ACTA ARITHMETICA
LXXV.4 (1996)

A proof of quintic reciprocity using the arithmetic of $y^2 = x^5 + 1/4$

by

David Grant (Boulder, Colo.)

0. Introduction. Elliptic curves have long been used as tools to prove reciprocity laws. Eisenstein employed elliptic functions to prove cubic, biquadratic, and octic reciprocity laws (we refer the reader to Cassels [C], Hilbert [H], Weil [W1, W2, W3], and Ireland–Rosen [IrR] for references to this work, work by Kummer, and related work by other 19th century mathematicians). Fueter [F] in 1927 proved quadratic reciprocity over all imaginary quadratic fields using the theory of complex multiplication of elliptic curves, and in 1961 Kubota derived cubic and biquadratic reciprocity from the theory of complex multiplication as well [K1].

Kubota's and Eisenstein's proofs of cubic and biquadratic reciprocity both used (in some guise) the distribution relation of genus one theta functions that is crucial to the construction of elliptic units.

In this paper we continue the theme, deriving the quintic reciprocity law (due first to Kummer) from the main theorems of complex multiplication of abelian varieties applied to the Jacobian J of the curve $C : y^2 = x^5 + 1/4$. Due to the lack of a distribution relation for higher genus theta functions, little progress has been made in generalizing elliptic units to genus 2 curves [BaBo, BoBa, Gra1, Gra2, Gra3]. However, the theorems of complex multiplication and the formal group at the origin of the Jacobian allow us to evaluate products of a function evaluated at torsion points up to fifth powers, which is insufficient for constructing units, but is sufficient for deriving a reciprocity law. Our proof was inspired by Kubota, who in [K2] derived facts about products of functions of torsion points via reciprocity, and we reverse his argument. Let ζ denote a primitive fifth root of 1. Our proof involves studying Kummer extensions of $\mathbb{Q}(\zeta)$ contained in division fields of J, and, as in [K1], uses "Gauss' Lemma" to obtain the reciprocity law.

Partially supported by NSF grant DMS-9303220.

In a paper where the main theorem is approaching its sesquicentennial, it is not surprising that several of the lemmas are not new. We prove what we easily can afresh, keeping our proof independent of more sophisticated techniques. We hope the present work can be considered a small contribution to the spirit of the *Jugendtraum*, and a demonstration of the growing utility of the arithmetic of curves of genus 2.

Despite the fact that the ℓth power reciprocity law was proved by Kummer for regular primes ℓ, and was completely proved by Fürtwangler (and that today it is a simple consequence of Artin reciprocity), it would be nice to know whether other power reciprocity laws can be derived from the arithmetic of rational images of Fermat curves. Shimura and Taniyama showed that a special case of Stickelberger's relation on ideal class groups can be derived as a consequence of the theory of complex multiplication applied to the Jacobians of these curves [ST, pp. 129–130].

In Section 1 we gather facts about $\mathbb{Q}(\zeta)$, and state the reciprocity law. In Section 2 we study the curve C and its Jacobian, recall facts from the theory of complex multiplication of abelian varieties, and prove a bevy of lemmas. In Section 3 we prove the reciprocity law.

1. Statement of the Theorem. Throughout we let ζ denote a primitive fifth root of unity, and $K = \mathbb{Q}(\zeta)$. Then $(\zeta - \zeta^2 - \zeta^3 + \zeta^4)^2 = 5$, so we will set $\sqrt{5} = (\zeta - \zeta^2 - \zeta^3 + \zeta^4)$. The ring of integers $\mathcal{O} = \mathbb{Z}[\zeta]$ of K is a unique factorization domain, and its units are all of the form $\pm\zeta^i\varepsilon^j$, for integers i, j, where

$$\varepsilon = -\zeta^2 - \zeta^3 = \frac{1+\sqrt{5}}{2}$$

is a fundamental unit in $\mathbb{Q}(\sqrt{5})$. For $i \in \mathbb{Z}$ prime to 5, we let σ_i denote the element of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma_i(\zeta) = \zeta^i$. If π is a prime of $\mathcal{O}$, we let $\mathcal{O}_\pi$ denote the completion of $\mathcal{O}$ at π, and K_π the fraction field of $\mathcal{O}_\pi$. We let $\lambda = 1 - \zeta$. Then λ generates the lone prime of $\mathcal{O}$ above 5, and a computation shows

$$\varepsilon \equiv 3 \bmod \lambda, \quad -\varepsilon^2 \equiv 1 - \lambda^2 \bmod \lambda^3. \tag{1}$$

Remark. That $-\varepsilon^2$ should have such an expansion is part of a general phenomenon for units in the ℓth cyclotomic field when ℓ is a regular prime (see [H, Lemma 29]).

Lemma 1. (a) *If $\alpha \in \mathcal{O}$ is prime to λ, then there is an associate α' of α such that $\alpha' \equiv 1 \bmod \lambda^3$.*

(b) *If α' and α'' are two associates $\equiv 1 \bmod \lambda^3$, their ratio is a fifth power of a unit in $\mathcal{O}$.*

(c) *Let $n \in \mathbb{Z}$ be prime to 5. Then any associate n^* of n with $n^* \equiv 1 \bmod \lambda^3$ is n times a fifth power of a unit in $\mathcal{O}$.*

P r o o f. (a) By (1), for some $0 \le i, j \le 1$, $(-1)^i \varepsilon^j \alpha \equiv 1 \bmod \lambda$. Then for some $0 \le k \le 4$, $\zeta^k (-1)^i \varepsilon^j \alpha \equiv 1 \bmod \lambda^2$. From (1) again we see that for some $0 \le l \le 4$, $\alpha' = \zeta^k (-1)^{i+l} \varepsilon^{j+2l} \alpha \equiv 1 \bmod \lambda^3$.

(b) If α' and α'' are two such associates, their ratio is a unit, and hence of the form

$$(-1)^{i+l+m} \zeta^k \varepsilon^{j+2l+10m} = (-1)^i \varepsilon^j \zeta^k (-\varepsilon^2)^l (-\varepsilon^{10})^m \tag{2}$$

for some $0 \le i, j \le 1$, $0 \le k, l \le 4$ and $m \in \mathbb{Z}$. Since the ratio is congruent to 1 mod λ^3, and $-\varepsilon^{10} \equiv 1 \bmod \lambda^3$, considering (2) sequentially mod λ, λ^2, and λ^3, and applying (1) gives in turn that $i = j = 0$, that $k = 0$, and that $l = 0$. Hence the ratio of the associates is a tenth power of a unit, so *a fortiori* a fifth power.

(c) Since $n^4 \equiv 1 \bmod 5$, and $(n^*)^4 \equiv 1 \bmod \lambda^3$ is an associate of n^4, by (b), $(n/n^*)^4$ is the fifth power of a unit, so dividing by $(n/n^*)^5$ shows that (n^*/n) is the fifth power of a unit.

R e m a r k. The lemma is a special case of a general pattern for integers in the ℓth cyclotomic field when ℓ is a regular prime. Compare (a) to the proof of Theorem 157 in [H] and (b) to the proof of Theorem 156 in [H].

Given Lemma 1, we can make the following conventions: If π (or any Greek letter) is a prime of $\mathcal{O}$ prime to λ, then we always assume that $\pi \equiv 1 \bmod \lambda^3$. We will set $\pi_i = \sigma_i(\pi)$, for $i \in \mathbb{Z}$ prime to 5, and so $\pi_i \equiv 1 \bmod \lambda^3$ and $\pi = \pi_1$. Note that if π is a second degree prime, then by Lemma 1(b), π_1 and π_4 differ by a fifth power, as do π_2 and π_3. If $p \in \mathbb{Z}$ is a fourth degree prime on $\mathcal{O}$, we will let p^* denote an associate of p such that $p^* \equiv 1 \bmod \lambda^3$. By Lemma 1(c), p and p^* differ by a fifth power.

If $\wp = (\pi)$ is a prime of $\mathcal{O}$ prime to λ, and $\alpha \in \mathcal{O}$ is prime to $\wp$, we define the quintic power residue symbol

$$\left(\frac{\alpha}{\wp}\right) = \left(\frac{\alpha}{\pi}\right)$$

to be the fifth root of unity such that

$$\left(\frac{\alpha}{\pi}\right) = \alpha^{(N(\pi)-1)/5} \bmod \pi,$$

where N is the absolute norm. The symbol is extended to non-prime ideals by the rule

$$\left(\frac{\alpha}{\mathcal{P}\mathcal{Q}}\right) = \left(\frac{\alpha}{\mathcal{P}}\right)\left(\frac{\alpha}{\mathcal{Q}}\right),$$

for ideals $\mathcal{P}, \mathcal{Q}$ prime to λ, and α prime to $\mathcal{P}\mathcal{Q}$.

We can now state the laws of quintic reciprocity.

THEOREM (Kummer). *Main Law of Quintic Reciprocity*: *If π and ν are non-associate primes of $\mathcal{O}$, both congruent to* $1 \bmod \lambda^3$, *then*

$$\left(\frac{\nu}{\pi}\right) = \left(\frac{\pi}{\nu}\right).$$

Complementary Laws: *If π is a prime of $\mathcal{O}$ with a λ-adic expansion*

$$\pi \equiv 1 + a\lambda^3 + b\lambda^4 + c\lambda^5 \bmod \lambda^6,$$

with $a, b, c \in \mathbb{Z}/5\mathbb{Z}$, then

$$\text{(i)} \qquad \left(\frac{\zeta}{\pi}\right) = \zeta^{a+b},$$

$$\text{(ii)} \qquad \left(\frac{\varepsilon}{\pi}\right) = \zeta^{a},$$

$$\text{(iii)} \qquad \left(\frac{\lambda}{\pi}\right) = \zeta^{-c}.$$

Remark. This is certainly not the standard way now to state quintic reciprocity, but it is akin to the classical form of Kummer reciprocity with the complementary laws worked out explicitly (see [H, Theorem 161]). It is not hard to verify that it is equivalent to the law as given by Artin and Hasse, and stated in [AT, pp. 172–173].

2. The curve and its Jacobian. Let C be the curve of genus 2 defined by

$$y^2 = x^5 + 1/4. \tag{3}$$

We let ∞ denote the lone point at infinity on the normalization of this model. The hyperelliptic involution I is given on this model by $I(x, y) = (x, -y)$. There is an embedding i of the group $\mu_5 = \langle\zeta\rangle$ into the automorphism group of C given by $i(\zeta) = [\zeta]$, where $[\zeta](x, y) = (\zeta x, y)$.

Let $M = K(\sqrt[5]{2})$. Then the field $L = M(\sqrt{\lambda})$ is totally ramified over (λ) since it is the compositum of M and $K(\sqrt{\lambda})$, which are extensions of K of relatively prime degree and which are both totally ramified over (λ). Let $\mathcal{O}_L$ be the ring of integers of L, Λ the lone prime of $\mathcal{O}_L$ above (λ), and ℓ the restriction of Λ to M.

LEMMA 2. *The curve C has good reduction at all primes of $\mathcal{O}$ prime to λ. It obtains good reduction everywhere over L.*

Proof. The model (3) has good reduction at all primes of $\mathcal{O}$ except 2 and (λ). Letting $x = X$, $y = Y + 1/2$ gives us the model

$$Y^2 + Y = X^5,$$

which has good reduction at 2. We now only have to show that over L, C has a model with good reduction at Λ. Substituting $x = \lambda X - \sqrt[5]{1/4}$, $y = \lambda^{5/2} Y$ into (3) gives us the model

$$\begin{aligned}(4)\quad Y^2 &= X(X - \sqrt[5]{1/4})(X - (1+\zeta)\sqrt[5]{1/4})(X - (1+\zeta+\zeta^2)\sqrt[5]{1/4}) \\ &\quad \times (X - (1+\zeta+\zeta^2+\zeta^3)\sqrt[5]{1/4})\end{aligned}$$

which has good reduction at Λ.

Let J be the Jacobian of C. Then there is an injection $\phi : C \to J$, given by

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

where cl denotes the divisor class map. The image of ϕ is a divisor Θ on J. By the Riemann–Roch theorem, every point other than the origin on J can be represented uniquely by a divisor of the form

$$P_1 + P_2 - 2\infty, \qquad P_2 \neq I(P_1),$$

for an unordered pair of points $\{P_1, P_2\}$ on C. As a consequence, J is birationally equivalent to the symmetric product $C^{(2)}$, so functions on J can be written as symmetric functions of a pair of points $P_i = (x_i, y_i)$, $i = 1, 2$, on C.

When the characteristic of our base field is not 2, we will take the model for J described in [Gra4]. The divisor 3Θ is very ample, so the 9-dimensional complete linear system $L(3\Theta)$ defines an embedding of J into $\mathbb{P}^8$. A basis for $L(2\Theta)$ is given by 1 and the even functions

$$\begin{aligned}(5)\qquad X_{22} &= x_1 + x_2, \qquad X_{12} = -x_1 x_2, \\ X_{11} &= \frac{(x_1 x_2)^2 (x_1 + x_2) + \frac{1}{2} - 2y_1 y_2}{(x_1 - x_2)^2}.\end{aligned}$$

A basis for $L(3\Theta)$ is then obtained by including the even function

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

and the odd functions

$$\begin{aligned}(6)\qquad X_{222} &= \frac{y_1 - y_2}{x_1 - x_2}, \quad X_{122} = \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2}, \quad X_{112} = \frac{x_2^2 y_1 - x_1^2 y_2}{x_1 - x_2}, \\ X_{111} &= \frac{y_2(3x_1^4 x_2 + x_1^3 x_2^2 + 1) - y_1(3x_2^4 x_1 + x_2^3 x_1^2 + 1)}{(x_1 - x_2)^3}.\end{aligned}$$

The action of μ_5 on C extends naturally to J to give us an embedding $i : \mathcal{O} \to \mathrm{End}(J)$, which we write as $i(\alpha) = [\alpha]$. For any isogeny $[\alpha] \in \mathrm{End}(J)$ we let $J[\alpha]$ denote its kernel. We also let $J[\alpha]'$ denote the non-trivial elements of $J[\alpha]$.

From (5) and (6) we get: $[\zeta]X_{22} = \zeta X_{22}$, $[\zeta]X_{12} = \zeta^2 X_{12}$, $[\zeta]X_{11} = \zeta^3 X_{11}$, $[\zeta]X = \zeta^4 X$, and $[\zeta]X_{111} = \zeta^2 X_{111}$.

In [Gra4] it was shown that

$$t_1 = \frac{-X_{11}}{X_{111}}, \qquad t_2 = \frac{-X}{X_{111}},$$

are odd functions which span the cotangent space of J at the origin, and that if $\pi \in \mathcal{O}$ is any prime of odd residue characteristic, then t_1 and t_2 form a set of parameters for the formal group at the origin defined over the completion $\mathcal{O}_\pi$. Since

$$[\zeta]t_1 = \zeta t_1, \qquad [\zeta]t_2 = \zeta^2 t_2, \tag{7}$$

we find that the CM-type of J is $\Phi = \{\sigma_1, \sigma_2\}$, and that for any $\alpha \in \mathcal{O}$,

$$[\alpha]t_1 = \alpha t_1 + (d^\circ \geq 2), \qquad [\alpha]t_2 = \sigma_2(\alpha)t_2 + (d^\circ \geq 2),$$

as endomorphisms of the formal group, where $(d^\circ \geq n)$ denotes a power series all of whose terms have total degree at least n.

Lemma 3. *For any $\alpha \in \mathcal{O}$,*

$$\begin{aligned}[\alpha]t_1 &= \alpha t_1 - \tfrac{1}{3}(\sigma_2(\alpha)^3 - \alpha)t_2^3 + (d^\circ \geq 4),\\ [\alpha]t_2 &= \sigma_2(\alpha)t_2 + (d^\circ \geq 4).\end{aligned}$$

Proof. The result is trivial for $\alpha = 0$, and follows from (7) for $\alpha = -\zeta$ since both t_1 and t_2 are odd. It now suffices to show that if the lemma holds for both $\alpha, \beta \in \mathcal{O}$, then it holds for both (i) $\alpha+\beta$, and (ii) $\alpha\beta$. We take these in turn. For (i) we need the cubic terms of the expansions of s^*t_i, $i = 1, 2$, where $s : J \times J \to J$ is the group morphism. An algorithm for computing this is given in [Gra4], and was carried out in [Gra2]. The resulting calculation in [Gra2] gives us

$$\begin{aligned}s^*t_1 &= u_1 + v_1 - u_2v_2(u_2 + v_2) + (d^\circ \geq 4),\\ s^*t_2 &= u_2 + v_2 + (d^\circ \geq 4),\end{aligned}$$

where (u_1, v_1) and (u_2, v_2) are corresponding pairs of parameters at the origin on 2 copies of J. So

$$\begin{aligned}[\alpha+\beta]t_1 &= [\alpha]t_1 + [\beta]t_1 - [\alpha]t_2[\beta]t_2([\alpha]t_2 + [\beta]t_2) + (d^\circ \geq 4)\\ &= \alpha t_1 - \tfrac{1}{3}(\sigma_2(\alpha)^3 - \alpha)t_2^3 + \beta t_1 - \tfrac{1}{3}(\sigma_2(\beta)^3 - \beta)t_2^3\\ &\quad - \sigma_2(\alpha)\sigma_2(\beta)\sigma_2(\alpha+\beta)t_2^3 + (d^\circ \geq 4)\\ &= (\alpha+\beta)t_1 - \tfrac{1}{3}(\sigma_2(\alpha+\beta)^3 - (\alpha+\beta))t_2^3,\end{aligned}$$

and

$$[\alpha+\beta]t_2 = [\alpha]t_2 + [\beta]t_2 + (d^\circ \geq 4) = \sigma_2(\alpha)t_2 + \sigma_2(\beta)t_2 + (d^\circ \geq 4),$$

as desired. As for (ii), we note

$$\begin{aligned}[\alpha\beta]t_1 &= [\alpha]([\beta]t_1) = \alpha(\beta t_1 - \tfrac{1}{3}(\sigma_2(\beta)^3 - \beta)t_2^3) \\ &\quad - \tfrac{1}{3}(\sigma_2(\alpha)^3 - \alpha)(\sigma_2(\beta)t_2)^3 + (d^\circ \geq 4) \\ &= \alpha\beta t_1 - \tfrac{1}{3}(\sigma_2(\alpha\beta)^3 - \alpha\beta)t_2^3 + (d^\circ \geq 4),\end{aligned}$$

and

$$[\alpha\beta]t_2 = [\alpha]([\beta]t_2) = \alpha(\beta t_2) + (d^\circ \geq 4).$$

LEMMA 4. (a) *Let π prime to λ be any first or second degree prime of $\mathcal{O}$. Then the only primes of $\mathcal{O}$ which ramify in $K(J[\pi])/K$ are (π_1), (π_2), and (λ).*

(b) *The extension $L(J[\pi])/L$ is unramified at Λ.*

P r o o f. (a) If ν is a prime of $\mathcal{O}$ prime to λ, then by Lemma 2, C and hence J has good reduction at ν. If the action of π on the cotangent space of J at the origin is invertible mod ν, then $[\pi]$ is étale mod ν, and hence ν is unramified in $K(J[\pi])$. From the CM-type we see that the action of $[\pi]$ on the cotangent space is invertible mod ν if (ν) is different from (π_1) and (π_2).

(b) This follows as in (a), since by Lemma 2, J obtains good reduction over L at Λ.

The following lemma is a special case of a general theorem of Greenberg [Gre, Theorem 1]. We give an elementary proof which suffices in our case.

LEMMA 5. *All points of $J[\lambda^3]$ are rational over K.*

P r o o f. We will show that $Q = (1, \sqrt{5}/2) - \infty$, which is rational over K, is a primitive $[\lambda^3]$-torsion point. The theorem then follows because all complex multiplications are defined over K, and $J[\lambda^3]$ is generated as an $\mathcal{O}$-module by Q.

To compute the order of Q, we first note that if $P = (0, 1/2) - \infty$, then $[\zeta]P = P$, so P is a primitive $[\lambda]$-torsion point. It is straightforward to check that the divisor of the function

$$y - (\zeta + 1)x^2 - \zeta^4 x + 1/2$$

on C is

$$I(P) + (1, \sqrt{5}/2) + 2(\zeta, -\sqrt{5}/2) + (\zeta^2, \sqrt{5}/2) - 5\infty,$$

so

$$\begin{aligned}[(1-\zeta)^2]Q &= [1-\zeta]((1, \sqrt{5}/2) + (\zeta, -\sqrt{5}/2) - 2\infty) \\ &= (1, \sqrt{5}/2) + 2(\zeta, -\sqrt{5}/2) + (\zeta^2, \sqrt{5}/2) - 4\infty = P.\end{aligned}$$

So Q is a primitive $[\lambda^3]$-torsion point, as desired.

We will keep the notation $P = (0, 1/2) - \infty$ and $Q = (1, \sqrt{5}/2) - \infty$ throughout.

LEMMA 6. *Let π prime to λ be a prime in $\mathcal{O}$, and $\widetilde{J}$ be the reduction of J mod π. Then $125 \mid \#\widetilde{J}(\mathcal{O}/(\pi))$.*

Proof. This follows directly from Lemma 5: by Lemma 2, J has good reduction at π, so the λ-power torsion remains distinct mod π.

Having found the CM-type of J, we can deduce various consequences of the theory of complex multiplication. We refer the reader to [L] or [Gra5]. Recall that the reflex type of J is $\Phi' = \{\sigma_1^{-1}, \sigma_2^{-1}\} = \{\sigma_1, \sigma_3\}$, and the reflex norm of an element $\alpha \in K$ is $\mathbb{N}_{\Phi'}(\alpha) = \alpha\sigma_3(\alpha)$. From Proposition 1.5 of [Gra5], we know that J is simple. Since Θ defines a polarization over K, and $i(\mathcal{O}) \subseteq \mathrm{End}(J)$ are all defined over K, the triple (J, i, Θ) is defined over K. Then if E is a Riemann form corresponding to Θ, since J is simple, E is necessarily "admissible" in the parlance of complex multiplication. As a consequence (J, i, Θ) is of type $(K, \Phi, \mathcal{O}, E)$ with respect to Θ, so we may apply the main theorems of complex multiplication. In particular, since the full ring of integers $\mathcal{O}$ of K embeds into $\mathrm{End}(J)$, the complex multiplication is "principal," and we can apply Theorems and Corollaries 1.1–1.6 of Chapter 4 of [L].

LEMMA 7. *Let π prime to λ be a prime in $\mathcal{O}$, and $\widetilde{J}$ be the reduction of J mod π. Then the endomorphism $[\pi_1\pi_3]$ induces the Frobenius on $\widetilde{J}$.*

Proof. By Theorem 1.2 on p. 86 of [L], the Frobenius on $\widetilde{J}$ is induced by an endomorphism $[\alpha]$. By Corollary 1.3 on p. 88 of [L], $\alpha = u\mathbb{N}_{\Phi'}(\pi_1)$, where u is a unit of $\mathcal{O}$ of absolute value 1 in every complex embedding, and so is a root of unity. Since $\pi_1\pi_3 \equiv 1 \bmod \lambda^2$, to show $u = 1$ it suffices to show that $\alpha \equiv 1 \bmod \lambda^2$. In fact, $\alpha \equiv 1 \bmod \lambda^3$. Indeed, by Lemma 6, $125 \mid \#\widetilde{J}(\mathcal{O}/(\pi))$, and by Theorem 1.6 on p. 92 of [L], the characteristic polynomial of the Frobenius is $f_\alpha(X) = \prod_{i=1}^{4}(X - \sigma_i(\alpha))$. Then by [M, p. 144], $\#\widetilde{J} = f_\alpha(1) = N(1 - \alpha)$, so we conclude that $\lambda^3 \mid 1 - \alpha$, so $u = 1$.

Remark. It follows from work of Weil that the roots of the characteristic polynomial of Frobenius mod π are given by Jacobi sums [W4], and Iwasawa showed that Jacobi sums are congruent to 1 mod λ^3 ([Iw]). Therefore the only place where we needed the theorems of complex multiplication in the proof of Lemma 7 was to show that the Frobenius mod π was induced by $[\alpha]$ for some $\alpha \in \mathcal{O}$, but this too can be argued directly (see [Gre, pp. 352–353]).

Throughout, for a prime π of $\mathcal{O}$, we will let

$$\delta = \delta(\pi) = \prod_{u \in J[\pi]'} t_1(u).$$

LEMMA 8. *Let π prime to λ be a first or second degree prime in $\mathcal{O}$. Then*

(a) $$\mathrm{ord}_{(\pi_1)}\, \delta = 1,$$

and

$$\text{(b)} \qquad \operatorname{ord}_{(\pi_2)} \delta = 3.$$

P r o o f. (a) The CM-action on the cotangent space at the origin shows that $[\pi_1]$ is not étale mod π_1, so $J[\pi_1]$ is in the kernel of reduction mod π_1. Hence $J[\pi_1]$ corresponds to points in the formal group at the origin. So for any point $u \in J[\pi_1]$, we have that $(t_1(u), t_2(u))$ is a solution of

$$\begin{aligned} 0 &= [\pi_1]t_1 = \pi_1 t_1 + (d^\circ \geq 2), \\ 0 &= [\pi_1]t_2 = \pi_2 t_2 + (d^\circ \geq 2). \end{aligned} \tag{8}$$

Since π is first or second degree, π_2 is invertible in $\mathcal{O}_{\pi_1}$, so by the implicit function theorem, we can solve for t_2 in terms of t_1; that is, there is a power series $f(t_1) \in \mathcal{O}_{\pi_1}[[t_1]]$ such that $t_2 = f(t_1)$ identically solves (8). Therefore there must be $N(\pi)$ distinct values of $t_1(u)$. Of course, $(t_1(u), t_2(u))$ is also a solution of

$$0 = g(t_1, t_2) := [\pi_1\pi_3]t_1 = \pi_1\pi_3 t_1 + (d^\circ \geq 2).$$

We know by Lemma 7 that $[\pi_1\pi_3]t_1 \equiv t_1^{N(\pi)} \bmod \pi_1$, so if we plug $t_2 = f(t_1)$ into g, we get

$$0 = h(t_1) := g(t_1, f(t_1)) = \pi_1\pi_3 t_1 + (d^\circ \geq 2) \equiv t_1^{N(\pi)} \bmod \pi_1.$$

By the π_1-adic Weierstrass Preparation Theorem, $h(t_1) = j(t_1)u(t_1)$, where u is a unit power series with constant coefficient 1, and $j(t_1)$ is a distinguished polynomial, i.e., $j(t_1) = \sum_{i=1}^{N(\pi)} a_i t_1^i$, where we know

$$a_1 = \pi_1\pi_3, \quad a_i \equiv 0 \bmod \pi_1, \quad 1 \leq i \leq N(\pi) - 1, \quad a_{N(\pi)} \equiv 1 \bmod \pi_1.$$

Therefore the roots of j are precisely the $t_1(u)$, $u \in J[\pi_1]$, and

$$\prod_{u \in J[\pi_1]'} t_1(u) = \pi_1\pi_3/a_{N(\pi)}$$

(since $N(\pi)$ is odd), where $\pi_3/a_{N(\pi)}$ is a unit in $\mathcal{O}_{\pi_1}$.

(b) Likewise, $[\pi_1]$ is not étale mod π_2, so we also know that $J[\pi_1]$ is in the kernel of reduction mod π_2, and such points are solutions to

$$0 = [\pi_1]t_1 = \pi_1 t_1 + (d^\circ \geq 2), \qquad 0 = [\pi_1]t_2 = \pi_2 t_2 + (d^\circ \geq 2). \tag{9}$$

So now we can find a power series $f'(t_2) \in \mathcal{O}_{\pi_2}[[t_2]]$ such that $t_1 = f'(t_2)$ identically solves (9). Therefore there must be $N(\pi)$ distinct values of $t_2(u)$, $u \in J[\pi_1]$. Again, $(t_1(u), t_2(u))$ is also a solution of

$$0 = g'(t_1, t_2) := [\pi_1\pi_2]t_2 = \pi_2\pi_4 t_2 + (d^\circ \geq 2) \equiv t_2^{N(\pi)} \bmod \pi_2.$$

So if we plug $t_1 = f'(t_2)$ into g', we get

$$0 = h'(t_2) := g'(f'(t_2), t_2) = \pi_2\pi_4 t_2 + (d^\circ \geq 2) \equiv t_2^{N(\pi)} \bmod \pi_2.$$

Again by the π_2-adic Weierstrass Preparation Theorem, $h'(t_2) = j'(t_2)u'(t_2)$, where u' is a unit power series which has constant coefficient 1, and $j'(t_2)$ is a distinguished polynomial. So $j'(t_2) = \sum_{i=1}^{N(\pi)} a_i' t_2^i$, where now

$$a_1' = \pi_2\pi_4, \quad a_i' \equiv 0 \bmod \pi_2, \quad 1 \le i \le N(\pi)-1, \quad a_{N(\pi)}' \equiv 1 \bmod \pi_2.$$

The roots of j' are precisely the $t_2(u)$, $u \in J[\pi_1]$, and $j'(t_2)/t_2$ is an irreducible Eisenstein polynomial of degree $N(\pi)-1$. We deduce that $K_{\pi_2}(J[\pi_1])$ is totally ramified over π_2, and that $t_2(u)$ is a uniformizer for the prime P_2 in $K_{\pi_2}(J[\pi_1])$ for any $u \in J[\pi_1]'$. By Lemma 3,

$$f'(t_2) = \frac{1}{3\pi_1}(\pi_2^3 - \pi_1)t_2^3 + (d^\circ \ge 4),$$

so $\operatorname{ord}_{P_2} t_1(u) = 3$ for any $u \in J[\pi_1]'$, and $\operatorname{ord}_{(\pi_2)} \delta = 3$.

LEMMA 9. *Let $\widetilde{J}$ be the reduction of J over L taken* $\bmod \Lambda$. *The Frobenius on $\widetilde{J}$ is induced by one of the endomorphisms $[\pm\sqrt{5}]$ on J.*

Proof. As in the proof of Lemma 7, the Frobenius is induced by some $[\alpha]$, where $(\alpha) = (N_{\Psi'}(\Lambda))$, and where Ψ' is the reflex type on L induced by Φ' on K. In addition, α has absolute value $\sqrt{N(\lambda)}$ in every complex absolute value. Since (λ) is totally ramified in L, $(N_{\Psi'}(\Lambda)) = (N_{\Phi'}(\lambda))$, so once again, $\alpha = u\lambda\sigma_3(\lambda)$, where u is a root of unity. Now mod Λ, the model (4) reduces to

$$Y^2 = X(X - \sqrt[5]{1/4})(X - 2\sqrt[5]{1/4})(X - 3\sqrt[5]{1/4})(X - 4\sqrt[5]{1/4}).$$

So the Weierstrass points are rational mod Λ, and hence so is $J[2]$. Therefore $16 \mid \#J(\mathcal{O}_L/\Lambda) = N(1-\alpha)$, and since 2 remains prime in $\mathcal{O}$, $2 \mid 1-\alpha$. So if $u = \pm\zeta^i$, $0 \le i \le 4$, we have

$$\alpha = \pm\zeta^i(1-\zeta)(1-\zeta^3) = -\pm\zeta^{i-3}\sqrt{5} \equiv 1 \bmod 2.$$

But $\sqrt{5} \equiv 1 \bmod 2$, so $i = 3$, and $\alpha = \pm\sqrt{5}$.

LEMMA 10. *Let $R \in J[5]$ be any point such that $[1-\zeta]R = Q$, and*

$$f = \frac{(\zeta + \zeta^2 - \zeta^3 - \zeta^4)X_{12}/2 + (\zeta^2 - \zeta^3)X_{22}^2/2}{(1+\zeta^2)X_{12}X_{222} + 2\zeta X_{112}} - \frac{(\zeta^2+\zeta^3)X_{22}X_{112} + X_{12}X_{122}}{(1+\zeta^2)X_{12}X_{222} + 2\zeta X_{112}}.$$

Then

(a) $\varepsilon^2 = f([2]R)^5$.

(b) *For all $z \in J$, $f(z+P) = \zeta^2 f(z)$.*

Proof. Let $z = P_1 + P_2 - 2\infty$ be a generic point of J, where $P_i = (x_i, y_i)$, $i = 1, 2$, are points of C. Set $[1-\zeta]z = P_3 + P_4 - 2\infty$, where $P_i = (x_i, y_i)$, $i = 3, 4$, and let $y' = y - 1/2$. Then there is a function $g \in K(z)(J)$ with

divisor $P_1+P_2+[\zeta]I(P_1)+[\zeta]I(P_2)+I(P_3)+I(P_4)-6\infty$, and so g has the form $y'-ax^3-bx^2-cx-d$, for some $a,b,c,d\in K(z)$. The zeros of g are also roots of

$$h(y')=\prod_{i=0}^{4}(y'-a\zeta^{3i}x^3-b\zeta^{2i}x^2-c\zeta^i x-d).$$

The lead term of h (in terms of the pole at ∞) is contributed by $-a^5x^{15}=-a^5(y')^3(y'+1)^3$, so is $-a^5(y')^6$. The constant term of h is $-d^5$. So the product of the 6 roots of h is d^5/a^5, so

$$\begin{aligned}d^5/a^5&=y'(P_1)y'(P_2)y'([\zeta]I(P_1))y'([\zeta]I(P_2))y'(I(P_3))y'(I(P_4))\\&=(y_1-1/2)(y_2-1/2)(y_1+1/2)(y_2+1/2)(y_3+1/2)(y_4+1/2).\end{aligned}$$

Hence

$$(y_3+1/2)(y_4+1/2)=(-d/aX_{12}(z))^5. \tag{10}$$

A computation with Cramer's rule shows that $-d/aX_{12}=f$. Specializing $z=[2]R$, (10) gives us (a), since $(y_1+1/2)(y_2+1/2)(2[Q])=\varepsilon^2$. As for (b), we first note that $f(z+P)/f(z)$ is a fifth root of 1 independent of the choice of $z\in J$. Specializing $z=w=S-\infty$, for $S=(x,y)$ a generic point on C, gives $f(w)=-\zeta^4x$. (One divides the numerator and denominator of f by $X_{22}X_{222}$, and uses the fact (proved in [Gra4]) that X_{12}/X_{22}, X_{122}/X_{222}, and X_{112}/X_{222} evaluated at w are $-x$, $-x$, and x^2, respectively.) Likewise, using the expressions (5) and (6), specializing $z=w+P$ gives $f(w+P)=-\zeta x$. Hence $f(w+P)/f(w)=\zeta^2$.

R e m a r k s. 1. What we have computed, in essence, is the Weil pairing $w(P,R)$ between P and R. The function $(y_1-1/2)(y_2-1/2)$ has as divisor 5 times Θ translated by P minus 5Θ. So $(y_1-1/2)(y_2-1/2)([5]z)=F(z)^5$, for some function F. We can take $F(z)=f([5/\lambda]z)$ as above, and then for any z where the functions are defined,

$$w(P,R)=\frac{F(z+R)}{F(z)}=\frac{f([5/\lambda](z+R))}{f([5/\lambda]z)}=\frac{f([5/\lambda]z-P)}{f([5/\lambda]z)}=\zeta^3.$$

2. A much more involved calculation shows that if we set

$$r=-(1/5)\sum_{i=0}^{4}\zeta^i X_{12}(R+[i]P),$$

then also $r^5=\varepsilon^2$ (see [Gra3]).

3. That $K(J[5])=K(\varepsilon^{1/5})$ is a special case of Theorem 4 of [Gre].

3. Proof of the Theorem

PROPOSITION. *Let π prime to λ be any first or second degree prime of $\mathcal{O}$. There is an $m\in\mathbb{Z}$, determined only up to multiples of* 5, *such that*

$K((2^m\delta)^{1/5})/K$ is unramified at (λ). Such m are determined by the property

$$2^{4m} \equiv \pi_1\pi_2^3 \bmod \lambda^5.$$

Furthermore, for some non-zero $\beta \in K$,

$$\delta = \pi_1\pi_2^3\beta^5.$$

Proof. Let S be a fifth-set of $J[\pi]'$, that is, a subset such that S, $[\zeta]S$, $[\zeta^2]S$, $[\zeta^3]S$, $[\zeta^4]S$ are mutually disjoint and have $J[\pi]'$ as their union. Then since $t_1([\zeta]u) = \zeta t_1(u)$, if we set $\gamma = \prod_{u\in S} t_1(u)$, we have $\gamma^5 = \delta$, so $K(\delta^{1/5})$ is contained in $K(J[\pi])$. Then by Lemmas 4 and 8 and Kummer theory, we know that

$$\delta = \pm\zeta^i\varepsilon^j\lambda^k\pi_1\pi_2^3\beta^5,$$

for some non-zero $\beta \in K$, where $0 \le i, j, k \le 4$. By Lemma 2, J has good reduction over L at Λ, so $L(\delta^{1/5})/L$ is unramified at Λ. Comparing ramification degrees shows that $M(\delta^{1/5})/M$ is also unramified at ℓ. Now if E is the compositum of two cyclic quintic extensions $L = K(2^{1/5})$ and $K(\delta^{1/5})$, then E is a Galois extension of K with Galois group $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$. Therefore if G is the inertia group in $\mathrm{Gal}(E/K)$ of any prime above λ, and E_G is its fixed field, then E_G/K is a cyclic quintic extension of K unramified over λ, and necessarily of the form $K((2^m\delta)^{1/5})$ for some $0 \le m \le 4$. Immediately we see that $k = 0$. This means that the splitting field of $x^5 - \pm\zeta^i\varepsilon^j\pi_1\pi_2^3 2^m$ over the local field K_λ is unramified. We now follow a standard argument to find i and j: by (1), $\pm\zeta^i\varepsilon^j\pi_1\pi_2^3 2^m \equiv \pm 3^j 2^m \bmod \lambda$, and setting $x = y \pm 3^j 2^m$, we have that the splitting field of

$$y^5 \pm 3^j 2^m 5y^4 + 3^{2j}2^{2m+1}5y^3 \pm 3^{3j}2^{3m+1}5y^2 + 3^{4j}2^{4m}5y \pm 3^{5j}2^{5m} - \pm\zeta^i\varepsilon^j\pi_1\pi_2^3 2^m$$

is unramified over K_λ. Comparing the order of y^5 and $\alpha = 3^{5j}2^{5m} - \zeta^i\varepsilon^j\pi_1\pi_2^3 2^m$ at any prime of $K((2^m\delta)^{1/5})$ above λ, we see that since $\lambda \mid \alpha$, we must have $\lambda^5 \mid \alpha$. Taking $\alpha \bmod \lambda^2$ shows that $i = 0$. Then taking $\alpha \bmod \lambda^3$ shows $j = 0$. Hence $2^{4m} \equiv \pi_1\pi_2^3 \bmod \lambda^5$, and $\delta = \pm\pi_1\pi_2^3\beta^5$, so without loss of generality, we can absorb the sign into the choice of β and get our result.

Proof of the Main Law. Let π and v be non-associate primes of $\mathcal{O}$ which are prime to λ.

Case 1: *π and ν are both fourth degree primes*. In this case $\pi = p^*$, $\nu = v^*$, for some rational primes p and v, both necessarily congruent to either 2 or 3 mod 5. We note that

$$\left(\frac{v}{p}\right) \equiv v^{(p^4-1)/5} \equiv (v^{(p-1)})^{(p^3+p^2+p+1)/5} \equiv (1)^{(p^3+p^2+p+1)/5} \equiv 1 \bmod p,$$

so by Lemma 2,

$$\left(\frac{\nu}{\pi}\right) = \left(\frac{v}{p}\right) = 1 = \left(\frac{p}{v}\right) = \left(\frac{\pi}{\nu}\right).$$

C a s e 2: *π or ν is a first or second degree prime*. Assume now without loss of generality that π is a first or second degree prime. We can assume that either (π_2) and (ν_1) are distinct, or, if not, reversing the roles of π and ν, that (ν_2) and (π_1) are distinct, unless π is second degree and $(\nu) = (\pi_2)$. But then by Lemma 2,

$$\left(\frac{\pi_1}{\pi_2}\right) = \left(\frac{\pi_4}{\pi_3}\right) = \left(\frac{\pi_1}{\pi_2}\right)^{\sigma_4} = \left(\frac{\pi_1}{\pi_2}\right)^4,$$

so $\left(\frac{\pi_1}{\pi_2}\right) = 1 = \left(\frac{\pi_2}{\pi_1}\right)$. So in what follows we will assume without loss of generality that (π_2) and (ν_1) are distinct.

As in the proof of the Proposition, let S be a fifth-set of $J[\pi]'$, and $\gamma = \prod_{u\in S} t_1(u)$, so that $\gamma^5 = \delta$. Hence if σ_ν is the Frobenius over ν in the extension $K(\gamma)/K$, then by the Proposition,

$$\left(\frac{\pi_1\pi_2^3}{\nu}\right) = \frac{\gamma^{\sigma_\nu}}{\gamma} = \frac{\prod_{u\in S} t_1(\nu_1\nu_3 u)}{\prod_{u\in S} t_1(u)},$$

by Lemma 7. Let $\psi : \mathcal{O}/(\pi) \to J[\pi]$ be the map $\psi(a) = [a]u$, and $T = \psi^{-1}(S)$. By Gauss' Lemma (say the version in [K2]) we have

$$\frac{\prod_{u\in S} t_1(\nu_1\nu_3 u)}{\prod_{u\in S} t_1(u)} = \zeta^i \equiv \frac{\prod_{a\in T} \nu_1\nu_3 a}{\prod_{a\in T} a} \equiv (\nu_1\nu_3)^{(N(\pi)-1)/5} \bmod \pi,$$

so

$$\left(\frac{\pi_1\pi_2^3}{\nu_1}\right) = \left(\frac{\nu_1\nu_3}{\pi_1}\right).$$

Now elementary manipulations give us

$$\begin{aligned}(11)\qquad \left(\frac{\nu_1\nu_3}{\pi_1}\right) &= \left(\frac{\pi_1\pi_2^3}{\nu_1}\right) = \left(\frac{\pi_1}{\nu_1}\right)\left(\frac{\pi_2}{\nu_1}\right)^3 \\ &= \left(\frac{\pi_1}{\nu_1}\right)\left(\frac{\pi_2}{\nu_1}\right)^{\sigma_3} = \left(\frac{\pi_1}{\nu_1}\right)\left(\frac{\pi_1}{\nu_3}\right) = \left(\frac{\pi_1}{\nu_1\nu_3}\right).\end{aligned}$$

C a s e 2(i): *ν is a fourth degree prime*. Assume that $\nu = v^*$, where $v \in \mathbb{Z}$ is a fourth degree prime. Then ν_1 and ν_3 are both associates of v, and applying Lemma 1 and (11) we get

$$\left(\frac{\pi_1}{\nu_1}\right)^2 = \left(\frac{\pi_1}{\nu_1\nu_3}\right) = \left(\frac{\nu_1\nu_3}{\pi_1}\right) = \left(\frac{\nu_1}{\pi_1}\right)^2,$$

so $\left(\frac{\pi_1}{\nu_1}\right) = \left(\frac{\nu_1}{\pi_1}\right)$.

Case 2(ii): *ν is a first or second degree prime*. With both π and ν first or second degree primes, we can use (11) symmetrically. From (11) we get

$$\left(\frac{\nu_1}{\pi_1}\right)\left(\frac{\nu_3}{\pi_1}\right) = \left(\frac{\nu_1\nu_3}{\pi_1}\right) = \left(\frac{\pi_1\pi_2^3}{\nu_1}\right) = \left(\frac{\pi_1\pi_2}{\nu_1}\right)\left(\frac{\pi_2^2}{\nu_1}\right). \tag{12}$$

Now since $\sigma_3(\pi_2) = \pi_1$, we can apply (11) to (12) with the roles of π and ν taken by ν_1 and π_2, and get

$$\begin{aligned}\left(\frac{\pi_1\pi_2}{\nu_1}\right)\left(\frac{\pi_2}{\nu_1}\right)^2 &= \left(\frac{\nu_1}{\pi_1\pi_2}\right)\left(\frac{\pi_2}{\nu_1}\right)^2 = \left(\frac{\nu_1}{\pi_1}\right)\left(\frac{\nu_1}{\pi_2}\right)\left(\frac{\pi_2}{\nu_1}\right)^2 \\ &= \left(\frac{\nu_1}{\pi_1}\right)\left(\frac{\nu_3}{\pi_1}\right)^{\sigma_2}\left(\frac{\pi_2}{\nu_1}\right)^2 = \left(\frac{\nu_1}{\pi_1}\right)\left(\frac{\nu_3}{\pi_1}\right)^2\left(\frac{\pi_2}{\nu_1}\right)^2.\end{aligned} \tag{13}$$

Equating expressions in (12) and (13) and dividing by $\left(\frac{\nu_1}{\pi_1}\right)\left(\frac{\nu_3}{\pi_1}\right)$ gives us

$$1 = \left(\frac{\nu_3}{\pi_1}\right)\left(\frac{\pi_2}{\nu_1}\right)^2 = \left(\frac{\nu_3}{\pi_1}\right)\left(\left(\frac{\pi_1}{\nu_3}\right)^{\sigma_2}\right)^2 = \left(\frac{\nu_3}{\pi_1}\right)\left(\frac{\pi_1}{\nu_3}\right)^4,$$

so

$$\left(\frac{\nu_3}{\pi_1}\right) = \left(\frac{\pi_1}{\nu_3}\right). \tag{14}$$

Since ν (and hence ν_3) was arbitrary, we can replace ν_3 in (14) by ν_1 to get our result.

In our proof of the complementary laws, we will let π prime to λ be a prime of $\mathcal{O}$ with a λ-adic expansion

$$\pi \equiv 1 + a\lambda^3 + b\lambda^4 + c\lambda^5 \bmod \lambda^6,$$

with $a, b, c \in \mathbb{Z}/5\mathbb{Z}$.

Proof of Complementary Law (i). It follows easily from the definition of the power residue symbol that $\left(\frac{\zeta}{\pi}\right) = \zeta^{(N(\pi)-1)/5}$. To compute this, we need only compute $N(\pi) \bmod \lambda^5$. But since $\pi \equiv 1 \bmod \lambda^3$ it is easy to see that mod λ^5, $N(\pi)$ is just $1 + T(a\lambda^3 + b\lambda^4)$, where T denotes the trace from K to $\mathbb{Q}$. Since $T(1) = 4$, $T(\zeta^i) = -1$ for $i = 1, 2, 3, 4$, it is easy to see that $T(\lambda^3) = T(\lambda^4) = 5$. Hence $(N(\pi) - 1)/5 \equiv a + b \bmod 5$, and $\left(\frac{\zeta}{\pi}\right) = \zeta^{a+b}$.

Proof of Complementary Law (ii). As in Lemma 10, we let $R \in J[5]$ be any point such that $[1-\zeta]R = Q$. Since $f([2]R)^5 = \varepsilon^2$, we have

$$\left(\frac{\varepsilon^2}{\pi}\right) = \frac{f([2]R)^{\sigma_\pi}}{f([2]R)}, \tag{15}$$

where σ_π is the Frobenius attached to π in the extension $K(J[5])/K$. By Lemma 7, $f([2]R)^{\sigma_\pi} = f([\pi_1\pi_3][2]R)$. Since R is λ^4-torsion, we only have to

compute $[\pi_1\pi_3] \bmod \lambda^4$. Since $\pi_1 \equiv 1 + a\lambda^3 \bmod \lambda^4$, it follows readily that $\pi_3 \equiv 1+2a\lambda^3 \bmod \lambda^4$, and hence $\pi_1\pi_3 \equiv 1+3a\lambda^3 \bmod \lambda^4$. Since $[\lambda^3]R = P$,

$$f([\pi_1\pi_3][2]R) = f([2]R + [6a]P) = f([2]R)\zeta^{12a},$$

by Lemma 10(b). Hence $f([2R])^{\sigma_\pi}/f([2]R) = \zeta^{2a}$. Combining this with (15) gives $\left(\frac{\varepsilon^2}{\pi}\right) = \zeta^{2a}$, so $\left(\frac{\varepsilon}{\pi}\right) = \zeta^a$.

R e m a r k. A different proof of complementary law (ii) can be based on the second remark following Lemma 10.

P r o o f o f C o m p l e m e n t a r y L a w (iii). As in the Proposition, there is an m (determined only up to multiples of 5) such that $K((2^m\delta)^{1/5})/K$ is unramified over λ, and such m are determined by the property that $2^{4m} \equiv \pi_1\pi_2^3 \bmod \lambda^5$. Let σ_λ be the Frobenius attached to λ in the extension $K((2^m\delta)^{1/5})/K$. Let γ be as in the proof of the Proposition. Then there is an prolongation τ_Λ of σ_λ in the Galois group of $L(\gamma)/K$ which is the Frobenius over Λ in the extension $L(\gamma)/L$. So we have

$$\frac{((2^m\delta)^{1/5})^{\sigma_\lambda}}{(2^m\delta)^{1/5}} = \frac{\gamma^{\tau_\Lambda}}{\gamma} = \left(\frac{\pm\sqrt{5}}{\pi_1}\right), \tag{16}$$

by Gauss' Lemma and Lemma 9. Let $((2^m\delta)^{1/5})^{\sigma_\lambda}/(2^m\delta)^{1/5} = \zeta^j$. We will compute j directly from the definition of the Frobenius. From our λ-adic expansion of $\pi = \pi_1$, we get sequentially

$$\begin{aligned}
\pi_2 &\equiv 1 + 3a\lambda^3 + (b-2a)\lambda^4 + (a-2b+2c)\lambda^5 \bmod \lambda^6,\\
\pi_2^3 &\equiv 1 - a\lambda^3 + (3b-a)\lambda^4 + (3a-b+c)\lambda^5 \bmod \lambda^6,\\
\pi_1\pi_2^3 &\equiv 1 + (-b-a)\lambda^4 + (3a-b+2c)\lambda^5 \bmod \lambda^6.
\end{aligned}$$

Since $2^4 \equiv 1+2\lambda^4-\lambda^5 \bmod \lambda^6$, we can take $m = 2(b+a)$, and get $2^{4m} \equiv \pi_1\pi_2^3 \bmod \lambda^5$, and

$$2^{-4m}\pi_1\pi_2^3 \equiv 1 + (2c+b)\lambda^5 \bmod \lambda^6. \tag{17}$$

So let $2^{-4m}\pi_1\pi_2^3 = 1 + d\lambda^5$, so that by (17), $d \equiv 2c + b \bmod \lambda$. Let α be a fifth root of $2^{-4m}\pi_1\pi_2^3$, so by (16), $\zeta^j = \alpha^{\sigma_\lambda}/\alpha$. We are trying to compute σ_λ in the splitting field of $x^5 - 2^{-4m}\pi_1\pi_2^3$. Letting $z = (x-1)/\lambda$, the extension is generated over K by $\beta = (\alpha-1)/\lambda$, a root of

$$z^5 + (5/\lambda)z^4 + (10/\lambda^2)z^3 + (10/\lambda^3)z^2 + (5/\lambda^4)z - d = 0. \tag{18}$$

Since $5/\lambda^4 \equiv -1 \bmod \lambda$, we deduce from (18) that mod λ, $\beta^5 = \beta + d$, so σ_λ is the automorphism that sends $\beta \to \beta + d \bmod \lambda$. Since $\beta = (\alpha-1)/\lambda$, we get

$$\frac{\zeta^j\alpha - 1}{\lambda} \equiv \frac{\alpha - 1}{\lambda} + d \bmod \lambda. \tag{19}$$

Since $1 \equiv 2^{-4m}\pi_1\pi_2^3 \equiv \alpha^5 \equiv \alpha^{\sigma_\lambda} \equiv \zeta^j\alpha \equiv \alpha \bmod \lambda$, (19) gives us

$$d \equiv \frac{\zeta^j - 1}{1-\zeta} \equiv -j \bmod \lambda.$$

Hence

$$\left(\frac{\sqrt{5}}{\pi_1}\right) = \zeta^{-b-2c}. \tag{20}$$

Since $\sqrt{5} = -\zeta^4\varepsilon\lambda^2$, (20) and the first two complementary laws give us

$$\zeta^{-b-2c} = \left(\frac{\zeta}{\pi_1}\right)^4\left(\frac{\varepsilon}{\pi_1}\right)\left(\frac{\lambda}{\pi_1}\right)^2 = \zeta^{4a+4b+a}\left(\frac{\lambda}{\pi_1}\right)^2,$$

so

$$\left(\frac{\lambda}{\pi_1}\right) = \zeta^{-c}.$$

References

[AT] E. Artin and J. Tate, *Class Field Theory*, Benjamin, Reading, 1967.

[BaBo] E. Bavencoffe et J. Boxall, *Valeurs des fonctions thêta associées à la courbe* $y^2 = x^5 - 1$, Séminaire de Théorie des Nombres de Caen 1991/1992.

[BoBa] J. Boxall et E. Bavencoffe, *Quelques propriétés arithmétiques des points de 3-division de la jacobienne de* $y^2 = x^5 - 1$, Séminaire de Théorie des Nombres, Bordeaux 4 (1992), 113–128.

[C] J. W. S. Cassels, *On Kummer sums*, Proc. London Math. Soc. (3) 21 (1970), 19–27.

[F] R. Fueter, *Reziprozitätsgesetze in quadratisch-imaginären Körpern*, Nachr. Ges. Wiss. Göttingen 1927, 1–11, 427–445.

[Gra1] D. Grant, *A generalization of a formula of Eisenstein*, Proc. London Math. Soc. (3) 62 (1991), 121–132.

[Gra2] —, *Units from 3- and 4-torsion on Jacobians of curves of genus 2*, Compositio Math. 95 (1994), 311–320.

[Gra3] —, *Units from 5-torsion on the Jacobian of* $y^2 = x^5 + 1/4$ *and the conjectures of Stark and Rubin*, in preparation.

[Gra4] —, *Formal groups in genus two*, J. Reine Angew. Math. 411 (1990), 96–121.

[Gra5] —, *Coates–Wiles towers in dimension two*, Math. Ann. 282 (1988), 645–666.

[Gre] R. Greenberg, *On the Jacobian variety of some algebraic curves*, Compositio Math. 42 (1981), 345–359.

[H] D. Hilbert, *Théorie des corps de nombres algébriques*, Jacques Gabay, Sceaux, 1991. Translation of: *Die Theorie der algebraischen Zahlkörper*, Jahresber. Deutsch. Math.-Verein 4 (1897), 175–546.

[IrR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Grad. Texts in Math. 84, Springer, 1982.

[Iw] K. Iwasawa, *A note on Jacobi sums*, Sympos. Math. 15 (1975), 447–459.

[K1] T. Kubota, *Reciprocities in Gauss' and Eisenstein's number fields*, J. Reine Angew. Math. 208 (1961), 35–50.

[K2] T. Kubota, *An application of the power residue theory to some abelian functions*, Nagoya Math. J. 27 (1966), 51–54.

[L] S. Lang, *Complex Multiplication*, Springer, 1983.

[M] J. Milne, *Abelian Varieties*, in: G. Cornell and J. Silverman (eds.), Arithmetic Geometry, Springer, New York, 1986, 103–150.

[ST] G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and its Applications to Number Theory*, The Mathematical Society of Japan, 1961.

[W1] A. Weil, *La cyclotomie jadis et naguère*, Enseign. Math. 20 (1974), 247–263.

[W2] —, *Review of* "*Mathematische Werke*, *by Gotthold Eisenstein*," Bull. Amer. Math. Soc. 82 (1976), 658–663.

[W3] —, Introduction to: E. E. Kummer, Collected Papers, Vol. 1, Springer, New York, 1975, 1–11.

[W4] —, *Jacobi sums as Grössencharaktere*, Trans. Amer. Math. Soc. 73 (1952), 487–495.

Department of Mathematics
Campus Box 395
University of Colorado at Boulder
Boulder, Colorado 80309-0395
U.S.A.
E-mail: grant@boulder.colorado.edu

Received on 14.7.1995 (2835)