COMPOSITIO MATHEMATICA

DAVID GRANT

Units from 3- and 4-torsion on jacobians of curves of genus 2

Compositio Mathematica, tome 94, nº 3 (1994), p. 311-320

<http://www.numdam.org/item?id=CM_1994__94_3_311_0>

Compositio Mathematica **94**: 311–320, 1994.

Units from 3- and 4-torsion on Jacobians of curves of genus 2

DAVID GRANT*

Department of Mathematics, University of Colorado at Boulder, Boulder, CO 80309–0395, USA

Received 14 July 1993; accepted in final form 23 November 1993

Abstract. Let C be a curve of genus 2 defined over a number field K, and suppose that C has everywhere potentially good reduction. We produce a function ξ on the Jacobian J of C, such that ξ evaluated at primitive 3-torsion points of J produces units in extension fields of K. We show that ξ evaluated at primitive 4-torsion points produces units at primes not dividing 2.

0. Introduction

Elliptic units play a central role in both the arithmetic of imaginary quadratic fields and the arithmetic of elliptic curves with complex multiplication [CW, K, Ro, Ru1, Ru2, S]. A major obstacle to the development of the Iwasawa theory of higher dimensional abelian varieties is the lack of a suitable analogue of such units.

Let E be an elliptic curve defined over a number field, and suppose that E has everywhere potentially good reduction. Elliptic units are built by evaluating functions at torsion points of E, exploiting the fact that if E has good reduction at a prime p, then the prime-to-p torsion of E remains distinct when reduced mod p. The primes dividing p are finessed away by using the distribution relation for genus 1 theta functions (see e.g. [deS]).

Little has been done to attach units to curves of higher genus or abelian varieties of higher dimension. The author recently built S-units by evaluating a function on a curve of genus 2 at points which do not correspond to torsion on its Jacobian [G2]. Baily has also been able to attach S-units to higher dimensional abelian varieties by using Hilbert modular forms [B-K].

Let C be a curve of genus 2 defined over a number field K, J its Jacobian, and Θ the image of C embedded into J with a Weierstrass point as base point. Boxall [Bo] recently noted that if p is a prime of good reduction for C with residue characteristic $\neq 3$, then the primitive 3-torsion of J does not lie on the support of Θ mod p. Since a single function on J can separate a point from an ample divisor, it is possible to build S-units from 3-torsion points on J. The same is true of primitive 4-torsion points.

*Partially supported by NSF grant DMS-9303220.

The remarkable thing is that one can actually produce units, even though there is no known distribution relation for genus 2 theta functions. This was shown recently by Boxall and Bavencoffe [BoBa] who made some wonderful calculations with the 3-torsion of the Jacobian J of $y^2 = x^5 - 1$. (See [BaBo] for analogous calculations with 4-torsion.) They evaluated a function g at a primitive 3-torsion point u of J, and proved algebraically that $g(u)$ is an algebraic integer. They then used theta functions to calculate the (necessarily integral) coefficients of the minimal polynomial of $g(u)$, and proved that $g(u)/\sqrt{5}$ is a unit (see Remark 2 for how this also follows from the techniques of this paper).

In this paper we consider a more general setting. Let C have a Weierstrass point defined over K. Then C has a model of the form

$$y^2 = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5,\ b_i \in K,\ 1 \leqslant i \leqslant 5. \tag{0.1}$$

Let $\Delta(C)$ be the discriminant of the quintic. Since J is birational to the symmetric product of C with itself, functions on J can be written as symmetric functions of two points on C. For any $n > 0$ we let $J[n]$ denote the n-torsion on J. Let O denote the origin of J.

THEOREM 1. *Let C be a curve of genus* 2 *defined over a number field K with a model as in* (0.1). *If C has everywhere potentially good reduction, then for all $u \in J[3]$, $u \neq O$,*

$$\xi(u) := \frac{\Delta(C)}{(y_1y_2(u))^4} \in K(J[3])$$

is a unit.

Even if C does not have a rational Weierstrass point over K, it has one which is rational over $K(J[2])$, so we can pick a model of the form (0.1) over this extension and find that $\xi(u) \in K(J[6])$.

Emulating a proof for the existence of elliptic units in [deS], it is not hard to show that $\xi(u)$ is a unit at primes not dividing 6. It is only slightly more painful to verify that it is a unit at the primes dividing 2. The somewhat surprising thing is that $\xi(u)$ is a unit at primes dividing 3, even when u is in the kernel of reduction of the prime. We will prove this using some explicit calculations with the formal group at the origin of the Jacobian. This has no analogue in the elliptic case, for if $E: Y^2 = X^3 + AX + B$ is an elliptic curve with integral j-invariant, and if u is a primitive 3-torsion point of E, then in general $(4A^3 + 27B^2)/y(u)^4$ is a unit only at primes not dividing 3.

By similar techniques we also show

THEOREM 2. *Let C be a curve of genus 2 defined over a number field K, and suppose that C has everywhere potentially good reduction. If we take a model for C of the form* (0.1) *defined over* $K(J[2])$, *then for all* $u \in J[4] - J[2]$, $\xi(u) \in K(J[4])$ *is a unit except perhaps at primes dividing* 2.

It would be interesting to see whether these units provide any information about the arithmetic of C or J, or whether there are units attached to torsion points of J of order greater than 4.

In Section 1 we gather together the facts we need about models of curves of genus 2. We prove the theorems in Section 2.

I would like to thank Jane Arledge for her comments on an earlier version of this paper.

1. Models of curves of genus 2

The main reference for this section is the seminal paper of Igusa [I]. Let K be a perfect field, and C a curve of genus 2 defined over K. We write $D_1 \sim D_2$ when the divisors D_1 and D_2 on C are linearly equivalent. For a function f on C, we let (f) denote its divisor of zeros and poles. For a divisor D on C, we let $\mathscr{L}(D)$ be the vector space of functions on C such that $(f) + D$ is effective.

By the Riemann-Roch theorem, the canonical class of C has an effective representative κ of degree 2, defined over K. Let z be a non-constant function in $K(C) \cap \mathscr{L}(\kappa)$. This makes $K(C)$ a quadratic extension of $K(z)$, and the non-trivial element of the Galois group of the extension gives an involution I on the curve.

We call a point $P \in C$ a Weierstrass point if $2P \sim \kappa$. These are precisely the fixed points of I. If the characteristic of K is not 2, the Hurwitz formula shows that there are 6 such points. If the characteristic is 2, there are 1, 2 or 3 such points. In any case, we can single out one Weierstrass point, which we call W_0. There is an extension of K of degree at most six over which W_0 is rational. Extending K if necessary, we will assume that W_0 is rational over K.

Let X be a non-constant function in $\mathscr{L}(2W_0) \cap K(C)$, Y be a function in $\mathscr{L}(5W_0) \cap K(C)$ which is not in $\mathscr{L}(4W_0)$. After normalizing X and Y by a suitable factor, the Riemann-Roch theorem produces a model $\mathscr{C}_0$ for C,

$$Y^2 + a_1 YX^2 + a_3 YX + a_5 Y = X^5 + a_2 X^4 + a_4 X^3 + a_6 X^2 + a_8 X + a_{10}, \quad (1.1)$$

where the $a_i \in K$. The involution I is given by $X \to X$, $Y \to -Y - a_1 X^2 - a_3 X - a_5$. So if the characteristic of K is 2, then the Weierstrass points of C are the point W_0 at infinity on the model $\mathscr{C}_0$, and the points whose X-coordinates are the roots of $a_1X^2 + a_3X + a_5$.

If $\operatorname{char}(K) \neq 2$, the transformation

$$T: x = X,\ y = Y + (a_1X^2 + a_3X + a_5)/2, \tag{1.2}$$

gives us a model $\mathscr{C}$ of the form

$$y^2 = f(x) := x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5. \tag{1.3}$$

The hyperelliptic involution on (1.3) is given by $x \to x$, $y \to -y$. So if α_i, $1 \leqslant i \leqslant 5$, are the (necessarily distinct) roots of $f(x)$ in an algebraic closure of K, then $(\alpha_i, 0)$ are the other Weierstrass points of C. We let $\Delta(\mathscr{C}) = \prod_{1 \leqslant i < j \leqslant 5}(\alpha_i - \alpha_j)^2$. The model (1.3) is unique up to transformations

$$T_{rs}: x' = r^2x + s,\ y' = r^5y, \tag{1.4}$$

where $r, s \in K$, $r \neq 0$, which give us another model $\mathscr{C}'$

$$y'^2 = x'^5 + b'_1x'^4 + b'_2x'^3 + b'_3x'^2 + b'_4x' + b'_5. \tag{1.5}$$

Igusa introduced a normal form for curves of genus 2, and functions J_{2i}, $1 \leqslant i \leqslant 5$, of his normal form. Igusa described his functions [I, p. 623] in terms of variables $v_i = (-1)^i 4b_i$, for $i = 0, \ldots, 5$, where $b_0 = 1$. In terms of a curve with model (1.3), his functions become:

$$\begin{aligned}
J_2(\mathscr{C}) &= 4(20b_4 - 8b_1b_3 + 3b_2^2), \qquad\qquad (1.6)\\
J_4(\mathscr{C}) &= -2(400b_3b_5 - 240b_4^2 - 240b_1b_2b_5 + 112b_1b_3b_4 + 8b_2^2b_4\\
&\quad - 16b_2b_3^2 + 64b_1^3b_5 - 16b_1^2b_2b_4 - 16b_1^2b_3^2 + 16b_1b_2^2b_3 - 3b_2^4),\\
J_6(\mathscr{C}) &= -4(4000b_2b_5^2 - 1600b_3b_4b_5 + 320b_4^3 - 1600b_1^2b_5^2 - 640b_1b_2b_4b_5\\
&\quad + 640b_1b_3^2b_5 - 64b_1b_3b_4^2 - 80b_2^2b_3b_5 - 176b_2^2b_4^2 + 224b_2b_3^2b_4\\
&\quad - 64b_3^4 + 384b_1^3b_4b_5 - 192b_1^2b_2b_3b_5 + 224b_1^2b_2b_4^2\\
&\quad - 128b_1^2b_3^2b_4 + 48b_1b_2^3b_5 - 112b_1b_2^2b_3b_4 + 64b_1b_2b_3^3 + 28b_2^4b_4\\
&\quad - 16b_2^3b_3^2 - 64b_1^4b_4^2 + 64b_1^3b_2b_3b_4 - 16b_1^2b_2^3b_4 - 16b_1^2b_2^2b_3^2\\
&\quad + 8b_1b_2^4b_3 - b_2^6),\\
J_8 &= \tfrac{1}{4}(J_2J_6 - J_4^2),\\
J_{10}(\mathscr{C}) &= 2^{-12}v_0^{10}\Delta(\mathscr{C}) = 2^8\Delta(\mathscr{C}).
\end{aligned}$$

These are polynomials in $\mathbb{Z}[b_1, b_2, b_3, b_4, b_5]$. Via the transformation (1.2), we can interpret the b_j as polynomials in the a_k, and write J_{2i}, $1 \leqslant i \leqslant 5$, as polynomials in the a_k with integral coefficients. It is these polynomials which one uses to calculate J_{2i} for a model of the form (1.1) over a field of characteristic 2.

Although it is not obvious from the definitions above, the J_{2i} are invariant under transformations of the form T_{1s}. We can see from (1.6) that if $T_{rs} = T_{r,0} \circ T_{1,s}$ maps a model $\mathscr{C}$ as in (1.3) to a model $\mathscr{C}'$ given by (1.5), then

$$J_{2i}(\mathscr{C}') = r^{8i} J_{2i}(\mathscr{C}). \tag{1.7}$$

Set $\eta_i = J_{2i}/J_{10}^{i/5}$ for $1 \leqslant i \leqslant 4$. Note that if $\operatorname{char}(K) \neq 2$, then $\eta_4 = \frac{1}{4}(\eta_1\eta_3 - \eta_2^2)$. Igusa showed that the η_i, $1 \leqslant i \leqslant 4$, are birational invariants of C, and that if A is defined as $\mathbb{Z}[\eta_1, \eta_2, \eta_3, \eta_4]$ modulo the action $\eta_i \to \zeta_5^i \eta_i$, where ζ_5 denotes a primitive fifth root of unity, then $\operatorname{Spec}(A)$ defines the (coarse) moduli space over $\mathbb{Z}$ for non-singular curves of genus 2. From his proof [I, Thm. 2] we can extract:

THEOREM 3. *Let R be a discrete valuation ring with maximal ideal m. Let C be a model of the form* (1.1) *or* (1.3) *for a curve of genus* 2 *with coefficients in R.*

(1) *C reduces* mod *m to a curve of genus* 2 *if and only if $J_{10} \in R^*$.*
(2) *C has potentially good reduction at m if and only if $\eta_1(C)$, $\eta_2(C)$, $\eta_3(C)$, $\eta_4(C)$ lie in R.*

2. Proofs of the theorems

Let C denote a curve of genus 2, and J its Jacobian. We will need some results on the primitive 3-torsion and 4-torsion points on J. Recall that the points on J can be identified with divisors of C of degree 0 modulo linear equivalence, and that by the Riemann-Roch theorem, any point other than the origin O on J can be represented uniquely by a divisor of the form

$$P + Q - 2W_0,$$

with P, $Q \in C$ and $P \neq I(Q)$. All divisors of the form $P + I(P) - 2W_0$ represent O. The theta divisor Θ on J is represented by all divisors of the form $P - W_0$, with $P \in C$.

LEMMA 1. *Let C be a curve of genus* 2 *defined over a perfect field K and $W \in C(K)$ be any Weierstrass point on C.*

(1) *There is no point* $P \in C$, $P \neq W$, *such that* $3P \sim 3W$.

(2) *There is no point* $P \in C$, *other than a Weierstrass point, such that* $4P \sim 4W$.

Proof. (1) By the Riemann-Roch Theorem, $\mathscr{L}(3W) = \mathscr{L}(2W)$, so $3P \sim 3W$ implies $3P = W + Q + I(Q)$ for some $Q \in C$. Hence $P = W$.

(2) If $4P \sim 4W$, then there is a function $f \in \mathscr{L}(4W)$ which has $4P$ for its divisor of zeros. But up to scaling by a constant, all such functions on C have the form $(x - a)(x - b)$ which can have $4P$ as a divisor of zeros only if $b = a$, and then only if $(a, 0)$ is a Weierstrass point.

This lemma was also recently proved by Boxall [Bo].

COROLLARY 1. *Let C be a curve of genus 2 defined over a discrete valuation ring R with maximal ideal m, perfect residue field, and quotient field K. Let $W \in C(K)$ be any Weierstrass point.*

(1) *Suppose $P, Q \in C(K)$ with $3P + 3Q \sim 6W$. Then if C has good reduction at m, and P specializes to W* mod m, *then Q must do so as well.*

(2) *Suppose $P, Q \in C(K)$ with $4P + 4Q \sim 8W$. If C has good reduction at m and P specializes to a Weierstrass point* mod m, *then Q must do so as well.*

Given a model for C as in (1.3), in [G1] we described a model for J, and a pair of parameters t_1, t_2 at the origin O of J. We will not need to recall everything about this model: the only things we have to know are that t_1 has a zero along Θ, and that t_2 restricted to Θ can be identified with a function on C. Also, let C be given as in (1.3) with coefficients in a ring R, and u and v be two independent generic points on J. Then if $s: J \times J \to J$ is the group morphism, in [G1] it is shown that for $i = 1, 2, t_i(s(u, v))$ lies in $R[[t_1(u), t_2(u), t_1(v), t_2(v)]]$, when it is considered as an element of the completed local ring at O. Hence if $F_i = s^* t_i$, $i = 1, 2$, then $\mathscr{F} = \{F_1, F_2\}$ defines a formal group over R.

In particular, let B_1, B_2, B_3, B_4, B_5 be indeterminates, and S the ring they generate over the 3-adic integers $\mathbb{Z}_3$. Then C given by

$$y^2 = x^5 + B_1 x^4 + B_2 x^3 + B_3 x^2 + B_4 x + B_5$$

is a curve of genus 2 defined over S. Let $\bar{S}$ denote the reduction of S mod 3, and $\bar{\mathscr{F}}$ the reduced formal group over $\bar{S}$. It follows from standard facts on formal groups that the multiplication-by-3 endomorphism [3] on $\bar{\mathscr{F}}$ has the zero matrix for its Jacobian matrix. From Theorem 2 in [F], we conclude that [3] must factor through the Frobenius on $\bar{\mathscr{F}}$. Hence there are power series $g_1, g_2, h_1, h_2 \in S[[t_1, t_2]]$, without constant term, such that on $\mathscr{F}$,

$$[3]t_i = 3g_i(t_1, t_2) + h_i(t_1^3, t_2^3) \ (i = 1, 2). \tag{2.1}$$

LEMMA 2. *Let K be a finite extension of $\mathbb{Q}_3$, and R its ring of integers with maximal ideal m. Suppose that C is a curve of genus 2 with a model $\mathscr{C}$ as in (1.3) with coefficients in R, and suppose that $\mathscr{C}$ reduces* $\bmod m$ *to a curve of genus 2. Let W_0 be the Weierstrass point at infinity of the model. Let J be the Jacobian of C. Suppose that $u \in J[3] - O$ is represented by $P + Q - 2W_0$, with $P, Q \in C(K)$, and that u is in the kernel of reduction* $\bmod m$. *Then P does not reduce to W_0* $\bmod m$.

Proof. Let J_1 denote the kernel of reduction of $J \bmod m$. In [G1] it was shown that the parameters t_1, t_2 map J_1 isomorphically onto $\mathscr{F}(m)$. Hence t_1 has no points of indeterminancy on J_1. Suppose $P \equiv W_0 \bmod m$. Then $v = P - W_0$ is in $J_1 \cap \Theta$, so $t_1(v) = 0$. In [G1] there is an algorithm for calculating the coefficients of F_1 and F_2, and a calculation with the symbolic manipulating program MAPLE shows that

$$F_1(t_1, t_2, s_1, s_2) = t_1 + s_1 - b_3 t_1 s_1(t_1 + s_1) - t_2 s_2(t_2 + s_2) + (d^\circ \geqslant 4),$$
$$F_2(t_1, t_2, s_1, s_2) = t_2 + s_2 - b_4 t_1 s_1(t_1 + s_1) + 2b_1 t_2 s_2(t_2 + s_2) + (d^\circ \geqslant 4), \quad (2.2)$$

where $(d^\circ \geqslant n)$ denotes a power series all of whose terms have degree at least n. Hence iterating (2.2) we can write

$$[3]t_1 = 3t_1 - 8b_3 t_1^3 - 8t_2^3 + (d^\circ \geqslant 4),$$
$$[3]t_2 = 3t_2 - 8b_4 t_1^3 + 16b_1 t_2^3 + (d^\circ \geqslant 4).$$

Specializing $S \to R$ by sending $B_i \to b_i$, $1 \leqslant i \leqslant 5$, and injecting $\mathbb{Z}_3$ into R, from (2.1) we also have

$$[3]t_i = 3g_i(t_1, t_2) + h_i(t_1^3, t_2^3) \ (i = 1, 2),$$

where now $g_i, h_i \in R[[t_1, t_2]]$. Setting $t_1 = 0$, and $G_i(t_2) = g_i(0, t_2)$, $H_i(t_2) = h_i(0, t_2)$ for $i = 1, 2$, we get

$$[3]t_1|_{t_1=0} = 3G_1(t_2) + H_1(t_2^3) = -8t_2^3 + (d^\circ \geqslant 4),$$
$$[3]t_2|_{t_1=0} = 3G_2(t_2) + H_2(t_2^3) = 3t_2 + (d^\circ \geqslant 3).$$

Therefore $G_2(t_2)$ has lead coefficient 1, and $H_1(t_2)$ has a lead coefficient which is congruent to $-8 \bmod 3$, and hence is a unit in R. Hence there exists a $\phi(t_2) \in R[[t_2]]$ such that $[3]t_2|_{t_1=0} - \phi([3]t_1|_{t_1=0}) \in 3R[[t_2]]$. Therefore if we set $\psi(t_2) = \frac{1}{3}([3]t_2|_{t_1=0} - \phi([3]t_1|_{t_1=0}))$, then $\psi(t_2) \in R[[t_2]]$, and $\psi(t_2)$ has lead coefficient 1.

Hence $\psi \circ t_2$ maps $J_1 \cap \Theta$ injectively into m. But since $u, v \in J_1$, then $v - u$, which is represented by $I(Q) - W_0$, is in $J_1 \cap \Theta$, too. And since $u \in J[3]$,

$$3(P - W_0) \sim 3(I(Q) - W_0).$$

This violates the injectivity of $\psi \circ t_2$ unless $P = I(Q)$. But then $u = O$, which violates our original assumptions. Hence P does not reduce to $W_0 \bmod m$

Let C be a curve of genus 2 defined by a model $\mathscr{C}$ as in (1.3). If we represent any $u \in J - \Theta$ as $P_1 + P_2 - 2W_0$, where $P_i = (x_i, y_i)$, for $i = 1, 2$, we define

$$\xi(u) = \frac{\Delta(\mathscr{C})}{(y_1 y_2)^4} = \frac{2^{-8} J_{10}(\mathscr{C})}{(y_1 y_2)^4}.$$

Proof of Theorem 1. By assumption, C has a model $\mathscr{C}$ given by

$$\begin{aligned} y^2 = f(x) &= x^5 + b_1 x^4 + b_2 x^3 + b_3 x^2 + b_4 x + b_5, \; b_i \in K \\ &= \prod_{j=1}^{5} (x - \alpha_j), \end{aligned} \tag{2.3}$$

where K is a number field over which C has everywhere potentially good reduction, and α_j, $1 \leqslant j \leqslant 5$, lie in a splitting field for f. Let $L = K(J[3])$, O_L be its ring of integers, and $\wp$ a prime of O_L. Then there is an extension M over the localization $L_\wp$ of L at $\wp$, for which C has good reduction, and for which the Weierstrass points of C are rational. Hence there is a model D for C with coefficients in O_M, the ring of integers of M, which reduces to a curve of genus 2 modulo the maximal ideal $\mathscr{P}$ of O_M. Therefore $J_{10}(D) \in O_M^*$. Let $u \in J[3] - O$ be represented by the divisor $P_1 + P_2 - 2W_0$ on C.

Assume now that $\wp$ does not divide 2. Then we can take D to be a model $\mathscr{C}'$ as in (1.5), and there is a map T_{rs} as in (1.4) defined over M which transforms $\mathscr{C}$ to $\mathscr{C}'$. In terms of the coordinates on $\mathscr{C}'$, $P_i = (x'_i, y'_i)$. By (1.7), we have that

$$\xi'(u) = \frac{\Delta(\mathscr{C}')}{(y'_1 y'_2)^4} = \frac{\Delta(\mathscr{C})}{(y_1 y_2)^4} = \xi(u).$$

Note that $\Delta(\mathscr{C}') \in O_M^*$ since it differs by a unit from $J_{10}(\mathscr{C}')$. Now suppose that $\wp$ does not divide 3. Then by Corollary 1, $x_i \not\equiv \alpha_j \bmod \mathscr{P}$ for $i = 1, 2$, $1 \leqslant j \leqslant 5$, and $x_i \not\equiv \infty \bmod \mathscr{P}$, $i = 1, 2$, so $y'_1 y'_2$ is a unit at $\mathscr{P}$, and hence $\xi(u) = \xi'(u)$ is a unit at $\mathscr{P}$, too. Now even if $\wp$ divides 3, and u is not in the kernel of reduction $\bmod m$, then once again by Corollary 1, $y'_1 y'_2$ is a unit at $\mathscr{P}$. And Lemma 2 shows that if u is in the kernel of reduction mod m, then $y'_1 y'_2$ is a unit at $\mathscr{P}$ anyway. In either case, $\xi(u) = \xi'(u)$ is a unit at $\mathscr{P}$.

Finally, if $\wp$ divides 2, then we can take $D = \mathscr{C}_0$ as in (1.1). Then there is a model $\mathscr{C}'$ of the form (1.5), and transformations T as in (1.2) and T_{rs} as in (1.4) defined over M, with T mapping $\mathscr{C}_0$ to $\mathscr{C}'$, and T_{rs} mapping $\mathscr{C}$ to $\mathscr{C}'$. Let $P_i = (X_i, Y_i)$ in the coordinates of $\mathscr{C}_0$. Since $\xi(u) = \xi'(u)$, we need only check that

$$\xi'(u) = \frac{J_{10}(\mathscr{C}')}{(2y'_1 2y'_2)^4} = \frac{J_{10}(\mathscr{C}_0)}{(2Y_1 + a_1X_1^2 + a_3X_1 + a_5)(2Y_2 + a_1X_2^2 + a_3X_2 + a_5)}$$

is a unit at $\mathscr{P}$. By Corollary 1, $P_i \not\equiv W_0 \bmod \mathscr{P}$, so X_i and Y_i are finite mod $\mathscr{P}$, and $J_{10}(\mathscr{C}_0) \in O_M^*$. So we need only verify that

$$\begin{aligned}(2Y_1 &+ a_1X_1^2 + a_3X_1 + a_5)(2Y_2 + a_1X_2^2 + a_3X_2 + a_5)\\ &\equiv (a_1X_1^2 + a_3X_1 + a_5)(a_1X_2^2 + a_3X_2 + a_5) \bmod \mathscr{P}\end{aligned}$$

is not 0 mod $\mathscr{P}$. Note that for $\mathscr{C}_0$ to reduce mod $\mathscr{P}$ to a curve of genus 2, $a_1X^2 + a_3X + a_5$ must not be the zero function mod $\mathscr{P}$, so if it is a constant, it is a unit at $\mathscr{P}$. If $a_1X^2 + a_3X + a_5$ is not constant, its zeros are Weierstrass points of C. So by Corollary 1 again,

$$(a_1X_1^2 + a_3X_1 + a_5)(a_1X_2^2 + a_3X_2 + a_5)$$

is a unit at $\mathscr{P}$, and so $\xi(u) = \xi'(u)$ is a unit at $\mathscr{P}$ as well.

Proof of Theorem 2. By assumption, C now has a model as in (2.3), with everywhere potentially good reduction, but now we only assume that $b_i \in K(J[2])$. We now let $L = K(J[4])$ and consider primes of O_L which do not divide 2. The proof is essentially the same as that of Theorem 1.

REMARK 1. Using the explicit function theory of hyperelliptic Jacobians given in [M] or [G1], it is not hard to write the complex value of $\xi(u)$ as a ratio of thetanullwerte with rational characteristic. There is no known distribution relation in general for genus 2 theta functions, but the formulas in [G3] for 3- and 4-torsion on the Jacobian are analogous to the genus 1 theta function formulas which can be combined with the genus 1 distribution relation to build units.

REMARK 2. In [BoBa] the authors studied the curve $C: y^2 = x^5 - 1$. Using the formulas from Section 1, we find that $\eta_1 = \eta_2 = \eta_3 = \eta_4 = 0$, so C has everywhere potentially good reduction, and $(1, 0)$ is a rational Weierstrass point for C. Let W_0 be the Weierstrass point at infinity on the curve. Let $u \in J[3] - O$ be represented by $P_1 + P_2 - 2W_0$, with $P_i = (x_i, y_i)$. If we set $\Xi(u) = \Delta(C)/((x_1 - 1)(x_2 - 1))^{10}$, then the techniques of this section show *mutatis mutandi* that $\Xi(u) \in \mathbb{Q}(J[3])$ is a unit. Since $\Delta(C) = 5^5$, $\Xi(u)$ is the negative tenth-power of $g(u)$, which Boxall and Bavencoffe computed to be a unit.

References

[B-K] W. L. Baily and M. L. Karel, appendix to: W.L. Baily, Reciprocity laws for special values of Hilbert modular functions, in *Algebra and Topology* (1986) 62–139, Korea Inst. Tech., Taejon, 1987.

[Bo] J. Boxall: Valeurs spéciales de fonctions abéliennes, *Groupe d'Etude sur les Problèmes Diophantiens 1990–91*, Publications Mathématiques de l'Université Pierre et Marie Curie No. 103.

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

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

[CW] J. Coates and A. Wiles: On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.* 39 (1977) 223–251.

[deS] E. de Shalit: *Iwasawa Theory of Elliptic Curves with Complex Multiplication. Perspectives in Mathematics* 3, Academic Press, Orlando, 1987.

[F] A. Fröhlich: *Formal Groups*, Lecture Notes in Math. 74, Springer-Verlag, Berlin, 1968.

[G1] D. Grant: Formal groups in genus two, *J. reine. angew. Math.* 411 (1990) 96–121.

[G2] D. Grant: On a generalization of a formula of Eisenstein, *Proc. London Math. Soc.* 3 (1991) 121–132.

[G3] D. Grant: Some product formulas for genus 2 theta functions, preprint.

[I] J.-I. Igusa: Arithmetic variety of moduli for genus two, *Ann. Math.* 72(3) (1960) 612–649.

[K] V. A. Kolyvagin: Euler systems, in *The Grothendieck Festschrift II*, *Prog. Math.* 87 (1990) 435–483.

[M] D. Mumford: *Tata Lectures on Theta II. Prog. Math.* 43 (Birkhäuser, Boston) 1984.

[Ro] G. Robert: Unités elliptiques, *Bull. Soc. Math. France. Mémoire* 36 (1973).

[Ru1] K. Rubin: Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication, *Invent. Math.* 89 (1987) 527–560.

[Ru2] K. Rubin: The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* 103 (1991) 25–68.

[S] H. Stark: L-functions at $s = 1$. *IV. First derivatives at* $s = 0$, *Adv. Math.* 35(3) (1980) 197–235.