JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

David GRANT

A higher-order generalization of Jacobi's derivative formula and its algebraic geometric analogue

Tome 33, n° 2 (2021), p. 361-386.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2021__33_2_361_0>

Journal de Théorie des Nombres
de Bordeaux **33** (2021), 361–386

A higher-order generalization of Jacobi's derivative formula and its algebraic geometric analogue

par David GRANT

Résumé. Nous généralisons la formule de la dérivée de Jacobi en écrivant, pour un m impair, un déterminant de taille m composé de dérivées d'ordre supérieur évaluées en 0 des fonctions thêta d'une variable avec vecteurs caractéristiques à coordonnées dans $\frac{1}{2m}\mathbb{Z}$ comme une constante explicite multipliée par une puissance de la fonction η de Dedekind. Nous déduisons ce résultat de sa version algébro-géométrique, qui est valable si la caractéristique ne divise pas $6m$.

Abstract. We generalize Jacobi's derivative formula for odd m by writing an $m \times m$ determinant of higher order derivatives at 0 of theta functions in 1 variable with characteristic vectors with entries in $\frac{1}{2m}\mathbb{Z}$ as an explicit constant times a power of Dedekind's η-function. We do so by deriving it from an algebraic geometric version that holds in characteristic not dividing $6m$.

Introduction

In the vast pantheon of theta function identities, a central position is held by Jacobi's derivative formula. Recall that for $\tau \in \mathfrak{h} = \{x+iy \,|\, y > 0\}$, and $a, b \in \mathbb{R}$, we define the theta function in one variable $z \in \mathbb{C}$ with characteristic vector $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ by

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\tau) = \sum_{n\in\mathbb{Z}} e^{\pi i(n+a)^2\tau + 2\pi i(n+a)(z+b)}. \tag{1}$$

A characteristic vector $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ with $a, b \in \frac{1}{2}\mathbb{Z}$ is called a theta characteristic, which is called odd or even depending on whether $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\tau)$ is an odd or even function of z. Modulo 1 there is a unique odd theta characteristic $\delta := \left[\begin{smallmatrix} 1/2 \\ 1/2 \end{smallmatrix}\right]$, and three even ones, $\epsilon_1 := \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$, $\epsilon_2 := \left[\begin{smallmatrix} 1/2 \\ 0 \end{smallmatrix}\right]$, $\epsilon_3 := \left[\begin{smallmatrix} 0 \\ 1/2 \end{smallmatrix}\right]$.

Manuscrit reçu le 6 février 2020, révisé le 2 février 2021, accepté le 18 mai 2021.
2010 *Mathematics Subject Classification.* 14K25, 14H42.
Mots-clefs. Theta functions, elliptic curves.

Jacobi's formula states that

$$\frac{\mathrm{d}}{\mathrm{d}z}(\theta[\delta](z,\tau))|_{z=0} = -\pi \prod_{i=1}^{3} \theta[\epsilon_i](0,\tau) = -2\pi\eta(\tau)^3, \tag{2}$$

where for $q = e^{2\pi i\tau}$,

$$\eta(\tau) = q^{1/24} \prod_{n\geq 1} (1-q^n)$$

is Dedekind's η-function ([22, p. 64 and 72]).

Jacobi's formula has been generalized in a number of directions: see the references in [12], [13], and [16] for information on what is known about generalizations to theta functions in several variables. One main goal of the paper is to prove for any odd m a generalization of (2) for higher derivatives in z of $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\tau)$ at $z=0$ and $a, b \in \frac{1}{2m}\mathbb{Z}$.

We note that first derivatives in z of $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\tau)$ at $z=0$ for $a, b \in \mathbb{Q}$ were studied in [5], [6], and [10], where their vanishing was related to the existence of "singular torsion" on the elliptic curve whose complex points are parameterized by $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$, and a genus 1 analogue of the Manin–Mumford conjecture. For higher-order derivatives we have:

Theorem I. *Let m be odd. Then*

$$\det_{\substack{0\leq j<m \\ 0\leq k\leq m-2, k=m}} \left[\left(\frac{\mathrm{d}}{\mathrm{d}z}\right)^k \left(\theta \begin{bmatrix} \frac{1}{2}+\frac{j}{m} \\ \frac{1}{2} \end{bmatrix} (z, m\tau) \right) \Big|_{z=0} \right]$$
$$= i^{(3m+1)/2} (2\pi/m)^{(m^2-m+2)/2} m! \left(\prod_{\ell=1}^{m-2} \ell! \right) \eta(\tau)^{m^2+2}.$$

Note that when $m=1$ we recover (2). The reason that $k = m-1$ is excluded as an index is explained in the Remark at the end of the Introduction.

Theorem I takes a more attractive form if for any characteristic vector $\mathfrak{c} = \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ and integer j, we set $f_{\mathfrak{c},j}(z,\tau) = \theta\left[\begin{smallmatrix} a+j/m \\ b \end{smallmatrix}\right](mz, m\tau)$ and let $f_{\mathfrak{c},j}^{[k]}(0,\tau)$ denote its k^{th}-Hasse derivative with respect to z at 0. (Recall this means that $f_{\mathfrak{c},j}^{[k]}(0,\tau)$ is the coefficient of z^k in the Taylor expansion of $f_{\mathfrak{c},j}(z,\tau)$ at $z=0$.) Then recalling that $\delta = \left[\begin{smallmatrix} 1/2 \\ 1/2 \end{smallmatrix}\right]$, Theorem I is equivalent to:

$$\det_{\substack{0\leq j<m \\ 0\leq k\leq m-2, k=m}} \left[f_{\delta,j}^{[k]}(0,\tau) \right] = i^{(3m+1)/2} (2\pi)^{(m^2-m+2)/2} \eta(\tau)^{m^2+2}. \tag{I.1}$$

We ask in advance for the reader's forbearance: we believe the computation of the constant in Theorem I is new, but inasmuch as the objects have been studied for the last two centuries, we cannot provide a guarantee of this fact. We note that using the transformation formula for theta functions

([8, p. 81]), Lemma 13 in the next section of this paper, and ([22, p. 124, Prop. 1.3]), one can show that the left hand side of (I.1) is a level-one modular form with character that doesn't vanish on $\mathfrak{h}$, so is a constant times a power of $\eta(\tau)$ (this also follows by combining the results on p. 270 and in Remark 1.1 on p. 272 of [8], obtained with rather more work via the heat equation and a study of Weierstrass points on modular curves). This means one could calculate the constant via q-expansions, but it would be unenlightening to do so.

More important perhaps then is the algebraic geometry that underlies the statement of Theorem I, and indeed, we will prove it by deriving it from results (Theorems II and III of the next section) that hold for any elliptic curve E defined over a field K of any characteristic not dividing $6m$.

To describe this, let E_τ be the complex elliptic curve

$$y^2 = x^3 + A(\tau)x + B(\tau)$$

whose points (x, y) are parameterized by $(\wp(z,\tau), \frac{1}{2}\wp'(z,\tau))$ for $z \in \mathbb{C}$, where $\wp(z,\tau)$ is the Weierstrass $\wp$-function for the lattice $L_\tau = \mathbb{Z} + \mathbb{Z}\tau$. Let O denote its origin, $t(z) = -x(z)/y(z) = z + \dots$ be a local parameter at O, and let $L(mO)$ denote the m-dimensional vector space of functions on E_τ with poles bounded by mO. Then the starting point of Mumford's theory of algebraic theta functions ([22, Chap. I §3, Chap. II, §1] [23, §§1–5]) is the fact that the functions on E_τ defined by

$$r_j(z,\tau) = \frac{f_{\delta,j}(z,\tau)}{\theta[\delta](z,\tau)^m},$$

$0 \le j \le m-1$, are eigenfunctions of Heisenberg operators on $L(mO)$ with different eigenvalues, so they form a canonical basis for $L(mO)$. The eigenfunctions are only determined up to constant, and if we let

$$g_j(z,\tau) = \left(\frac{e^{2\pi ij/m}}{2\pi i}\right)^{(m-1)/2} r_j(z,\tau),$$

then we will prove in Proposition 22 of Section 2 that if we also set

$$T(\tau) := \det_{\substack{0\le j<m \\ 0\le k\le m-2, k=m}} (z^m g_j)^{[k]}(0,\tau), \tag{3}$$

then (I.1) is equivalent to

$$T(\tau) = 1/(2\pi\eta^2(\tau))^{m^2-1}. \tag{I.2}$$

In other words,

$$T(\tau) = \Delta(\tau)^{-(m^2-1)/12}, \tag{I.3}$$

(up to a choice of cube-root of the righthand side when 3 divides m), where $\Delta(\tau) = -16(4A(\tau)^3 + 27B(\tau)^2) = (2\pi)^{12}\eta(\tau)^{24}$ is Dedekind's discriminant

modular form. Once we note using Lemma 21(c) of Section 2 that

$$T(\tau) = \det_{\substack{0\le j<m \\ 0\le k\le m-2, k=m}} (t^m g_j)^{[k]_t}(0,\tau),$$

where $(t^m g_j)^{[k]_t}(z,\tau)$ denotes the k^{th}-Hasse derivative of $t^m g_j(z,\tau)$ with respect to t, (I.3) has an algebraic meaning for elliptic curves over any field.

Indeed, let K be any field of characteristic not dividing $6m$, and E be any elliptic curve over K given by a Weierstrass model, $y^2 = x^3 + Ax + B$ over K, with $t = -x/y$ a local parameter at the origin O. In the next section we will develop what we need of the theory of Heisenberg operators for E and K. Then in Theorem II we will use this to calculate the determinant of the $0, \dots, m-2$, and m^{th}-Hasse derivatives with respect to t of t^m times a basis for $L(mO)$ of normalized eigenfunctions for the Heisenberg operators, and then in Theorem III express this determinant as in (I.3), in terms of the discriminant of the Weierstrass model.

Then in Section 2, we will show that when $K = \mathbb{C}$ and $E = E_\tau$, this normalized basis of eigenfunctions for $L(mO)$ is precisely the $g_j(z,\tau)$, $0 \le j \le m-1$, and derive Theorem I from Theorems II and III.

We remark that some analogous but more complicated results should hold for m even and in the case that K has characteristic 2 or 3. Also it would be nice to know what the appropriate generalization of Theorem I is for higher derivatives of theta functions in several variables.

Remark 1. If for any theta characteristic $\mathfrak{c}$, we let $W_{\mathfrak{c},m}(z,\tau)$ denote the Wronskian with respect to z of $f_{\mathfrak{c},0}(z,\tau), \dots, f_{\mathfrak{c},m-1}(z,\tau)$, then Lemma 13 of the next section will show that $W_{\delta,m}(0,\tau)$ vanishes, and we will see in Lemma 21 of Section 2 that therefore we can rewrite Theorem I as

$$\text{(I.4)}\quad \frac{\mathrm{d}}{\mathrm{d}z}(W_{\delta,m}(z))|_{z=0} = i^{(3m+1)/2}\left(\frac{2\pi}{m}\right)^{(m^2-m+2)/2} m!\left(\prod_{\ell=1}^{m-2}\ell!\right)\eta(\tau)^{m^2+2}.$$

We note that the lefthand side of (I.4) is a "lacunary Wronskian" in the language of Anderson [1]. See also [20].

On the other hand, recalling that $\{\epsilon_1, \epsilon_2, \epsilon_3\}$ is a set representing the even theta characteristics modulo 1, similar reasoning to that in the discussion above shows that

$$\prod_{i=1}^{3} W_{\epsilon_i,m}(0,\tau)$$

is a non-vanishing modular form of level one and weight $3m^2/2$ with character on $\mathfrak{h}$, and so is a constant times $\eta(\tau)^{3m^2}$, which gives a supplemental generalization of (2). Presumedly the constant can be determined along the lines of this paper but we have not tried to do so.

1. Algebraic geometric version of Theorem I

Let m be an odd integer, K a field of characteristic not dividing $6m$, and E/K an elliptic curve over K. Let E be given by a Weierstrass model,

$$y^2 = x^3 + Ax + B. \tag{4}$$

Let $\omega = \mathrm{d}x/2y$ be a choice of invariant differential for E, and $t = -x/y$ be a parameter at the origin O of E. We let D be the derivation on the function field $K(E)$ given by $D = \mathrm{d}/\omega$, i.e. the unique derivation determined by $Dx = 2y$. Since ω is translation-invariant, so is D.

Let $L(mO)$ denote the m-dimensional $\overline{K}$-vector space of functions on E whose poles are bounded by mO (along with the zero function), where $\overline{K}$ is an algebraic closure of K. Let $E[m]$ denote the m-torsion in $E(\overline{K})$. For any $R \in E(\overline{K})$ and $\ell \in \mathbb{Z}$, we let $[\ell]R$ denote the image of R under the multiplication-by-ℓ endomorphism of E. For $f \in \overline{K}(E)^*$ we let (f) denote its divisor. For any $R \in E(\overline{K})$ we let T_R denote the translation-by-R map on E, and T_R^* its pullback to $\overline{K}(E)$.

For a point $R \in E(\overline{K})$, let v_R denote the valuation of the local ring $\mathcal{O}_R$ of E at R. Let $\mathrm{Div}(E)$ denote the group of divisors of E over $\overline{K}$. If f is a non-zero function and $\mathcal{D} = \sum_{R\in E} n_R R$ is a divisor on E whose support is disjoint from the support of (f), we let $f(\mathcal{D}) = \prod_{R\in E} f(R)^{n_R}$.

Identifying E with its jacobian, if $\mathcal{D}$ is a divisor of degree 0 linearly equivalent to $S - O$ for some $S \in E(\overline{K})$, we will say that $\mathcal{D}$ *sums* to S.

For every $u, v \in E[m]$, let $e_m(u, v)$ denote their Weil pairing. For lack of a suitable reference, we give a lemma expressing the Weil pairing in terms of local contributions.

Lemma 2. *For non-zero functions $\phi, \psi \in \overline{K}(E)$ whose divisors are in $m\,\mathrm{Div}(E)$, we define for every $R \in E(\overline{K})$,*

$$(\phi, \psi)_{m,R} = (-1)^{v_R(\phi)v_R(\psi)/m}(\phi^{v_R(\psi)/m}/\psi^{v_R(\phi)/m})(R).$$

Let $u, v \in E[m]$. Then if functions ρ_u and ρ_v have divisors mD_u and mD_v such that D_u sums to u and D_v sums to v, we have

$$e_m(u, v) = \prod_{R\in E} (\rho_u, \rho_v)_{m,R}.$$

Proof. If D_u and D_v have distinct support, Example 3.16 in [27] gives that $e_m(u, v) = \rho_u(D_v)/\rho_v(D_u)$. It is clear from the definitions that we have $\rho_u(D_v)/\rho_v(D_u) = \prod_{R\in E}(\rho_u, \rho_v)_{m,R}$, which gives the Lemma in this case.

More generally, recall for any non-zero functions ϕ, ψ and point $R \in E(\overline{K})$, we have the local symbol

$$(\phi, \psi)_R = (-1)^{v_R(\phi)v_R(\psi)}(\phi^{v_R(\psi)}/\psi^{v_R(\phi)})(R),$$

which is bilinear, and satisfies the product formula $\prod_{R\in E}(\phi, \psi)_R = 1$ ([26, p. 34–35]). For ϕ, ψ which have divisors in $m\,\mathrm{Div}(E)$, $(\phi, \psi)_{m,R}$ is also

bilinear, and for any function ρ, $(\phi,\rho)_R = (\phi,\rho^m)_{m,R}$. So if $(\rho_u) = mD_u$ and $(\rho_v) = mD_v$, and D_u and D_v do not have disjoint support, we can find linearly equivalent divisors D'_u and D'_v with disjoint support, so there are functions ψ_u, ψ_v with divisors $D'_u - D_u$ and $D'_v - D_v$, such that $\phi_u := \rho_u\psi_u^m$ and $\phi_v := \rho_v\psi_v^m$, have divisors mD'_u and mD'_v. Then

$$\begin{aligned} e_m(u,v) &= \prod_{R\in E} (\phi_u,\phi_v)_{m,R} \\ &= \prod_{R\in E} (\rho_u,\rho_v)_{m,R}(\rho_u,\psi_v)_R(\psi_u,\rho_v)_R(\psi_u,\psi_v)_R^m = \prod_{R\in E} (\rho_u,\rho_v)_{m,R}, \end{aligned}$$

which gives the Lemma. □

Following Mumford ([23, p. 43], [21, p. 289]) we now define:

Definition 3. The group $\mathcal{H} = \mathcal{H}_m$ of Heisenberg linear operators on $L(mO)$ consists of pairs h_u of the form (u, f_u) where $u \in E[m]$ and $(f_u) = mu - mO$, with the group composition of $h_u = (u, f_u)$ and $h_v = (v, f_v)$ given by $h_u \circ h_v = (u+v, f_u T_{-u}^* f_v)$.

It is straightforward to verify that $\mathcal{H}$ is indeed a group with $(O,1)$ as its identity, and that $\mathcal{H}$ acts on $L(mO)$ by setting for any $g \in L(mO)$, and $h_u = (u, f_u) \in \mathcal{H}$,

$$h_u(g) = T_{-u}^*(g) f_u. \tag{5}$$

Definition 4.

(i) For any $u \in E[m]$ there is a distinguished choice F_u for f_u, given as follows: Using that m is odd, let d_u be any function with divisor $\sum_{i=0}^{m-1}[i]u - mO$. Then let $F_u = d_u/T_{-u}^* d_u$, which is independent of the choice of d_u.

(ii) We let H_u denote (u, F_u).

Lemma 5. *Let $u \in E[m]$.*

(a) $[-1]^* F_u = F_{-u}$.

(b) $H_u^{-1} = H_{-u}$.

Proof. Any choice of d_u is an even function, so $[-1]^* d_u = d_u$ and we can take $d_{-u} = d_u$. Hence $[-1]^* F_u = [-1]^* d_u / [-1]^* T_{-u}^* d_u = d_u / T_u^* d_u = F_{-u}$, which gives (a).

Likewise,

$$H_u \circ H_{-u} = (O, F_u T_{-u}^* F_{-u}) = (O, F_u (T_{-u}^* d_u / d_u)) = (O,1),$$

which gives (b). □

We now recall Mumford's definition of algebraic theta functions.

Definition 6. For any $s \in L(mO)$, and $u \in E[m]$, we define the algebraic theta function

$$\Theta_s(u) = t^m H_u^{-1}(s)|_{t=0} = t^m H_{-u}(s)|_{t=0}.$$

When $s = 1$, we will let $\Theta(u)$ denote $\Theta_1(u) = t^m F_{-u}|_{t=0}$.

Remark 7. Let $\mathcal{L}(mO)$ be the invertible sheaf attached to the divisor mO. Mumford defines elements of the Heisenberg group attached to $\mathcal{L}(mO)$ as pairs (u, ψ) where $u \in E[m]$ and $\psi : \mathcal{L}(mO) \to T_u^*(\mathcal{L}(mO))$ is an isomorphism of invertible sheaves, which as in [14, II, Prop. 6.13], is given by multiplication by a function whose divisor is $mO - T_u^*(mO) = mO - m([-1]u)$. Since we are studying functions in $L(mO)$, we found it more natural to replace his elements (u, ψ) by the pair $(u, T_{-u}^*\psi)$ in the definition of $\mathcal{H}$, since $T_{-u}^*\psi \in L(mO)$. This gives us different formulas for the group law of $\mathcal{H}$ and its action on $L(mO)$, but the group and the action are the same that Mumford uses.

In Mumford's definition of algebraic theta function (see the versions in [23, p. 76] and [21, p. 300]) we are simplifying by considering the theta function directly as a function of torsion points of E, obviating the need to pick a "theta structure", and are using $s \to t^m s|_{t=0}$ as the required choice of linear functional on $L(mO)$. Also it is an exercise to show that since m is odd, our map $u \to H(u)$ agrees with the map τ defined in [23, p. 58] that is needed in his definition of algebraic theta function.

Let $\{P, Q\}$ be an ordered basis for $E[m]$ as a $\mathbb{Z}/m\mathbb{Z}$-module, and let $\zeta = e_m(P, Q)$, which is a primitive $m^{th}-$root of unity.

Definition 8. Let $S = \sum_{i=0}^{m-1} \zeta^{i^2}$ be the quadratic Gauss sum.

(a) Set ν_0 to be $(-1)^{(m-1)/2}/S$ times any chosen m^{th}-root of

$$\prod_{k=1}^{(m-1)/2} \Theta([k]P)^3.$$

(b) Let $g_P = \nu_0 \prod_{k=1}^{(m-1)/2}(x - x([k]P))$.

(c) For any $0 \le j < m$, set $g_j = H_{-[j]Q}(g_P)$ (so in particular, $g_0 = g_P$).

The definition of ν_0 is perhaps overly perspicacious: it is chosen to simplify the later statement of Theorem II. Note that g_P is a specific choice for d_P.

Definition 9. Identifying the completed local ring at the origin $\widehat{\mathcal{O}}_O$ with the power series ring $\overline{K}[\![t]\!]$, for $0 \le j < m$ and $n \ge 0$, define $\theta_{j,n} \in \overline{K}$ as the coefficients in the expansions

$$t^m g_j = \sum_{n \ge 0} \vartheta_{j,n} t^n.$$

Remark 10. From Definition 6 we have

$$\Theta_{g_P}([j]Q) = t^m H_{-[j]Q}(g_P)\,|_{t=0} = t^m g_j|_{t=0} = \vartheta_{j,0}.$$

Therefore it makes sense to think of the $\vartheta_{j,n}$ as analogous to Hasse derivatives in t of an algebraic theta function (see also [4, §2.2]).

The goal of this section is to compute

$$T(P,Q) = \det_{\substack{0\le j<m\\ 0\le k\le m-2, k=m}} [\vartheta_{j,k}], \tag{6}$$

which we relate in the next section to $T(\tau)$ when $K=\mathbb{C}$ and $E=E_\tau$ for a particular choice of P and Q. We will need a sequence of lemmas.

Most of the following Lemma comes directly from the definitions and is standard (see e.g., [22, p. 2], [23, p. 44, Prop. 3.6(c)]). We provide proofs to keep the paper self-contained.

Lemma 11. *Let $u,v\in E[m]$, and let $e_m(u,v)$ denote their Weil pairing.*

(a) $\Theta(-u) = -\Theta(u)$.
(b) $H_u\circ H_v = c(u,v)H_{u+v}$, *where* $c(u,v)=1$ *if* $u=O$ *or if* $u=-v$, *and* $c(u,v) = F_v(-u)\Theta(u)/\Theta(u+v)$ *otherwise.*
(c) $H_u\circ H_v = e_m(u,v)H_v\circ H_u$.
(d) $c(u,v) = e_m(u,v)^{(m+1)/2}$, *i.e.,* $c(u,v)^2 = e_m(u,v)$.
(e) $H_{[k]P}(g_P) = g_P$ *for all* $k\ge 1$.
(f) *For each* $0\le j<m$, g_j *is an eigenfunction of* $H_{[k]P}$ *with eigenvalue* ζ^{-jk}.
(g) *The set* g_j, $0\le j<m$, *forms a basis for* $L(mO)$.
(h) *For every* $1\le k<m$,

$$\frac{1}{\Theta([k]P)} = 2y([k]P)\prod_{\substack{1\le k'\le (m-1)/2\\ k'\ne k,m-k}} (x([k]P)-x([k']P)) = \frac{1}{\nu_0}D(g_P)([k]P).$$

Proof. (a). Using Lemma 5(a), $\Theta(-u) = t^m F_u|_{t=0} = [-1]^*(t^m F_u|_{t=0}) = (-t)^m F_{-u}|_{t=0} = -t^m F_{-u}|_{t=0} = -\Theta(u)$.

(b). This is trivial if $u=O$ or follows from Lemma 5(b) if $u=-v$, so assume not. From (5), for any $f\in L(mO)$,

$$\begin{aligned} H_u\circ H_v(f) = H_u\left(T^*_{-v}(f)F_v\right) &= T^*_{-u-v}(f)T^*_{-u}(F_v)\,F_u \\ &= \left(T^*_{-u}(F_v)\,F_u/F_{u+v}\right)H_{u+v}(f). \end{aligned}$$

Then comparing divisors shows $T^*_{-u}(F_v)F_u/F_{u+v}$ is a constant, which we find by multiplying numerator and denominator by t^m and evaluating at O to be $F_v(-u)\Theta(-u)/\Theta(-u-v)$, and the result follows from (a).

(c). By (b), we need to show that $c(u,v)/c(v,u) = e_m(u,v)$. This is trivial if $u = O$, $v = O$, or $v = -u$, so assume not. In all other cases, by (a), and Lemma 5 (a), we get from (b) and then Definition 6 that

$$c(u,v)/c(v,u) = \frac{F_v(-u)\Theta(u)}{F_u(-v)\Theta(v)} = \frac{-F_v(-u)\Theta(u)}{F_{-u}(v)\Theta(-v)} = \prod_{R\in E} (F_v, F_{-u})_{m,R} = e_m(v,-u),$$

by Lemma 2, which since the Weil pairing is bilinear and antisymmetric is $e_m(u,v)$.

(d). We first claim $c(u,v) = c(-u,-v)$. This is trivial if $u = O$ or $v = O$ or $v = -u$, so assume not. Using Lemma 5 (a), we have by (a) and (b), that

$$c(-u,-v) = \frac{F_{-v}(u)\Theta(-u)}{\Theta(-u-v)} = \frac{F_v(-u)\Theta(u)}{\Theta(u+v)} = c(u,v). \tag{7}$$

Also, taking inverses of $c(v,u)H_{u+v} = H_v \circ H_u$ gives by Lemma 5 (b) that $c(v,u)^{-1}H_{-u-v} = H_{-u} \circ H_{-v}$, so

$$c(-u,-v) = c(v,u)^{-1} = e_m(u,v)c(u,v)^{-1},$$

by (c). Combining this with (7) gives $c(u,v)^2 = e_m(u,v)$.

(e). We will show this by induction. First of all, by the definition of F_P, $H_P(g_P) = T^*_{-P}(g_P)F_P = g_P$. Now assume $H_{[k-1]P}(g_P) = g_P$ for some $k \geq 2$. Using (b) we get $H_{[k]P}(g_P) = c([k-1]P, P)^{-1}H_{[k-1]P} \circ H_P(g_P) = g_P$ since $e_m([k-1]P, P) = 1$ implies $c([k-1]P, P) = 1$ by (d).

(f). Using (c) again and (e),

$$H_{[k]P}(g_j) = H_{[k]P}\left(H_{-[j]Q}(g_P)\right) = e_m([k]P, -[j]Q)H_{-[j]Q}\left(H_{[k]P}(g_P)\right) = \zeta^{-jk}H_{-[j]Q}(g_P) = \zeta^{-jk}g_j.$$

(g). The Riemann–Roch Theorem gives that the dimension of $L(mO)$ over $\overline{K}$ is m, and the g_j, $0 \leq j < m$, are m eigenfunctions for H_P with different eigenvalues.

(h). For all $k \geq 1$, (e) and Lemma 5 (a) gives $F_{-[k]P} = g_P/T^*_{[k]P}g_P$. So since $g_P = \nu_0 \prod_{k'=1}^{(m-1)/2}(x - x([k']P))$, we have for $1 \leq k \leq m-1$,

$$1/\Theta([k]P) = t^{-m}\, F^{-1}_{[-k]P}\Big|_{t=0} = \left.\frac{(T^*_{[k]P}g_P)/t}{t^{m-1}g_P}\right|_{t=0} = \left.\frac{T^*_{[k]P}(x - x([k]P))}{t}\right|_{t=0} \prod_{\substack{1\leq k'\leq (m-1)/2,\\ k'\neq k, m-k}} (x([k]P) - x([k']P)).$$

Now since D is translation-invariant and $\mathrm{d}t/\omega$ is 1 at the origin, we have by L'Hôpital's rule,

$$\left.\frac{T^*_{[k]P}(x - x([k]P))}{t}\right|_{t=0} = \left.\frac{D\big(T^*_{[k]P}(x - x([k]P))\big)}{Dt}\right|_{t=0}$$
$$= T^*_{[k]P}\, D(x - x([k]P))|_{t=0} = 2y([k]P).$$

This also shows $1/\Theta([k]P) = D(g_P)([k]P)/\nu_0$. □

Definition 12. For any function $f \in L(mO)$ we write the expansion of $t^m f$ in terms of t over $\overline{K}$ as $\sum_{n\geq 0} a_{f,n}t^n$.

(a) We define a linear transformation $\phi : L(mO) \to \overline{K}^m$ by $\phi(f) = (a_{f,0}, \ldots, a_{f,(m-2)}, a_{f,m})$.

(b) If $B = \{b_1, \ldots, b_m\}$ is any ordered basis for $L(mO)$, we let $\det(\phi(B))$ denote the determinant of the matrix whose rows are $\phi(b_1), \ldots, \phi(b_m)$.

By Definition 9, $\phi(g_j) = (\vartheta_{j,0}, \ldots, \vartheta_{j,m-2}, \vartheta_{j.m})$, for $0 \leq j \leq m-1$. Note that in (6) we have already defined $T(P,Q) = \det(\phi(G))$, where G is the ordered basis $\{g_0, \ldots, g_{m-1}\}$.

Lemma 13. *Let $B = \{b_1, \ldots, b_m\}$ be an ordered basis for $L(mO)$, thought of as a column vector in $\overline{K}(E)^m$.*

(a) *The map ϕ is an isomorphism. Hence $\det(\varphi(B))$ is non-vanishing.*

(b) *If M is an invertible $m \times m$ matrix with entries in $\overline{K}$, so $B' = MB$ is another ordered basis for $L(mO)$, then $\det(\phi(B')) = \det(M)\det(\phi(B))$.*

(c) *If for $f \in L(mO)$ we set $\rho(f) = (a_{f,0}, \ldots, a_{f,m-2}, a_{f,m-1})$, then we have $\det(\rho(B)) = 0$, where $\rho(B)$ is the matrix whose rows are $\rho(b_1), \ldots, \rho(b_m)$.*

Proof. (a). If $a_{f,i} = 0$ for all $0 \leq i \leq m-2$, then f has a pole of at worst order 1 at the origin, so is constant. Then $a_{f,m} = 0$ means that this constant is 0. Hence ϕ is injective, and the Riemann–Roch Theorem gives that the dimension of $L(mO)$ over $\overline{K}$ is m, so ϕ is an isomorphism.

(b). This is clear.

(c). It is enough to note that $1 \in L(mO)$ and $\rho(1) = 0$. □

We have one ordered basis for $L(mO)$, namely G. We will compute $T(P,Q)$ by writing down another ordered basis, and comparing the two.

Definition 14.

(a) Set $w_0 = 1$, and for $2 \leq j \leq m$ set $w_j = x^{j/2}$ if j is even, and $w_j = x^{(j-3)/2}(-y)$ if j is odd. Let $W = \{w_0, w_2, \ldots, w_m\}$, which is an ordered basis for $L(mO)$.

(b) Let L denote the change of basis matrix with entries in $\overline{K}$ expressing G in terms of W, so $G = LW$.
(c) For $0 \le k < m$, applying operations entry-by-entry to elements of a vector, let $G_k = H_{[k]P}(G)$, and $W_k = H_{[k]P}(W)$.
(d) Let Γ and Ω be the matrices which respectively have k-th column G_k and W_k, so $\Gamma = L\Omega$.

We note that since $x = \frac{1}{t^2} + \ldots$, $y = \frac{-1}{t^3} + \ldots$, by design the Laurent expansion of w_j at the origin in t has lead term $1/t^j$. Hence the first non-zero entry of $\phi(w_j)$ is a 1 in the $(m+1-j)^{th}$ entry for $2 \le j \le m$, and the first non-zero entry of $\phi(w_0)$ is a 1 in the m^{th} entry. Therefore $\det(\phi(W)) = (-1)^{(m-1)/2}$ since reversing the columns of $\phi(W)$ yields an upper-triangular matrix with 1s on the diagonal.

Hence by Lemma 13 (b),

$$T(P,Q) = \det(\phi(G)) = (-1)^{(m-1)/2} \det(L). \tag{8}$$

So we concentrate now on computing $\det(L)$, which by Definition 14 (d) satisfies

$$\det \Gamma = \det L \det \Omega. \tag{9}$$

Proposition 15. *Let* $Z = \det_{0\le j,k<m}\left[\zeta^{jk}\right]$, ν_0 *be as in Definition 8, and* Γ *and* Ω *be as in Definition 14.*

(a) $t^{m^2-1} \det \Gamma|_{t=0}$
$$= (-1)^{(m-1)/2} Z \nu_0^m \prod_{j=1}^{m-1} \Theta([j]Q) \prod_{j,k=1}^{(m-1)/2} (x([j]Q) - x([k]P))^2.$$
(b) $t^{m^2-1} \det \Omega|_{t=0} = (-1)^{(m^2-1)/8} m \prod_{k=1}^{(m-1)/2} \Theta([k]P)$.

Proof. (a). Note that $\Gamma_{jk} = H_{[k]P}(g_j) = \zeta^{-jk} g_j$ by Lemma 11 (f), so $\det \Gamma = (-1)^{(m-1)/2} \left(\prod_{j=0}^{m-1} g_j\right) Z$, since reversing the 2nd through the m^{th} rows of $[\zeta^{-jk}]_{0\le j,k<m}$ yields $[\zeta^{jk}]_{0\le j,k<m}$. Hence $\det \Gamma$ has a pole of order m^2-1 at the origin, and letting $\mathfrak{m}$ denote the maximal ideal of $\widehat{\mathcal{O}}_O$, we have

$$t^{m^2-1} \det \Gamma \equiv (-1)^{(m-1)/2} Z \prod_{j=0}^{m-1} \nu_j \mod \mathfrak{m},$$

where for $1 \le j \le m-1$, we set $\nu_j = g_j t^m|_{t=0}$, using from Definition 8 that $\nu_0 = g_0 t^{m-1}|_{t=0}$. So for $1 \le j \le m-1$, using (5) and Definitions 6 and 8 we have

$$\begin{aligned} \nu_j = H_{-[j]Q}(g_P) t^m|_{t=0} &= T^*_{[j]Q}(g_P)\, F_{-[j]Q}\, t^m|_{t=0} \\ &= \nu_0 \Theta([j]Q) \prod_{k=1}^{(m-1)/2} (x([j]Q) - x([k]P)). \end{aligned}$$

Hence

$$t^{m^2-1}\det\Gamma \equiv (-1)^{(m-1)/2} Z\nu_0^m \prod_{j=1}^{m-1}\Theta([j]Q)\prod_{j,k=1}^{(m-1)/2}(x([j]Q)-x([k]P))^2 \mod \mathfrak{m},$$

since x is an even function.

(b). Since $\Omega_{jk}=H_{[k]P}(w_j)=\left(T^*_{[-k]P}w_j\right)F_{[k]P}$, we have that

$$\det\Omega=\det_{\substack{j=0,2\le j\le m\\ 0\le k<m}}\left[T^*_{[-k]P}w_j\right]\prod_{k=0}^{m-1}F_{[k]P},$$

so since $F_{[0]P}=1$ and $F_{[k]P}$ has a pole of order m at O for $1\le k<m$, we see from (a) and (9) that $\det[T^*_{[-k]P}w_j]$ has a pole of order $m-1$ at the origin. Hence if we let C_j denote the cofactor of w_j in $[T^*_{[-k]P}w_j]$, we have that C_m vanishes at O. Therefore since $\det[T^*_{[-k]P}w_j]=w_0C_0+\sum_{j=2}^m w_jC_j$, we have from $w_j=\frac{1}{t^j}+\ldots$, that

$$t^{m^2-1}\det\Omega|_{t=0}=\left(\prod_{k=1}^{m-1}\Theta(-[k]P)\right)(D(C_m)+C_{m-1})|_{t=0}\,.$$

Applying a derivation to a determinant yields a sum of the determinants of the derivation applied to each column. Since for $j=0$ and $2\le j\le m-2$, $D(w_j)$ is in the span of $\{w_0,\ldots,w_{j-1},w_{j+1}\}$, all summands in $D(C_m)$ vanish except for the one with the derivation applied to the last column. Then since $Dw_{m-1}=Dx^{(m-1)/2}=\frac{m-1}{2}x^{(m-3)/2}(2y)=-(m-1)w_m$, and D is translation invariant, accounting for the signs attached to the two cofactors we have that

$$D(C_m)=(m-1)C_{m-1}.$$

Hence by Lemma 11 (a),

$$t^{m^2-1}\det\Omega|_{t=0}=\left(\prod_{k=1}^{m-1}\Theta([k]P)\right)mC_{m-1}|_{t=0}\,. \tag{10}$$

Now

$$C_{m-1}|_{t=0}=(-1)^{m-1+1}\det_{\substack{j=0,2,3,\ldots,m-2,m\\ 1\le k\le m-1}}[w_j([-k]P)]\,. \tag{11}$$

Applying $\sum_{i=1}^{(m-5)/2} i=(m-5)(m-3)/8$ transpositions to the rows of the matrix in the righthand side of (11) gives the matrix

$$\Omega'=[w_j([-k]P)]_{\substack{j=0,2,4,\ldots,m-3,3,5,\ldots,m\\ 1\le k\le m-1}},$$

so if $\epsilon = (-1)^{(m-3)(m-5)/8}$, since m is odd, (11) can be rewritten as

$$C_{m-1}|_{t=0} = -\epsilon \det \Omega'. \tag{12}$$

Subtracting the jth-column of Ω' from the $(m-j)$th-column for $j = 1, \ldots, (m-1)/2$, yields a block lower-diagonal matrix, whose upper-lefthand block is the Vandermonde matrix

$$V = \left[x([k]P)^j\right]_{\substack{0\le j\le (m-3)/2\\ k=1,\ldots,(m-1)/2}},$$

and whose lower-righthand-block is

$$V' = \left[2y([k]P)x([k]P)^j\right]_{\substack{0\le j\le (m-3)/2\\ k=(m+1)/2,\ldots,m}},$$

since $-y([-k]P) = y([k]P)$. Note that $\det V'$ is $\prod_{k=(m+1)/2}^{m} 2y([k]P)$ times the determinant of $\left[x([k]P)^j\right]_{0\le j\le (m-3)/2; k=(m+1)/2,\ldots,m}$, which is the determinant of the matrix V with its columns reversed. Hence

$$\begin{aligned}\det\left(\Omega'\right) &= \det V \det V' \\ &= (-1)^{(m-1)/2} \prod_{k=1}^{(m-1)/2} 2y([k]P) \prod_{1\le k\ne k'\le (m-1)/2} \left(x([k]P) - x\left([k']P\right)\right) \\ &= (-1)^{(m-1)/2} \prod_{k=1}^{(m-1)/2} \Theta([k]P)^{-1},\end{aligned} \tag{13}$$

by Lemma 11 (h), using that y is odd. Putting together (10), (12), and (13) gives

$$t^{m^2-1} \det \Omega|_{t=0} = \left(\prod_{k=1}^{m-1} \Theta([k]P)\right) m(-\epsilon)(-1)^{(m-1)/2} \prod_{k=1}^{(m-1)/2} \Theta([k]P)^{-1},$$

and the result follows from Lemma 5 (a) since $-\epsilon = (-1)^{(m^2-1)/8}$. □

Corollary 16. *With notation as in Proposition 15,*

$$T(P,Q) = (-1)^{(m^2-1)/8} \frac{Z}{m} \nu_0^m \prod_{j,k=1}^{(m-1)/2} (x([j]Q) - x([k]P))^2 \frac{\prod_{j=1}^{m-1} \Theta([j]Q)}{\prod_{k=1}^{(m-1)/2} \Theta([k]P)}.$$

Proof. By (9), $\det L = \det \Gamma / \det \Omega$, which by Proposition 15 is

$$(-1)^{\frac{m^2-1}{8}+\frac{m-1}{2}} \frac{Z}{m} \nu_0^m \prod_{1\le j,k\le (m-1)/2} (x([j]Q) - x([k]P))^2 \frac{\prod_{j=1}^{m-1} \Theta([j]Q)}{\prod_{k=1}^{(m-1)/2} \Theta([k]P)}.$$

The result follows from (8). □

Theorem II. *Recall* $S = \sum_{i=0}^{m-1} \zeta^{i^2}$ *is the quadratic Gauss sum and that we set* ν_0 *to be* $(-1)^{(m-1)/2}/S$ *times any* m^{th}*-root of* $\prod_{k=1}^{(m-1)/2} \Theta([k]P)^3$*. Then*

$$T(P,Q) = \lambda(P,Q)/m,$$

where $\lambda(P,Q) =$

$$(-1)^{(m-1)/2} \prod_{1\le j,k\le (m-1)/2} (x([j]Q) - x([k]P))^2 \prod_{j=1}^{m-1} \Theta([j]Q) \prod_{k=1}^{m-1} \Theta([k]P).$$

Proof. It follows from work of Schur ([24], see also [27, Chap. 6, App. §2]), that $(-1)^{(m^2-1)/8+(m-1)/2} Z = S^m$ (to show this holds in any K, it suffices to show it holds in $\mathbb{Z}[\zeta]$, and for that it suffices to show it holds in any complex embedding of $\mathbb{Z}[\zeta]$, which is what Schur does). Hence with this choice of ν_0, Corollary 16 can be rewritten as $T(P,Q) = \lambda(P,Q)/m$, where $\lambda(P,Q) =$

$$\prod_{1\le j,k\le (m-1)/2} (x([j]Q) - x([k]P))^2 \prod_{j=1}^{m-1} \Theta([j]Q) \prod_{k=1}^{(m-1)/2} \Theta([k]P)^2.$$

The result now follows from Lemma 5(a). □

Theorem II gives the formula for $T(P,Q)$ we will use in the next section to derive (I.2). We will finish the section by relating $\lambda(P,Q)$ to the discriminant of the curve as we do in (I.3), though the best we can do when $3|m$ is to determine $\lambda(P,Q)$ up to a third root of unity.

Lemma 17. *Let* m *be odd and* K *be of characteristic not dividing* $6m$*. Let* n *be any non-zero integer not divisible by the characteristic of* K*, and let* ψ_n *be the* n*-division polynomial with divisor* $\sum_{u\in E[n]} u - n^2 O$ *normalized by* $t^{(n^2-1)}\psi_n|_{t=0} = n$ *([19, App. 1]), and let* $E[n]^*$ *denote* $E[n] - O$*.*

(a) *Suppose* $n+m$*, and* $n-m$ *are not divisible by the characteristic of* K*. Then* $[n]^*x - [m]^*x = \frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2}$*.*

(b) *For independent generic points* α *and* β *of* E*,*

$$\frac{x([n]\alpha) - x([n]\beta)}{(x(\alpha) - x(\beta))^{n^2}} = \frac{\psi_n(\beta+\alpha)\psi_n(\beta-\alpha)}{\psi_n(\alpha)^2\psi_n(\beta)^2}.$$

(c) *For a generic point* α *of* E*,*

$$(-1)^{(n^2-1)} \frac{2y([n]\alpha)}{(2y(\alpha))^{n^2}} = \frac{\psi_n([2]\alpha)}{\psi_n(\alpha)^4}.$$

(d) *Let* $\Delta = -16\,(4A^3 + 27B^2)$ *be the discriminant of the Weierstrass model* (4) *for* E*. Let* $\phi_n = ([n]^*x)\cdot\psi_n^2$*. Then*

$$\prod_{u\in E[n]^*} \phi_n(u) = n^{-2n^2} \Delta^{n^2(n^2-1)/6}.$$

(e) *We have*

$$m^3 \prod_{u\in E[m]^*} \psi_2(u) = 2^{m^2-1} \prod_{e\in E[2]^*} \psi_m(e) = (-1)^{(m-1)/2}\Delta^{(m^2-1)/4}.$$

(f) *If n is not a multiple of 3, then*

$$n^8 \prod_{u\in E[n]^*} \psi_3(u) = 3^{n^2-1} \prod_{e\in E[3]^*} \psi_n(e) = (-1)^{(n^2-1)/3}\Delta^{2(n^2-1)/3}.$$

Proof. (a). This is a special case of Proposition 1 of [19, App. I].

(b). Both sides are functions on $E \times E$, with divisor

$$[n]^*(\mathcal{D}+\mathcal{D}'-2(E\times O+O\times E)) - n^2(\mathcal{D}+\mathcal{D}'-2(E\times O+O\times E)),$$

where $\mathcal{D}$ and $\mathcal{D}'$ are respectively the diagonal and antidiagonal on $E\times E$. So the formula holds up to a multiplicative constant. Now let $t_\alpha = t(\alpha)$. Then the lead term in the Laurent expansion of both sides in the neighborhood of $\alpha = O$ is $\frac{1}{n^2}t_\alpha^{2n^2-2}$, so the constant is 1.

(c). By the chain rule for division polynomials, Proposition 2 of [19, App. I], $[n]^*\psi_2 = \psi_{2n}/\psi_n^4 = ([2]^*\psi_n)\psi_2^{n^2}/\psi_n^4$. The result follows since $\psi_2 = -2y$.

(d). We will only need this for $n = 2$ and $n = 3$ for which it can be verified by direct computation. More generally, since ϕ_n is a monic polynomial in x of degree n^2, for n odd this follows from standard properties of resultants using any of a number of people's proof that the resultant in x of ϕ_n and ψ_n^2 is $\Delta^{n^2(n^2-1)/6}$ (see [15], [7, Lem. 1.7.11(b)], [2, Lem. 2]). For n even, this same result is stated without proof in [3, (1.3)], and proven in [9].

(e). The first equality comes from the product formula for local symbols as in the proof of Lemma 2. The second equality comes from induction on m. Clearly when $m = -1$ and $m = 1$ the value of $\epsilon_m := \prod_{e\in E[2]^*}\psi_m(e)$ is respectively -1 and 1. Now take $m \geq 3$ to be odd. From (a) we have $\psi_{m+2}\psi_{m-2}/\psi_m^2 = \psi_2^2([2]^*x - [m]^*x)$, which is ϕ_2 minus a function that vanishes at 2-torsion points. From (d) we have $\prod_{e\in E[2]^*}\phi_2(e) = 2^{-8}\Delta^2$, and hence $\epsilon_{m+2} = 2^{-8}\Delta^2\epsilon_m^2/\epsilon_{m-2}$, and the result follows inductively for $m > 0$. That suffices since $\psi_{-m} = -\psi_m$.

(f). Again, the first equality comes from the product formula for local symbols as in the proof Lemma 2. The second inequality comes by induction on n. Now let $\epsilon_n := \prod_{e\in E[3]^*}\psi_n(e)$. We have trivially that $\epsilon_{-1} = \epsilon_1 = 1$, and from (e), that $\epsilon_{-2} = \epsilon_2 = (-1/27)\Delta^2$. As in (e), from (a) we have $\psi_{n+3}\psi_{n-3}/\psi_n^2$ is ϕ_3 minus a function that vanishes at 3-torsion points. So from (d), we have for n not a multiple of 3, that $\epsilon_{n+3} = 3^{-18}\Delta^{12}\epsilon_n^2/\epsilon_{n-3}$. The result follows by a two-step induction for $n > 0$, which as in (e) suffices for the result. □

Theorem III. *Let $T(P,Q)$ be as in* (6) *and Δ be the discriminant of the Weierstrass model* (4)*. Then for all odd m we have*

$$T(P,Q)^3 = \Delta^{-(m^2-1)/4}.$$

If in addition m is not a multiple of 3, then

$$T(P,Q) = \Delta^{-(m^2-1)/12}.$$

Proof. Theorem II gives $T(P,Q) = \lambda(P,Q)/m$, and we will get the result by applying Lemma 17 to each factor in $\lambda(P,Q)$ Let $\ell > 0$ be not divisible by the characteristic of K and prime to m. Lemma 11 (h) with Q playing the role of P gives

$$\prod_{j=1}^{m-1} \Theta([j]Q) = \prod_{1\le j'\ne j\le (m-1)/2} \frac{1}{(x([j]Q)-x([j']Q))^2} \prod_{j=1}^{m-1} \frac{1}{2y([j]Q)}, \tag{14}$$

which for ℓ prime to m is also $\prod_{j=1}^{m-1}\Theta([j\ell]Q)$. Hence $\prod_{j=1}^{m-1}\Theta([j]Q)^{\ell^2-1} = \prod_{j=1}^{m-1}\Theta([j]Q)^{\ell^2}/\Theta([j\ell]Q)$, which by (14) and Lemma 17 (b) and (c) taking $n=\ell$ is

$$\prod_{j=1}^{m-1}(-1)^{\ell^2-1}\frac{\psi_\ell([2j]Q)}{\psi_\ell([j]Q)^4} \prod_{1\le j'\ne j\le (m-1)/2} \frac{\psi_\ell([j'+j]Q)^2\psi_\ell([j'-j]Q)^2}{\psi_\ell([j']Q)^4\psi_\ell([j]Q)^4} = \prod_{j=1}^{m-1}\psi_\ell([j]Q)^{-m},$$

since ψ_ℓ^2 is an even function, and $(-1)^{(\ell^2-1)(m-1)} = 1$. By the same reasoning, $\prod_{k=1}^{m-1}\Theta([k]P)^{\ell^2-1} = \prod_{k=1}^{m-1}\psi_\ell([k]P)^{-m}$.

Finally, again since ℓ is prime to m, $\prod_{1\le j,k\le (m-1)/2}(x([j]Q)-x([k]P))^2$ to the ℓ^2-1 power is by Lemma 17 (b),

$$\prod_{j,k=1}^{(m-1)/2} \frac{\psi_\ell([k]P)^4\psi_\ell([j]Q)^4}{\psi_\ell([k]P+[j]Q)^2\psi_\ell([k]P-[j]Q)^2} = \frac{(\prod_{j=1}^{m-1}\psi_\ell([j]P)\psi_\ell([j]Q))^m}{\prod_{u\in E[m]^*}\psi_\ell(u)},$$

since ψ_ℓ is even or odd.

Hence

$$\lambda(P,Q)^{\ell^2-1} = (-1)^{\frac{m-1}{2}(\ell^2-1)} \prod_{u\in E[m]^*}\psi_\ell(u)^{-1}. \tag{15}$$

When $\ell = 2$, by Lemma 17(e), (15) gives us

$$\lambda(P,Q)^3 = m^3\Delta^{-(m^2-1)/4},$$

which when m is a multiple of 3 is the best we can do, and determines $\lambda(P,Q)$ up to a third-root of unity. Hence by Theorem II,

$$T(P,Q)^3 = \Delta^{-(m^2-1)/4}.$$

When m is not a multiple of 3, we can also take $\ell = 3$ in (15), and now by Lemma 17(f) with $n = m$,

$$\lambda(P,Q)^8 = m^8 \Delta^{-2(m^2-1)/3},$$

since when m is odd, $(-1)^{(m^2-1)/3} = 1$. Combining this with the above gives

$$\lambda(P,Q) = m\Delta^{-(m^2-1)/12},\ T(P,Q) = \Delta^{-(m^2-1)/12},$$

which we note is independent of the choice of P and Q. □

Remark 18. The obstruction to calculating $T(P,Q)$ when $3|m$ is that it depends on the choice of P and Q and not just upon their Weil pairing (or, from another point of view, $\Delta^{1/3}$ is a modular form of level one with a non-trivial character). When $m = 3$, Theorem III gives that $\lambda(P,Q)\Delta/3$ is a cube root of Δ. We note that it is well-known that a cube root of Δ can be expressed in terms of coordinates of $E[3]$: see e.g. [25, p. 305].

2. Theorem I from Theorems II and III

Our discussion of the complex theta function will be aided by gathering some of the basic properties that follow directly from its definition (1). For any $\tau \in \mathfrak{h}$, let $L_\tau = \mathbb{Z} + \mathbb{Z}\tau$.

Lemma 19. *Let $z \in \mathbb{C}$ and $\tau \in \mathfrak{h}$. For any $a, b, c, d \in \mathbb{R}$ and $p, q \in \mathbb{Z}$ we have:*

(a) $\theta\left[\begin{smallmatrix} a+p \\ b+q \end{smallmatrix}\right](z,\tau) = (-1)^{2\pi i a q}\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\tau)$.

(b) $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z + c\tau,\tau) = e^{-\pi i c^2\tau - 2\pi i c(z+b)}\theta\left[\begin{smallmatrix} a+c \\ b \end{smallmatrix}\right](z,\tau)$.

(c) $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z + d,\tau) = \theta\left[\begin{smallmatrix} a \\ b+d \end{smallmatrix}\right](z,\tau)$.

(d) *For any $\lambda \in L_\tau$, define the factor of automorphy $\rho_{\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right],z,\tau}(\lambda)$ by*

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z+\lambda,\tau) = \rho_{\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right],z,\tau}(\lambda)\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\tau).$$

Then $\rho_{\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right],z,\tau}(p\tau + q) = e^{-\pi i p^2\tau - 2\pi i p(z+b) + 2\pi i a q}$.

(e) $\theta\left[\begin{smallmatrix} -a \\ -b \end{smallmatrix}\right](-z,\tau) = \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\tau)$.

Proof. Proofs of (a), (b), and (c) can be found in [22, p. 5–11]. Then (d) follows from (a)–(c). Note (e) follows by replacing a, b, z, and n by their negatives in (1). □

Let $E_\tau : y^2 = x^3 + A(\tau)x + B(\tau)$ be the complex elliptic curve whose complex points can be parameterized by $x = \wp(z,\tau)$, $y = \frac{1}{2}\wp'(z,\tau)$, for $z \in \mathbb{C}$, where $\wp(z,\tau)$ is the Weierstrass $\wp$-function attached to L_τ, and $\wp'(z,\tau)$ denotes its derivative with respect to z. Note that since $t(z) = -2\wp(z,\tau)/\wp'(z,\tau)$, we have

$$t(z) = z + \dots \tag{16}$$

for the beginning of its Taylor expansion at $z = 0$.

The first goal of this section is to specialize the quantities discussed in the last section for general E over general fields to the case of E_τ over $\mathbb{C}$.

As in Section 1, let m denote an odd integer. Now define characteristic vectors $\mathrm{top}_j = \left[\begin{smallmatrix} 1/2+j/m \\ 1/2 \end{smallmatrix}\right]$, and $\mathrm{bot}_j = \left[\begin{smallmatrix} 1/2 \\ 1/2+j/m \end{smallmatrix}\right]$, for any $j \in \mathbb{Z}$, and set $\delta = \mathrm{top}_0 = \mathrm{bot}_0$. One sees readily from Lemma 19 (d) that $\rho_{\mathrm{top}_j,mz,m\tau}(\lambda) = \rho_{\mathrm{bot}_j,z,\tau/m}(\lambda) = \rho_{\delta,z,\tau}(\lambda)^m$, for all $\lambda \in L_\tau$. Therefore since $\theta[\delta](z,\tau)$ is analytic in z and its zeroes consist of just a simple zero at points of L_τ ([22, p. 1 and 11]), for $0 \le j < m$ the functions $r_j(z,\tau) = \theta[\mathrm{top}_j](mz, m\tau)/\theta[\delta](z,\tau)^m$ and $s_j(z,\tau) = \theta[\mathrm{bot}_j](z,\tau/m)/\theta[\delta](z,\tau)^m$ are functions on E_τ and are in $L(mO)$. Note that our definition here of $r_j(z,\tau)$ agrees with the one given in the Introduction.

From now on let us fix $P = \frac{1}{m} \bmod L_\tau$, $Q = \frac{\tau}{m} \bmod L_\tau$, and $\zeta_m = e^{2\pi i/m}$. Note unlike the last section, we have the luxury of fixing choices for P and Q with representatives in $\mathbb{C}$ and not just $E(\mathbb{C})$ (which is why Mumford's full theory of algebraic theta functions is an adelic one.) It is standard that $e_m(P,Q) = \zeta_m$ ([27, p. 352]).

Let us now take the F_u, $\Theta([k]P)$, $\Theta([j]Q)$, ν_0, g_j, and $T(P,Q)$ from Definitions 4, 6, 8 and equation (6) defined in the last section for a general elliptic curve over a general field, and specify these for the elliptic curve E_τ over $\mathbb{C}$ and our choices of P and Q, and denote these by writing them as a function of $\tau \in \mathfrak{h}$, or where appropriate, $z \in \mathbb{C}$ and $\tau \in \mathfrak{h}$.

Proposition 20. *Given our choices for P and Q on E_τ, we have:*

(a) *For $1 \le k \le m-1$,* $F_{[k]P}(z,\tau) = (-1)^k \dfrac{\theta\left[\begin{smallmatrix} 1/2 \\ 1/2-k/m \end{smallmatrix}\right](z,\tau)^m}{\theta\left[\begin{smallmatrix} 1/2 \\ 1/2 \end{smallmatrix}\right](z,\tau)^m}$.

(b) *For $1 \le k \le m-1$,* $\Theta([k]P)(\tau) = (-1)^k \dfrac{\theta\left[\begin{smallmatrix} 1/2 \\ 1/2+k/m \end{smallmatrix}\right](0,\tau)^m}{\theta\left[\begin{smallmatrix} 1/2 \\ 1/2 \end{smallmatrix}\right]'(0,\tau)^m}$.

(c) *For $1 \le j \le m-1$,* $F_{[j]Q}(z,\tau) = \dfrac{\theta\left[\begin{smallmatrix} 1/2-j/m \\ 1/2 \end{smallmatrix}\right](z,\tau)^m}{\theta\left[\begin{smallmatrix} 1/2 \\ 1/2 \end{smallmatrix}\right](z,\tau)^m}$.

(d) *For $1 \le j \le m-1$,* $\Theta([j]Q)(\tau) = \dfrac{\theta\left[\begin{smallmatrix} 1/2+j/m \\ 1/2 \end{smallmatrix}\right](0,\tau)^m}{\theta\left[\begin{smallmatrix} 1/2 \\ 1/2 \end{smallmatrix}\right]'(0,\tau)^m}$.

(e) *We can take $\nu_0(\tau)$ to be* $\dfrac{i^{(1-m)/2} m \eta(m\tau)^3}{(2\pi)^{3(m-1)/2} \eta(\tau)^{3m}}$.

(f) *With* $\nu_0(\tau)$ *as in* (e), $g_P(z,\tau) = (2\pi i)^{-(m-1)/2}\dfrac{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](mz,m\tau)}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)^m}$.

(g) *With* $\nu_0(\tau)$ *as in* (e), *for* $0 \le j \le m-1$,

$$g_j(z,\tau) = (2\pi i\zeta_m^{-j})^{-(m-1)/2}\frac{\theta\left[\begin{smallmatrix}1/2+j/m\\1/2\end{smallmatrix}\right](mz,m\tau)}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)^m} = (2\pi i\zeta_m^{-j})^{-(m-1)/2} r_j(z,\tau),$$

which agrees with the definition given in the Introduction.

Proof. (a). It is easy to check that the divisor of $r_0(z,\tau)$ is $\sum_{k=0}^{m-1}[k]P - mO$, so in the notation of Definition 4, we can take $d_P(z,\tau) = r_0(z,\tau)$. It follows from Lemma 11(e) that

$$F_{[k]P}(z,\tau) = \frac{d_P(z,\tau)}{T^*_{-[k]P}d_P(z,\tau)} = \frac{\left(\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z-k/m,\tau)/\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)\right)^m}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](mz-k,m\tau)/\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](mz,m\tau)} = (-1)^k\frac{\theta\left[\begin{smallmatrix}1/2\\1/2-k/m\end{smallmatrix}\right](z,\tau)^m}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)^m},$$

by Lemma 19 (a) and (c).

(b). From (a), using (16) and Definition 6 we have

$$\Theta([k]P)(\tau) = z^m\, F_{-[k]P}(z,\tau)\Big|_{z=0} = (-1)^k\frac{\theta\left[\begin{smallmatrix}1/2\\1/2+k/m\end{smallmatrix}\right](0,\tau)^m}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau)^m}.$$

(c). Similar to (a), one can check that we can take $d_Q(z,\tau) = s_0(z,\tau)$. Hence applying Lemma 11 (e) with P replaced by Q, we have

$$F_{[j]Q}(z,\tau) = \frac{d_Q(z,\tau)}{T^*_{-[j]Q}d_Q(z,\tau)} = \frac{\left(\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z-j\tau/m,\tau)/\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)\right)^m}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z-j\tau/m,\tau/m)/\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau/m)} = \frac{\theta\left[\begin{smallmatrix}1/2-j/m\\1/2\end{smallmatrix}\right](z,\tau)^m}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)^m},$$

by Lemma 19 (a) and (b).

(d). From (c), as in (b),

$$\Theta([j]Q)(\tau) = z^m \, F_{-[j]Q}(z,\tau)\Big|_{z=0} = \frac{\theta\left[\begin{smallmatrix}1/2+j/m\\1/2\end{smallmatrix}\right](0,\tau)^m}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau)^m}.$$

(e). Recall that $S = \sum_{i=0}^{m-1} \zeta_m^{i^2}$, the quadratic Gauss sum, and Definition 8 defines $\nu_0(\tau)$ to be $(-1)^{(m-1)/2}/S$ times any m^{th} root of $\prod_{k=1}^{(m-1)/2} \Theta([k]P)^3$. From (b) and (2), one choice of m-th-root is

$$(-1)^{(m^2-1)/8}\kappa(\tau)^3/(-2\pi\eta(\tau)^3)^{3(m-1)/2},$$

where

$$\kappa(\tau) = \prod_{k=1}^{(m-1)/2} \theta\left[\begin{smallmatrix}\frac{1}{2}\\ \frac{1}{2}+\frac{k}{m}\end{smallmatrix}\right](0,\tau).$$

Now from Lemma 19 one gets that:

$$\theta\left[\begin{smallmatrix}\frac{1}{2}\\ \frac{1}{2}+\frac{m-k}{m}\end{smallmatrix}\right](0,\tau) = \theta\left[\begin{smallmatrix}\frac{1}{2}\\ -\frac{1}{2}-\frac{k}{m}\end{smallmatrix}\right](0,\tau) = \theta\left[\begin{smallmatrix}-\frac{1}{2}\\ \frac{1}{2}+\frac{k}{m}\end{smallmatrix}\right](0,\tau) = \theta\left[\begin{smallmatrix}\frac{1}{2}\\ \frac{1}{2}+\frac{k}{m}\end{smallmatrix}\right](0,\tau).$$

Hence we also have

$$\kappa(\tau) = \prod_{k=1}^{(m-1)/2} \theta\left[\begin{smallmatrix}1/2\\ 1/2+2k/m\end{smallmatrix}\right](0,\tau).$$

Now taking the coefficient of u in both sides of formula (7) of [28, p. 84] and accounting for the fact that Weber's definition of $\theta_{11}(z)$ is the negative of our $\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)$, $\kappa(\tau)^3$ is seen to be[1]

$$(-1)^{(m-1)/2}\sqrt{m}^3\eta(\tau)^{3(m-3)/2}\eta(m\tau)^3.$$

Hence $\nu_0(\tau) = (-1)^{(m^2-1)/8+(m-1)/2}\eta(m\tau)^3\sqrt{m}^3/S(2\pi)^{3(m-1)/2}\eta(\tau)^{3m}$. The proof of (e) now follows the standard fact (see e.g., [17, Chap. 6, Appendix]) that $S = i^{(1-m)/2}(-1)^{(m^2-1)/8}\sqrt{m}$.

(f). By Definition 8 we have $g_P(z,\tau) = \nu_0(\tau)\prod_{k=1}^{(m-1)/2}(\wp(z,\tau)-\wp([k]P,\tau))$, which has a Laurent expansion at the origin whose lead term is $\nu_0(\tau)/z^{m-1}$. Hence comparing divisors as in (a), and expansions at the origin, we also have that $g_P(z,\tau)$ is

$$\nu_0(\tau)\frac{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](mz,m\tau)/\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)^m}{m\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,m\tau)/\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau)^m}.$$

[1]One can also derive this expression for $\kappa(\tau)$ from the product expansion for theta functions: one plugs in $z=0$, $a=1/2$, and $b=1/2+k/m$ into (2.53) of [8, p. 141] and takes the product over $1 \le k \le (m-1)/2$ to verify the formula.

So by (e) and (2),

$$g_P(z,\tau) = (2\pi i)^{-(m-1)/2}\frac{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](mz,m\tau)}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)^m}.$$

(g). From (f) and Definition 8, we can now calculate

$$\begin{aligned} g_j(z,\tau) &= H_{-[j]Q}\left(g_P(z,\tau)\right) = T^*_{[j]Q}\left(g_P\right)F_{-[j]Q}(z,\tau)\\ &= (2\pi i)^{-(m-1)/2}\frac{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](mz+j\tau,m\tau)}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z+j\tau/m,\tau)^m}\frac{\theta[\begin{smallmatrix}1/2+j/m\\1/2\end{smallmatrix}](z,\tau)^m}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)^m}\\ &= (2\pi i)^{-(m-1)/2}\zeta_m^{j(m-1)/2}\frac{\theta[\begin{smallmatrix}1/2+j/m\\1/2\end{smallmatrix}](mz,m\tau)}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)^m}, \end{aligned}$$

by (c) and Lemma 19(b). □

We will need a lemma in Proposition 22 to verify the claim in the Introduction that the version in (I.1) of Theorem I is equivalent to the version in (I.2).

Lemma 21. *Let $f, f_0, \dots, f_{m-1}$ be any functions analytic at the origin, and let $W_z(f_0,\dots,f_{m-1})(z)$ denote the Wronskian*

$$\det_{0\le j,k<m}\left(\frac{\mathrm{d}}{\mathrm{d}z}\right)^k f_j(z).$$

(a) $\dfrac{\mathrm{d}}{\mathrm{d}z}W_z(f_0,\dots,f_{m-1})(z) = \det\limits_{\substack{0\le j<m\\0\le k\le m-2,k=m}}\left(\dfrac{\mathrm{d}}{\mathrm{d}z}\right)^k f_j(z).$

(b) *If $W_z(f_0,\dots,f_{m-1})(0)=0$ then*

$$\det_{\substack{0\le j<m\\0\le k\le m-2,k=m}}\left(\frac{\mathrm{d}}{\mathrm{d}z}\right)^k f(z)f_j(z)|_{z=0} = \det_{\substack{0\le j<m\\0\le k\le m-2,k=m}}\left(\frac{\mathrm{d}}{\mathrm{d}z}\right)^k f_j(z)|_{z=0}f(0)^m.$$

(c) *If $W_z(f_0,\dots,f_{m-1})(0)=0$ and t is a local parameter at the origin, then*

$$\det_{\substack{0\le j<m\\0\le k\le m-2,k=m}}\left(\frac{\mathrm{d}}{\mathrm{d}t}\right)^k f_j(z)|_{t=0} = \det_{\substack{0\le j<m\\0\le k\le m-2,k=m}}\left(\frac{\mathrm{d}}{\mathrm{d}z}\right)^k f_j(z)|_{z=0}\frac{\mathrm{d}z}{\mathrm{d}t}(0)^{\frac{m^2-m+2}{2}}.$$

Proof. (a). The derivative with respect to z of $\det_{0\le j,k<m}(\frac{\mathrm{d}}{\mathrm{d}z})^k f_j(z)$ is the sum over $1\le\ell\le m$ of $\det_{0\le j,k<m}(\frac{\mathrm{d}}{\mathrm{d}z})^{k+\delta(\ell,k)}f_j(z)$, where $\delta(\ell,k)$ is the Kronecker delta. These summands all vanish unless $\ell=m$.

(b). Using the product formula for derivatives and properties of determinants, it is elementary that

$$W_z(ff_0, \ldots, ff_{m-1})(z) = W_z(f_0, \ldots, f_{m-1})(z) f(z)^m,$$

in a neighborhood of the origin. Suppose that $W_z(f_0, \ldots, f_{m-1})(z)$ vanishes at the origin. Then differentiating with respect to z gives

$$\frac{\mathrm{d}}{\mathrm{d}z} W_z(ff_0, \ldots, ff_{m-1})(0) = \frac{\mathrm{d}}{\mathrm{d}z} W_z(f_0, \ldots, f_{m-1})(0) f(0)^m.$$

The result now follows from (a).

(c). Using the chain rule for derivatives and properties of determinants, it is elementary that

$$W_t(f_0, \ldots, f_{m-1})(z) = W_z(f_0, \ldots, f_{m-1})(z) \left(\frac{\mathrm{d}z}{\mathrm{d}t}\right)^{m(m-1)/2},$$

in a neighborhood of the origin. Suppose that $W_z(f_0, \ldots, f_{m-1})(z)$ (and hence $W_t(f_0, \ldots, f_{m-1})(z)$) vanishes at the origin. Then differentiating with respect to t gives

$$\frac{\mathrm{d}}{\mathrm{d}t} W_t(f_0, \ldots, f_{m-1})(0) = \frac{\mathrm{d}}{\mathrm{d}z} W_z(f_0, \ldots, f_{m-1})(0) \frac{\mathrm{d}z}{\mathrm{d}t}(0)^{\frac{m^2-m+2}{2}}.$$

The result now follows from two applications of (a). □

Using this we now get:

Proposition 22.

(a) *Given our choices for P and Q on E_τ, we have*

$$T(\tau) = T(P, Q).$$

(b) *The version of Theorem I in* (I.1) *is equivalent to the version in* (I.2).

(c) *If m is not a multiple of 3, Theorem I follows from Theorem III, and if $3|m$, we have established Theorem I up to a third root of unity.*

Proof. (a). We get from part (g) of Proposition 20 that g_j for E_τ matches with $g_j(z, \tau)$ as given in the Introduction. The only difference then in the definitions in (3) and (6) of $T(\tau)$ and $T(P, Q)$ is that the expansions of the g_j in the former are taken with respect to z and the latter are taken with respect to t. Because of Lemma 13 (c), we can apply Lemma 21 (c) and then (16) to see that we get $T(\tau) = T(P, Q)$.

(b). By the definition of $g_j(z, \tau)$ in the Introduction,

$$z^m g_j(z, \tau) = \left(\frac{e^{2\pi i j/m}}{2\pi i}\right)^{(m-1)/2} f_{\delta,j}(z, \tau) \left(\frac{z}{\theta[\delta](z, \tau)}\right)^m.$$

Hence because of Lemma 13(c), it follows from Lemma 21(b) that

$$T(\tau) = \det_{\substack{0\le j<m\\ 0\le k\le m-2, k=m}} (z^m g_j)^{[k]}(0,\tau)$$
$$= \frac{(\prod_{j=1}^{m-1} e^{2\pi ij/m})^{(m-1)/2}}{(2\pi i)^{m(m-1)/2}(\theta[\delta](0,\tau)')^{m^2}} \det_{\substack{0\le j<m\\ 0\le k\le m-2, k=m}} [f_{\delta,j}^{[k]}(0,\tau)].$$

Since m is odd, $\prod_{j=1}^{m-1} e^{2\pi ij/m} = 1$, $i^{-m(m-1)/2} = i^{3m(m-1)/2} = i^{(3-3m)/2}$, and $(-1)^{m^2} = -1$, so using Jacobi's formula (2), we get that

$$T(\tau) = \frac{i^{(-1-3m)/2} \det_{\substack{0\le j<m\\ 0\le k\le m-2, k=m}} [f_{\delta,j}^{[k]}(0,\tau)]}{(2\pi)^{(3m^2-m)/2}\eta(\tau)^{3m^2}},$$

so (I.1) is equivalent to (I.2).

(c). This follows from (a), (I.2), and (I.3). □

If 3 divides m, we will now determine the ambiguous (or better, triguous[2]) cube root of 1 in Theorem III by applying Theorem II to E_τ.

Proposition 23. *For E_τ, and our choices of P and Q,*

$$T(\tau) = T(P,Q) = 1/(2\pi\eta(\tau)^2)^{m^2-1}.$$

Hence Theorem II implies Theorem I.

Proof. We start by specializing the formula for $\lambda(P,Q)$ given in Theorem II to E_τ.

Let $\sigma(z,\tau)$ denote the Weierstrass sigma-function (see e.g., [18, p. 239]), which is an odd function of z, whose second logarithmic derivative with respect to z is the negative of the Weierstrass $\wp(z,\tau)$-function, and is normalized by $\sigma'(0,\tau) = 1$. It is well-known (see e.g., the argument on [22, p.25] coupled with the fact that $\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)$ is an odd functions of z) that

$$\sigma(z,\tau) = e^{c(\tau)z^2}\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)/\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau),$$

for a well-studied function $c(\tau)$ we needn't specify here[3]. We get immediately from this that the well-known analytic statement of the Theorem of the Square (see e.g., [18, p. 243])

$$\wp(v,\tau) - \wp(u,\tau) = \frac{\sigma(u+v,\tau)\sigma(u-v,\tau)}{\sigma^2(u,\tau)\sigma^2(v,\tau)},$$

[2]Coined by Sydney Lamb for when something can be interpreted three ways: *Linguistic Data Processing*, in *The use of computers in anthropology*, de Gruyter (2011), 159–188.

[3]The argument in Theorem 3 in [18, p. 246] shows that $c(\tau)$ is $-1/2$ times a quasi-period of the Weierstrass ζ-function. [28] also shows on p. 95 that $c(\tau)$ is $-\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'''(0,\tau)/6\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau)$. For its life as a quasimodular form, see [29].

can be rewritten as

$$\wp(v,\tau)-\wp(u,\tau)=\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau)^2\frac{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](u+v,\tau)\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](u-v,\tau)}{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]^2(u,\tau)\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]^2(v,\tau)}.$$

If we now write $u=u_1\tau+u_2$, $v=v_1\tau+v_2$ for arbitrary $u_1,u_2,v_1,v_2\in\mathbb{R}$, then by Lemma 19(b) and (c), using that $\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](-z,\tau)=-\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\tau)$ we have

$$\wp(v,\tau)-\wp(u,\tau)=-\frac{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau)^2\theta\left[\begin{smallmatrix}1/2+u_1+v_1\\1/2+u_2+v_2\end{smallmatrix}\right](0,\tau)\theta\left[\begin{smallmatrix}1/2+u_1-v_1\\1/2+u_2-v_2\end{smallmatrix}\right](0,\tau)}{\theta\left[\begin{smallmatrix}1/2+u_1\\1/2+u_2\end{smallmatrix}\right](0,\tau)^2\theta\left[\begin{smallmatrix}1/2+v_1\\1/2+v_2\end{smallmatrix}\right](0,\tau)\theta\left[\begin{smallmatrix}1/2-v_1\\1/2-v_2\end{smallmatrix}\right](0,\tau)}.$$

Using this we get

$$\begin{aligned}&\prod_{k=1}^{(m-1)/2}\prod_{j=1}^{m-1}(\wp([j]Q,\tau)-\wp([k]P,\tau))\\&\quad=\prod_{k=1}^{(m-1)/2}\prod_{j=1}^{m-1}\frac{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau)^2\theta\left[\begin{smallmatrix}1/2+j/m\\1/2+k/m\end{smallmatrix}\right](0,\tau)\theta\left[\begin{smallmatrix}1/2-j/m\\1/2+k/m\end{smallmatrix}\right](0,\tau)}{\theta\left[\begin{smallmatrix}1/2\\1/2+k/m\end{smallmatrix}\right](0,\tau)^2\theta\left[\begin{smallmatrix}1/2+j/m\\1/2\end{smallmatrix}\right](0,\tau)\theta\left[\begin{smallmatrix}1/2-j/m\\1/2\end{smallmatrix}\right](0,\tau)}.\end{aligned}$$

From Lemma 19 we get

$$\begin{aligned}(17)\quad&\theta\left[\begin{smallmatrix}1/2-j/m\\1/2+k/m\end{smallmatrix}\right](0,\tau)=\theta\left[\begin{smallmatrix}-1/2+j/m\\-1/2-k/m\end{smallmatrix}\right](0,\tau)=\theta\left[\begin{smallmatrix}1/2+j/m\\-1/2-k/m\end{smallmatrix}\right](0,\tau)\\&\quad=e^{2\pi i(1/2+j/m)(2)}\theta\left[\begin{smallmatrix}1/2+j/m\\1/2+(m-k)/m\end{smallmatrix}\right](0,\tau)=\zeta_m^{2j}\theta\left[\begin{smallmatrix}1/2+j/m\\1/2+(m-k)/m\end{smallmatrix}\right](0,\tau).\end{aligned}$$

Hence applying (17) three times (once as is, once with $j=0$, and once with $k=0$), we get

$$\begin{aligned}(18)\quad&\prod_{k=1}^{(m-1)/2}\prod_{j=1}^{m-1}(\wp([j]Q,\tau)-\wp([k]P,\tau))\\&=\frac{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau)^{(m-1)^2}\prod_{j,k=1}^{m-1}\theta\left[\begin{smallmatrix}1/2+j/m\\1/2+k/m\end{smallmatrix}\right](0,\tau)}{\prod_{k=1}^{m-1}\theta\left[\begin{smallmatrix}1/2\\1/2+k/m\end{smallmatrix}\right](0,\tau)^{m-1}\left(\prod_{j=1}^{m-1}\theta\left[\begin{smallmatrix}1/2+j/m\\1/2\end{smallmatrix}\right](0,\tau)\theta\left[\begin{smallmatrix}1/2+j/m\\3/2\end{smallmatrix}\right](0,\tau)\right)^{(m-1)/2}}.\\&=\frac{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau)^{(m-1)^2}\prod_{j,k=0,(j,k)\neq(0,0)}^{m-1}\theta\left[\begin{smallmatrix}1/2+j/m\\1/2+k/m\end{smallmatrix}\right](0,\tau)}{\prod_{k=1}^{m-1}\theta\left[\begin{smallmatrix}1/2\\1/2+k/m\end{smallmatrix}\right](0,\tau)^m\prod_{j=1}^{m-1}\theta\left[\begin{smallmatrix}1/2+j/m\\1/2\end{smallmatrix}\right](0,\tau)^m},\end{aligned}$$

using Lemma 19(a).

Hence, using the result from [11] that

$$\prod_{j,k=0,(j,k)\neq(0,0)}^{m-1} \theta\left[\begin{smallmatrix}1/2+j/m\\1/2+k/m\end{smallmatrix}\right](0,\tau) = m\eta^{m^2-1}(\tau),$$

Theorem II, Proposition 20(b) and (d), and (18), we get $\lambda(P,Q) =$

$$\begin{aligned}(-1)^{\frac{m-1}{2}} \prod_{k=1}^{\frac{m-1}{2}} \prod_{j=1}^{m-1} (\wp([j]Q,\tau) - \wp([k]P,\tau)) \prod_{k=1}^{m-1} \Theta([k]P,\tau) \prod_{j=1}^{m-1} \Theta([j]Q,\tau)\\ = \theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau)^{(m-1)^2} m\eta(\tau)^{m^2-1} / \theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau)^{2m(m-1)}\\ = m\left(\eta(\tau)/\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]'(0,\tau)\right)^{m^2-1} = m/(2\pi\eta(\tau)^2)^{m^2-1},\end{aligned}$$

by (2). Hence by Theorem II,

$$T(P,Q) = \lambda(P,Q)/m = 1/(2\pi\eta(\tau)^2)^{m^2-1}.$$

By Proposition 22(a) this gives (I.2) and then Proposition 22(b) gives Theorem I. □

Acknowledgments. I would like to thank Clifford Blakestad, Harold Stark, and Paul Voutier for helpful discussions on this material. I would also like to thank the referee for a bevy of sagacious suggestions.

References

[1] G. W. Anderson, "Lacunary Wronskians on genus one curves", *J. Number Theory* **115** (2005), no. 2, p. 197-214.

[2] M. Ayad, "Points Δ-entiers sur les courbes elliptiques", *J. Number Theory* **38** (1991), no. 3, p. 323-337.

[3] ———, "Points S-entiers des courbes elliptiques", *Manuscr. Math.* **76** (1992), no. 3-4, p. 305-324.

[4] K. Bannai & S. Kobayashi, "Algebraic theta functions and the p-adic interpolation of Eisenstein-Kronecker numbers", *Duke Math. J.* **153** (2010), no. 2, p. 229-295.

[5] J. Boxall & D. Grant, "Theta functions and singular torsion on elliptic curves", in *Number theory for the millennium I*, A K Peters, 2002, p. 111-126.

[6] ———, "Singular torsion on elliptic curves", *Math. Res. Lett.* **10** (2003), no. 5-6, p. 847-866.

[7] I. Connell, "Elliptic Curve Handbook", unpublished.

[8] H. M. Farkas & I. Kra, *Theta constants, Riemann surfaces and the modular group. An introduction with applications to uniformization theorems, partition identities and combinatorial number theory*, Graduate Studies in Mathematics, vol. 37, American Mathematical Society, 2001.

[9] D. Grant, "Resultants of Division Polynomials. I: Reciprocity and Elliptic Units", in preparation.

[10] ———, "Resultants of Division Polynomials. II: Singular torsion on Elliptic Curves", in preparation.

[11] ———, "Some product formulas for theta functions in one and two variables", *Acta Arith.* **102** (2002), no. 3, p. 223-238.

[12] ———, "A generalization of Jacobi's derivative formula to dimension two. II", *Acta Arith.* **190** (2019), no. 4, p. 403-420.

[13] S. Grushevsky & R. Salvati Manni, "Two generalizations of Jacobi's derivative formula", *Math. Res. Lett.* **12** (2005), no. 5-6, p. 921-932.
[14] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer, 1977.
[15] M. Hindry, "Polynômes de Cassels P_N et Q_N et résultant", `https://webusers.imj-prg.fr/~marc.hindry/cassels.pdf`.
[16] J.-i. Igusa, "On Jacobi's derivative formula and its generalizations", *Am. J. Math.* **102** (1980), no. 2, p. 409-446.
[17] E. Landau, *Elementary Number Theory*, American Mathematical Society, 1999.
[18] S. Lang, *Elliptic Functions*, 2nd ed., Graduate Texts in Mathematics, vol. 112, Springer, 1987.
[19] B. Mazur & J. Tate, "The p-adic sigma function", *Duke Math. J.* **62** (1991), no. 3, p. 663-688.
[20] A. Milas, E. Mortenson & K. Ono, "Number theoretic properties of wronskians of Andrews-Gordon series", *Int. J. Number Theory* **4** (2008), no. 2, p. 323-337.
[21] D. Mumford, "On the equations defining abelian varieties I", *Invent. Math.* **1** (1966), p. 287-354.
[22] ———, *The Tata Lectures on Theta. I: Introduction and motivation: Theta functions in one variable. Basic results on theta functions in several variables*, Progress in Mathematics, vol. 28, Birkhäuser, 1983.
[23] ———, *The Tata Lectures on Theta. III*, Progress in Mathematics, vol. 97, Birkhäuser, 1991.
[24] I. Schur, "Über die Gaußschen Summen", *Gött. Nachr.* **1921** (1921), p. 147-153.
[25] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15** (1971), p. 259-331.
[26] ———, *Algebraic Groups and Class Fields*, Graduate Texts in Mathematics, vol. 117, Springer, 1988.
[27] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, 2000.
[28] H. Weber, *Elliptische Functionen und Algebraische Zahlen*, Vieweg u. Sohn., 1891.
[29] S. Zemel, "A direct evaluation of the periods of the Weierstrass zeta function", *Ann. Univ. Ferrara, Sez. VII, Sci. Mat.* **60** (2014), p. 495-505.

David Grant
Department of Mathematics
University of Colorado Boulder
Boulder, CO 80309-0395 USA
E-mail: `grant@colorado.edu`