TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 259, Number 1, May 1980

THE GROUP OF RATIONAL SOLUTIONS OF $y^2 = x(x-1)(x-t^2-c)$

BY

CHARLES F. SCHWARTZ

ABSTRACT. In this paper, we show that the Mordell-Weil group of the Weierstrass equation $y^2 = x(x-1)(x-t^2-c)$, $c \neq 0, 1$ (i.e., the group of solutions (x, y), with $x, y \in \mathbf{C}(t)$) is generated by its elements of order 2, together with one element of infinite order, which is exhibited.

1. Introduction. The object of this paper is to compute the Mordell-Weil group of the elliptic curve (over $\mathbf{C}(t)$) given by

$$y^2 = x(x-1)(x-t^2-c), \tag{1.1}$$

that is, the group of solutions (x, y), with $x, y \in \mathbf{C}(t)$. The Mordell-Weil theorem tells us, if the discriminant is not constant, that the Mordell-Weil group of a Weierstrass equation over a function field, is finitely generated. In this case, we prove the following:

THEOREM 1.1. *The Mordell-Weil group of*

$$y^2 = x(x-1)(x-t^2-c)$$

is generated by two elements of order 2,

$$P_1 = (0, 0) \quad \textit{and} \quad P_2 = (1, 0),$$

together with an element of infinite order (*given in* §2),

$$P_0 = (x_0, y_0).$$

The theorem is proved as follows. In §2, the solution P_0 is presented. In §3, we use a function μ, defined by Manin [**10**], to show that P_0 has infinite order. In §4, we show that the Mordell-Weil group has rank 1. In §7, we define a bilinear form, $I(P, Q)$, on the group of $\mathbf{C}(t)$-rational solutions of (1.1), and show that $4I(P, Q)$ is an integer for all P and Q. We calculate that $I(P_0, P_0) = \frac{1}{4}$ in §8, which shows that P_0 is not a multiple of any other solution, so that it generates the free part of the group. Finally, in §9, it is shown by an argument of Hoyt [**2**] that the torsion subgroup consists of the four elements

$$\{(0, 0), (1, 0), (t^2 + c, 0), \infty\}$$

and that the three finite elements are of order 2. This will conclude the proof.

Received by the editors August 15, 1977; presented to the Society April 15, 1977.

AMS (MOS) subject classifications (1970). Primary 14D05, 14H05; Secondary 14E30, 10D05, 10D15.

Key words and phrases. Weierstrass equation over function field, Mordell-Weil group, Gauss-Manin operator, modular forms, period relations.

0002-9947/80/0000-0201/$04.50

Throughout this paper, the point at ∞ is used as the identity element of the group.

2. A C(t)-rational solution.

PROPOSITION 2.1. *There is a* $\mathbf{C}(t)$*-rational solution*

$$P_0 = (x_0, y_0),$$
$$x_0 = mt + b,$$
$$y_0 = im(x_0 - t^2 - c),$$

of the Weierstrass equation

$$y^2 = x(x-1)(x - t^2 - c),$$

where

$$b = c + \sqrt{c^2 - c}\,, \quad \text{and} \quad m = \sqrt{1 - 2b}\,.$$

PROOF. This solution was found by substituting $mt + b$ for x, and then finding m and b so that

$$(mt + b)(mt + b - 1) = -m^2(mt + b - t^2 - c).$$

This solution was suggested by G. Shimura to W. Hoyt, who communicated it to me.

Throughout what follows, let c be a constant different from 0 and 1.

In solving for m and b, we found the following useful relations

$$m^2 = 1 - 2b, \tag{2.1}$$

and

$$c^2 - c = (c - b)^2. \tag{2.2}$$

Furthermore, one can show, using these relations:

LEMMA 2.2. *If* λ *denotes the quantity* $t^2 + c$ *we get the relation*

$$-(x_0 - \lambda)(x_0 - 2b + \lambda) = \lambda(\lambda - 1).$$

3. The Gauss-Manin operator applied to an elliptic integral. The following is well known (cf. [**10**], [**8**]) and can be checked by a routine calculation:

PROPOSITION 3.1. *Let* y *be defined implicitly as a function of the two independent variables* x *and* λ *by the Legendre equation* $y^2 = x(x-1)(x-\lambda)$, *and let* $\mathfrak{L}$ *be the different operator*

$$\mathfrak{L} = 4\lambda(\lambda - 1)\frac{\partial^2}{\partial\lambda^2} + 4(2\lambda - 1)\frac{\partial}{\partial\lambda} + 1.$$

Then

$$\mathfrak{L}(y^{-1}) = \frac{\partial}{\partial x}\left(\frac{-2y}{(x-y)^2}\right).$$

For a fixed $\lambda_0 \in \mathbf{C} - \{0, 1\}$, let γ_1 and γ_2 be loops about 0 and 1 and about 1 and λ, respectively. Then there are holomorphic functions $\omega_1(\lambda)$ and $\omega_2(\lambda)$ defined near λ_0 by

$$\omega_i(\lambda) = \int_{\gamma_i} (x(x-1)(x-\lambda))^{-1/2}\, dx,$$

where the integrand is obtained from a fixed determination of the square root along the path γ_i.

COROLLARY 3.2. $\mathfrak{L}(\omega_i) = 0$.

PROOF. Observe that the determination of the square root is the same at the end of a tour around a loop γ_i as at the start, since exactly two of the zeros of $x(x-1)(x-\lambda)$ lie inside γ_i. The result follows. Q.E.D.

Let G_K denote the group of solutions of $y^2 = x(x-1)(x-\lambda)$ in some finite algebraic extension K of $\mathbf{C}(\lambda)$. Let G denote $G_{\mathbf{C}(\sqrt{\lambda-c})}$.

Let $P = (x, y) \in G_K$. Following Manin **[10]**, we define a group homomorphism μ, from G_K to K, by

$$\mu(P) = \mathfrak{L}\int_{\infty}^{P} (x(x-1)(x-\lambda))^{-1/2}\, dx.$$

PROPOSITION 3.3. *If $P_0 = (x_0, y_0)$ is the solution presented in* §2, *then* $\mu(P_0) = i(b-c)t^{-3}$.

The proof of this is a calculation, making use of Proposition 3.1, Lemma 2.2, and equations (2.1) and (2.2).

Clearly, the map μ annihilates torsion. Thus we get

COROLLARY 3.4. *P_0 has infinite order. Hence G has rank at least one.*

4. The rank of the Mordell-Weil group. In this section, we use a formula of Shioda to show that the rank r of G is at most 1. Since we have seen that $r > 1$, this will prove that $r = 1$.

Observe that the substitutions

$$x = X + (1+\lambda)/3, \qquad y = Y/2$$

transform the Legendre equation $y^2 = x(x-1)(x-\lambda)$ into an equation of the form

$$Y^2 = 4X^3 - G_2X - G_3,$$

with

$$G_2 = (4/3)(\lambda^2 - \lambda + 1),$$
$$G_3 = (-4/27)(\lambda+1)(\lambda-2)(1-2\lambda),$$
$$\Delta = G_2^3 - 27G_3^2 = 2^4\lambda^2(\lambda-1)^2,$$

and

$$J = 12^3G_2^3/\Delta = 2^8(\lambda^2-\lambda+1)^3/\left(\lambda^2(\lambda-1)^2\right).$$

Let $\bar{X}$ be the t-sphere, and let $X = \bar{X} - \{\sqrt{-c}, -\sqrt{-c}, \sqrt{1-c}, -\sqrt{1-c}, \infty\}$. Let $\bar{V} \to \bar{X}$ be the Neron model of

$$y^2 = x(x-1)(x-t^2-c)$$

relative to $\mathbf{C}(t)$. Recall from Neron [**11**] that $\bar{V}$ is the minimal desingularization of the subvariety B of $\bar{X} \times P^2$ defined by (1.1), relative to projection on $\bar{X}$.

Observe that $\bar{V}$ has singular fibers over $\bar{X} - X$ only, since the singular fibers occur only above the zeros and poles of $\Delta = 2^4(t^2+c)^2(t^2+c-1)^2$.

PROPOSITION 4.1 (SHIODA'S FORMULA). *Let $W \to Y$ be the Neron model of an elliptic surface. Let g be the genus of the base Y, ν the number of singular fibers of the Neron model, ν_1 the number of singular fibers of Kodaira type I_b with $b \geq 1$, and p_g the geometric genus of W. Let r be the rank of the group of rational sections of the elliptic surface over Y. Then $r \leq 4g - 4 + 2\nu - \nu_1 - 2p_g$.*

PROOF. This formula is taken from Shioda [**13**, p. 30, Corollary 2.7]. Q.E.D.

Since the $\mathbf{C}(t)$-rational solution P of (1.1) can be viewed as a section of $B \to \bar{X}$, and the r in the formula is the rank of the group G,

THEOREM 4.2. *The rank of G is* 1.

PROOF. One can read the structure types of the singular fibers of the Neron model from Neron [**11**, pp. 123–125], if one knows the order of each of the functions G_3, Δ, and J at each of the points of $\bar{X} - X$. Kodaira [**9**, pp. 563–565] gives the Kodaira type of each of these fibers.

The result follows from counting fibers, and from the fact that $g = 0$, $p_g \geq 0$, and $r \geq 1$. Q.E.D.

5. Functions associated to rational solutions. Much of what occurs in this section is a specialization of results of Hoyt ([**2**]–[**5**]).

Let Γ_0 denote the subgroup of $SL(2, \mathbf{Z})$ generated by $\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&0\\2&1\end{smallmatrix}\right)$. Note that $-\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \notin \Gamma_0$, and that Γ_0 is a subgroup of index 2 in the principal congruence subgroup

$$\Gamma_2 = \Gamma_0 \cdot \pm \begin{pmatrix}1&0\\0&1\end{pmatrix}$$

of level 2.

We would now like to consider λ as modular function for Γ_0.

PROPOSITION 5.1. *There are holomorphic modular forms e_1, e_2, e_3 of weight 2, and λ and s of weight 0 and 1, respectively, for Γ_0; these can be defined in terms of the Weierstrass $\wp$-function by*

$$\begin{aligned} e_1(\tau) &= \wp(\tau/2, \tau, 1), \\ e_2(\tau) &= \wp(1/2, \tau, 1), \\ e_3(\tau) &= \wp((\tau+1)/2, \tau, 1), \\ \lambda(\tau) &= (e_3 - e_1)/(e_2 - e_1), \end{aligned}$$

and

$$s(\tau) = (e_2 - e_1)^{1/2}.$$

The first four functions are well known: see Ahlfors [1]. Hoyt [3] shows that $s(\tau)$ is a modular form for Γ_0.

As in [3], λ: $H \to \mathbf{C} - \{0, 1\}$ and Γ_0 may be identified with the universal cover and fundamental group of $\mathbf{C} - \{0, 1\}$ with an element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of Γ_0 acting on H by $\tau \to (a\tau + b)/(c\tau + d)$.

Let $g_2(\tau)$ and $g_3(\tau)$ be the usual modular forms of weight 4 and 6, respectively, and let G_2 and G_3 be as in §4. Then

PROPOSITION 5.2. $G_2 = g_2(\tau)s(\tau)^{-4}$ *and* $G_3 = g_3(\tau)s(\tau)^{-6}$.

This follows from the definitions of G_2, G_3, and s, and from the fact that the e_i are the roots of the polynomial $4z^3 - g_2(\tau)z - g_3(\tau)$.

It is well known that every finite algebraic extension K of $\mathbf{C}(\lambda)$ corresponds to a nonconstant holomorphic map φ: $\overline{X} \to \mathbf{P}^1$ from the compact Riemann surface $\overline{X}$ for K onto the Riemann surface $\mathbf{P}^1$ for $\mathbf{C}(\lambda)$. Let ψ: $U \to X$ be the universal cover of $X = \varphi^{-1}(\mathbf{P}^1 - \{0, 1, \infty\})$, and let $\pi_1(X)$ be the fundamental group of X. Then it follows from basic properties of covering spaces that there are a holomorphic map ω: $U \to H$, and a homomorphism M: $\pi_1(X) \to \Gamma_0$ such that $\lambda \circ \omega = \varphi \circ \psi$, and $\omega \circ \sigma = M(\sigma) \circ \omega$, for $\sigma \in \pi_1(X)$. (In the present case, the map φ is given by $\varphi(t) = t^2 + c$, and $X = \mathbf{C} - \{\pm\sqrt{-c}, \pm\sqrt{1-c}\}$.)

Let V be the subvariety of $X \times \mathbf{P}^2$ defined by (1.1). Then

PROPOSITION 5.3. *The universal cover of V can be identified with the map* Φ: $U \times \mathbf{C} \to X \times \mathbf{P}^2$ *defined by*

$$\Phi(u, z) = (\psi(u), (0, 0, 1)) \quad \text{if } z \in \mathbf{Z}\omega(u) + \mathbf{Z}$$

and

$$\Phi(u, z) = \left(\psi(u), \left(1, \frac{\wp(z, \omega(u), 1)}{s(\omega(u))^2} + \frac{\lambda(\omega(u)) + 1}{3}, \frac{\wp'(z, \omega(u), 1)}{2s(\omega(u))^3}\right)\right)$$

otherwise,

and the fundamental group of V can be identified with a semidirect product of $\pi_1(X)$ and $\mathbf{Z} \times \mathbf{Z}$, acting on $U \times \mathbf{C}$ by the map

$$g(\sigma, m, n)(u, z) = \left(\sigma(u), (c\omega(u) + d)^{-1}(z + m\omega(u) + n)\right)$$

for $\sigma \in \pi_1(X)$ with $M(\sigma) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $(m, n) \in \mathbf{Z} \times \mathbf{Z}$, $u \in U$, and $z \in \mathbf{C}$.

PROOF. See Hoyt [4].

PROPOSITION 5.4. *For each $u \in U$, the holomorphic differential dx/y on the fiber of $V \to X$ above $\psi(u)$ pulls back via Φ to the differential $dx/y = 2s(\omega(u))\,dz$ on $\{u\} \times \mathbf{C}$. Also, the line segments $\{u\} \times [0, \omega(u)]$ and $\{u\} \times [0, 1]$ on $\{u\} \times \mathbf{C}$ map via Φ to closed loops $C_1(u)$ and $C_2(u)$, which generate the homology of the fiber of*

$V \to X$ above $\psi(u)$. Consequently, the periods of dx/y on those loops are

$$\int_{C_1(u)} y^{-1}\,dx = 2s(\omega(u))\omega(u)$$

and

$$\int_{C_2(u)} y^{-1}\,dx = 2s(\omega(u)).$$

This follows from the definition of the map Φ.

Each $\mathbf{C}(t)$-rational solution P may be viewed as a holomorphic section (also denoted P) of $B \to \overline{X}$. Then it follows, by analytic continuation, that P determines (uniquely, up to choice of base point) a holomorphic function F_P such that the following maps commute:

$$\begin{array}{ccc} U \times \mathbf{C} & \xrightarrow{\ \Phi\ } & V \subset B \\ \downarrow \ \text{(identity, } F_P) & & \downarrow \quad \downarrow \ P \\ U & \xrightarrow[\ \psi\ ]{} & X \subset \overline{X} \end{array}$$

PROPOSITION 5.5. (i) $F_P(u) = (2s(\omega(u)))^{-1}\int_\infty^P y^{-1}\,dx$, *where the path of integration is the image under Φ of the line segment $\{u\} \times [0, F_P(u)]$ in $\{u\} \times \mathbf{C}$.*

(ii) *F_P transforms as follows: if $\sigma \in \pi_1(X)$, and $M(\sigma) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then,*

$$F_P \circ \sigma = (c\omega(u) + d)^{-1}\left[F_P + q(F_P, \sigma)\omega(u) + r(F_P, \sigma)\right],$$

where $q(F_P, \sigma)$ and $r(F_P, \sigma)$ are integers, called the periods of F_P at σ.

(iii) *The function F_P may be regarded as an Eichler integral, with integer periods, of a meromorphic function $f_P = d^2F_P/d\omega(u)^2$; that is,*

$$F_P(u) = \int_{u_1}^{u} f_P(\xi)(\omega(u) - \omega(\xi))\,d\omega(\xi) + c_1\omega(u) + c_2,$$

where c_1 and c_2 are constants of integration.

PROOF. (i) follows from the definition of the universal cover Φ:

$$\int_\infty^P y^{-1}\,dx = \int_{(u,0)}^{(u, F_P(u))} 2s(\omega(u))\,dz$$
$$= 2s(\omega(u))F_P(u).$$

(ii) follows from the fact that $(u, F_P(u))$, and $(\sigma(u), F_P(\sigma(u)))$ must map via Φ to the same point.

(iii) is proved by a calculation to show that

$$\frac{d^2}{d\omega(u)^2}\int_{u_1}^{u} f_P(\xi)(\omega(u) - \omega(\xi))\,d\omega(\xi) = f_P(u).$$

We remark that the function f_P may be regarded as a cusp form of the second kind, of weight 3, relative to a process of base extension determined by the field extension $K|\mathbf{C}(\lambda)$, as in Hoyt [5].

6. The image of the monodromy map. We now calculate the image of the monodromy map $M: \pi_1(X) \to \Gamma_0$. This is done by calculating explicitly the image of a set of generators of $\pi_1(X)$.

As before, Γ_0 can be identified with $\pi_1(\mathbf{C} - \{0, 1\}) = \pi_1(\mathbf{P}^1 - \{0, 1, \infty\})$. More explicitly,

LEMMA 6.1. *One may identify* $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$, *and* $\begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix} \in \Gamma_0$ *with the homotopy classes of suitably oriented closed curves* C_0, C_1, *and* C_∞, *with base point* $\lambda_0 \neq c$, *passing around* 0, 1, *and* ∞ *respectively.*

PROOF. See Hoyt [3]. Q.E.D.

The following continuous maps

$$\begin{array}{ccc} \mathbf{P}^1 - \{\pm\sqrt{-c}, \pm\sqrt{1-c}, \infty, 0\} & \xrightarrow{t \mapsto t^2+c} & \mathbf{P}^1 - \{0, 1, \infty, c\} \\ \big\downarrow j & & \big\downarrow i \\ \mathbf{P}^1 - \{\pm\sqrt{-c}, \pm\sqrt{1-c}, \infty\} & \xrightarrow{t \mapsto t^2+c} & \mathbf{P}^1 - \{0, 1, \infty\} \end{array}$$

induce homomorphisms of the fundamental groups

$$\begin{array}{ccc} \pi_1(\mathbf{P}^1 - \{\pm\sqrt{-c}, \pm\sqrt{1-c}, \infty, 0\}) & \xrightarrow{M'} & \pi_1(\mathbf{P}^1 - \{0, 1, \infty, c\}) \\ \big\downarrow j_* & & \big\downarrow i_* \\ \pi_1(\mathbf{P}^1 - \{\pm\sqrt{-c}, \pm\sqrt{1-c}, \infty\}) & \xrightarrow{M} & \pi_1(\mathbf{P}^1 - \{0, 1, \infty\}) = \Gamma_0. \end{array}$$

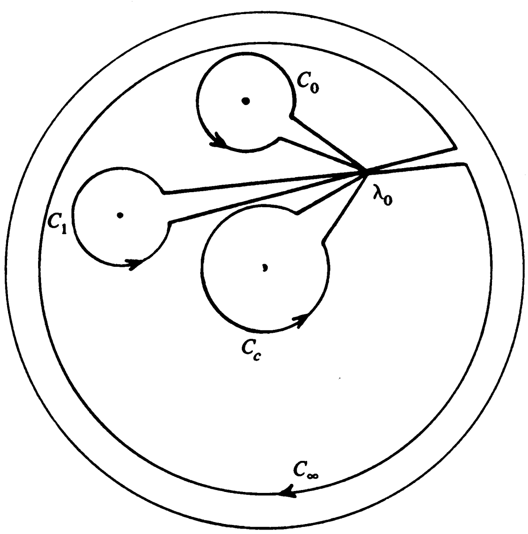

FIGURE 1

We may assume that C_0, C_1, and C_∞ do not go around c. Let C_c be a path around c, as in Figure 1. Then the homotopy classes $[C_0]$, $[C_1]$, $[C_\infty]$, and $[C_c]$ generate the fundamental group $\pi_1(\mathbf{P}^1 - \{0, 1, \infty, c\})$; also,

$$i_*[C_0] = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad i_*[C_1] = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix},$$
$$i_*[C_\infty] = \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}, \qquad i_*[C_c] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Since $t \mapsto t^2 + c$ is a two-sheeted cover, each of the paths C_0, C_1, C_∞, and C_c lifts to two paths in $\mathbf{P}^1 - \{\pm\sqrt{-c}, \pm\sqrt{1-c}, \infty, 0\}$; let C_0^+, C_1^+, C_∞^+, and C_c^+ denote the liftings with base point $\sqrt{\lambda_0 - c}$ and let C_0^-, C_1^-, C_∞^-, and C_c^- denote the liftings with base point $-\sqrt{\lambda_0 - c}$, as in Figure 2. Notice that C_0^+, C_0^-, C_1^+, and C_1^- are closed paths, while C_∞^+, C_∞^-, C_c^+ and C_c^- are not.

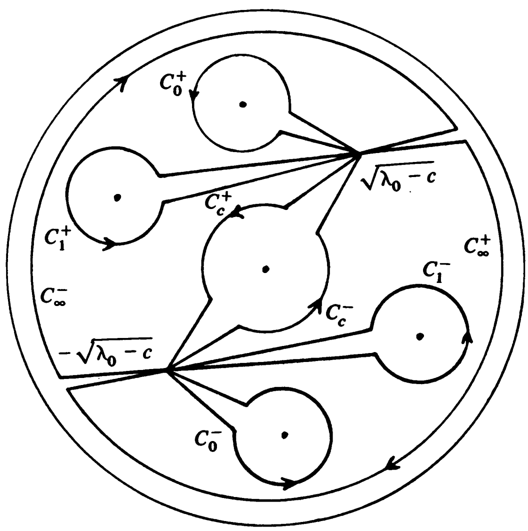

FIGURE 2

Let

$$D_0 = C_c^+ C_c^-, \quad D_{\sqrt{-c}} = C_0^+, \quad D_{\sqrt{1-c}} = C_1^+,$$
$$D_{-\sqrt{-c}} = C_\infty^+ C_0^- (C_\infty^+)^{-1}, \quad D_{-\sqrt{1-c}} = C_\infty^+ C_1^- (C_\infty^+)^{-1},$$

and

$$D_\infty = C_\infty^+ C_\infty^-.$$

Then the homotopy classes of the D's generate

$$\pi_1(\mathbf{P}^1 - \{\pm\sqrt{-c}, \pm\sqrt{1-c}, \infty, 0\}).$$

It is clear from Figure II that the product

$$[D_{\sqrt{-c}}][D_{\sqrt{1-c}}][D_0][D_{-\sqrt{-c}}][D_{-\sqrt{1-c}}][D_\infty] = 1.$$

The above definitions imply the following results.

LEMMA 6.2. *The images $M'([D])$ and $i_*(M'([D]))$ are as listed in Table* I. *Furthermore, if $\delta = j_*([D])$, then $M(\delta) = i_*(M'([D]))$. Finally, the $M(\delta)$'s can be written in the form $A^{-1}\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}A$, for some $A \in \mathrm{SL}(2, \mathbf{Z})$.*

COROLLARY 6.3. *The map*

$$M: \pi_1(\mathbf{P}^1 - \{\pm\sqrt{-c}, \pm\sqrt{1-c}, \infty\}) \to \pi_1(\mathbf{P}^1 - \{0, 1, \infty\})$$

is surjective.

TABLE I

$[D]$	$M'[D]$	$i_*(M'([D]))$	$A^{-1}\begin{pmatrix}1 & q\\0 & 1\end{pmatrix}A$
$[D_0]$	$[C_c]^2$	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$
$[D_{\sqrt{-c}}]$	$[C_0]$	$\begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}$
$[D_{\sqrt{1-c}}]$	$[C_1]$	$\begin{pmatrix}1 & 0\\-2 & 1\end{pmatrix}$	$\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}^{-1}\begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}$
$[D_{-\sqrt{-c}}]$	$[C_\infty][C_0][C_\infty]^{-1}$	$\begin{pmatrix}1 & -2\\2 & -3\end{pmatrix}\begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\begin{pmatrix}1 & -2\\2 & -3\end{pmatrix}^{-1}$	$\begin{pmatrix}-3 & 2\\-2 & 1\end{pmatrix}^{-1}\begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\begin{pmatrix}-3 & 2\\-2 & 1\end{pmatrix}$
$[D_{-\sqrt{1-c}}]$	$[C_\infty][C_1][C_\infty]^{-1}$	$\begin{pmatrix}1 & -2\\2 & -3\end{pmatrix}\begin{pmatrix}1 & 0\\-2 & 1\end{pmatrix}\begin{pmatrix}1 & -2\\2 & -3\end{pmatrix}^{-1}$	$\begin{pmatrix}2 & -1\\-3 & 2\end{pmatrix}^{-1}\begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\begin{pmatrix}2 & -1\\-3 & 2\end{pmatrix}$
$[D_\infty]$	$[C_\infty]^2$	$\begin{pmatrix}1 & -2\\2 & -3\end{pmatrix}^2$	$\begin{pmatrix}1 & 0\\-1 & 1\end{pmatrix}^{-1}\begin{pmatrix}1 & 4\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\-1 & 1\end{pmatrix}$

7. The scalar product. The following is a specialization of **[6]**, which is in turn an application of techniques of Shimura **[12]**.

For $P, Q \in G$, let F_P, f_P, F_Q and f_Q be as in §5. We define a scalar product on G as follows:

$$I(P, Q) = \int_{\partial\Pi} F_P f_Q \, d\omega(u),$$

where Π is any fundamental domain for $\pi_1(X)$ with u_0 (the point above $t = 0$) in the interior of Π.

For the proof that this integral converges, we refer to Hoyt (**[2]** and **[5]**). That $I(P, Q)$ is independent of the choice of Π follows from the way F_P, f_Q and ω are transformed by $\sigma \in \pi_1(X)$, together with the proof of bilinearity below.

PROPOSITION 7.1. *$I(P, Q)$ is a symmetric bilinear form on G.*

PROOF. Observe that F_P and f_Q are holomorphic on $\partial\Pi$, and that $\omega' = 0$ only at points where $t = 0$. Then

$$\frac{dF_P}{d\omega} = \left(\frac{dF_P}{d\omega}\right) \Big/ \left(\frac{d\omega}{du}\right),$$

$dF_Q/d\omega$, $d^2F_P/d\omega^2 = f_P$, and f_Q are all holomorphic on $\partial\Pi$.

That $I(P, Q) = I(Q, P)$ follows from the definition, together with two applications of integration by parts.

That $I(P + P', Q) = I(P, Q) + I(P', Q)$ follows from the fact that $F_{P+P'} = F_P + F_{P'} + a\omega(u) + b$, for some integers a and b. Thus, one need only observe that

$$\int_{\partial\Pi} (a\omega(u) + b) f_Q \, d\omega(u) = \int_{\partial\Pi} \frac{d^2}{d\omega^2}(a\omega(u) + b) F_Q \, d\omega(u) = 0. \quad \text{Q.E.D.}$$

We remark that this bilinear form is the restriction of a bilinear form defined on the space of cusp forms of the second kind, of weight 3, relative to a process of base extension, as in Hoyt [5]. The above proof is an adaptation of a proof in [5].

THEOREM 7.2. *For all* $P, Q \in G$, $4I(P, Q)$ *is an integer.*

For the proof, denote F_P by F, f_P by f, F_Q by G and f_Q by g; denote $\omega(u)$ by τ.

PROOF. Recall that F is an Eichler integral for f:

$$F(u) = \int_{u_1}^{u} f(\xi)(\omega(u) - \omega(\xi))\, d\omega(\xi).$$

Then the integrand in the definition of I can be rewritten as

$$Fg\, d\tau = {}^t\mathbf{F}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} d\mathbf{G}$$

in terms of the vector valued differentials and functions

$$d\mathbf{G} = \begin{pmatrix} \tau \\ 1 \end{pmatrix} g\, d\tau,$$

$$\mathbf{F} = \int_{u_1}^{u} \begin{pmatrix} \tau \\ 1 \end{pmatrix} f\, d\tau = \int_{u_1}^{u} d\mathbf{F},$$

$$F = -(\tau, 1)\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\mathbf{F}.$$

If $\sigma \in \pi_1(X)$ and if $M(\sigma) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then F and $\mathbf{F}$ have periods $(p(\sigma), q(\sigma))$ and $\mathbf{X}(\sigma)$, respectively, which satisfy

$$F \circ \sigma = (c\tau + d)^{-1}(F + p(\sigma)\tau + q(\sigma)),$$
$$\mathbf{F} \circ \sigma = M(\sigma)\mathbf{F} + \mathbf{X}(\sigma),$$

and

$$\mathbf{X}(\sigma^{-1}) = \begin{pmatrix} q(\sigma) \\ -p(\sigma) \end{pmatrix} = -M(\sigma^{-1})\mathbf{X}(\sigma).$$

As in §5, $p(\sigma)$ and $q(\sigma)$ are integers, hence, $\mathbf{X}(\sigma)$ is an integer vector. Similarly let $\mathbf{Y}(\sigma)$ be defined by

$$\mathbf{G} \circ \sigma = M(\sigma)\mathbf{G} + \mathbf{Y}(\sigma).$$

Observe that $\mathbf{X}$ and $\mathbf{Y}$ satisfy the cocycle condition: if $\rho, \sigma \in \pi_1(X)$, then

$$\mathbf{X}(\rho\sigma) = \mathbf{X}(\rho) + M(\rho)\mathbf{X}(\sigma).$$

Finally, observe that, for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL(2, \mathbf{Z})$,

$${}^t\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Denote the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ by $\mathbf{P}$.

Choose Π as in Shimura [12]. However, in the present (specialized) case, the genus of the Riemann surface X is zero, and the generators of $\pi_1(X)$ are all parabolic. Then Π is a polygon with five pairs of edges, D_k, $-\delta_k D_k$, corresponding to the five generators δ_k, with the relation $\delta_5\delta_4\delta_3\delta_2\delta_1 = 1$. (Each δ_k is one of the δ's of Table I.) Let v_0 (the starting point of the edge D_1) be chosen to be a point not a cusp and not above $t = 0$. Let s_k be the cusp stabilized by δ_k. Observe that the edge D_k runs from $\delta_{k-1} \cdots \delta_1(v_0)$ to s_k, and that $-\delta_k D_k$ runs from s_k to $\delta_k \cdots \delta_1(v_0)$.

Then

$$I(P,Q) = \int_{\partial \Pi} {}^t\mathbf{F}\mathbf{P}\, d\mathbf{G} = \sum_{k=1}^{5} \int_{D_k} {}^t\mathbf{F}\mathbf{P}\, d\mathbf{G} - \int_{\delta_k D_k} {}^t\mathbf{F}\mathbf{P}\, d\mathbf{G}.$$

But

$$\begin{aligned}\int_{\delta_k D_k} {}^t\mathbf{F}\mathbf{P}\, d\mathbf{G} &= \int_{D_k} {}^t(\mathbf{F} \circ \delta_k)\mathbf{P}\, d(\mathbf{G} \circ \delta_k) \\ &= \int_{D_k} {}^t(M(\delta_k)\mathbf{F} + \mathbf{X}(\delta_k))\mathbf{P} M(\delta_k)\, d\mathbf{G} \\ &= \int_{D_k} {}^t\mathbf{F}\mathbf{P}\, d\mathbf{G} + {}^t\mathbf{X}(\delta_k)\mathbf{P} M(\delta_k) \int_{D_k} d\mathbf{G}.\end{aligned}$$

So

$$\begin{aligned}I(P,Q) &= \sum_{k=1}^{5} -{}^t\mathbf{X}(\delta_k)\mathbf{P}M(\delta_k)\int_{D_k} d\mathbf{G} = \sum_{k=1}^{5} {}^t\mathbf{X}(\delta_k^{-1})\mathbf{P}\int_{D_k} d\mathbf{G} \\ &= \sum_{k=1}^{5} {}^t\mathbf{X}(\delta_k^{-1})\mathbf{P}\left[\mathbf{G}(s_k) - \mathbf{G}(\delta_{k-1} \cdots \delta_1 v_0)\right] \\ &= \sum_{k=1}^{5} {}^t\mathbf{X}(\delta_k^{-1})\mathbf{P}\mathbf{G}(s_k) \\ &\quad - \sum_{k=1}^{5} {}^t\mathbf{X}(\delta_k^{-1})\mathbf{P}\left[M(\delta_{k-1} \cdots \delta_1)\mathbf{G}(v_0) + \mathbf{Y}(\delta_{k-1} \cdots \delta_1)\right].\end{aligned}$$

Observe that

$$\begin{aligned}\sum_{k=1}^{5} {}^t\mathbf{X}(\delta_k^{-1})\mathbf{P}M(\delta_{k-1} \cdots \delta_1) &= \sum_{k=1}^{5} {}^t\mathbf{X}(\delta_k^{-1})\,{}^tM((\delta_{k-1} \cdots \delta_1)^{-1})\mathbf{P} \\ &= \sum_{k=1}^{5} {}^t(M(\delta_{k-1} \cdots \delta_1)^{-1}\mathbf{X}(\delta_k^{-1}))\mathbf{P} \\ &= \sum_{k=1}^{5} {}^t\left[\mathbf{X}((\delta_k \cdots \delta_1)^{-1}) - \mathbf{X}((\delta_{k-1} \cdots \delta_1)^{-1})\right]\mathbf{P} \\ &= 0,\end{aligned}$$

since $\delta_5\delta_4\delta_3\delta_2\delta_1 = 1$. But

$$\sum_{k=1}^{5} {}^t\mathbf{X}(\delta_k^{-1})\mathbf{P}\mathbf{Y}(\delta_{k-1} \cdots \delta_1)$$

is an integer. We now show that four times ${}^t\mathbf{X}(\delta_k^{-1})\mathbf{P}\mathbf{G}(s_k)$ is an integer, $k = 1, \ldots, 5$.

It has already been observed that, for each δ_k in Table I, $M(\delta_k)$ can be written in the form $A^{-1}\begin{pmatrix} 1 & q_k \\ 0 & 1 \end{pmatrix}A$, for some $A = A_k = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z})$. Notice, from the definition of $\mathbf{X}(\delta)$, and from the fact that $\delta_k^{-1}(s_k) = s_k$, that

$$\mathbf{X}(\delta_k^{-1}) = (I - M(\delta_k^{-1}))\mathbf{F}(s_k),$$

where I is the identity matrix. If $\mathbf{F}(s_k) = \binom{u}{v}$ and $\mathbf{G}(s_k) = \binom{w}{z}$, then

$$\mathbf{X}(\delta_k^{-1}) = q(cu + dv)\begin{pmatrix} d \\ -c \end{pmatrix},$$

$$\mathbf{Y}(\delta_k^{-1}) = q(cw + dz)\begin{pmatrix} d \\ -c \end{pmatrix},$$

$${}^t\mathbf{X}(\delta_k^{-1})\mathbf{P}\mathbf{G}(s_k) = -q(cu + dv)(cw + dz),$$

and

$${}^t\mathbf{X}(\delta_k^{-1}){}^tAA\mathbf{Y}(\delta_k^{-1}) = q^2(cu + dv)(cw + dz).$$

But this last expression is necessarily an integer, being a product of integer matrices; hence $q_k{}^t\mathbf{X}(\delta_k^{-1})\mathbf{P}\mathbf{G}(s_k)$ is an integer for all k. Hence $4I(P, Q)$ must be an integer, since 4 is the least common multiple of the q_k's. Q.E.D.

8. Application of the bilinear form. In this section, we show that P_0 (the solution found in §2) is not a multiple of any other solution. We will need the following

LEMMA 8.1. *The following two differential operators are equal*:

$$(2\pi i)^{-2}\lambda(\lambda - 1)s^3\mathfrak{L}(-) = (d^2/d\tau^2)(-/s).$$

PROOF. See [7, Theorem 1.7].

We will also need

LEMMA 8.2. $\lambda'(\tau) = (1/\pi i)\lambda(\lambda - 1)s^2$.

PROOF. See [7, Lemma 1.6].

PROPOSITION 8.3. $I(P_0, P_0) = \frac{1}{4}$.

PROOF. We wish to find the residue of the integrand $F_{P_0}f_{P_0}\,d\omega(u)$ at each of its poles in Π. However, since F_{P_0} and ω are holomorphic in Π, the only pole is where ω' is zero, that is, at u_0, a point lying above $t = 0$. Since $\tau = \omega(u)$ is ramified of order 2 at $u = u_0$, we will take $(\tau - \tau_0)^{1/2}$ as the parameter near u_0 ($\tau_0 = \omega(u_0)$), and will find the expansion of the integrand in terms of this parameter.

Since F_{P_0} can be computed by $F_{P_0}(u) = (2s(\omega(u)))^{-1}\int_\infty^P y^{-1}\,dx$, then

$$f_{P_0} = \frac{d^2}{d\omega^2}F_{P_0} = \frac{\lambda(\lambda - 1)s^3}{2(2\pi i)^2}\mathfrak{L}\int_\infty^{P_0} y^{-1}\,dx = \left[\frac{\lambda(\lambda - 1)s^3}{(2(2\pi i)^2)}\right] i\,\frac{(b - c)}{t^3}.$$

We compute the leading term of each of the functions λ, $\lambda - 1$, s^3, and t^{-3}, in terms of the parameter $(\tau - \tau_0)^{1/2}$:

$$\begin{aligned}\lambda &= \lambda(\tau_0) + \lambda'(\tau_0)(\tau - \tau_0) + \text{higher order terms}\\ &= c + (1/\pi i)\lambda(\tau_0)(\lambda(\tau_0) - 1)s(\tau_0)^2(\tau - \tau_0) + \text{H.O.T.}\\ &= c + (1/\pi i)(c^2 - c)s(\tau_0)^2(\tau - \tau_0) + \text{H.O.T.},\end{aligned}$$

$$\lambda - 1 = (c - 1) + \text{H.O.T.},$$

$$s(\tau)^3 = s(\tau_0)^3 + \text{H.O.T.},$$

$$t = (\lambda - c)^{1/2} = \left((1/\pi i)(c^2 - c)s(\tau_0)^2(\tau - \tau_0)\right)^{1/2} + \text{H.O.T.}$$

and

$$t^{-3} = s(\tau_0)^{-3}((1/\pi i)(c^2 - c))^{-3/2}(\tau - \tau_0)^{-3/2} + \text{H.O.T.}$$

Since $(b-c)^2 = c^2 - c$ (equation (2.2))

$$f_{P_0} = \big(i/\big(8(\pi i)^{1/2}\big)\big)(\tau - \tau_0)^{-3/2} + \text{H.O.T.}$$

Suppose F_{P_0} has the power series expansion $\sum_{j=0}^{\infty} a_j(\tau - \tau_0)^{j/2}$. Then f_{P_0} has the expansion

$$-\tfrac{1}{4}a_1(\tau - \tau_0)^{-3/2} + \sum_{j=3}^{\infty}\left(\frac{j(j-2)}{4}\right)a_j(\tau - \tau_0)^{(j-4)/2},$$

and $a_1 = -i/(2(\pi i)^{1/2})$. Notice that f_{P_0} has no term in $(\tau-\tau_0)^{-2}$ or $(\tau - \tau_0)^{-1}$, so that the a_0 and a_2 terms of F_{P_0} will not enter into the calculation.

Since $\tau = ((\tau - \tau_0)^{1/2})^2 + \tau_0$, $d\tau = 2(\tau - \tau_0)^{1/2}d(\tau - \tau_0)^{1/2}$. Then

$$\begin{aligned} I(P_0, P_0) &= \int_{\partial\Pi} f_{P_0}F_{P_0}\,d\tau = 2\pi i(\text{residue of } f_{P_0}F_{P_0}\,d\tau \text{ at } u_0) \\ &= 2\pi i\big(i/\big(8(\pi i)^{1/2}\big)\big)\big(-i/\big(2(\pi i)^{1/2}\big)\big)\cdot 2 = \tfrac{1}{4}. \quad \text{Q.E.D.} \end{aligned}$$

COROLLARY 8.4. *P_0 is not a multiple of any element of G.*

PROOF. Suppose P_0 is some multiple, say $P_0 = qQ_0$. Since I is bilinear,

$$1 = 4I(P_0, P_0) = 4I(qQ_0, qQ_0) = 4q^2I(Q_0, Q_0).$$

Since $4I(P, Q) \in \mathbf{Z}$, it follows that $1/q^2$ must be an integer. Q.E.D.

9. The torsion subgroup. In this section we prove the following:

THEOREM 9.1. *The torsion subgroup of G is $\{(0, 0), (1, 0), (t^2 + c, 0), \infty\}$.*

PROOF. These are obviously solutions; by the definition of addition in the group, it is clear that the first three are of order 2. The following is well known:

LEMMA 9.2. *The group of solutions of a Weierstrass equation has at most N^2 elements whose order divides N.*

PROOF. See Tate [**14**, pp. 2–5]. Q.E.D.

The following proposition will complete the proof of Theorem 9.1, and also Theorem 1.1.

PROPOSITION 9.3. *If P is a torsion element of G, then P is of order* 2.

PROOF. Let P be a torsion element; then $\mu(P) = 0$. Since $F_P = (1/2s)\int_{\infty}^{P} y^{-1}\,dx$, $(d^2/d\omega^2)F_P = 0$. Hence $F_P = \alpha\omega(u) + \beta$, for some $\alpha, \beta \in \mathbf{C}$.

For $\sigma \in \pi_1(\mathbf{C} - \{\pm\sqrt{-c}, \pm\sqrt{1-c}\})$, let $M(\sigma) = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$. Then

$$\omega(\sigma(u)) = (M(\sigma)\circ\omega)(u) = (a\omega(u) + b)(c\omega(u) + d)^{-1};$$

also

$$\begin{aligned} (F_P \circ \sigma)(u) &= (c\omega(u) + d)^{-1}(F_P(u) + m\omega(u) + n) \\ &= (c\omega(u) + d)^{-1}((\alpha + m)\omega(u) + \beta + n), \end{aligned}$$

where $m, n \in \mathbf{Z}$.

On the other hand,

$$(F_P \circ \sigma)(u) = \alpha\omega(\sigma(u)) + \beta = \alpha(a\omega(u) + b)(c\omega(u) + d)^{-1} + \beta.$$

Therefore

$$\alpha(a\omega(u) + b) + \beta(c\omega(u) + d) = (\alpha + m)\omega(u) + \beta + n.$$

Let

$$\sigma = j_*\left(\left[D_{\sqrt{1-c}}\right]^{-1}\left[D_{\sqrt{-c}}\right]\right),$$

as in Table I. Then

$$M(\sigma) = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}.$$

Then, using this σ, we get

$$\alpha(\omega(u) + 2) + \beta(2\omega(u) + 5) = (\alpha + m)\omega(u) + \beta + n,$$

so $\alpha + 2\beta = \alpha + m$, and $2\alpha + 5\beta = \beta + n$. Therefore $\alpha = n/2 - m$, and $\beta = m/2$. Then $2F_P$ is an integer combination of ω and 1, and $\int_\infty^{2P} y^{-1}\,dx$ is an integer combination of the periods $2s(\omega(u))\omega(u)$ and $2s(\omega(u))$. Hence the path from ∞ to $2P$ is a loop, and $2P = \infty$. Therefore P has order 2. Q.E.D.

Bibliography

1. L. Ahlfors, *Complex analysis*, McGraw-Hill, New York, 1966.
2. W. Hoyt, *On holomorphic sections of elliptic surfaces* (in preparation).
3. ______, *On the Legendre equation* (in preparation).
4. ______, *On Weierstrass equations over function fields*, Trans. Amer. Math. Soc. (submitted).
5. ______, *Parabolic cohomology and cusp forms of the second kind for extensions of fields of modular functions*, to be submitted to Proc. Sympos. Automorphic Forms and Fuchsian Groups, held at the University of Pittsburgh, 1978.
6. W. Hoyt and C. Schwartz, *On period relations for cusp forms of the second kind* (in preparation).
7. ______, *On Picard-Fuchs operators for elliptic surfaces*, to be submitted to Proc. Sympos. Automorphic Forms and Fuchsian Groups, held at the University of Pittsburgh, 1978.
8. N. Katz, *On the differential equations satisfied by period matrices*, Publ. Math. Inst. Hautes Etudes Sci., no. 35.
9. K. Kodaira, *On compact analytic surfaces*. II, Ann. of Math. (2) **77** (1963), 563–626.
10. Ju. I. Manin, *Rational points on algebraic curves over function fields*, Amer. Math. Soc. Transl. (2) **50** (1966), 189–234.
11. A Neron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publ. Math. Inst. Hautes Etudes Sci., no. 21.
12. G. Shimura, *Sur les intégrales attachées aux formes automorphes*, J. Math. Soc. Japan **11** (1959), 291–311.
13. T. Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan **24** (1972), 20–59.
14. J. Tate, *Rational points in elliptic curves*, Philips Lectures, Haverford College, 1961.

Department of Mathematics, Texas Tech University, Lubbock, Texas 79409

Current address: Department of Mathematics, Temple University, Philadelphia, Pennsylvania 19122