A GENERALIZATION OF A FORMULA OF EISENSTEIN

DAVID GRANT

[Received 18 December 1989]

Introduction

Let E be the elliptic curve defined by

$$y^2 = x^3 + \tfrac{1}{4}.$$

Let $\omega = e^{2\pi i/3}$. Then E has complex multiplication by $\mathbb{Z}[\omega]$. If $\rho \equiv 1 \bmod (3)$ is in $\mathbb{Z}[\omega]$, then a classic formula states that

$$\prod_{P \in E[\rho]'} x(P) = \frac{1}{\rho^2}, \tag{0.1}$$

where $E[\rho]'$ denotes the non-zero ρ-torsion of E. (Equation (0.1) was probably known to Eisenstein: he published a similar formula. See **[1]** for a proof of (0.1) and related history.) The automorphism $x \to \omega x$, $y \to y$ acts on $E[\rho]'$, and (0.1) gives a non-canonical way to extract a cube root of ρ. This played a crucial role in Matthews's proof of Cassels's conjecture on the value of the cubic Gauss sum **[1, 8]**.

The purpose of this paper is to produce an analogue of (0.1), relating integers in $\mathbb{Z}[e^{2\pi i/5}]$ to points on a curve of genus 2. Specifically, let C be the curve of genus 2 given by

$$y^2 = x^5 + \tfrac{1}{4}. \tag{0.2}$$

Let ∞ denote the point at infinity on the model (0.2). Then we can embed C into its Jacobian J by mapping a point P on C to its divisor class $P - \infty$. We let Θ denote its image, a theta divisor. In **[4]** (and (1.3)) we describe a function X on J, whose divisor of zeros we denote by $(X)_0$. Let $\zeta = e^{2\pi i/5}$. Then the automorphism

$$x \to \zeta x, \quad y \to y$$

of C extends to give an embedding of $\mathbb{Z}[\zeta]$ into $\mathrm{End}(J)$. If $\alpha \in \mathbb{Z}[\zeta]$, and D is a divisor on J, we let $(\alpha)^{-1}D$ denote the inverse image of D under α in the Picard group of J. Our main result is:

THEOREM. *Let $\beta \equiv \pm 1 \bmod (1-\zeta)^2$ in $\mathbb{Z}[\zeta]$. Then*

$$\prod_{\substack{z \in \Theta \cap (\beta\sigma^{-1}(\beta))^{-1}(X)_0 \\ z \notin J[2]}} x(z) = \frac{1}{(\beta\sigma\beta)^2},$$

where $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ maps ζ to ζ^2, and we identify a point $z \in \Theta$ with $(x(z), y(z))$ on C.

Eisenstein's formula is a special case of a general phenomenon for elliptic units, which play a central role in the study of elliptic curves with complex multiplication and the arithmetic of imaginary quadratic fields **[2, 3, 9, 10, 11, 12, 13, 14]**.

A.M.S. (1980) subject classification: 11G10, 11G16, 14K25.

Proc. London Math. Soc. (3) 62 (1991) 121–132.

This represents the first time classes of S-units have been produced from special values of functions defined on a curve of genus 2. There are similar units which can be constructed from general curves of genus 2: we hope to discuss them in a future paper. It remains to be seen what relationship they might have to the arithmetic of such curves.

REMARKS. (1) In [4] we showed that there are functions t_1, t_2 on J, which for all primes p of $\mathbb{Z}[\zeta]$ not dividing 2, are parameters for the formal group on the kernel of reduction $J_0(p)$ of $J \bmod p$. The divisor of zeros of t_1 contains Θ as a component, and the divisor of zeros of t_2 is $(X)_0$. It follows from standard properties of formal groups that the $x(z)$ in the product are integral outside primes dividing $2\beta\sigma(\beta)$. Likewise, since $(0, \pm\frac{1}{2})$ are $(1-\zeta)$-torsion on J, $x(z)$ is not divisible by any primes not dividing 10.

(2) The theorem gives a non-canonical way to extract a fifth root of $\beta\sigma(\beta)$. There should be some way to relate a fifth root to the value of the quintic Gauss sum.

(3) By evaluating functions on J at torsion points, Kubota obtained a formula expressing $\beta(\sigma(\beta))^3$ up to a fifth power [5].

Sections 1 and 2 give preliminary information on the geometry of J and the action of $\mathbb{Z}[\zeta]$ on divisors on J. Section 3 contains a somewhat messy induction based on the proof of (0.1) in [1]. The proof of the theorem is completed in the last section.

Acknowledgements. This work was undertaken while the author was supported by a NATO postdoctoral fellowship and was enjoying the hospitality of Cambridge University. I would like to thank J. Coates for many useful discussions and suggestions. I am indebted to C. R. Matthews, who not only suggested this problem to me, but also provided continued encouragement.

1. *Functions on C and J*

Recall that we have identified C with its image Θ under the map

$$P \to \mathrm{Cl}(P - \infty),$$

where Cl is the divisor class map into the Picard group Pic(C). Let U be the open set $J - \Theta$. Then every point on U has a unique representative in Pic(C) of the form

$$(x_1, y_1) + (x_2, y_2) - 2\infty \quad (y_2 \neq y_1 \text{ if } x_1 = x_2),$$

and functions on J can be written as symmetric functions in x_1, x_2, y_1, y_2. For the basic facts about J and its analytic parameterization, we refer the reader to [4]. We will freely use results of that paper.

Given an ordering of the Weierstrass points of C, there is a standard way to pick a symplectic basis of $H_1(C, \mathbb{Z})$. Integrating the holomorphic differentials $dx/2y$, $x\,dx/2y$ over this basis gives rise to a period lattice L, and gives us an analytic isomorphism Φ: $J \to \mathbb{C}^2/L$ via

$$P_1 + P_2 - 2\infty \xrightarrow{\Phi} \int_\infty^{P_1} \frac{dx}{2y}, \int_\infty^{P_2} \frac{x\,dx}{2y} \quad \mathrm{mod}\, L,$$

where the $P_i = (x_i, y_i)$ or ∞ are points on C. So if $z = (z_1, z_2) = \Phi(P_1 + P_2 - 2\infty)$, we see that ζ maps $(z_1, z_2) \to (\zeta z_1, \zeta^2 z_2)$. Hence J has CM-type $(1, \sigma)$, where $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ maps $\zeta \to \zeta^2$. These choices also determine a sigma-function $\sigma(z)$, which is analytic and odd on $\mathbb{C}^2$, has a zero of order 1 precisely along the pullback of Θ to $\mathbb{C}^2$, and has no other zeros. Associated with σ is its alternating Riemann form E, defined by the quasi-periodicity of σ. Specifically, there is a linear form $F(z, l)$ such that

$$\sigma(z + l) = \sigma(z) e^{2\pi i (F(z,l) + c(l))},$$

for every $l \in L$, where $c(l)$ is independent of z, and we set

$$E(z, l) = F(z, l) - F(l, z). \tag{1.1}$$

This quasi-periodicity shows that

$$X_{ij}(z) = -\frac{d}{dz_i}\frac{d}{dz_j} \log \sigma(z), \tag{1.2}$$

and

$$X_{ijk}(z) = \frac{1}{2}\frac{d}{dz_k} X_{ij}(z),$$

are functions on J, regular on U. From [4] it follows that

$$\begin{aligned}
X_{11}(z) &= \frac{(x_1 + x_2)(x_1 x_2)^2 + \frac{1}{2} - 2y_1 y_2}{(x_1 - x_2)^2}, \qquad (1.3)\\
X_{12}(z) &= -x_1 x_2,\\
X_{22}(z) &= x_1 + x_2,\\
X(z) &= \tfrac{1}{2}(X_{11}(z) X_{22}(z) - X_{12}^2(z)) = \frac{2(x_1 x_2)^3 + \frac{1}{4}(x_1 + x_2) - (x_1 + x_2) y_1 y_2}{(x_1 - x_2)^2},\\
X_{111}(z) &= \frac{y_2(1 + 3x_1^4 x_2 + x_1^3 x_2^2) - y_1(1 + 3x_1 x_2^4 + x_1^2 x_2^3)}{(x_1 - x_2)^3},\\
X_{222}(z) &= \frac{y_1 - y_2}{x_1 - x_2}.
\end{aligned}$$

We also have the Taylor expansions

$$\begin{aligned}
\sigma(z) &= z_1 - \tfrac{1}{3} z_2^3 + (d^0 \geqslant 5), \qquad (1.4)\\
\sigma^2(z) X_{11}(z) &= 1 + (d^0 \geqslant 4),\\
\sigma^2(z) X_{12}(z) &= -z_2^2 + (d^0 \geqslant 4),\\
\sigma^2(z) X_{22}(z) &= 2 z_1 z_2 + (d^0 \geqslant 4),\\
\sigma^3(z) X(z) &= z_2 + (d^0 \geqslant 3),\\
\sigma^3(z) X_{111}(z) &= -1 + (d^0 \geqslant 2),\\
\sigma^3(z) X_{222}(z) &= z_1^2 + (d^0 \geqslant 4),
\end{aligned}$$

where $(d^0 \geqslant n)$ denotes a power series, all of whose terms have degree at least n.

On Θ, $\sigma(z) = 0$, so by the implicit function theorem and (1.4),

$$z_1 = \tfrac{1}{3} z_2^3 + (d^0 \geqslant 5). \tag{1.5}$$

If we set $\sigma_i(z) = d\sigma(z)/dz_i$, then from (1.4),

$$\sigma_1(z) = 1 + (d^0 \geqslant 2),$$
$$\sigma_2(z) = -z_2^2 + (d^0 \geqslant 4).$$

So for $z \in \Theta$, it follows from (1.2) and (1.3) that

$$x(z) = \frac{x_1x_2}{x_1+x_2}\bigg|_\Theta = \frac{-X_{12}(z)}{X_{22}(z)} = \frac{-\sigma_1(z)\sigma_2(z)}{\sigma_2(z)^2} = \frac{-\sigma_1(z)}{\sigma_2(z)} = \frac{1}{z_2^2} + \dots$$

and

$$y(z) = \frac{(x_1+x_2)y_1y_2 - \frac{1}{4}(x_1+x_2) - 2(x_1x_2)^3}{(y_1-y_2)(x_1-x_2)}\bigg|_\Theta = \frac{-X(z)}{X_{222}(z)} = \frac{-z_2+\dots}{(-\sigma_2(z))^3} = \frac{-1}{z_2^5} + \dots .$$

Note that $x(z)$ and $y(z)$ generate the ring of functions on Θ regular away from the origin O. In particular, $\sigma_2(z) = 0$ only when $z = O$.

We will also need the formula of Baker [4]: for $u, v, u+v, u-v \in U$,

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = X_{11}(v) - X_{11}(u) + X_{12}(v)X_{22}(u) - X_{12}(u)X_{22}(v). \quad (1.6)$$

Multiplying by $\sigma^2(v)/\sigma_2^2(v)$ shows that for $v \in \Theta$, $v \neq O$,

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma_2(v)^2} = x(v)^2 - x(v)X_{22}(u) - X_{12}(u). \quad (1.7)$$

Let $P = (0, \frac{1}{2}) - \infty \in \Theta$. Then $\zeta P = P$, so P is $(1-\zeta)$-torsion on J. Note that for $\alpha \in \mathbb{Z}[\zeta]$, $\alpha P \in \Theta$ precisely when $\alpha \equiv -1, 0, 1 \bmod (1-\zeta)$. We see immediately from (1.3) that $X_{12}(2P) = X_{22}(2P) = 0$. Less immediately, we calculate that

$$X_{222}(2P) = \frac{(y_1-y_2)(y_1+y_2)}{(x_1-x_2)(y_1+y_2)}\bigg|_{2P} = \frac{x_1^4 + x_1^3x_2 + x_1^2x_2^2 + x_1x_2^3 + x_2^4}{y_1+y_2}\bigg|_{2P} = 0,$$

and that

$$X_{11}(2P) = X_{222}^2(2P) - X_{22}^3(2P) - X_{12}(2P)X_{22}(2P) = 0.$$

So plugging $v = 2P$ into (1.6) yields

$$\frac{\sigma(u+2P)\sigma(u-2P)}{\sigma(u)^2\sigma(2P)^2} = -X_{11}(u), \quad (1.8)$$

and substituting $v = P$ into (1.7) gives

$$\frac{\sigma(u+P)\sigma(u-P)}{\sigma(u)^2\sigma_2(P)^2} = -X_{12}(u). \quad (1.9)$$

Proposition 1. *Let*

$$W(z) = \frac{1}{2}\frac{\sigma(z+P)\sigma(z+2P)\sigma(z-3P) + \sigma(z-P)\sigma(z-2P)\sigma(z+3P)}{\sigma(z)^3\sigma_2(P)\sigma(2P)\sigma(-3P)}.$$

Then $W(z) = X(z)$.

Proof. First we note that $W(z)$ is a function on J by the quasi-periodicity of $\sigma(z)$. Since σ is odd, W is even, and has a pole of order at most 3 along Θ, and no other poles. By the results in [4], we know that the space of such functions is spanned by X, X_{11}, X_{12}, X_{22}, 1, so

$$W = \alpha X + \beta X_{11} + \gamma X_{12} + \delta X_{22} + \varepsilon,$$

for constants α, β, γ, δ, ε. But $W(2P) = 0$, and

$$X(2P) = \tfrac{1}{2}(X_{11}(2P)X_{22}(2P) - X_{12}^2(2P)) = 0,$$

so $\varepsilon = 0$. We compute the Taylor series

$$\begin{aligned}\sigma^3(z)W(z) &= \frac{(\sigma_1(P)z_1 + \sigma_2(P)z_2)(\sigma(2P))(\sigma(-3P))}{\sigma_2(P)\sigma(2P)\sigma(-3P)} + (d^0 \geqslant 3)\\ &= z_2 + (d^0 \geqslant 3),\end{aligned}$$

since $0 = x(P) = -\sigma_1(P)/\sigma_2(P)$. Comparing with (1.4) gives $\alpha = 1$ and $\beta = 0$, so

$$W = X + \gamma X_{12} + \delta X_{22}.$$

Let (x_0, y_0) be a variable point on C, and set $z = P + (x_0, y_0) - \infty$. Then $W(z) = 0$ precisely when $z + P$, $z + 2P$, or $z - 3P$ is on Θ, which happens only when $(x_0, y_0) = (0, \pm\frac{1}{2})$. But $X_{12}(z) = 0$, and

$$\begin{aligned}X(z) + \gamma X_{12}(z) + \delta X_{22}(z) &= \frac{\frac{1}{4}x_0 - x_0(y_0/2)}{x_0^2} + \delta x_0\\ &= \frac{\frac{1}{4} - (y_0/2) + \delta x_0^2}{x_0},\end{aligned}$$

which has a zero when $x_0^3 = 4\delta^2 x_0^2 + 2\delta$. Therefore $\delta = 0$, and

$$W = X + \gamma X_{12}.$$

Likewise, if $z = 2P + (x_0, y_0) - \infty$, then $W(z) = 0$ precisely when $z + P$, $z + 2P$, or $z - 3P$ is on Θ, which happens only when $(x_0, y_0) = (0, \frac{1}{2})$. On the other hand, $X_{11}(z) = 0$, and hence

$$X(z) + \gamma X_{12}(z) = -\tfrac{1}{2}X_{12}^2(z) + \gamma X_{12}(z) = X_{12}(z)(\gamma - \tfrac{1}{2}X_{12}(z)).$$

Note that the function

$$y - ((y_0 - \tfrac{1}{2})/x_0^2)x^2 - \tfrac{1}{2}$$

on C has a pole of order 5 at ∞, and zeros of order 1 at (x_0, y_0) and 2 at P. So from the group law on J,

$$X_{12}(z) = (\tfrac{1}{2} - y_0)/(x_0^3),$$

and $\gamma - \frac{1}{2}X_{12}(z) = 0$ when $4\gamma^2 x_0^3 - x_0^2 - 2\gamma = 0$. Therefore $\gamma = 0$, and $W = X$.

2. *Actions of* $\mathbb{Z}[\zeta]$ *on divisors*

Let Pic(J) denote the Picard group of divisors on J modulo linear equivalence, and NS(J) the Néron–Severi group of divisors modulo algebraic equivalence. If two divisors D_1 and D_2 are algebraically equivalent, we write $D_1 \approx D_2$; if they are linearly equivalent, we write $D_1 \sim D_2$. If $D \in \mathrm{Pic}(J)$ and $\alpha \in \mathrm{End}(J)$, we let $(\alpha)^{-1}D$ denote the inverse image of D under α in Pic(J).

The complex multiplication of J forces the alternating Riemann form $E_\Theta(z, l) = E(z, l)$ defined by (1.1) to have a particularly nice form. Indeed, if we consider $K = \mathbb{Q}(\zeta)$ embedded in $\mathbb{C}^2$ via $\alpha \to (\alpha, \sigma\alpha)$, then there exists a $\xi \in K$ such that

$$E_\Theta(z, l) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi \bar{z} l) \quad \text{whenever } z, l \in K,$$

and where $\bar{z}$ denotes the complex conjugate of z. This suffices to determine E_Θ, since it is $\mathbb{R}$-bilinear. There is a unique alternating Riemann form E_D associated to any divisor D in NS(J), and in [6], it is shown that for any $\alpha \in \mathbb{Z}[\zeta]$,

$$E_{(\alpha)^{-1}\Theta}(z, l) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\bar{\alpha}\xi\bar{z}l), \tag{2.1}$$

and so if $\alpha = \beta\sigma^{-1}(\beta)$ for some $\beta \in \mathbb{Z}[\zeta]$, then

$$E_{(\beta\sigma^{-1}(\beta))^{-1}\Theta} = \mathbb{N}_{K/\mathbb{Q}}(\beta)E. \tag{2.2}$$

Here the addition of Riemann forms corresponds to the addition of the corresponding divisors in NS(J).

Let $\varepsilon = \frac{1}{2}(1+\sqrt{5}) = \zeta + \zeta^{-1} + 1$. Then ε is a fundamental unit of $\mathbb{Z}[\zeta]$. Since $\varepsilon^2 = \varepsilon + 1$, we have $\varepsilon^4 = 3\varepsilon^2 - 1$, so by (2.1),

$$E_{(\varepsilon^2)^{-1}\Theta}(z, l) = \mathrm{Tr}_{K/\mathbb{Q}}((3\varepsilon^2 - 1)\bar{z}l\xi) = 3E_{(\varepsilon)^{-1}\Theta} - E_\Theta. \tag{2.3}$$

In fact these relations hold in Pic(J):

Lemma 1. *If $D \approx 0$, and $(\pm\zeta^i)^{-1}D \sim D$, then $D \sim 0$.*

Proof. If $D \approx 0$, then since Θ is a principal polarization, $D \sim \Theta_u - \Theta$, where Θ_u is the translate of Θ by a unique $u \in J$. But since $(\pm\zeta^i)^{-1}\Theta = \Theta$, we get $-\Theta_u \sim \Theta_u$, and $(\zeta)^{-1}\Theta_u \sim \Theta_u$; which means u is both 2-torsion and $(1-\zeta)$-torsion on J. Therefore $u = O$ and $D \sim 0$.

Since $(\pm\zeta^i)^{-1}(\alpha)^{-1}\Theta = (\alpha)^{-1}\Theta$, we get as an immediate corollary to the lemma that (2.2) and (2.3) imply:

$$(\beta\sigma^{-1}(\beta))^{-1}\Theta \sim \mathbb{N}_{K/\mathbb{Q}}(\beta)\Theta, \tag{2.4}$$

and

$$(\varepsilon^2)^{-1}\Theta \sim 3(\varepsilon)^{-1}\Theta - \Theta.$$

In general [7], for any D in NS(J) we have

$$(\alpha-\beta)^{-1}D + (\alpha+\beta)^{-1}D \approx 2(\alpha)^{-1}D + 2(\beta)^{-1}D \quad (\alpha, \beta \in \mathrm{End}(J)),$$

so Lemma 1 implies that

$$(\alpha+\beta)^{-1}\Theta + (\alpha-\beta)^{-1}\Theta \sim 2(\alpha)^{-1}\Theta + 2(\beta)^{-1}\Theta, \tag{2.5}$$

and that

$$(\alpha+2)^{-1}\Theta + (\alpha+1)^{-1}\Theta + (\alpha-3)^{-1}\Theta \sim 3(\alpha)^{-1}\Theta + 14\Theta. \tag{2.6}$$

We want to compute $(\alpha)^{-1}\Theta$ for any $\alpha \in \mathbb{Z}[\zeta]$. Indeed, since Θ gives a principal polarization, we can use the formula [7]

$$\left(\sum m_i\alpha_i\right)^{-1}\Theta \sim \tfrac{1}{2}\sum m_i m_j D_\Theta(\alpha_i, \alpha_j), \tag{2.7}$$

where $D_\Theta(\alpha_i, \alpha_j) = (\alpha_i + \alpha_j)^{-1}\Theta - (\alpha_i)^{-1}\Theta - (\alpha_j)^{-1}\Theta$.

PROPOSITION 2. *Let* $\alpha = a + b\varepsilon + c\zeta + d\zeta\varepsilon \in \mathbb{Z}[\zeta]$. *Then*

$$(\alpha)^{-1}\Theta \sim n_\alpha\Theta + m_\alpha(\varepsilon)^{-1}\Theta,$$

where

$$n_\alpha = a^2 + c^2 - 2ab - 2ac + ad + bc - bd - 2cd,$$

and

$$m_\alpha = b^2 + d^2 + 2ab + ac + bd + 2cd.$$

Proof. We will first write $\alpha = \sum_{i=1}^{4} m_i\zeta^{i-1}$. Since $(\pm\zeta^i)^{-1}\Theta \sim \Theta$,

(i) $$D_\Theta(\zeta^i, \zeta^i) = (2\zeta)^{-1}\Theta - 2(\zeta)^{-1}\Theta \sim 2\Theta \quad \text{by (2.5)},$$

(ii) $$\begin{aligned} D_\Theta(\zeta, \zeta^2) = D_\Theta(\zeta^2, \zeta^3) = D_\Theta(1, \zeta) &= (1+\zeta)^{-1}\Theta - (\zeta)^{-1}\Theta - \Theta \\ &= (-\zeta^2 - \zeta^3)^{-1}\Theta - 2\Theta = (\varepsilon)^{-1}\Theta - 2\Theta, \end{aligned}$$

and

(iii) $$\begin{aligned} D_\Theta(1, \zeta^2) = D_\Theta(1, \zeta^3) &= D_\Theta(\zeta, \zeta^3) \\ &= (\zeta + \zeta^4)^{-1}\Theta - (\zeta)^{-1}\Theta - (\zeta^4)^{-1}\Theta = (\varepsilon - 1)^{-1}\Theta - 2\Theta. \end{aligned}$$

Note that, by (2.4) and (2.5),

$$(\varepsilon - 1)^{-1}\Theta = 2(\varepsilon)^{-1}\Theta + 2\Theta - (\varepsilon^2)^{-1}\Theta \sim 3\Theta - (\varepsilon)^{-1}\Theta.$$

So piecing together (i), (ii) and (iii) and using (2.7) yields

$$\begin{aligned} \left(\sum_{l=1}^{4} m_i\zeta^{i-1}\right)^{-1}\Theta = (m_1^2 &+ m_2^2 + m_3^2 + m_4^2 + m_1m_3 + m_1m_4 \\ &+ m_2m_4 - 2m_1m_2 - 2m_2m_3 - 2m_3m_4)\Theta \\ &+ (m_1m_2 + m_2m_3 + m_3m_4 - m_1m_3 - m_1m_4 - m_2m_4)(\varepsilon)^{-1}\Theta. \end{aligned}$$

The proposition follows immediately from setting

$$m_1 = a + d, \quad m_2 = c + d, \quad m_3 = d - b, \quad \text{and} \quad m_4 = -b.$$

3. *The induction*

In the last section we showed that for any $\alpha \in \mathbb{Z}[\zeta]$, there are integers n_α, m_α such that

$$\phi_\alpha = \frac{\sigma(\alpha z)}{\sigma(z)^{n_\alpha}(-\sigma(\varepsilon z))^{m_\alpha}}$$

has the divisor of a function on J. *A priori*, $\phi_\alpha(z)$ might differ from a function on J by multiplication by a trivial theta function $e^{Q(z)+\Lambda(z)+\Gamma}$, where $Q(z)$ and $\Lambda(z)$ are quadratic and linear forms in z, and Γ is a constant. Likewise, $\sigma(z)$ and $\sigma(\zeta z)$ differ by multiplication by $e^{q(z)+\lambda(z)+\gamma}$ where q, λ, and γ are quadratic, linear, and constant, respectively. Since σ is odd, $\Lambda = \lambda = 0$. Since X_{11}, X_{12}, X_{22} are all eigenfunctions for the action of ζ, $q = 0$, and comparing Taylor expansions shows that $\sigma(\zeta z) = \zeta\sigma(z)$. Applying this to $\phi(\zeta z)/\phi(z)$ shows that $Q = 0$, so $\phi_\alpha(z)$ is a function on J. This function has a pole on Θ, but if we set $\psi_\alpha = \phi_\alpha / X_{22}^{(n_\alpha)/2}$ when n_α is even, and $\psi_\alpha = \phi_\alpha / X_{222}(X_{22})^{(n_\alpha - 3)/2}$ when n_α is odd, we find for $z \in \Theta$ that

$$\psi_\alpha(z) = \frac{\sigma(\alpha z)}{\sigma_2(z)^{n_\alpha}(-\sigma(\varepsilon z))^{m_\alpha}} \tag{3.1}$$

is a function on Θ. We will take (3.1) as the definition of $\psi_\alpha(z)$, and think of it as a function on C. Note that for z on Θ, $\varepsilon z \in \Theta$ only when $(\zeta^2 + \zeta^3)z \in \Theta$, which by the results of § 1, is when $z = O$. Likewise $\sigma_2(z) = 0$ precisely when $z = O$. Therefore, by (1.4) and (1.5),

$$\psi_\alpha(z) = \frac{\frac{1}{3}(\alpha - \sigma(\alpha)^3)z_2^3 + \dots}{(-z_2^2)^{n_\alpha}(-\frac{1}{3}(\varepsilon - \sigma(\varepsilon)^3)z_2^3)^{m_\alpha}} = \frac{\frac{1}{3}(\alpha - \sigma(\alpha)^3)}{(-1)^{n_\alpha}(\sigma(\varepsilon))^{m_\alpha}} z_2^{3-2n_\alpha-3m_\alpha} + \dots \quad (3.2)$$

is the Taylor expansion of a polynomial in x and y. Recall that

$$\alpha P = \alpha((0, \tfrac{1}{2}) - \infty) \in \Theta$$

precisely when $\alpha \equiv -1, 0, 1 \bmod (1 - \zeta)$.

LEMMA 2.
(a) $\psi_{\pm\zeta^i\alpha} = \pm\zeta^i\psi_\alpha$, *for* $i \in \mathbb{Z}$.
(b) $\psi_2(P) = 1$.
(c) $\psi_\varepsilon = -1$.
(d) $\psi_{\varepsilon-1} = 1$.
(e) $\psi_3(P) = -1$.
(f) $\psi_{1+\zeta^i} = \zeta^{3i}$, *for* $i \in \mathbb{Z}$.
(g) $\psi_{2+\zeta^i}(P) = -\zeta^{2i}$, *for* $i \in \mathbb{Z}$.

Proof. (a) Since $(\pm\zeta^i)(\alpha)^{-1}\Theta = (\alpha)^{-1}(\Theta)$, we see from the expansion (1.4) and from the CM-type that $\psi_{\pm\zeta^i\alpha}/\psi_\alpha = \sigma(\pm\zeta^i\alpha)/\sigma(\alpha) = \pm\zeta^i$.

(b) By Proposition 2, $\psi_2(z) = \sigma(2z)/\sigma_2(z)^4 = (-2/z_2^5) + \dots$ by (3.2). Since $\psi_2(z)$ is a polynomial in x and y, $\psi_2(z) = 2y$. Hence $\psi_2(P) = 1$.

(c) By Proposition 2, $\psi_\varepsilon(z) = \sigma(\varepsilon z)/-\sigma(\varepsilon z) = -1$.

(d) By Proposition 2, $\psi_{\varepsilon-1}(z) = \sigma((\varepsilon - 1)z)(-\sigma(\varepsilon z))/\sigma_2(z)^3 = 1 + \dots$ by (3.2). Since it is a polynomial in x and y, $\psi_{\varepsilon-1}(z) = 1$.

(e) By Proposition 2, $\psi_3(z) = \sigma(3z)/\sigma_2(z)^9 = (8/z_2^{15}) + \dots$ by (3.2). Since for $z \in \Theta$, $3z \in \Theta$ only when $z \in J[2]$, we have $\psi_3(z) = (\text{constant})y\prod_{j=1}^5 (x - a_j)^{n_j}$ where $n_j \in \mathbb{Z}^+$, and a_j is a root of $x^5 + \frac{1}{4} = 0$. Since the divisor of $\psi_3(z)$ is invariant under the action of ζ, we must have $\psi_3(z) = -8y^3$, which is -1 when $y = \frac{1}{2}$.

(f) When $i \equiv 0 \bmod 5$, this is just (b). When $i \equiv 1 \bmod 5$ we compute

$$\psi_{1+\zeta} = -\zeta^3\psi_{-\zeta^2-\zeta^3} = -\zeta^3\psi_\varepsilon = \zeta^3$$

by (a) and (c). Likewise when $i \equiv 2 \bmod 5$,

$$\psi_{1+\zeta^2} = \zeta\psi_{\zeta+\zeta^4} = \zeta\psi_{\varepsilon-1} = \zeta$$

by (a) and (d). Finally, for $i \equiv 3$ or $4 \bmod 5$, we use (a) and the fact that $1 + \zeta^3 = \zeta^3(1 + \zeta^2)$ and that $(1 + \zeta^4) = \zeta^4(1 + \zeta)$.

(g) When $i \equiv 0 \bmod 5$, this is just (e). For $i \equiv 1, 4 \bmod 5$, we find by Proposition 2 that

$$\psi_{2+\zeta^i}(z) = \frac{\sigma((2 + \zeta^i)z)}{\sigma_2(z)(-\sigma(\varepsilon z))^2} = \frac{2\zeta^{2i}}{z_2^5} + \dots \quad \text{by (3.2).}$$

So $\psi_{2+\zeta^i}(z) = -2\zeta^{2i}y$, which is $-\zeta^{2i}$ when $y = \frac{1}{2}$. For $i \equiv 2, 3 \bmod 5$, we find by Proposition 2 that

$$\psi_{2+\zeta^i}(z) = \frac{\sigma((2 + \zeta^i)z)(-\sigma(\varepsilon z))^2}{(\sigma_2(z))^7} = \frac{2\zeta^{2i}}{z_2^5} + \dots \quad \text{by (3.2).}$$

Again $\psi_{2+\zeta^i}(P) = -\zeta^{2i}$.

LEMMA 3. *Suppose $\alpha \equiv 2 \bmod (1-\zeta)$. Then for all $i \in \mathbb{Z}$,*

$$\frac{\psi_{\alpha+(1-\zeta^i)}(P)\psi_{\alpha-(1-\zeta^i)}(P)}{\psi_\alpha^2(P)} = -\psi_{3-\zeta^i}(P)\psi_{-1-\zeta^i}(P).$$

Proof. Assume for the moment only that $\alpha, \beta \in \mathbb{Z}[\zeta]$. Then for $z \in \Theta$, (2.5) and (1.6) imply that

$$\begin{aligned}\frac{\psi_{\alpha+\beta}(z)\psi_{\alpha-\beta}(z)}{\psi_\alpha^2(z)\psi_\beta^2(z)} &= \frac{\sigma((\alpha+\beta)z)\sigma((\alpha-\beta)z)}{\sigma(\alpha z)^2\sigma(\beta z)^2} \\ &= X_{11}(\beta z) - X_{11}(\alpha z) + X_{12}(\beta z)X_{22}(\alpha z) - X_{12}(\alpha z)X_{22}(\beta z).\end{aligned}$$

Using this three times we get

$$\begin{aligned}\frac{\psi_{\alpha+\beta}(z)\psi_{\alpha-\beta}(z)}{\psi_\alpha^2(z)\psi_\beta^2(z)} - \frac{\psi_{\alpha+2}(z)\psi_{\alpha-2}(z)}{\psi_\alpha^2(z)\psi_2^2(z)} + \frac{\psi_{\beta+2}(z)\psi_{\beta-2}(z)}{\psi_\beta^2(z)\psi_2^2(z)} \\ = X_{12}(\beta z)X_{22}(\alpha z) - X_{12}(\alpha z)X_{22}(\beta z) \\ + X_{12}(\alpha z)X_{22}(2z) - X_{12}(2z)X_{22}(\alpha z) \\ + X_{12}(2z)X_{22}(\beta z) - X_{12}(\beta z)X_{22}(2z).\end{aligned} \tag{3.3}$$

Multiplying (3.3) by $\psi_\alpha^2(z)\psi_\beta^2(z)$ gives a function which is regular at $z = P$. Using (1.2), we see that the right-hand side is zero at P if $\beta \equiv 0 \bmod (1-\zeta)$, since $X_{12}(2P) = X_{22}(2P) = 0$ and $\sigma(\beta P) = \sigma_2(\beta P) = 0$. Hence when $\beta \equiv 0 \bmod (1-\zeta)$,

$$\psi_{\alpha+\beta}(P)\psi_{\alpha-\beta}(P) - \frac{\psi_{\alpha+2}(P)\psi_{\alpha-2}(P)\psi_\beta^2(P)}{\psi_2^2(P)} = \frac{-\psi_{\beta+2}(P)\psi_{\beta-2}(P)\psi_\alpha^2(P)}{\psi_2^2(P)}.$$

But $\psi_2(P) = 1$, $\psi_\beta(P) = 0$, and the lemma follows by taking $\beta = 1 - \zeta^i$.

COROLLARY 1. *We have $\psi_{3-\zeta^i}(P) = \zeta^{2i}$, whence*

$$\psi_{\alpha+(1-\zeta^i)}(P)\psi_{\alpha-(1-\zeta^i)}(P) = \psi_\alpha^2(P).$$

Proof. Plugging $\alpha = 1 + \zeta^i$ into Lemma 3 yields

$$\frac{\psi_2(P)\psi_{2\zeta^i}(P)}{\psi_{1+\zeta^i}^2(P)} = -\psi_{3-\zeta^i}(P)\psi_{-1-\zeta^i}(P),$$

so the result follows immediately from Lemma 2, (a), (b) and (f).

PROPOSITION 3. *Let $\alpha \equiv 2 + i(1-\zeta) \bmod (1-\zeta^2)$. Then $\psi_\alpha(p) = \zeta^{2i}$. Equivalently, $\psi_{-\alpha}(P) = -\zeta^{2i}$.*

Proof. Our proof will be in two steps.

Step 1. *If the proposition holds for α and $\alpha - (1-\zeta^j)$, then it holds for $\alpha + (1-\zeta^j)$.*

Proof. Taking $j \geqslant 1$ we compute

$$\begin{aligned}\alpha-(1-\zeta^j) &\equiv 2+i(1-\zeta)-(1-\zeta^j) \mod (1-\zeta)^2\\ &\equiv 2+i(1-\zeta)-(1-\zeta)(1+\ldots+\zeta^{j-1}) \mod (1-\zeta)^2\\ &\equiv 2+(i-j)(1-\zeta) \mod (1-\zeta)^2,\end{aligned}$$

and

$$\alpha+(1-\zeta^j) \equiv 2+(i+j)(1-\zeta) \mod (1-\zeta)^2.$$

Therefore, by Corollary 1,

$$\psi_{\alpha+(1-\zeta^j)}(P)=\frac{\psi_\alpha^2(P)}{\psi_{\alpha-(1-\zeta^j)}(P)}=\frac{(\zeta^{2i})^2}{\zeta^{2(i-j)}}=\zeta^{2(i+j)},$$

as desired.

Step 2. *Let* $\alpha=2+(1-\zeta)(a+b(1+\zeta)+c(1+\zeta+\zeta^2)+d(1+\zeta+\zeta^2+\zeta^3))$. *Then the proposition holds for all choices of* $a, b, c, d \in \{0, -1\}$.

Proof. We compute the proposed value of $\psi_\alpha(P)=\zeta^{2(a+2b+3c+4d)}$. The results are shown in Table 1. These sixteen cases all follow from Lemma 2, applying (a) to (b), (e), (f) and (g).

TABLE 1

a	b	c	d	α	$\zeta^{2(a+2b+3c+4d)}$
0	0	0	0	2	1
0	0	0	−1	$1+\zeta^4$	ζ^2
0	0	−1	0	$1+\zeta^3$	ζ^4
0	0	−1	−1	$\zeta^3+\zeta^4$	ζ
0	−1	0	0	$1+\zeta^2$	ζ
0	−1	0	−1	$\zeta^2+\zeta^4$	ζ^3
0	−1	−1	0	$\zeta^2+\zeta^3$	1
0	−1	−1	−1	$-2-\zeta$	ζ^2
−1	0	0	0	$1+\zeta$	ζ^3
−1	0	0	−1	$\zeta+\zeta^4$	1
−1	0	−1	0	$\zeta+\zeta^3$	ζ^2
−1	0	−1	−1	$-2-\zeta^2$	ζ^4
−1	−1	0	0	$\zeta+\zeta^2$	ζ^4
−1	−1	0	−1	$-2-\zeta^3$	ζ
−1	−1	−1	0	$-2-\zeta^4$	ζ^3
−1	−1	−1	−1	−3	1

Proof of Proposition 3. The proof follows directly from Steps 1 and 2, once we observe that adding $1-\zeta^j$ to α for $j=1, 2, 3, 4$ increments a, b, c, d, respectively, by 1.

4. *Proof of the theorem*

Let $\beta \in \mathbb{Z}[\zeta]$ so that $\beta \equiv \pm 1 \bmod (1-\zeta)^2$. Then $\sigma^{-1}(\beta) \equiv \pm 1 \bmod (1-\zeta)^2$ and $\beta\sigma^{-1}(\beta) \equiv 1 \bmod (1-\zeta)^2$.

Note that $X(\beta\sigma^{-1}(\beta)z)$ is a function on J, and by (1.2), (1.3) and (3.1), for

$z \in \Theta$, $(\psi_{\beta\sigma^{-1}(\beta)}(z))^3 X(\beta\sigma^{-1}(\beta)z)$ is a function on C, with poles only at $z = O$; hence it is a polynomial in x and y. We use the Taylor expansion to compute the lead term:

$$X(\beta\sigma^{-1}(\beta)z)(\psi_{\beta\sigma^{-1}(\beta)}(z))^3 = \frac{\sigma(\beta\sigma^{-1}(\beta)z)^3 X(\beta\sigma^{-1}(\beta)z)}{\sigma_2(z)^{3\mathbb{N}_{K/\mathbb{Q}}(\beta)}} \quad \text{(by (2.2))}$$
$$= \frac{(-1)^{3\mathbb{N}_{K/\mathbb{Q}}(\beta)}\beta\sigma(\beta)}{z_2^{6\mathbb{N}_{K/\mathbb{Q}}(\beta)-1}} + \dots,$$

because of the CM-type of J. Hence

$$X(\beta\sigma^{-1}(\beta)z)(\psi_{\beta\sigma^{-1}(\beta)}(z))^3 = (-1)^{\mathbb{N}_{K/\mathbb{Q}}(\beta)-1}\beta\sigma(\beta)yx^{3\mathbb{N}_{K/\mathbb{Q}}(\beta)-3} + \dots$$
$$= (-1)^{\mathbb{N}_{K/\mathbb{Q}}(\beta)-1}\beta\sigma(\beta)y \prod_{\substack{z\in\Theta\cap(\beta\sigma^{-1}(\beta))^{-1}(X)_0/\pm 1 \\ z\notin J[2]}} (x - x(z)).$$

So plugging in $z = P$ yields

$$X(\beta\sigma^{-1}(\beta)z)(\psi_{\beta\sigma^{-1}(\beta)}(z))^3|_{z=P} = \tfrac{1}{2}\beta\sigma(\beta) \prod_{\substack{z\in\Theta\cap(\beta\sigma^{-1}(\beta))^{-1}(X)_0/\pm 1 \\ z\notin J[2]}} x(z). \tag{4.1}$$

But since $\beta\sigma^{-1}(\beta) \equiv 1 \bmod (1-\zeta)$, Proposition 1 and (2.6) give

$$(\psi_{\beta\sigma^{-1}(\beta)}(z))^3 X(\beta(\sigma^{-1}(\beta))z)|_{z=P}$$
$$= \frac{1}{2}\frac{\sigma((\beta\sigma^{-1}(\beta)+1)P)\sigma((\beta\sigma^{-1}(\beta)+2)P)\sigma((\beta\sigma^{-1}(\beta)-3)P)}{\sigma_2(P)^{3\mathbb{N}_{K/\mathbb{Q}}(\beta)+1}\sigma(2P)\sigma(-3P)}$$
$$= \frac{1}{2}\frac{\psi_{\beta\sigma^{-1}(\beta)+1}(P)\psi_{\beta\sigma^{-1}(\beta)+2}(P)\psi_{\beta\sigma^{-1}(\beta)-3}(P)}{\psi_2(P)\psi_{-3}(P)}. \tag{4.2}$$

Now by Proposition 3, $\psi_{\beta\sigma^{-1}(\beta)+1}(P) = 1$, and $\psi_{\beta\sigma^{-1}(\beta)+2}(P) = \psi_{\beta\sigma^{-1}(\beta)-3}(P) = -1$. Likewise, $\psi_2(P) = \psi_{-3}(P) = 1$. So combining (4.1) and (4.2) gives

$$\beta\sigma(\beta) \prod_{\substack{z\in\Theta\cap(\beta\sigma^{-1}(\beta))^{-1}(X)_0/\pm 1 \\ x\notin J[2]}} x(z) = 1,$$

which proves the theorem.

Remark. In the theorem we are taking the product over the zero cycle $\Theta \cap (\beta\sigma^{-1}(\beta))^{-1}(X)_0 - J[2]$ accounting for intersection multiplicities. Implicitly, we are using the fact that there are six points in the support of $J[2] \cap \Theta$, the origin O and the images e_i of the five points $(a_i, 0)$ on C, and that each of the six points appears with multiplicity 1. This can be verified using the definitions of Θ and $(X)_0$ in terms of sigma functions. Moreover, we claim that when β is a prime not dividing 10, the support of the zero-cycle contains $6(\mathbb{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\beta) - 1)$ points, each with multiplicity 1, and one-sixth of the points lie in $J_0(\beta)$. Indeed, the intersection number can be computed by noting that $(X)_0 \sim 3\Theta$, $(\beta\sigma^{-1}(\beta))^{-1}\Theta \sim \mathbb{N}_{K/\mathbb{Q}}(\beta)\Theta$, and that the self-intersection number of Θ is 2. To compute the multiplicities, note that $z \in (\beta\sigma^{-1}(\beta))^{-1}(X)_0 \cap \Theta$ precisely when

$$\beta\sigma^{-1}(\beta)z \in (X)_0 \quad \text{and} \quad z \in \Theta,$$

and by the theory of complex multiplication [6, p. 86, Theorem 1.2], when β is prime this implies that

$$\mathrm{Fr}_\beta(z) \in (X)_0 \quad \text{and} \quad z \in \Theta \mod \beta,$$

or that

$$z \in (X)_0 \cap \Theta \mod \beta,$$

where Fr_β is the Frobenius mod β. Since $-X/X_{222}$ restricts to y on Θ, $(X)_0 \cap \Theta$ consists of O and $e_1, \ldots, e_5$. Using formal groups [4] it is possible to show that there are $\mathbb{N}_{K/\mathbb{Q}}(\beta)$ distinct points in the support of $(\beta\sigma^{-1}(\beta))^{-1}(X)_0 \cap \Theta$ which reduce to each of O, e_1, e_2, e_3, e_4 or e_5 mod β.

References

1. J. W. S. Cassels, 'On Kummer sums', *Proc. London Math. Soc.* (3) 21 (1970) 19–27.
2. J. Coates and A. Wiles, 'On the conjecture of Birch and Swinnerton-Dyer', *Invent. Math.* 39 (1977) 223–251.
3. E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication*, Perspectives in Mathematics 3 (Academic Press, Orlando, 1987).
4. D. Grant, 'Formal groups in genus two', *J. reine angew. Math.*, to appear.
5. T. Kubota, 'An application of power residue theory to some Abelian functions', *Nagoya Math. J.* 27 (1966) 51–54.
6. S. Lang, *Complex multiplication* (Springer, New York, 1983).
7. S. Lang, *Abelian varieties* (Interscience, New York, 1959).
8. C. R. Matthews, 'Gauss sums and elliptic functions: I. the Kummer sum', *Invent. Math.* 52 (1979) 163–185.
9. K. Ramachandra, 'Some applications of Kronecker's limit formulas', *Ann. of Math.* 80 (1964) 104–148.
10. G. Robert, 'Unités elliptiques', *Bull. Soc. Math. France. Mémoire* 36 (1973).
11. K. Rubin, 'Tate–Shafarevich groups and L-functions of elliptic curves with complex multiplication', *Invent. Math.* 89 (1987) 527–560.
12. K. Rubin, 'The main conjecture', *Cyclotomic fields I and II* (S. Lang), Graduate Texts in Mathematics 121 (Springer, New York, 1990), appendix.
13. C. L. Siegel, *Lectures on advanced analytic number theory* (Tata Institute of Fundamental Research, Bombay, 1961).
14. H. Stark, 'L-function at $s = 1$. IV. First derivatives at $s = 0$', *Adv. in Math.* 35, No. 3 (1980) 197–235.

Department of Mathematics
University of Colorado at Boulder
Boulder
Colorado 80309
U.S.A.

E-mail: grant@boulder.colorado.edu