Note that $T$ is $K$-rational, since $\ker\hat{\varphi} = \varphi(E[N])$ is defined over $K$, and that $T_3^* := \iota^{-1}(T_3)$ is a point of order 2 different from $[N/2](0,0)$. In particular $T_3^* \neq \pm(0,0)$, so $\theta = x(0,0) - x(T_3^*) \neq 0$.

*Remark* 4.2. Let $S$ be a $K$-rational point of order 2 on an elliptic curve $E/K$. For $Q \in E(K) \setminus \{\mathcal{O}, S\}$, the class of $x(Q) - x(S)$ in $K^\times/K^{\times 2}$ does not depend on the Weierstrass model: a change of coordinates (1) multiplies it by $u^2$. Moving $S$ to $(0,0)$ and completing the square shows that $Q \mapsto x(Q) - x(S)$ is the connecting homomorphism of the 2-isogeny descent for the isogeny $E/\langle S\rangle \to E$ dual to $E \to E/\langle S\rangle$ [Sil09, Proposition X.4.9]. In particular it is a homomorphism, and its kernel is the image of $(E/\langle S\rangle)(K)$. We write

$$t_2(S, Q) \in K^\times/K^{\times 2}$$

for this class; it is the reduced 2-Tate pairing. Since $x(0,0) = 0$ on $E_{b',c'}$, Theorem 4.1 says that $\beta \equiv t_2(T_3, P')$ modulo squares whenever $\beta \in K$. In [CDHV22, Conjecture 10], a statement of this kind was formulated for the radical $f_{N,P}(-P)$, involving $b$ and a modular unit $\Delta$; in our normalisation, these are replaced by $x(T_3^*)$.

## 4.1 An explicit square root over $\mathbb{C}$

We use the notation of Sections 2.5 and 3.2. Extend $\eta$ $\mathbb{Q}$-linearly to $\mathbb{Q}\Lambda$. Then Lemma 3.8(2) reads $\eta'(a) = N\eta(a) + Sa$ for all $a \in \Lambda'$, since $\eta(z_0) = \eta(\omega)/N$. Consequently, the Legendre pairings $\mathcal{E}$ of $\Lambda$ and $\mathcal{E}'$ of $\Lambda'$ satisfy

$$\mathcal{E}'(a,b) = \eta'(a)b - \eta'(b)a = N\,\mathcal{E}(a,b) \qquad (a, b \in \Lambda'), \tag{14}$$

where $\mathcal{E}$ is extended $\mathbb{Q}$-bilinearly. Put $\langle a, b\rangle = \mathcal{E}(a,b)/2\pi i$. By (C2), $\langle \Lambda, \Lambda\rangle \subset \mathbb{Z}$ and $N\langle \Lambda', \Lambda'\rangle \subset \mathbb{Z}$. Let $\chi$ and $\chi'$ be the sign characters of (C1) for $\Lambda$ and $\Lambda'$.

**Lemma 4.3.** *For $a, b \in \Lambda$ we have $\chi(a+b) = \chi(a)\chi(b)(-1)^{\langle a,b\rangle}$. If $a, b \notin 2\Lambda$ and $a \not\equiv b \pmod{2\Lambda}$, then $\langle a, b\rangle$ is odd.*

*Proof.* Both sides of the identity only depend on $a, b$ modulo $2\Lambda$. By (C2), $\langle\ ,\ \rangle$ induces a non-degenerate alternating form on $\Lambda/2\Lambda \cong \mathbb{F}_2^2$. Such a form takes the value 1 on any two distinct non-zero vectors, which is the second claim. The identity is now checked directly: it is trivial if $a$ or $b$ lies in $2\Lambda$; if $a \equiv b \not\equiv 0$, both sides equal 1; and if $a, b$ are distinct non-zero classes, then $a + b$ is the third one and both sides equal $-1$. □

Now let $(\mathbb{C}/\Lambda, z_0) \cong (E_{b,c}, P)$ and let $\beta$ correspond to the $P$-distinguished class $w_0$ as in the proof of Theorem 3.1, so that $\beta = \varepsilon(w_0)\sigma(z_0)^2/\kappa_0^2$ with $\varepsilon(w_0) = \exp(\eta(\lambda_0)z_0 - \eta(\omega)w_0)$ and $Nw_0 = z_0 + \lambda_0$.

Since $\hat{\varphi}$ is $z \mapsto Nz$ (Lemma 3.7), we have $\ker\hat{\varphi} = N^{-1}\Lambda/\Lambda'$. The point $T$ is $\varphi(S)$ for any $S \in E[2]$ outside $\langle P\rangle$, because $\varphi(E[2]) \subset \varphi(E[N]) = \ker\hat{\varphi}$ and $\varphi(S) \neq \mathcal{O}$. Hence $T$ is the class of $\mu/2$ for some

$$\mu \in \Lambda \setminus (2\Lambda + \mathbb{Z}\omega).$$

Since $z_0$ has even order $N$, the period $\omega = Nz_0$ is not in $2\Lambda$. Lemma 4.3 therefore gives

$$\chi(\omega) = -1, \qquad \langle\mu, \omega\rangle \equiv 1 \pmod 2. \tag{15}$$

Let $t_3 \in \mathbb{C}$ be any representative of $T_3$, for instance $t_3 = \frac{N}{2}w_0 + \frac{1}{2}\mu$, and put $\gamma = 2t_3 \in \Lambda'$. Since $T_3$ has order 2 in $\mathbb{C}/\Lambda'$, we have $\gamma \notin 2\Lambda'$ and $\chi'(\gamma) = -1$. Finally, let $\kappa_1 = \kappa_{\Lambda'}(w_0)$. By the proof of Theorem 3.1, $E_{b',c'} = E_{\Lambda'}^{T_B}$, so a class $z \in \mathbb{C}/\Lambda'$ has $x$-coordinate $\kappa_1^2(\wp'(z) - \wp'(w_0))$ on $E_{b',c'}$. In particular

$$\theta = \kappa_1^2\big(\wp'(w_0) - \wp'(t_3)\big).$$

**Definition 4.4.** With the data $(\Lambda, z_0, w_0, t_3)$ as above, put

$$\Omega = \chi(\lambda_0)\, e^{\Theta}\, \frac{\sigma(z_0)\,\kappa_1\,\sigma'(w_0 - t_3)}{\kappa_0\,\sigma'(w_0)\,\sigma'(t_3)}, \qquad 2\Theta = \eta(\lambda_0)z_0 - \eta(\omega)w_0 + \eta'(\gamma)w_0.$$

**Lemma 4.5.** $\Omega^2 = \beta\theta$.

*Proof.* For any lattice, $\wp(u) - \wp(v) = -\sigma(u+v)\sigma(u-v)/(\sigma(u)^2\sigma(v)^2)$ [Lan87, Ch. 18, §1]. Apply this to $\Lambda'$ with $u = w_0$ and $v = t_3$. By (C1) with $\gamma = 2t_3$,

$$\sigma'(w_0 + t_3) = \sigma'\big((w_0 - t_3) + \gamma\big) = \chi'(\gamma)e^{\eta'(\gamma)w_0}\sigma'(w_0 - t_3) = -e^{\eta'(\gamma)w_0}\sigma'(w_0 - t_3).$$

Hence

$$\theta = \kappa_1^2\, e^{\eta'(\gamma)w_0}\, \frac{\sigma'(w_0 - t_3)^2}{\sigma'(w_0)^2\sigma'(t_3)^2}.$$

Multiplying by $\beta = e^{\eta(\lambda_0)z_0 - \eta(\omega)w_0}\sigma(z_0)^2/\kappa_0^2$ gives $\Omega^2$, since $\chi(\lambda_0)^2 = 1$. □

**Lemma 4.6.** *$\Omega$ does not depend on the choice of the data. More precisely, $\Omega$ is unchanged under each of the following operations:*

1. *replacing $t_3$ by $t_3 + \delta$ with $\delta \in \Lambda'$;*
2. *replacing $w_0$ by $w_0 + \lambda'$ with $\lambda' \in \Lambda'$ (so that $\lambda_0$ becomes $\lambda_0 + N\lambda'$);*
3. *replacing $z_0$ by $z_0 + \lambda$ with $\lambda \in \Lambda$ (so that $\omega$ becomes $\omega + N\lambda$ and $\lambda_0$ becomes $\lambda_0 - \lambda$, while $\Lambda'$, $w_0$ and $t_3$ stay the same);*
4. *replacing $(\Lambda, z_0, w_0, t_3)$ by $(c\Lambda, cz_0, cw_0, ct_3)$ with $c \in \mathbb{C}^\times$.*

*Proof.* Throughout we use (C1) in the form $\sigma(z+a) = \chi(a)e^{\eta(a)(z+a/2)}\sigma(z)$, for $\Lambda$ and for $\Lambda'$.

(1) The factor $\sigma'(w_0 - t_3)/\sigma'(t_3)$ is multiplied by

$$\frac{\chi'(\delta)e^{-\eta'(\delta)(w_0-t_3-\delta/2)}}{\chi'(\delta)e^{\eta'(\delta)(t_3+\delta/2)}} = e^{-\eta'(\delta)w_0},$$

and $\Theta$ increases by $\frac{1}{2}\eta'(2\delta)w_0 = \eta'(\delta)w_0$. Nothing else changes.

(2) Write $\lambda' = \lambda + kz_0$ with $\lambda \in \Lambda$ and $k \in \mathbb{Z}$. By (1) we may simultaneously replace $t_3$ by $t_3 + \frac{N}{2}\lambda'$, so that $\gamma$ becomes $\gamma + N\lambda'$. The arguments $w_0$, $w_0 - t_3$ and $t_3$ of $\sigma'$ are shifted by $\lambda'$, $(1-\frac{N}{2})\lambda'$ and $\frac{N}{2}\lambda'$. The signs $\chi'$ contribute $\chi'(\lambda')^{1+(1-N/2)+N/2} = 1$. Write $e' = \eta'(\lambda')$. The exponential factors of the $\sigma'$-quotient contribute

$$e'\Big[-\big(w_0+\tfrac{\lambda'}{2}\big) + \big(1-\tfrac{N}{2}\big)\big(w_0 - t_3 + \big(1-\tfrac{N}{2}\big)\tfrac{\lambda'}{2}\big) - \tfrac{N}{2}\big(t_3 + \tfrac{N}{4}\lambda'\big)\Big] = -e'\big(\tfrac{N}{2}w_0 + t_3 + \tfrac{N}{2}\lambda'\big).$$

The new value of $2\Theta$ is $\eta(\lambda_0 + N\lambda')z_0 - \eta(\omega)(w_0+\lambda') + \eta'(\gamma+N\lambda')(w_0+\lambda')$, so $\Theta$ increases by

$$\tfrac{1}{2}\big(N\eta(\lambda')z_0 - \eta(\omega)\lambda'\big) + \tfrac{1}{2}\eta'(\gamma)\lambda' + \tfrac{N}{2}e'w_0 + \tfrac{N}{2}e'\lambda'.$$

Adding up, and using $\gamma = 2t_3$, the total change of log of $e^{\Theta}$ times the $\sigma'$-quotient is

$$\tfrac{1}{2}\mathcal{E}(\lambda',\omega) + \tfrac{1}{2}\mathcal{E}'(\gamma,\lambda') = \tfrac{1}{2}\mathcal{E}(\lambda,\omega) + \tfrac{N}{2}\mathcal{E}(\gamma,\lambda'),$$

using $\mathcal{E}(z_0,\omega) = 0$ and (14). So this part of $\Omega$ is multiplied by $(-1)^{\langle\lambda,\omega\rangle + N\langle\gamma,\lambda'\rangle}$. Now write $\gamma = z_0 + \lambda_0 + \mu + 2\delta$ with $\delta \in \Lambda'$. Since $N$ is even and $N\langle\delta,\lambda'\rangle \in \mathbb{Z}$,

$$N\langle\gamma,\lambda'\rangle \equiv N\langle z_0,\lambda\rangle + k\langle\lambda_0+\mu,\omega\rangle = \langle\omega,\lambda\rangle + k\langle\lambda_0+\mu,\omega\rangle \pmod 2.$$

Hence the sign is $(-1)^{k\langle\lambda_0+\mu,\omega\rangle}$. On the other hand, $\chi(\lambda_0)$ becomes $\chi(\lambda_0+N\lambda+k\omega) = \chi(\lambda_0+k\omega) = \chi(\lambda_0)\chi(\omega)^k(-1)^{k\langle\lambda_0,\omega\rangle}$ by Lemma 4.3. The product of the two signs is $(-1)^{k(\langle\mu,\omega\rangle+1)} = 1$ by (15).

(3) Here $\sigma(z_0)$ is multiplied by $\chi(\lambda)e^{\eta(\lambda)(z_0+\lambda/2)}$, the quantities $\kappa_0$, $\kappa_1$ and the $\sigma'$-factors do not change, and $\Theta$ increases by

$$\tfrac{1}{2}\big(\eta(\lambda_0)\lambda - \eta(\lambda)(z_0+\lambda) - N\eta(\lambda)w_0\big) = \tfrac{1}{2}\mathcal{E}(\lambda_0,\lambda) - \eta(\lambda)\big(z_0 + \tfrac{\lambda}{2}\big),$$

where we used $Nw_0 = z_0 + \lambda_0$. So the part of $\Omega$ without $\chi(\lambda_0)$ is multiplied by $\chi(\lambda)(-1)^{\langle\lambda_0,\lambda\rangle}$, which is exactly the factor by which $\chi(\lambda_0)$ changes when $\lambda_0$ becomes $\lambda_0 - \lambda$ (Lemma 4.3). The condition on $\mu$ is preserved because $\omega + N\lambda \equiv \omega \pmod{2\Lambda}$.

(4) We have $\sigma_{cL}(cz) = c\,\sigma_L(z)$, $\zeta_{cL}(cz) = c^{-1}\zeta_L(z)$ and $\eta_{cL}(ca) = c^{-1}\eta_L(a)$. Hence $\Theta$ and $\chi(\lambda_0)$ are invariant, $\kappa_0$ and $\kappa_1$ are multiplied by $c$, and the remaining $\sigma$-quotient has weight $1 - 1 = 0$. □

## 4.2 From $\mathbb{C}$ to $\mathbb{Z}[1/2N]$

Recall from Section 3.4 that $Y = \operatorname{Spec} R'[\beta]/(\beta^N - \rho_N)$ is smooth over $\mathbb{Z}[1/2N]$, and that $\beta \mapsto P'$ identifies $Y$ with $\hat{\varphi}^{-1}(P)$. The point $T$ is a section of the finite étale group scheme $\ker\hat{\varphi}[2]$ of order 2, so $\theta$ is a regular function on $Y$. It is a unit, because $T_3^* \neq \pm(0,0)$ in every geometric fibre. Hence

$$f := \beta\theta \in R_Y^\times.$$

**Lemma 4.7.** *$Y(\mathbb{C})$ is connected.*

*Proof.* Over $\tau$ in the upper half plane, take $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$ and $z_0 = 1/N$, so that $\Lambda' = \mathbb{Z}\tau + \frac{1}{N}\mathbb{Z}$. The $P$-distinguished classes are $w_0 = 1/N^2 + j\tau/N$ with $j \in \mathbb{Z}/N\mathbb{Z}$. The matrix $\left(\begin{smallmatrix} 1 & 0 \\ N & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$ maps $\tau$ to $\tau' = \tau/(N\tau+1)$, and multiplication by $N\tau+1$ identifies $\mathbb{C}/(\mathbb{Z}\tau'+\mathbb{Z})$ with $\mathbb{C}/\Lambda$. It maps $1/N$ to $\tau + 1/N \equiv 1/N$, and $1/N^2 + j\tau'/N$ to $1/N^2 + (j+1)\tau/N + 1/N \equiv 1/N^2 + (j+1)\tau/N \pmod{\Lambda'}$. So a path from $\tau$ to $\tau'$ in the upper half plane connects the sheet $j$ to the sheet $j+1$. Since $Y_1(N)(\mathbb{C})$ is connected, so is $Y(\mathbb{C})$. □

**Lemma 4.8.** *Let $t$ be an indeterminate. There is a point $y_\infty \in Y(\mathbb{Q}(\!(t)\!))$ such that $\beta(y_\infty) = t^{1-N}(1+O(t))$ and $\theta(y_\infty) = t\,(1+O(t))$. In particular $f(y_\infty)$ is a square in $\mathbb{Q}(\!(t)\!)$.*

*Proof.* Let $\mathbf{E}_q$ be the Tate curve over $\mathbb{Q}(\!(q)\!)$, with coordinates $X(u,q), Y(u,q)$ for $u \in \mathbb{G}_m/q^{\mathbb{Z}}$ [Sil94, §V.3]. Take $q = t^{N^2}$, $E = \mathbf{E}_q$ and $P = t^N$, a $\mathbb{Q}(\!(t)\!)$-rational point of order $N$. Then $E' = E/\langle P\rangle = \mathbf{E}_s$ with $s = t^N$, the isogeny $\varphi$ is the identity on $\mathbb{G}_m$, and $\hat\varphi$ is $u \mapsto u^N$. So $P' = t$ is $P$-distinguished, and $T = -1$. Through the identification $Y \cong \hat\varphi^{-1}(P)$ of Theorem 3.1(3), the triple $(E, P, P')$ defines $y_\infty$.

Over $\mathbb{C}$ and for $\operatorname{Im}\tau \gg 0$, the specialisation $t = e^{2\pi i\tau/N^2}$ corresponds to $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$, $z_0 = \tau/N$, $w_0 = \tau/N^2$ and $\lambda_0 = 0$, via $u = e^{2\pi i z}$ [Sil94, Theorem V.1.1]. The expansions of regular functions at $y_\infty$ are the convergent $t$-expansions of their analytic counterparts. By the Legendre relation $\eta(1)\tau - \eta(\tau) = 2\pi i$, we get $\varepsilon(w_0) = e^{-\eta(\tau)\tau/N^2} = t\,e^{-\eta(1)\tau^2/N^2}$. The product expansion of $\sigma$ [Lan87, Ch. 18, §2],

$$\sigma(z) = \frac{1}{2\pi i}\, e^{\eta(1)z^2/2}\big(u^{1/2} - u^{-1/2}\big) \prod_{n\geq 1} \frac{(1-q^n u)(1-q^n u^{-1})}{(1-q^n)^2},$$

gives $\sigma(z_0)^2 = (2\pi i)^{-2} e^{\eta(1)\tau^2/N^2} t^{-N}(1+O(t))$. Its logarithmic derivative gives

$$\zeta(3z_0) - 3\zeta(z_0) = \pi i\Big(\frac{u^3+1}{u^3-1} - 3\frac{u+1}{u-1}\Big) + O(t) = 2\pi i\,(1+O(t))$$

with $u = t^N$, so $\kappa_0 = (2\pi i)^{-1}(1+O(t))$. Hence $\beta = \varepsilon\sigma(z_0)^2/\kappa_0^2 = t^{1-N}(1+O(t))$. The same computation for $\Lambda' = \mathbb{Z}\frac{\tau}{N} + \mathbb{Z}$ and $u = t$ gives $\kappa_1 = (2\pi i)^{-1}(1+O(t))$; here $N \geq 4$ ensures that $s/u^3 = t^{N-3}$ is small. Moreover $\wp' = (2\pi i)^2(X(u,s) + \frac{1}{12})$, and $T_3 = [N/2]P' + T$ corresponds to $u = -t^{N/2}$. From $X(u,s) = u + O(u^2) + O(s/u) + O(s)$ we get $X(t,s) = t + O(t^2)$ and $X(-t^{N/2}, s) = O(t^2)$, because $N/2 \geq 2$. Therefore $\theta = \kappa_1^2(\wp'(w_0) - \wp'(t_3)) = t(1+O(t))$, and $f(y_\infty) = t^{2-N}(1+O(t))$ is a square in $\mathbb{Q}(\!(t)\!)$, as $N$ is even. □

*Proof of Theorem 4.1.* By Lemma 4.6, $\Omega$ only depends on the point of $Y(\mathbb{C})$ described by $(\Lambda, z_0, w_0)$. Near any point we can choose $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$ and $z_0, w_0, t_3$ as fixed $\mathbb{Q}$-linear combinations of 1 and $\tau$, with $\tau$ a local coordinate. Hence $\Omega$ is a holomorphic function on $Y(\mathbb{C})$, and $\Omega^2 = f$ by Lemma 4.5.

Consider the finite étale double cover $Z = \operatorname{Spec}(R_Y \otimes \mathbb{C})[X]/(X^2 - f)$ of $Y_{\mathbb{C}}$. If $X^2 - f$ were irreducible over $\mathbb{C}(Y)$, then $Z$ would be irreducible and $Z(\mathbb{C})$ connected. But $\Omega$ defines a holomorphic section of $Z(\mathbb{C}) \to Y(\mathbb{C})$, whose image is open and closed. Hence $f = g_1^2$ with $g_1 \in \mathbb{C}(Y)$, and $g_1 \in R_Y \otimes \mathbb{C}$ because $Y_{\mathbb{C}}$ is normal.

By Lemma 4.7, $Y_{\mathbb{Q}}$ is geometrically irreducible. So $g_1$, being algebraic over $\mathbb{Q}(Y)$, lies in $F(Y)$ for some number field $F$, and every $\sigma \in \operatorname{Gal}(F/\mathbb{Q})$ maps $g_1$ to $\pm g_1$. The resulting character cuts out a field $\mathbb{Q}(\sqrt{d})$, and $g_0 := g_1/\sqrt{d} \in \mathbb{Q}(Y)$ satisfies $f = d\,g_0^2$ with $d \in \mathbb{Q}^\times$. Evaluating at the point $y_\infty$ of Lemma 4.8, which lies over the generic point of $Y_{\mathbb{Q}}$, shows that $d$ is a square in $\mathbb{Q}(\!(t)\!)$, hence in $\mathbb{Q}$. Thus $f = g^2$ with $g \in \mathbb{Q}(Y)$.

Finally, $Y$ is smooth over $\mathbb{Z}[1/2N]$ with geometrically connected generic fibre, so $R_Y$ is a normal domain with fraction field $\mathbb{Q}(Y)$. Since $g$ is integral over $R_Y$, we get $g \in R_Y$, and $g$ is a unit because $g^2 = f$ is. Specialising to $K$ gives the theorem. □

### 4.3 Horizontal walks over $\mathbb{F}_p$

Let $p \equiv 7 \pmod 8$ and let $E/\mathbb{F}_p$ lie on the surface, with $\mathcal{O} = \mathbb{Z}[(1+\pi)/2]$ and $2\mathcal{O} = \mathfrak{l}\bar{\mathfrak{l}}$ as in Section 2.6. Let $r = \operatorname{ord}_2(p+1) \geq 3$. By (5), $E(\mathbb{F}_p) \cong \mathcal{O}/(\pi-1)\mathcal{O}$. Now $\pi - 1 = 2 \cdot \frac{\pi-1}{2}$ with $\frac{\pi-1}{2} \in \mathcal{O} \setminus 2\mathcal{O}$ (its half has trace $-\frac{1}{2}$), and the norm $p+1$ of $\pi-1$ has 2-adic valuation $r$. After possibly swapping $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ we may therefore assume $\operatorname{ord}_{\mathfrak{l}}(\pi-1) = r-1$ and $\operatorname{ord}_{\bar{\mathfrak{l}}}(\pi-1) = 1$. Hence

$$E(\mathbb{F}_p)[2^\infty] = M_{\mathfrak{l}} \oplus M_{\bar{\mathfrak{l}}} \cong \mathbb{Z}/2^{r-1} \oplus \mathbb{Z}/2, \tag{16}$$

where $M_{\mathfrak{l}} \cong \mathcal{O}/\mathfrak{l}^{r-1}$ and $M_{\bar{\mathfrak{l}}} \cong \mathcal{O}/\bar{\mathfrak{l}}$ are the $\mathfrak{l}$- and $\bar{\mathfrak{l}}$-primary parts. The same holds for every curve on the surface, with the same $\mathfrak{l}$. We write points of (16) as pairs $(n_1, n_2)$, and put $S_{\mathfrak{l}} = (2^{r-2}, 0)$ and $S_{\bar{\mathfrak{l}}} = (0,1)$, the rational points of $E[\mathfrak{l}]$ and $E[\bar{\mathfrak{l}}]$.

**Lemma 4.9.** *For $Q \in E(\mathbb{F}_p)$ with 2-primary component $(n_1, n_2)$, we have $t_2(S_{\mathfrak{l}}, Q) = (-1)^{n_2}$ and $t_2(S_{\bar{\mathfrak{l}}}, Q) = (-1)^{n_1}$.*

*Proof.* Let $\psi\colon E \to E''$ be the horizontal 2-isogeny with kernel $\langle S_{\mathfrak{l}} \rangle = E[\mathfrak{l}]$. Its dual $\hat{\psi}$ has kernel $E''[\bar{\mathfrak{l}}]$ and is $\mathcal{O}$-linear. By Remark 4.2, $t_2(S_{\mathfrak{l}}, Q) = 1$ if and only if $Q \in \hat{\psi}(E''(\mathbb{F}_p))$. Since $\ker\hat{\psi}$ has a rational generator and $\#E''(\mathbb{F}_p) = \#E(\mathbb{F}_p)$, this image has index 2. On the $\mathfrak{l}$-primary parts, $\hat{\psi}$ is injective (its kernel is $\bar{\mathfrak{l}}$-primary), hence bijective onto $M_{\mathfrak{l}}$, as both have order $2^{r-1}$. Odd-order components are always in the image. So the image is the index-2 subgroup that contains $M_{\mathfrak{l}}$, namely $\{n_2 = 0\}$. The second claim follows in the same way, using that $2^{r-2}$ is even. □

**Corollary 4.10.** *Let $p \equiv 7 \pmod 8$, $r = \operatorname{ord}_2(p+1)$, and let $E_{b,c}/\mathbb{F}_p$ lie on the surface. Let $N \geq 4$ be even with $N \mid p+1$, and assume that $\langle P \rangle$ is the kernel of a horizontal isogeny. Then:*

1. *$\rho_N$ has exactly two $N$th roots in $\mathbb{F}_p$, namely $\pm\beta_0$ with $\beta_0 = \rho_N^{(p+1)/(2N)}$. Here $\beta_0$ is a square and $-\beta_0$ is not.*
2. *Exactly one of them yields a point $P'$ for which $\langle P' \rangle$ is again horizontal (equivalently, the composition of two steps is horizontal). It is $\beta_0$ if $P \in 2E(\mathbb{F}_p)$, and $-\beta_0$ otherwise.*
3. *In both cases, the point $(0,0) \in E_{b',c'}$ is halvable over $\mathbb{F}_p$ if and only if $P$ is. So the rule does not change along a horizontal walk.*

*Proof.* Write $N = 2^k n$ with $n$ odd, and let $\langle P \rangle = E[\mathfrak{a}]$ with $\mathfrak{a}$ invertible of norm $N$. Then $\varphi$ and $\hat{\varphi}$ correspond to $\mathfrak{a}$ and $\bar{\mathfrak{a}}$, and $\ker\hat{\varphi} = E'[\bar{\mathfrak{a}}]$. Since $\mathfrak{a}$ and $\bar{\mathfrak{a}}$ are coprime (2 and all odd $\ell \mid N$ split), $\hat{\varphi}$ restricts to an injection $E'[\mathfrak{a}] \to E[\mathfrak{a}] = \langle P \rangle$, hence to a bijection. The group $E'[\mathfrak{a}]$ consists of rational points, because $E'(\mathbb{F}_p) \cong \mathcal{O}/(\pi-1)$ and $E(\mathbb{F}_p) \supset E[\mathfrak{a}]$ show $\mathfrak{a} \mid \pi - 1$. So there is a rational $P'_h \in E'[\mathfrak{a}]$ with $\hat{\varphi}(P'_h) = P$, and $\langle P'_h \rangle = E'[\mathfrak{a}]$ is horizontal. The other rational $P$-distinguished point is $P'_h + T$, which does not lie in $E'[\mathfrak{a}]$.

Since $r$ and $t$ are given by expressions in $\beta$ with coefficients in $\mathbb{F}_p$, the bijection $\beta \mapsto P'$ of Theorem 3.1(3) commutes with the Frobenius. Hence the two rational $P$-distinguished points $P'_h$ and $P'_h + T$ correspond to two distinct roots of $X^N - \rho_N$ in $\mathbb{F}_p$. In particular $\rho_N$ is an $N$th power in $\mathbb{F}_p$, and hence a square since $N$ is even. Since $n \mid p+1$, we have $\gcd(N, p-1) = 2$, so these are the only $N$th roots of $\rho_N$ in $\mathbb{F}_p$. As $2N \mid p+1$ (note $k \leq r-1$ by (16)), $\beta_0^N = \rho_N^{(p+1)/2} = \rho_N$, and $\beta_0$ is a square since $\rho_N$ is. As $p \equiv 3 \pmod 4$, $-\beta_0$ is not a square. This proves (1).

Only the 2-primary component matters for horizontality, and it determines halvability. Let $(n_1, n_2)$ be the 2-primary component of a rational $P$-distinguished point $P'$; the other one is $P' + T$. By Theorem 4.1 and Remark 4.2, $\beta \equiv t_2(T_3, P') = t_2(T_1, P')\, t_2(T, P')$ with $T_1 = [N/2]P'$. There are three cases.

*Case* $\langle P\rangle_2 = E[\mathfrak{l}^k]$ *with* $k \geq 2$. Then $\hat{\varphi}$ has 2-part $\bar{\mathfrak{l}}^k$, so $T = S_{\bar{\mathfrak{l}}}$, and $n_1$ has order $2^k$. Moreover $T_1 = S_{\mathfrak{l}}$, because $N/2$ is even. The subgroup $\langle P'\rangle$ is horizontal if and only if $n_2 = 0$. Lemma 4.9 gives $\beta \equiv (-1)^{n_1+n_2}$. Here $n_1$ is odd if and only if $k = r-1$, which is the case exactly when $P \notin 2E(\mathbb{F}_p)$.

*Case* $\langle P\rangle_2 = E[\mathfrak{l}]$, $k = 1$. Again $T = S_{\bar{\mathfrak{l}}}$. Now $n_1 = 2^{r-2}$ and $n_2 \in \{0, 1\}$, and $n_2 = 0$ is the horizontal one. As $N/2$ is odd, $T_1 = (n_1, n_2)$ and $T_3 = (n_1, n_2 + 1)$, so $\beta \equiv (-1)^{n_2} \cdot (-1)^{n_1(n_2+1)} = (-1)^{n_2}$, because $n_1 = 2^{r-2}$ is even. Here $P \in 2E(\mathbb{F}_p)$.

*Case* $\langle P\rangle_2 = E[\bar{\mathfrak{l}}]$, $k = 1$. Now $\ker\hat{\varphi}$ has 2-part $\mathfrak{l}$, so $T = S_{\mathfrak{l}}$, $n_2 = 1$ and $n_1 \in \{0, 2^{r-2}\}$, and $n_1 = 0$ is the horizontal one. Then $T_3 = (n_1 + 2^{r-2}, 1)$, and Lemma 4.9 gives $\beta \equiv (-1) \cdot 1 = -1$ for $n_1 = 0$, and $\beta \equiv 1$ for $n_1 = 2^{r-2}$. Here $P \notin 2E(\mathbb{F}_p)$.

In all cases the horizontal root is a square if and only if $P \in 2E(\mathbb{F}_p)$. Moreover, the horizontal $P'$ has the same $k$ and the same direction as $P$, so it is halvable if and only if $P$ is. This proves (2) and (3). □

In the notation of [CDHV22], $P \in 2E(\mathbb{F}_p)$ is the case where $P$ points in the direction $\mathfrak{l}$ (their "$P\rightarrow$") and $\operatorname{ord}_2 N < r - 1$. Corollary 4.10 is therefore the analogue, in our normalisation, of the root selection rule of [CDHV22, Proposition 12], which was proved there for $N \leq 14$ by verifying [CDHV22, Conjecture 10] in the function field of $X_1(N)$; for $N = 4$ it is consistent with [OM22]. In practice, one chooses $p$ with $2N \mid (p+1)/2$, i.e. $\operatorname{ord}_2 N \leq r - 2$, and walks in the direction $\mathfrak{l}$. Then the correct root is always the square one, $\rho_N^{(p+1)/(2N)}$: no Legendre symbol has to be evaluated, and the exponent is fixed.

# 5 Computational aspects

We count field operations in $\mathbb{F}_p$: **M**, **S**, **I** and **E** denote a multiplication, squaring, inversion and exponentiation with an exponent of size about $p$. Unless stated otherwise, squarings and multiplications by curve constants count as **M**, and additions are ignored. As a rule of thumb we use $\mathbf{E} \approx 1.2 \log_2 p\, \mathbf{M}$, which corresponds to a fixed-window exponentiation when squarings are counted as multiplications. An algorithm is called *constant-time* if, for fixed $N$, it executes the same sequence of field operations on all inputs.

## 5.1 An optimised inversion-free radical step

**The scaled model.** Let $(B : C : Z)$ represent $(b, c) = (B/Z, C/Z)$. Instead of $E_{b,c}$ we work on $\tilde{E} = E_{b,c}^{(1/Z,0,0,0)}$, whose coefficients are polynomials:

$$\tilde{a}_1 = A := Z - C, \qquad \tilde{a}_2 = -BZ, \qquad \tilde{a}_3 = -BZ^2, \qquad \tilde{a}_4 = \tilde{a}_6 = 0.$$

Its $x$-coordinate is $\tilde{x} = Z^2 x$.

**Lemma 5.1.** *Let* $E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2$ *and* $Q \in E$ *with* $Q, Q \pm (0,0) \neq \mathcal{O}$. *Then*

$$x\big(Q + (0,0)\big) + x\big(Q - (0,0)\big) = \frac{a_3\big(a_3 + a_1x(Q)\big)}{x(Q)^2}.$$

*Proof.* The slopes of the chords from $Q = (x, y)$ to $(0,0)$ and to $-(0,0) = (0, -a_3)$ are $y/x$ and $(y + a_3)/x$. By the addition formula [Sil09, Algorithm III.2.3], the left-hand side equals $\lambda_+^2 + \lambda_-^2 + a_1(\lambda_+ + \lambda_-) - 2a_2 - 2x$. Its numerator over $x^2$ is $2(y^2 + a_1xy + a_3y - x^3 - a_2x^2) + a_3^2 + a_1a_3x = a_3(a_3 + a_1x)$. □

Write $\tilde{x}_k = \tilde{x}([k]P)$. Lemma 5.1 gives $\tilde{x}_1 = 0$, $\tilde{x}_2 = BZ$, $\tilde{x}_3 = CZ$ and

$$\tilde{x}_k = \frac{\tilde{a}_3(\tilde{a}_3 + A\tilde{x}_{k-1})}{\tilde{x}_{k-1}^2} - \tilde{x}_{k-2} \qquad (k \geq 4). \tag{17}$$

Since $\tilde{x}_{N-k} = \tilde{x}_k$, this is only needed for $k \leq N/2$. Since $\prod_{k=2}^{N-2} \tilde{x}_k = Z^{2N-6} \prod_{k=2}^{N-2} x_k$ and $\tilde{a}_3^2 = Z^6 b^2$, Proposition 3.2 gives

$$\tilde{\alpha} := \alpha/Z^2, \qquad \tilde{\alpha}^N = -\Big(\tilde{a}_3^2 \prod_{k=2}^{N-2} \tilde{x}_k\Big)^{-1}, \qquad \tilde{\alpha}\, \tilde{x}_k = \alpha x_k.$$

**Algorithm 5.2** (Radical step)**.** *Input:* $(B : C : Z)$ such that $(0, 0) \in E_{B/Z, C/Z}$ has exact order $N \geq 4$, and a procedure for $N$th roots. *Output:* $(B' : C' : Z')$ representing $(b', c')$.

1. *Multiples.* Put $(X_2, D_2) = (BZ, 1)$ and $(X_3, D_3) = (CZ, 1)$. For $4 \leq k \leq N/2$ compute

   $$X_k = \tilde{a}_3 D_{k-1}\big(\tilde{a}_3 D_{k-1} + A X_{k-1}\big) D_{k-2} - X_{k-2} X_{k-1}^2, \qquad D_k = X_{k-1}^2 D_{k-2},$$

   so that $\tilde{x}_k = X_k/D_k$. Extend by $(X_{N-k}, D_{N-k}) = (X_k, D_k)$.

2. *Radical.* Put $\Pi_X = \prod_{k=2}^{N-2} X_k$ and $\Pi_D = \prod_{k=2}^{N-2} D_k$, computed from the half products, and $\mu = \tilde{a}_3^2 \Pi_X$. Compute $\gamma$ with $\gamma^N = v := -\Pi_D\, \mu^{N-1}$. Then $\tilde{\alpha} = \gamma/\mu$.

3. *Terms.* Put $\xi_k = \gamma X_k$ and $\eta_k = \mu D_k$, so that $\alpha x_k = \xi_k/\eta_k$. Compute prefix products $\Xi_1 = \gamma$, $\Xi_i = \Xi_{i-1}\xi_i$ and $H_1 = 1$, $H_j = H_{j-1}\eta_j$, and put

   $$e_i = \Xi_i\, H_{N-1-i} \quad (1 \leq i \leq N-2), \qquad \mathcal{D} = \mu H_{N-2}, \qquad g = \gamma\mathcal{D}, \qquad \nu = BZ\gamma.$$

4. *Sums.* Compute

   $$\Sigma_1 = \sum e_i, \qquad \Sigma_{11} = \sum e_i^2, \qquad \Sigma_2 = \sum e_i e_{i+1},$$
   $$\Sigma_3 = \sum e_i e_{i+1} e_{i+2}, \qquad \Sigma_{12} = \sum e_i^2 e_{i+1},$$

   over all indices for which the terms are defined, and put $\bar{e} = e_{N-2}$.

5. *Assembly.* Compute

   $$V = \mu^2\Sigma_3 - \mu g\bar{e}^2 - g^2\bar{e}, \qquad U = g^3 + 3\nu\Sigma_1 g^2 - \mu V, \qquad S = \nu\big(g(2\Sigma_1 + \bar{e}) - \mu\Sigma_2\big),$$
   $$\mathcal{R} = 2\nu(g\Sigma_1 + \mu\Sigma_2 - g\bar{e})(g^3 - \mu V) + 3\nu^2(\Sigma_1^2 - \Sigma_{11})g^3 - 2\nu^2\mu\Sigma_{12}g^2.$$

6. *Output.*

   $$B' = g\big(2Bg^5 + 2ASg^3 + 2ZS^2 g - 3Z\mathcal{R}\big),$$
   $$C' = 2U\big(ZU - g(Ag^2 + 2SZ)\big), \qquad Z' = 2ZU^2.$$

**Proposition 5.3.** *Algorithm 5.2 is correct. Apart from the $N$th root and the power $\mu^{N-1}$ (at most $2\log_2 N$ multiplications), it uses*

$$\tfrac{1}{2}(25N - 13)\,\mathbf{M} \ \textit{ for odd } N \geq 11, \qquad \tfrac{1}{2}(25N - 2)\,\mathbf{M} \ \textit{ for even } N \geq 10,$$

*of which about $1.5N$ are squarings. It uses no inversions, no branches and no Legendre symbols, so it is constant-time.*

*Proof.* By the identity $\tilde{\alpha}\tilde{x}_k = \alpha x_k$, the quantities $h_i$ of (10) equal $\alpha \prod_{k=2}^{i} \xi_k/\eta_k$. Using $\eta_k = \eta_{N-k}$ and $\alpha = Z^2\gamma/\mu$, this is $Z^2 e_i/\mathcal{D}$. Substituting into Proposition 3.2 gives

$$\mathcal{S}_1 = \frac{\nu\Sigma_1}{g}, \quad \mathcal{S}_2 = \frac{\nu(\mu\Sigma_2 - g\bar{e})}{g^2}, \quad \mathcal{S}_3 = \frac{\mu V}{g^3}, \quad \mathcal{S}_{1,1} = \frac{\nu^2\Sigma_{11}}{g^2}, \quad \mathcal{S}_{1,2} = \frac{\nu^2\mu\Sigma_{12}}{g^3}.$$

Hence $u = U/g^3$, $s = S/g^2$ and $r = \mathcal{R}/(2g^5)$ by (8), and (9) gives $b' = B'/Z'$ and $c' = C'/Z'$.

For the count, the recursion (17) costs 7 operations per $k \le N/2$, i.e. $3.5N$ in total. The products $\Pi_X$ and $\Pi_D$ cost about $N$, the $\xi_k, \eta_k$ about $N$, the prefix products $2N$, the $e_i$ another $N$, and the five sums $4N$. The assembly costs a constant number of operations. For example, $N = 13$, 31 and 199 cost 156, 381 and 2481 **M**. □

For comparison, a single radical step in [Dec24, §4] costs $\mathbf{E}+3\mathbf{I}+(16N-25)\mathbf{M}$. The new step is therefore cheaper for every odd $N \ge 11$, the range covered by Proposition 5.3, even when inversions are free; for smaller $N$ the two counts are comparable. In constant-time implementations, where an inversion is usually computed by an exponentiation, the saving is about $3\mathbf{E}$ per step.

### 5.2 Odd degrees

For odd $N \mid p+1$ we have $\gcd(p-1, N) = 1$, so $v$ in Algorithm 5.2 has a unique $N$th root $\gamma = v^e$ in $\mathbb{F}_p$, with $e \equiv N^{-1} \pmod{p-1}$. By Theorem 3.1 and Section 2.6, iterating computes the action of $\prod_{\ell \mid N}[(\ell, \pi - 1)]^k$ [CDV20, Lemma 8]. The inverse action is obtained on the quadratic twist, which for $p \equiv 3 \pmod 4$ only changes signs of curve coefficients and $x$-coordinates.

### 5.3 Radical $2^m$-isogenies

Let $p \equiv 7 \pmod 8$ and $r = \mathrm{ord}_2(p+1)$, and take $N = 2^m$ with $m \le r - 2$. We start on the surface with a point $P$ in the direction $\mathfrak{l}$ of Section 4.3. Then $P \in 2E(\mathbb{F}_p)$, and by Corollary 4.10 the horizontal root is always the square one. One radical step computes $m$ horizontal 2-isogenies at once, using one exponentiation.

**Selecting the square root without a Legendre symbol.** Algorithm 5.2 works with $\gamma = \mu\tilde{\alpha}$, and $\beta = -\alpha = -Z^2\gamma/\mu$ has the square class of $-\gamma\mu$. Put $\delta = \gamma\mu$, so that $\delta^N = v\mu^N = -\Pi_D \mu^{2N-1}$. Run Algorithm 5.2 with $(\gamma, \mu)$ replaced by $(\delta, \mu^2)$; this leaves $\tilde{\alpha}$, and hence the output, unchanged. Then $\beta$ is a square if and only if $-\delta$ is. So the horizontal step is obtained from

$$\delta = -\left(-\Pi_D \mu^{2N-1}\right)^{(p+1)/(2N)},$$

which costs one exponentiation with a fixed exponent and $O(\log N)$ extra multiplications. If $P \notin 2E(\mathbb{F}_p)$, the sign is flipped.

**Cost.** Per 2-isogeny, a radical $2^m$-step costs about

$$c(m) = \frac{\mathbf{E} + (12.5 \cdot 2^m - 1 + 2m)\mathbf{M}}{m}.$$

The first term favours large $m$ and the second small $m$; the optimum lies near $m \approx \log_2(\mathbf{E}/12.5\mathbf{M}) - 1$. Table 1 gives $c(m)$ for typical sizes of $p$.

The radical 4-isogenies of [CDHV22, OM22] cost $\mathbf{E} + 3\mathbf{M} + \mathbf{I}$, so the last column is a lower bound for them; the optimal $2^m$-step gains a factor 1.5 at 512 bits and 2.6 at 4096 bits. The 8- and 16-isogenies of [CDHV22] cost $\mathbf{E}+11\mathbf{M}+2\mathbf{I}$ and $\mathbf{E}+120\mathbf{M}+3\mathbf{I}$. With free

| $\log_2 p$ | $m=2$ | 3 | 4 | 5 | 6 | 7 | 8 | best | $\mathbf{E}/2$ |
|---|---|---|---|---|---|---|---|---|---|
| 512 | 338 | 240 | 206 | **205** | 238 | 319 | 479 | $m=5$ | 308 |
| 1024 | 645 | 445 | 359 | **328** | 340 | 406 | 556 | $m=5$ | 615 |
| 2048 | 1259 | 854 | 667 | 574 | **545** | 582 | 710 | $m=6$ | 1229 |
| 4096 | 2488 | 1674 | 1281 | 1065 | 955 | **933** | 1017 | $m=7$ | 2458 |

Table 1: Cost $c(m)$ in $\mathbf{M}$ per horizontal 2-isogeny of a radical $2^m$-step, rounded up, with $\mathbf{E} = 1.2\log_2 p\,\mathbf{M}$. For $m = 2, 3$, where the count of Proposition 5.3 does not apply, $12.5{\cdot}2^m{-}1$ is replaced by the exact counts 56 and 98 of Algorithm 5.2. The last column is a lower bound for any method that uses one exponentiation per 4-isogeny.

inversions, the latter cost 184, 338, 645 and 1259 $\mathbf{M}$ per 2-isogeny for the sizes of Table 1: about 10% less than the best $2^m$-step at 512 bits, on par at 1024 bits, and 1.18 and 1.35 times more at 2048 and 4096 bits. With $\mathbf{I} \approx \mathbf{E}$, the $2^m$-steps are at least 3 times faster at all sizes. The price is the condition $2^{m+2} \mid p+1$, which for $p = 2^a f \prod \ell_i - 1$ costs only a few bits of $p$. For the VDF of [DFMPS19], the delay of a walk of length $T$ then becomes about $T/m$ exponentiations.

### 5.4 Pushing points through a radical step

Let $R$ be a point on $\tilde{E}$, given by its $x$-coordinate $\tilde{x}(R) = X_R/Z_R$. To compute $\tilde{x}$ of its image on the next scaled model, we use Kohel's form of Vélu's formulae [Koh96]. Let $\mathcal{Q}$ be a set of representatives of $(\langle P\rangle \setminus \{\mathcal{O}, [N/2]P\})/\pm$ (for odd $N$, of $(\langle P\rangle \setminus \{\mathcal{O}\})/\pm$), let $d = \#\mathcal{Q}$, and put

$$F(x) = 4x^3 + b_2x^2 + 2b_4x + b_6, \qquad G(x) = 6x^2 + b_2x + b_4,$$

with the $b$-invariants of $\tilde{E}$. Then

$$x(\varphi(R)) = (2d+1)x - 2\sum_{Q\in\mathcal{Q}} x_Q + F(x)\sum_{Q\in\mathcal{Q}} \frac{1}{(x-x_Q)^2} - G(x)\sum_{Q\in\mathcal{Q}} \frac{1}{x-x_Q} + \epsilon_N \frac{G(x_{N/2})}{2(x-x_{N/2})},$$

where $x = x(R)$, $x_Q = x(Q)$, and $\epsilon_N \in \{0,1\}$ indicates whether $N$ is even. This follows from Vélu's formula $x + \sum_{Q\in\mathcal{Q}}\big(G(x_Q)/(x-x_Q) + F(x_Q)/(x-x_Q)^2\big)$, plus the term for $[N/2]P$ if $N$ is even, by expanding $F(x_Q)$ and $G(x_Q)$ around $x$. The isomorphism to the next scaled model is

$$\tilde{x}^* = 2gU^2\big(2g^5\tilde{x}' - Z^2\mathcal{R}\big),$$

with $U, g, \mathcal{R}$ from Algorithm 5.2. It follows from $x^* = (x'-r)/u^2$, $\tilde{x}' = Z^2x'$ and $\tilde{x}^* = Z'^2x^*$.

The $x_Q = X_Q/D_Q$ are known from Algorithm 5.2; after bringing them to a common denominator, the three sums are accumulated along one running product of the differences $X_RD - \bar{X}_QZ_R$, at 6$\mathbf{M}$ per element of $\mathcal{Q}$.

**Proposition 5.4.** *After a shared precomputation of about $2N\mathbf{M}$ per radical step, pushing one $x$-only point through the step, including the change of model, costs at most $(3N+19)\mathbf{M}$ for odd $N$ and $(3N+28)\mathbf{M}$ for even $N$. No inversion is needed.*

*Proof.* Let $R \notin \langle P\rangle$ with $\tilde{x}(R) = X_R/Z_R$. The shared precomputation writes $x_Q = \bar{X}_Q/D$ with a common denominator $D$, using prefix and suffix products of the $D_k$. It also computes $\sum_{Q\in\mathcal{Q}} \bar{X}_Q$, $D^2$, $D^3$, the $b$-invariants of $\tilde{E}$, for even $N$ the value $G(x_{N/2})$, and the constants $gU^2$, $g^5$ and $Z^2\mathcal{R}$. Altogether this costs about $1.5N\,\mathbf{M}$, which we round up to $2N\,\mathbf{M}$ in the statement.

For each $Q \in \mathcal{Q}$ put $\Delta_Q = X_R D - \bar{X}_Q Z_R$, so that $x - x_Q = \Delta_Q/(Z_R D)$. We keep $\Pi = \prod \Delta_Q$ and $\Pi^{(2)} = \Pi^2$, together with $K_1$ and $K_2$ such that $\sum_Q \Delta_Q^{-1} = K_1/\Pi$ and $\sum_Q \Delta_Q^{-2} = K_2/\Pi^{(2)}$. Adding a new $\Delta = \Delta_Q$ amounts to

$$K_1 \leftarrow K_1\Delta + \Pi, \qquad K_2 \leftarrow K_2\Delta^2 + \Pi^{(2)}, \qquad \Pi \leftarrow \Pi\Delta, \qquad \Pi^{(2)} \leftarrow \Pi^{(2)}\Delta^2.$$

Together with $\bar{X}_Q Z_R$ and $\Delta^2$, this costs $6\mathbf{M}$ per element of $\mathcal{Q}$. The element $Q = P$ has $x_Q = 0$, so it only costs $\Delta^2$, and $X_R D$ costs one more multiplication. With $F_h, G_h$ the homogenisations of $F, G$ in $(X_R : Z_R)$, computed by Horner's rule in $8\mathbf{M}$, the formula above becomes

$$x(\varphi(R)) = \frac{(2d+1)X_R D\,\Pi^{(2)} - 2\big(\sum_Q \bar{X}_Q\big) Z_R \Pi^{(2)} + D^3 F_h K_2 - D^2 G_h K_1 \Pi}{Z_R D\,\Pi^{(2)}},$$

which takes $10\mathbf{M}$. For even $N$, the term $G(x_{N/2})/\big(2(x - x_{N/2})\big) = G(x_{N/2})Z_R/(2D\Delta_{N/2})$ is added as a fraction in $6\mathbf{M}$. Finally, the change of model $\tilde{x}^* = 2gU^2(2g^5\tilde{x}' - Z^2\mathcal{R})$ takes $3\mathbf{M}$ in projective form. In total this is $(6d+17)\mathbf{M}$, plus $6\mathbf{M}$ for even $N$, that is, $(3N+14)\mathbf{M}$ for odd $N$ and $(3N+17)\mathbf{M}$ for even $N$. The bounds in the statement leave some room for a less careful implementation, and we use them in Section 5.6. No step inverts an element. □

### 5.5 Changing the degree without inversions

Suppose we are given $(B : C : Z)$ and an $x$-only point $R = (X_R : Z_R)$ on $\tilde{E}$ of order $N' \geq 4$ coprime to $N$. Since $(E, R) \cong (E, -R)$, the Tate normal form of $(E, R)$ only depends on $x(R)$.

**Proposition 5.5.** *Let $E$ have b-invariants $b_2, b_4, b_6$ and let $R \in E$ have order at least 4. With $F$, $G$ as in Section 5.4, put $W = (12x + b_2)F(x) - G(x)^2 = 4\psi_3(x)$ with $x = x(R)$. Then the Tate normal form of $(E, R)$ is $E_{b,c}$ with*

$$b = -\frac{W^3}{64F^4}, \qquad c = 1 - \frac{GW}{4F^2}.$$

*In projective form, with $F_h, G_h, W_h$ the homogenisations in $(X_R : Z_R)$:*

$$(B : C : Z) = \big(-W_h^3 :\ 16F_h^2(4F_h^2 - G_h W_h) :\ 64F_h^4\big).$$

*This costs $16\mathbf{M}$, plus about $4\mathbf{M}$ for the b-invariants of $\tilde{E}$.*

*Proof.* In Lemma 2.2, $\psi_2(R)^2 = F(x)$ and $x(R) - x(2R) = \psi_3(x)/F(x)$, by the duplication formula. Hence $b = -(x(R) - x(2R))^3/\psi_2(R)^2 = -\psi_3^3/F^4$. Moreover $a_1 + 2\lambda = G(x)/\psi_2(R)$, so $(a_1 + 2\lambda)/u_R = G\psi_3/F^2$. Finally, expanding $(12x + b_2)F(x) - G(x)^2$ and using $4b_8 = b_2b_6 - b_4^2$ gives $W = 4\psi_3$.

For the cost, Horner's rule gives $G_h = (6X_R + b_2Z_R)X_R + b_4Z_R^2$ and $F_h = \big((4X_R + b_2Z_R)X_R + 2b_4Z_R^2\big)X_R + b_6Z_R^3$ in $8\mathbf{M}$. Then $W_h = (12X_R + b_2Z_R)F_h - G_h^2$ takes $2\mathbf{M}$. Finally $F_h^2$, $F_h^4$, $W_h^2$, $W_h^3$, $G_hW_h$ and $F_h^2(4F_h^2 - G_hW_h)$ take $6\mathbf{M}$; the factors 16 and 64 cost only additions. □

If only a point of order $N'k$ is available, it is first multiplied by $k$, using an $x$-only ladder on the short Weierstrass model obtained by $\bar{x} = 36x + 3b_2$ [Sil09, §III.1]. The $x$-only ladder of [BJ02] needs about 19 field multiplications per bit, counting squarings and multiplications by curve constants [BL]. To keep some margin, we count $21\mathbf{M}$ per bit in Section 5.6. This is more than on a Montgomery curve [Mon87], but avoids the root extraction needed to reach Montgomery form. The ladders of [Ham20], at $8\mathbf{M} + 3\mathbf{S}$ per bit, would reduce this cost further.

### 5.6 Constant-time class group actions

We now estimate the cost of a class group action $[\prod_i \mathfrak{l}_i^{e_i}]$ with $|e_i| \le b_i$, evaluated in constant time with *dummy steps*: for every degree $\ell_i$, exactly $b_i$ steps are computed, and constant-time selections decide whether a step is kept and whether a chain runs on the curve or on its twist. The cost then equals that of the maximal exponent vector, which is therefore a lower bound for any dummy-based constant-time implementation; cf. [Dec24, §5].

**Kernel points without sampling.** Fix $x$-only points $R^{\pm}$ of order $L = \prod_i \ell_i$ (over the radical degrees) on the starting curve and on its twist; for a fixed starting curve they can be precomputed. Keeping one point on the curve and one on its twist is also the approach of [OAYT19] for Vélu-based constant-time CSIDH; here, the radical chains need no further points. A chain of $\ell_i$-steps starts from the pushed image of $R^{\pm}$, multiplied by the remaining degrees, via Proposition 5.5; both points are pushed through every step, and a final multiplication by $\ell_i$ removes a surviving $\ell_i$-part after dummy chains. Intermediate multiples are pushed rather than recomputed, along a strategy [DFJP14, CDRH22] found by dynamic programming, with multiplications by $\ell$ costing $21 \log_2 \ell \, \mathbf{M}$ and pushing through the $b_i$ steps of degree $\ell_i$ costing $b_i(3\ell_i + 19)\mathbf{M}$. Such torsion images must stay private, as they are what the attacks [CD23, MMP+23, Rob23] exploit.

**Rounds.** Degrees treated with Vélu formulae are evaluated in *rounds* [MCR19]: since $\ell$ divides $p+1$ only once, a point of full order yields at most one $\ell$-isogeny per degree. Round $k = 1, 2, \ldots$ therefore samples a fresh point, multiplies it by the cofactor that removes all degrees with $b_\ell < k$, and computes one (real or dummy) $\ell$-isogeny for every degree with $b_\ell \ge k$ along an optimal strategy. The number of rounds is the largest Vélu bound, and every round pays a cofactor ladder of up to $\log_2 p$ bits, about $8\mathbf{E}$, however few degrees are still active. Radical chains need only one kernel point per degree, whatever its bound.

**Cost model.** We use the primes of [Dec24] at 512, 1024 and 2048 bits, and $p_{4096} = 2^4 \cdot 3 \cdot \prod_{3 \le \ell \le 2861} \ell \cdot f - 1$ with $f = 4194395$. We take $\mathbf{S} = \mathbf{M}$, $\mathbf{E} = 1.2 \log_2 p \, \mathbf{M}$ and $\mathbf{I} = \mathbf{E}$ (inversion by exponentiation), ignore the 2-part of $p+1$, and use the degree 3 through radical 9-steps. The bounds are chosen greedily to minimise the cost subject to $\prod_i (2b_i + 1) \ge \sqrt{p}$. For the Vélu part we use Montgomery ladders ($10\mathbf{M}$ per bit) and $c_v(\ell) = \min\big(6(\ell+2), c\sqrt{\ell} \log_2 \ell\big)\mathbf{M}$ per $\ell$-isogeny, with $c$ fitted to $2180\mathbf{M}$ for $\ell = 587$, and $c_v(\ell)/3$ for pushing a point, where the second term models the square-root Vélu formulae of [BDFLS20]; this part is scaled by 1.35 to match the constant-time count of about $10^6\mathbf{M}$ at 512 bits in [ACDRH23]. For [Dec24] we charge $\mathbf{E} + 3\mathbf{I} + (16N - 25)\mathbf{M}$ per step for $N \ge 19$, only $\mathbf{E} + \mathbf{I}$ for the formulae of [CDHV22] for $N \le 17$, and per chain a Montgomery-ladder sample plus $\mathbf{I} + 20\mathbf{M}$; other conversions are ignored, which favours [Dec24]. For this work we use Algorithm 5.2 and the strategy above, or per-chain sampling if cheaper; we charge slightly more than Propositions 5.3 and 5.5, which only disfavours our method. Degrees up to a cutoff $\ell^*$ use radical steps and the others the Vélu part. We consider the cutoff of [Dec24] (199, 373, 751 at 512, 1024, 2048 bits, extrapolated to 1487 at 4096 bits), and an optimised cutoff $\ell^* \in \{7, 13, 23, 31, 43, 61, 83, 113, 151, 199\}$ for each method separately. Table 2 shows the results.

**Discussion.** With the cutoff of [Dec24], the radical part becomes 1.8–1.9 times cheaper and the whole action 1.44–1.56 times cheaper, mostly because the three inversions per step disappear; with free inversions, the whole action would be within 2%. A fully radical action, on the other hand, is 1.3–2 times slower than Vélu only in this model. The best choice lies

| | Vélu only | | cutoff of [Dec24] | | | optimised cutoff | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $\log_2 p$ | cost | rounds | [Dec24] | this work | ratio | [Dec24] | | this work | | ratio |
| 512 | 1.06 | 47 | 1.61 | 1.12 | 1.44 | 0.97 | (13, 24) | 0.88 | (31, 15) | 1.10 |
| 1024 | 4.40 | 99 | 6.93 | 4.71 | 1.47 | 3.91 | (23, 37) | 3.59 | (61, 20) | 1.09 |
| 2048 | 18.2 | 207 | 31.4 | 20.7 | 1.52 | 15.4 | (23, 78) | 14.4 | (61, 43) | 1.07 |
| 4096 | 76.2 | 447 | 144 | 92.6 | 1.56 | 61.8 | (31, 143) | 58.2 | (83, 74) | 1.06 |

Table 2: Estimated cost in $10^6\,\mathbf{M}$ of a dummy-based constant-time action ($\mathbf{I} = \mathbf{E}$). Pairs give $\ell^*$ and the number of Vélu rounds.

in between. With optimised cutoffs, the action is 1.2–1.3 times faster than with Vélu only, and 6–10% faster than with the steps of [Dec24]; the radical part then accounts for 7–14% of the cost, and pushing is cheaper than sampling.

The reason is the round structure. In the Vélu-only action, the optimal bounds decrease steeply with $\ell$: from $b_5 = 47$ (the degree 3 is only used through radical 9-steps) to $b_\ell = 2$ at 512 bits, and from 447 to 7 at 4096 bits. The last rounds thus serve only a handful of small degrees; radical steps for these degrees remove such thin rounds, cutting their number by a factor of 3 to 6. The radical bounds are nearly equal, since at the optimum every degree has the same marginal cost per bit of key space, raising $b_\ell$ adds about $1/(b_\ell \ln 2)$ bits, and a radical step costs $\mathbf{E} + O(\ell)$. For this work they range from 17 down to 8 at 512 bits and from 43 down to 23 at 4096 bits. For [Dec24] they are exactly equal up to $\ell = 17$ and drop by about half at $\ell = 19$, where the step cost jumps from $\mathbf{E} + \mathbf{I}$ to $\mathbf{E} + 3\mathbf{I} + (16\ell - 25)\mathbf{M}$.

The cutoff is where a radical step, $\mathbf{E} + 12.5\ell\,\mathbf{M}$ plus pushing, stops being cheaper than a Vélu $\ell$-isogeny including its share of the fixed cost of the rounds it occupies. Both $\mathbf{E}$ and the round cost scale with $\log p$, but the term $12.5\ell$ does not: at $\ell^*$ it is 63% of $\mathbf{E}$ at 512 bits and only 21% at 4096 bits. Hence the cutoff moves up with $p$, whereas for [Dec24] the jump at $\ell = 19$ keeps it at 13–31. The optimum is flat: at 4096 bits, every cutoff between 61 and 113 is within about 0.3% of the best one.

These are lower bounds within a simple model, ignoring additions, conditional swaps and model conversions; nor does the model capture point transport or 2-power degrees (Section 5.3).

### 5.7 Verification

We provide two short Magma scripts [Cod26]. They are proofs of concept for correctness, not optimised or constant-time implementations. The first, `radical_main.m`, works over the toy prime $p = 4f \prod_{3 \le \ell \le 97} \ell - 1$. It evaluates the class group action on five random keys with exponents in $\{-3, \ldots, 3\}$ and on the maximal key, handling negative exponents via the quadratic twist, in two ways: with Vélu's formulae, and with Algorithm 5.2 combined with Proposition 5.5, using Vélu's formulae only for the degree 3. It checks that the two resulting curves are $\mathbb{F}_p$-isomorphic, and that the inverse key leads back to the starting curve.

The second, `radical_even.m`, tests the root choice for even $N$. It takes $p = 2^7 \cdot 15 \cdot f - 1$, the curve $y^2 = x^3 - x$ on the surface, $N \in \{4, 6, 8, 10, 12, 16, 24, 32, 64, 96, 192\}$ and random points $P$ of order $N$ that span horizontal kernels, including non-halvable ones. For both rational roots $\pm\beta_0$ it computes one radical step and compares it with Vélu's formulae. It checks that the step yields the Vélu codomain with $(r, t)$ on it (Theorem 3.1), that $\beta\theta$ is a square (Theorem 4.1), and that exactly one root keeps the next kernel horizontal, namely $\beta_0$ if and only if $P$ is halvable (Corollary 4.10).

## 6 Open questions and future work

**Dummy-free constant time.** Section 5.6 relies on dummy steps, which are vulnerable to fault attacks. Dummy-free techniques [CVCCD+19] replace a dummy step by a pair of steps in opposite directions, and CTIDH [BBC+21] batches degrees so that the chosen degree is hidden. Neither carries over to radical steps directly [Dec24]. Changing direction within a chain means switching between the curve and its twist, which for radical steps requires a fresh conversion via Proposition 5.5. Moreover, a radical step depends on its degree through the exponent of the root, so batching would need several exponentiations. Whether radical steps can be made dummy-free at moderate cost is open.

**Composite degrees.** A radical step for $N = \ell_1\ell_2$ computes an $\ell_1$- and an $\ell_2$-isogeny with one exponentiation. This pays off when $12.5(\ell_1\ell_2 - \ell_1 - \ell_2)\mathbf{M} < \mathbf{E}$: at 512 bits for instance for $3 \cdot 5$ or $5 \cdot 13$, but not for $7 \cdot 11$. The exponents of $\ell_1$ and $\ell_2$ are then tied together, which changes the shape of the key space. Since $\mathbf{E}$ grows with $\log p$ while the step cost does not, the gain grows with the size of $p$. Optimising parameter sets for this is left for future work.

**Transporting points.** Actions on oriented curves [CK20, DFFK+23] or with level structure [DFFP24] transport torsion points along the walk, which Sections 5.4 and 5.5 now allow for radical steps. Our pushing is $x$-only. This suffices when only the subgroup generated by a point matters. For a basis $(P_1, P_2)$ one can push $x(P_1)$, $x(P_2)$ and $x(P_1 - P_2)$, as is common in SIDH-style implementations, which determines the image basis up to a common sign. Concrete parameters, and a comparison with transport through Vélu's formulae, are left for future work.

**Higher dimensions.** Multiradical isogenies [CD22] generalise radical isogenies to isogenies with kernel of type $(N, \ldots, N)$ between principally polarised abelian varieties of higher dimension, with explicit formulae obtained from moduli computations in small cases. Our proof suggests a different route. The Kronecker function and its distribution relation have analogues for theta functions in several variables, and the Tate normal form would be replaced by a normal form for an abelian variety with a point of order $N$. Whether this leads to compact formulae whose size is polynomial in $N$, and to an analogue of the root choice of Section 4, is open.

## References


[ACDRH23] Gora Adj, Jesús-Javier Chi-Domínguez, and Francisco Rodríguez-Henríquez. Karatsuba-based square-root Vélu's formulas applied to two isogeny-based protocols. *Journal of Cryptographic Engineering*, 13(1):89–106, 2023. `https://doi.org/10.1007/s13389-022-00293-y`.

[BBC+21] Gustavo Banegas, Daniel J. Bernstein, Fabio Campos, Tung Chou, Tanja Lange, Michael Meyer, Benjamin Smith, and Jana Sotáková. CTIDH: Faster constant-time CSIDH. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(4):351–387, 2021. `https://doi.org/10.46586/tches.v2021.i4.351-387`.

[BDFLS20] 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 *The Open Book Series*, pages 39–55. Mathematical Sciences Publishers, 2020. https://doi.org/10.2140/obs.2020.4.39.

[BJ02] Éric Brier and Marc Joye. Weierstraß elliptic curves and side-channel attacks. In *Public Key Cryptography – PKC 2002*, volume 2274 of *Lecture Notes in Computer Science*, pages 335–345. Springer, 2002. https://doi.org/10.1007/3-540-45664-3_24.

[BKV19] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In *Advances in Cryptology – ASIACRYPT 2019, Part I*, volume 11921 of *Lecture Notes in Computer Science*, pages 227–247. Springer, 2019. https://doi.org/10.1007/978-3-030-34578-5_9.

[BL] Daniel J. Bernstein and Tanja Lange. SafeCurves: choosing safe curves for elliptic-curve cryptography. https://safecurves.cr.yp.to. Accessed 21 October 2026. See the page "Ladders". https://safecurves.cr.yp.to/ladder.html.

[CD20] Wouter Castryck and Thomas Decru. CSIDH on the surface. In *Post-Quantum Cryptography – PQCrypto 2020*, volume 12100 of *Lecture Notes in Computer Science*, pages 111–129. Springer, 2020. https://doi.org/10.1007/978-3-030-44223-1_7.

[CD22] Wouter Castryck and Thomas Decru. Multiradical isogenies. In *Arithmetic, Geometry, Cryptography, and Coding Theory 2021*, volume 779 of *Contemporary Mathematics*, pages 57–89. American Mathematical Society, 2022. https://doi.org/10.1090/conm/779/15671.

[CD23] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In *Advances in Cryptology – EUROCRYPT 2023, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 423–447. Springer, 2023. https://doi.org/10.1007/978-3-031-30589-4_15.

[CDHV22] Wouter Castryck, Thomas Decru, Marc Houben, and Frederik Vercauteren. Horizontal racewalking using radical isogenies. In *Advances in Cryptology – ASIACRYPT 2022, Part II*, volume 13792 of *Lecture Notes in Computer Science*, pages 67–96. Springer, 2022. https://doi.org/10.1007/978-3-031-22966-4_3.

[CDRH22] Jesús-Javier Chi-Domínguez and Francisco Rodríguez-Henríquez. Optimal strategies for CSIDH. *Advances in Mathematics of Communications*, 16(2):383–411, 2022. https://doi.org/10.3934/amc.2020116.

[CDV20] Wouter Castryck, Thomas Decru, and Frederik Vercauteren. Radical isogenies. In *Advances in Cryptology – ASIACRYPT 2020, Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 493–519. Springer, 2020. https://doi.org/10.1007/978-3-030-64834-3_17.

[CK20] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *Journal of Mathematical Cryptology*, 14(1):414–437, 2020. https://doi.org/10.1515/jmc-2019-0034.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In *Advances in Cryptology – ASIACRYPT 2018, Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018. https://doi.org/10.1007/978-3-030-03332-3_15.

[Cod26] Magma scripts accompanying "Getting to the right root: radical isogenies of every degree". https://github.com/TDecru/Fully_radical_isogenies, 2026.

[CVCCD+19] Daniel Cervantes-Vázquez, Mathilde Chenu, Jesús-Javier Chi-Domínguez, Luca De Feo, Francisco Rodríguez-Henríquez, and Benjamin Smith. Stronger and faster side-channel protections for CSIDH. In *Progress in Cryptology – LATINCRYPT 2019*, volume 11774 of *Lecture Notes in Computer Science*, pages 173–193. Springer, 2019. https://doi.org/10.1007/978-3-030-30530-7_9.

[Dec24] Thomas Decru. Radical $\sqrt[n]{\text{élu}}$ isogeny formulae. In *Advances in Cryptology – CRYPTO 2024, Part V*, volume 14924 of *Lecture Notes in Computer Science*, pages 107–128. Springer, 2024. Full version: Cryptology ePrint Archive, Paper 2024/878. https://doi.org/10.1007/978-3-031-68388-6_5.

[DFFK+23] Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. SCALLOP: Scaling the CSI-FiSh. In *Public-Key Cryptography – PKC 2023, Part I*, volume 13940 of *Lecture Notes in Computer Science*, pages 345–375. Springer, 2023. https://doi.org/10.1007/978-3-031-31368-4_13.

[DFFP24] Luca De Feo, Tako Boris Fouotsa, and Lorenz Panny. Isogeny problems with level structure. In *Advances in Cryptology – EUROCRYPT 2024, Part VII*, volume 14657 of *Lecture Notes in Computer Science*, pages 181–204. Springer, 2024. Full version: Cryptology ePrint Archive, Paper 2024/459. https://doi.org/10.1007/978-3-031-58754-2_7.

[DFJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014. https://doi.org/10.1515/jmc-2012-0015.

[DFMPS19] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. Verifiable delay functions from supersingular isogenies and pairings. In *Advances in Cryptology – ASIACRYPT 2019, Part I*, volume 11921 of *Lecture Notes in Computer Science*, pages 248–277. Springer, 2019. https://doi.org/10.1007/978-3-030-34578-5_10.

[DG16] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, 78(2):425–440, 2016. https://doi.org/10.1007/s10623-014-0010-1.

[Ham20] Mike Hamburg. Faster Montgomery and double-add ladders for short Weierstrass curves. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020(4):189–208, 2020. https://doi.org/10.46586/tches.v2020.i4.189-208.

[Hus04] Dale Husemöller. *Elliptic Curves*, volume 111 of *Graduate Texts in Mathematics*. Springer, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence, and Stefan Theisen. https://doi.org/10.1007/b97292.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, 1985. https://doi.org/10.1515/9781400881710.

[Koh96] David Kohel. *Endomorphism Rings of Elliptic Curves over Finite Fields*. PhD thesis, University of California, Berkeley, 1996. https://www.i2m.univ-amu.fr/perso/david.kohel/pub/thesis.pdf.

[Lan87] Serge Lang. *Elliptic Functions*, volume 112 of *Graduate Texts in Mathematics*. Springer, second edition, 1987. https://doi.org/10.1007/978-1-4612-4752-4.

[Len96] Hendrik W. Lenstra, Jr. Complex multiplication structure of elliptic curves. *Journal of Number Theory*, 56(2):227–241, 1996. https://doi.org/10.1006/jnth.1996.0015.

[MCR19] Michael Meyer, Fabio Campos, and Steffen Reith. On Lions and Elligators: An efficient constant-time implementation of CSIDH. In *Post-Quantum Cryptography – PQCrypto 2019*, volume 11505 of *Lecture Notes in Computer Science*, pages 307–325. Springer, 2019. https://doi.org/10.1007/978-3-030-25510-7_17.

[MMP+23] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on SIDH. In *Advances in Cryptology – EUROCRYPT 2023, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 448–471. Springer, 2023. https://doi.org/10.1007/978-3-031-30589-4_16.

[Mon87] Peter L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, 1987. https://doi.org/10.1090/S0025-5718-1987-0866113-7.

[OAYT19] Hiroshi Onuki, Yusuke Aikawa, Tsutomu Yamazaki, and Tsuyoshi Takagi. (short paper) a faster constant-time algorithm of CSIDH keeping two points. In *Advances in Information and Computer Security – IWSEC 2019*, volume 11689 of *Lecture Notes in Computer Science*, pages 23–33. Springer, 2019. https://doi.org/10.1007/978-3-030-26834-3_2.

[OM22] Hiroshi Onuki and Tomoki Moriya. Radical isogenies on Montgomery curves. In *Public-Key Cryptography – PKC 2022, Part I*, volume 13177 of *Lecture Notes in Computer Science*, pages 473–497. Springer, 2022. https://doi.org/10.1007/978-3-030-97121-2_17.

[Rob23] Damien Robert. Breaking SIDH in polynomial time. In *Advances in Cryptology – EUROCRYPT 2023, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 472–503. Springer, 2023. https://doi.org/10.1007/978-3-031-30589-4_17.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, 1994. https://doi.org/10.1007/978-1-4612-0851-8.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, second edition, 2009. https://doi.org/10.1007/978-0-387-09494-6.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris, Série A*, 273:238–241, 1971. https://zbmath.org/?q=an:0225.14014.

[War48] Morgan Ward. Memoir on elliptic divisibility sequences. *American Journal of Mathematics*, 70(1):31–74, 1948. https://doi.org/10.2307/2371930.

[Zag91] Don Zagier. Periods of modular forms and Jacobi theta functions. *Inventiones Mathematicae*, 104(1):449–465, 1991. https://doi.org/10.1007/BF01245085.

# A Comparison with [Dec24]

In this appendix we relate Theorem 3.1 to the formulae conjectured in [Dec24], and we point out two corrections to their statement.

**Notation of [Dec24].** Let $P = (0,0) \in E_{b,c}$ have exact order $N$, and put $x_k = x([k]P)$. Following [Dec24], set $\varpi_0 = 2$ and $\varpi_i = \prod_{k=1}^{i} x_k$ for $i \geq 1$, with the conventions

$$x_1 := 1, \qquad x_{N-1} := 1, \qquad x_N := b^2, \qquad x_{k+N} := x_k.$$

These conventions replace the actual values $x(P) = x(-P) = 0$. For $1 \leq i \leq N-2$ one simply has $\varpi_i = \prod_{k=2}^{i} x_k$, while $\varpi_{N-1} = \varpi_{N-2}$ and $\varpi_N = b^2\varpi_{N-2}$. In [Dec24] an $N$th root $\alpha$ of a representative $\tau_N$ of the Tate pairing $t_N(P,-P)$ is fixed, and the following was conjectured for odd $N$. We state it with two corrections, explained below.

**Conjecture A.1** ([Dec24, Conjecture 1], corrected)**.** *Let $N \geq 5$ be odd and let $\alpha^N = \tau_N := -\varpi_N^{-1}$. Define*

$$u = 1 + 3b\sum_{i=1}^{N-2} \varpi_i\alpha^i - \sum_{\substack{i=1 \\ i\neq N-3}}^{N-2} \varpi_i\varpi_{i+1}\varpi_{i+2}\alpha^{3i} + \varpi_{N-1}\varpi_N\varpi_{N+1}\alpha^{3(N-1)},$$

$$s = b\sum_{i=1}^{N-2} \varpi_i\alpha^i - b^3\tau_N^2 \sum_{i=2}^{N-1} \varpi_{2i}\varpi_{2i+1}\varpi_{N-i-1}\varpi_{N-i}\alpha^{2i}.$$

*Then $(u,s)$ determines an isomorphism $\iota\colon E_{b',c'} \to E'$ from a Tate normal form onto $E'$ (via [Dec24, Lemma 2]), and $\iota(0,0)$ is $P$-distinguished.*

The statement in [Dec24] differs from Conjecture A.1 in two places. First, the representative in [Dec24, Proposition 2] is printed as $\tau_N = -(b^2\varpi_N)^{-1}$. With the conventions above, the correct representative is $\tau_N = -\varpi_N^{-1}$; the printed value is in general not even in the class of $t_N(P,-P)$ modulo $N$th powers. Second, in the cubic sum of $u$, the term with $i = N-1$ enters with a plus sign.

**Dictionary.** By Lemma 3.4, $\varpi_i = (-1)^i W_{i+1}/(bW_i)$ and $h_i = \varpi_i \alpha^i$ for $1 \le i \le N-2$, and $\rho_N = (-1)^{N+1}/\varpi_N$. Hence $\alpha^N = (-1)^N \rho_N = -\varpi_N^{-1} = \tau_N$ for every $N$, odd or even, so our $\beta = -\alpha$ is an $N$th root of the corrected representative. The sums in [Dec24] are taken over $1 \le i \le N-1$, with exceptional indices and the conventions above. Our sums (7) run over all $i \in \{1, \dots, N-1\}$, i.e. over $\mathbb{Z}/N\mathbb{Z} \setminus \{0\}$, without exceptions. All boundary behaviour is absorbed by $W_N = 0$ and by the values $W_{N+1}, W_{N+2}$, which are computed from (D2). This also explains the corrected representative: by Lemma 3.3, it is the unique one for which all summands are $N$-periodic. Finally, instead of $(u, s)$ followed by [Dec24, Lemma 2], Theorem 3.1 gives closed formulae for $(u, r, s)$, from which $b'$, $c'$ and $t$ follow directly.

Substituting $h_i = \varpi_i \alpha^i$ into Proposition 3.2 gives

$$\mathcal{S}_1 = b \sum_{i=1}^{N-2} \varpi_i \alpha^i, \qquad \mathcal{S}_2 = b \sum_{i=1}^{N-3} \varpi_i \varpi_{i+1} \alpha^{2i} - b\, \varpi_{N-2}\, \alpha^{N-2},$$

$$\mathcal{S}_{1,1} = b^2 \sum_{i=1}^{N-2} \varpi_i^2 \alpha^{2i}, \qquad \mathcal{S}_3 = \sum_{i=1}^{N-4} \varpi_i \varpi_{i+1} \varpi_{i+2} \alpha^{3i} - \varpi_{N-2}^2 \alpha^{2N-6} - \varpi_{N-2}\, \alpha^{N-3},$$

$$\mathcal{S}_{1,2} = b^2 \sum_{i=1}^{N-3} \varpi_i^2 \varpi_{i+1} \alpha^{3i}.$$

**Corollary A.2.** *For odd $N \ge 5$, the element $u$ of Theorem 3.1 coincides with the element $u$ of Conjecture A.1.*

*Proof.* The terms $3b \sum \varpi_i \alpha^i = 3\mathcal{S}_1$ agree, and so do the cubic terms with $i \le N-4$. The excluded index $i = N-3$ in Conjecture A.1 corresponds to the vanishing summand of $\mathcal{S}_3$. Using $\varpi_{N-1} = \varpi_{N-2}$, $\varpi_N = \varpi_{N+1} = b^2 \varpi_{N-2}$ and $\alpha^N = -(b^2 \varpi_{N-2})^{-1}$, the two remaining boundary terms of Conjecture A.1 are

$$-\varpi_{N-2}\varpi_{N-1}\varpi_N \alpha^{3N-6} = \varpi_{N-2}^2 \alpha^{2N-6} \qquad \text{and} \qquad \varpi_{N-1}\varpi_N\varpi_{N+1}\alpha^{3N-3} = \varpi_{N-2}\alpha^{N-3}.$$

These are exactly the boundary terms of $-\mathcal{S}_3$ above. □

The expression for $s$ in Conjecture A.1 is a rearrangement of $2\mathcal{S}_1 - \mathcal{S}_2$ that uses the index doubling $i \mapsto 2i$, which is a permutation of $\mathbb{Z}/N\mathbb{Z}$ only for odd $N$. We do not prove that the two expressions agree; Theorem 3.1 provides $s$ for all $N$ in any case. With $s = 2\mathcal{S}_1 - \mathcal{S}_2$, the conclusion of [Dec24, Proposition 3] holds unconditionally (Section 5.2). The index doubling also explains why the shape of $s$ in [Dec24] could not be extended to even $N$ (cf. [Dec24, Remark 4]).

**Cost.** In [Dec24, §4], one radical step costs $\mathbf{E} + 3\mathbf{I} + (16N - 25)\mathbf{M}$: the multiples of $P$ in $(X : Z)$-coordinates, the products $\varpi_i$ (one inversion), the $N$th root, the quantities $u$ and $s$ (one inversion), the Vélu coefficients of $E'$, and finally $(b', c')$ (one inversion). Algorithm 5.2 replaces this by $\mathbf{E} + (12.5N + O(\log N))\mathbf{M}$.