Tôhoku Math. J.
44 (1992), 335–344

THE MORDELL-WEIL GROUP OF CERTAIN ABELIAN VARIETIES DEFINED OVER THE RATIONAL FUNCTION FIELD

FUMIO HAZAMA*

(Received July 8, 1991, revised November 14, 1991)

Abstract. An explicit method of construction of a family of abelian varieties each member of which has a large Mordell-Weil rank is given. Also, an example of elliptic curve defined over a function field of one variable such that its Mordell-Weil group is of arbitrarily high rank is constructed.

Introduction. In our earlier paper [3], we proved the following theorem:

THEOREM 0.1. *Let C be a hyperelliptic curve over a field k and let A be an abelian variety over k. Let A_b denote the twist of A by the quadratic extension $k(C)/k(\boldsymbol{P}^1)$ so that A_b is an abelian variety over $k(\boldsymbol{P}^1)=k(t)$. Then we have an isomorphism of abelian groups*

$$A_b(k(t))\cong \mathrm{Hom}_k(J(C), A)\oplus A_2(k),$$

where $A_2(k)$ denotes the group of k-rational 2-division points on A.

In PART A of this paper we investigate what occurs if one specializes the value of t in (0.1) (see Theorem 2.1). This enables one to reduce the problem of the injectivity of the specialization map of the family to that of the unsolvability of a certain Diophantine equation. Such examples are given in Section 3. In particular, we obtain an example of a family E_t of elliptic curves over $\boldsymbol{P}^1$ such that for any $t\in \boldsymbol{P}^1(\boldsymbol{Q})-\{0, \pm 1, \infty\}$, the Mordell-Weil group $E_t(\boldsymbol{Q})$ has rank ≥ 2. In PART B we formulate a generalization of Theorem 0.1 to the case of arbitrary double coverings (see Theorem 4.1). As a corollary, we obtain an elliptic curve E defined over the function field of a curve C over $\boldsymbol{Q}$ such that its Mordell-Weil group $E(\boldsymbol{Q}(C))$ is of arbitrarily high rank (see Theorem 4.5). For the construction, we use certain modular curves and its *Atkin-Lehner involutions*.

Thanks are due to Professor Tomoyoshi Ibukiyama for valuable suggestions. Thanks are also due to Ms. Michiko Toki for useful conversation.

1991 *Mathematics Subject Classification*. Primary 14K15.

* Partially supported by Grant-in-Aid for General Scientific Research, the Ministry of Education, Science and Cluture, Japan.

PART A

1. Preliminaries. First we recall the following criterion:

LEMMA 1.1 (cf. [10, p. 152]). *Let* $\varphi: M \to N$ *be a homomorphism of abelian groups and let* n *be an integer* ≥ 2. *We assume that*

(1) M *is finitely generated,*

(2) $M/nM \to N/nN$ *is injective,*

(3) φ *is injective on the torsion subgroup of* M,

(4) φ *defines an isomorphism of* $M_n = \{x \in M; nx = 0\}$ *onto* N_n.

Then φ *is injective.*

Next we recall the following construction. This is explained in Silverman's book [11, Ch. X, Th. 1.1] in the case of elliptic curves. The following description is a straightforward generalization to the hyperelliptic case. Let k be a field of arbitrary characteristic and denote by C the hyperelliptic curve defined by

$$y^2 = (x - e_1) \cdots (x - e_{2g+1}),$$

where $e_i \in k$, $e_i \neq e_j$ for $i \neq j$. We denote by ∞ the point at infinity of C. We define a map $\alpha: J(C) \to (k^*/k^{*2})^{2g}$ by

$$\alpha\left(\sum_{i=1}^{g} (P_i - (\infty))\right) = \left(\prod_{i=1}^{g} \mu_j(P_i)\right)_{j=1,\dots,2g},$$

where

$$\mu_j(P) = \begin{cases} x(P) - e_j & \text{if} \quad P \neq (e_j, 0), \infty, \\ \left(\prod_{i=1}^{2g+1} (x(P) - e_i)\right) \Big/ (x(P) - e_j) & \text{if} \quad P = (e_j, 0), \\ 1 & \text{if} \quad P = \infty. \end{cases}$$

It is known that this α gives a well-defined homomorphism $J(C)(k) \to (k^*/k^{*2})^{2g}$. Note that Silverman's proof in [loc. cit.] for the elliptic case also goes through in the hyperelliptic case, since the divisor $(x - e_i)$ of the function $x - e_i$ is equal to $2(e_i, 0) - 2(\infty)$.

2. Specialization. In this section we formulate a theorem which gives us a large supply of abelian varieties whose Mordell-Weil groups are of rank ≥ 1.

THEOREM 2.1. *Let* c *be a rational number and let* $g(X)$ *be an irreducible polynomial of even degree* $2g$ *in* $\mathbf{Q}[X]$ *such that* $g(c)$ *is not a square in* $\mathbf{Q}$. *Let* $f(X) = (X - c)g(X)$ *and let* C_t *denote the hyperelliptic curve over* $\mathbf{Q}(t)$ *defined by the equation*

$$f(t)y^2 = f(x).$$

If, for a given $a \in \boldsymbol{Q}$, *neither* $g(a)$ *nor* $g(c)g(a)$ *is a square in* $\boldsymbol{Q}$, *then the* $\boldsymbol{Q}$*-rational point* $(a, 1)-(\infty) \in J(C_a)(\boldsymbol{Q})$ *is not torsion.*

PROOF. Let $\theta_1, \ldots, \theta_{2g}$ denote the roots of $g(X)=0$ and let k denote the field $\boldsymbol{Q}(\theta_1, \ldots, \theta_{2g})$. We put $\theta_0 = c$ for convenience. First we note that there is an isomorphism of curves over $\boldsymbol{Q}(t)$

$$\beta_t\colon C_t \to X_t\,,$$

where X_t denotes the hyperelliptic curve defined by

$$y^2 = (x - f(t)c) \times \prod_{i=1}^{2g} (x - f(t)\theta_i)$$

and $\beta_t(x, y) = (f(t)x, (f(t))^g y)$. Further, for $a \in \boldsymbol{Q} - \{c\}$ we denote by φ_a the specialization homomorphism of $J(C_t)(\boldsymbol{Q}(t))$ to $J(C_a)(\boldsymbol{Q})$. By Theorem 0.1, we see that the point $P_t = (t, 1) - (\infty) \in J(C_t)(\boldsymbol{Q}(t))$ is not torsion in $J(C_t)(\boldsymbol{Q}(t))$, since it corresponds to the identity $\in \mathrm{End}_{\boldsymbol{Q}}(J(C))$ via the isomorphism. Now we apply Lemma 1.1 to the case:

$$M = \boldsymbol{Z} \cdot P_t \oplus \langle (c, 0) - (\infty) \rangle \ (\cong \boldsymbol{Z} \oplus \boldsymbol{Z}/2\boldsymbol{Z}) \subset J(C_t)(\boldsymbol{Q}(t))\,,$$

$$N = J(C_a)(\boldsymbol{Q})\,,$$

$$\varphi_a\colon M \to N\,, \quad \text{the specialization homomorphism, and}$$

$$n = 2\,.$$

The condition (1) of Lemma 1.1 is assured by the Mordell-Weil theorem. The condition (3) is implied by (4) in view of Theorem 0.1. As for the condition (4), recall that the set of the two division points $J(X_t)_2(k(t))$ consists of the points $\sum_{i \in T}((\theta_i, 0) - (\infty))$, where T runs through the subsets of $\{0, 1, \ldots, 2g\}$ (see [6, Ch. IIIa, §2]). Therefore $J(X_t)_2(\boldsymbol{Q}(t))$ consists only of $Q = (c, 0) - (\infty)$ and the zero element $\mathbf{0}$ of $J(X_t)$. Since this also holds for $J(X_a)_2(\boldsymbol{Q})$, the condition (4) is satisfied. Hence we are reduced to checking the condition (2), namely, the injectivity of the induced map $M/2M \to N/2N$. This amounts to showing that $\varphi_a(P_t)$, $\varphi_a(Q)$, and $\varphi_a(P_t + Q)$ are not divisible by two in $J(C_a)(\boldsymbol{Q})$. Using the homomorphisms β_t (which is bijective) and α (which is injective) constructed above, we are reduced to showing that

(i) $\alpha(\beta_a(\varphi_a(P_t)))$,
(ii) $\alpha(\beta_a(\varphi_a(Q)))$,
(iii) $\alpha(\beta_a(\varphi_a(P_t + Q)))$,

are not equal to the identity element of $(k^*/k^{*2})^{2g}$.

(i) $\alpha(\beta_a(\varphi_a(P_t)))$: By the definition of β_a and α, we see that the condition $\alpha(\beta_a(\varphi_a(P_t))) = 1$ in $(k^*/k^{*2})^{2g}$ is equivalent to

$$\begin{cases} \qquad (a-\theta_1)(a-\theta_2)\cdots\cdots\cdots\cdots(a-\theta_{2g})\in k^{*2}\,, \\ (a-c)\times \qquad (a-\theta_2)\cdots\cdots\cdots\cdots(a-\theta_{2g})\in k^{*2}\,, \\ \qquad\cdots\cdots\cdots\cdots\cdots\cdots \\ (a-c)(a-\theta_1)(a-\theta_2)\cdots(a-\theta_{2g-2})\times(a-\theta_{2g})\in k^{*2}\,. \end{cases}$$

This, as a whole, is equivalent to

$$(a-c)(a-\theta_i)\in k^{*2} \qquad (i=1,\dots,2g)\,.$$

Considering the norm of $(a-c)(a-\theta_1)$ with respect to the extension $k/\boldsymbol{Q}$, this implies $\prod_{i=1}^{2g}(a-\theta_i)\in\boldsymbol{Q}^{*2}$, namely $g(a)$ is a square in $\boldsymbol{Q}^*$. But this is not the case by the assumption of the theorem.

(ii) $\alpha(\beta_a(\varphi_a(Q)))$: By the definition, we see that the equality $\alpha(\beta_a(\varphi_a(Q)))=1$ in $(k^*/k^{*2})^{2g}$ is equivalent to the condition that

$$\begin{cases} \prod_{i=1}^{2g}(f(a)c-f(a)\theta_i)\in k^{*2} \quad \text{and} \\ f(a)c-f(a)\theta_i\in k^{*2} \qquad (i=1,\dots,2g-1)\,. \end{cases}$$

If we take the norm of $c-\theta_1$, this implies that $g(c)\in\boldsymbol{Q}^{*2}$, which is not the case by the assumption of the theorem.

(iii) $\alpha(\beta_a(\varphi_a(P_t+Q)))$: Since φ_a, β_a and α are homomorphisms, we see that the condition $\alpha(\beta_a(\varphi_a(P_t+Q)))=1$ in $(k^*/k^{*2})^{2g}$ is equivalent to

$$\begin{cases} (a-c)g(c)\in k^{*2} \quad \text{and} \\ (a-\theta_i)(c-\theta_i)\in k^{*2} \qquad (i=1,\dots,2g-1)\,. \end{cases}$$

If we take the norm of $(a-\theta_1)(c-\theta_1)$, this implies that $g(a)g(c)\in\boldsymbol{Q}^{*2}$, which is not possible by the assumption of the theorem. This completes the proof of Theorem 2.1.

3. Examples. In this section we give some examples of abelian varieties defined over the rational function field $\boldsymbol{Q}(t)$ such that each specialized member has Mordell-Weil rank ≥ 1 when the variable t is specialized to a value in $\boldsymbol{Q}-S$, where S is an explicitly determinable finite subset of $\boldsymbol{Q}$.

EXAMPLE 3.1. Given a positive integer n, let $g(X)=X^{4n}+1$ and let $f(X)=(X-1)(X^{4n}+1)$, so that in the notation of Theorem 2.1, $c=1$ and $g(c)=2\notin\boldsymbol{Q}^{*2}$. It is known that, for $n\geq 1$, the equation

$$y^2=x^{4n}+1$$

has no rational solution except $(x,y)=(0,\pm 1)$, and it is also known that

$$2y^2=x^{4n}+1$$

has no rational solution except $(x,y)=(\pm 1,\pm 1)$ (see [5, p. 16 and p. 18]). Hence by

Theorem 2.1, we obtain the following:

PROPOSITION 3.1.1. *Let n denote a positive integer. For the hyperelliptic curve C_t over $\boldsymbol{Q}(t)$ defined by the equation*

$$C_t\colon (t-1)(t^{4n}+1)y^2=(x-1)(x^{4n}+1)\,,$$

the Mordell-Weil group $J(C_a)(\boldsymbol{Q})$ of the jacobian variety of the specialized curve C_a for any $a\in\boldsymbol{Q}-\{0,\pm 1\}$ is infinite. More precisely, the rational point $(a, 1)-(\infty)\in J(C_a)(\boldsymbol{Q})$ gives rise to a non-torsion element for each such a.

EXAMPLE 3.2. Let C denote the hyperelliptic curve over $\boldsymbol{Q}$ defined by the equation

$$y^2=f(x)=x^6+2x^4+2x^2+1\ (=(x^2+1)(x^4+x^2+1))\,.$$

Let E denote the elliptic curve defined by the equation

$$y^2=x^3+2x^2+2x+1\,.$$

Then we have two morphisms $\pi_1, \pi_2\colon C\to E$ defined by

$$\pi_1(x, y)=(x^2, y)\,,$$
$$\pi_2(x, y)=(1/x^2, y/x^3)\,.$$

One can check that $\pi_1^*(dx/y)$ and $\pi_2^*(dx/y)$ span the vector space of regular 1-forms on C. Therefore the morphism $(\pi_1, \pi_2)\colon C\to E\times E$ induces an isogeny $J(C)\to E\times E$. Hence it follows from Theorem 0.1 that the $\boldsymbol{Q}(t)$-rational points $(t^2, 1)$ and $(1/t^2, 1/t^3)$ give a set of generators of the free part of the Mordell-Weil group $E_t(\boldsymbol{Q}(t))$, where E_t denotes the elliptic curve over $\boldsymbol{Q}(t)$ defined by

$$(t^6+2t^4+2t^2+1)y^2=x^3+2x^2+2x+1\,.$$

As for specializations of this curve, we obtain the following:

PROPOSITION 3.2.1. *For any $a\in\boldsymbol{Q}-\{0,\pm 1\}$, the Mordell-Weil group $E_a(\boldsymbol{Q})$ has rank ≥ 2.*

PROOF. Let us put $P_t=(t^2, 1)$, $Q_t=(1/t^2, 1/t^3)$ and $R=(-1, 0)$. We know by Theorem 0.1 that these elements give rise to a set of generators of $E_t(\boldsymbol{Q}(t))$. Reasoning as in the proof of Proposition 3.1.1, we are reduced to showing the following:

CLAIM. *None of the points P_a, Q_a, R, P_a+Q_a, P_a+R, Q_a+R, P_a+Q_a+R can be divided by two in $E_a(\boldsymbol{Q})$ for any $a\in\boldsymbol{Q}-\{0,\pm 1\}$.*

PROOF OF THE CLAIM. We put $b=f(a)$ and let X_a denote the curve

$$y^2=x^3+2bx^2+2b^2x+b^3\,.$$

Then we have an isomorphism $\beta_a\colon E_a\to X_a$ of elliptic curves defined by

$$\beta_a(x, y)=(bx, b^2y).$$

For notational simplicity, we use the convention that $P' \in X_a$ represents the element which corresponds to $P \in E_a$ under the isomorphism β_a.

(i) Indivisibility of P_a: By the definition of α, we have

$$\alpha(P'_a)=(a^4+a^2+1, (a^2+1)(a^2-\omega^2), (a^2+1)(a^2-\omega)) \in (\boldsymbol{Q}(\omega)^*/\boldsymbol{Q}(\omega)^{*2})^3,$$

where ω denotes a primitive cube root of unity. The condition $a^4+a^2+1 \in \boldsymbol{Q}(\omega)^{*2}$ is equivalent to $a^4+a^2+1 \in \boldsymbol{Q}^{*2}$, since a^4+a^2+1 is a positive rational number. But this is not possible since there is no non-trivial solution of the Diophantine equation $z^2=x^4+x^2y^2+y^4$ (see [5, p. 19]). Therefore P'_a cannot be divisible by two in $X_a(\boldsymbol{Q})$, hence P_a is not divisible by two in $E_a(\boldsymbol{Q})$.

(ii) Indivisibility of Q_a: We compute

$$\alpha(Q'_a)=(1/a^4+1/a^2+1, (1/a^2+1)(1/a^2-\omega^2), (1/a^2+1)(1/a^2-\omega)).$$

Hence for the same reason as in (i), we see that Q_a is not divisible by two in $E_a(\boldsymbol{Q})$.

(iii) Indivisibility of R: We compute

$$\alpha(R')=(b^2, -b(1+\omega), -b(1+\omega^2)).$$

Since $-b(1+\omega)=\omega^2 b$, we are reduced to showing that the equation

$$z^2=x^6+2x^4y^2+2x^2y^4+y^6$$

has no integer solution with $(x, y)=1$. Note that the right hand side of this equation can be factored as

$$(x^2+y^2)(x^2-xy+y^2)(x^2+xy+y^2),$$

and that the three factors are relatively prime. Hence $(x^2-xy+y^2)(x^2+xy+y^2)=x^4+x^2y^2+y^4$ must be a square. But this is not possible as we saw in (i). Hence R is not divisible by two in $E_a(\boldsymbol{Q})$.

(iv) P_a+Q_a: We compute

$$\alpha(P'_a+Q'_a)=\alpha(P'_a)\alpha(Q'_a)=(1, (a^2-\omega^2)(1-\omega^2a^2), (a^2-\omega)(1-\omega a^2)).$$

As for the second coordinate,

$$(a^2-\omega^2)(1-\omega^2a^2)=-\omega^2(a^4+a^2+1)=-(a^4+a^2+1)$$

in $\boldsymbol{Q}(\omega)^*/\boldsymbol{Q}(\omega)^{*2}$. Since $\boldsymbol{Q}(\omega)=\boldsymbol{Q}(\sqrt{-3})$ and $a^4+a^2+1>0$, the condition $-(a^4+a^2+1) \in \boldsymbol{Q}(\omega)^{*2}$ is equivalent to the condition that there exists $d \in \boldsymbol{Q}^*$ such that $3d^2=a^4+a^2+1$. Hence we are only to show the following:

LEMMA. *There is no triple $(x, y, z) \in \boldsymbol{Z}^3$ such that $3z^2=x^4+x^2y^2+y^4$ holds except the obvious ones $(x, y, z)=(x, \pm x, \pm x)$.*

(Note that the last solutions give rize to the solutions $(a, d)=(\pm 1, \pm 1)$ of the equation $3d^2=a^4+a^2+1$.)

PROOF. We may assume $(x, y)=1$. Then x^2-xy+y^2 and x^2+xy+y^2 are relatively prime. Hence there is a pair (m, n) of integers such that

$$\begin{cases} x^2-xy+y^2=m^2 \\ x^2+xy+y^2=3n^2 . \end{cases}$$

(Replace y by $-y$ if necessary.) This implies

$$\begin{cases} 9n^2-m^2=2U^2 \\ 3m^2-3n^2=2V^2 , \end{cases}$$

where $U=x+y$, $V=x-y$. Therefore we have

$$\begin{cases} U^2+3V^2=4m^2 \\ 3U^2+V^2=12n^2 . \end{cases}$$

The last equation implies that V is divisible by 3, hence, if we put $V=3v$, then we obtain

$$\begin{cases} U^2+27v^2=(2m)^2 \\ U^2+3v^2=(2n)^2 . \end{cases}$$

Now it is known that, for any $M, N\in \boldsymbol{Z}$ with $M\neq N$, the curve

$$E(M, N): \begin{cases} X^2+MY^2=Z^2 \\ X^2+NY^2=W^2 \end{cases}$$

in $\boldsymbol{P}^3$ with coordinate (X, Y, Z, W) and the elliptic curve

$$C(M, N): y^2z=(N-M)x(x-z)(x-(N/(N-M))z)$$

in $\boldsymbol{P}^2$ with coordinate (x, y, z) are isomorphic by the map

$$(X, Y, Z, W)\to((Z-X)/M, Y, ((M-N)/(MN))X+Z/M-W/N)$$

(see [9]). Hence it suffices to show that

$$C(27, 3)(\boldsymbol{Q})=\{(0, 0, 1), (1, 0, 1), (-1/8, 0, 1), (0, 1, 0)\}$$
$$(=C(27, 3)_2(\boldsymbol{Q})) ,$$

since these four points correspond exactly to the ones deleted in the statement of the lemma. The equation of the curve $C(27, 3)$ is transformed into

$$E^*: y^2=x(x-3)(x+24)=(x+7)^3-219(x+7)+1190 .$$

The invariants of this elliptic curve are computed as follows (in the notation of [2]):

$$\begin{cases} c_4 = 2^4 \cdot 3^2 \cdot 73\,, \\ \Delta = 6^{10} = 2^{10} \cdot 3^{10}\,. \end{cases}$$

Therefore the conductor of E^* must be of the form $2^a \cdot 3^b$. Such curves are completely classified in [loc. cit.]. We see from the table there that this elliptic curve is called $72C$ and its Mordell-Weil group consists exactly of its 2-division points. This completes the proof of the lemma. Hence $P_a + Q_a$ is not divisible by two in $E_a(\boldsymbol{Q})$.

(v) Indivisibility of $P_a + R$: Since

$$\alpha(P'_a + R) = \alpha(P'_a)\alpha(R') = (a^4 + a^2 + 1, *, *)\,,$$

the proof in (i) shows that this is not equal to the identity of $(\boldsymbol{Q}(\omega)^*/\boldsymbol{Q}(\omega)^{*2})^3$. Hence $P_a + R$ is not divisible by two in $E_a(\boldsymbol{Q})$.

(vi) Indivisibility of $Q_a + R$: A similar argument as in (v) shows the indivisibility.

(vii) Indivisibility of $P_a + Q_a + R$: It follows from the computation in (i), (ii), (iii) that

$$\begin{aligned} \alpha(P_a + Q_a + R) &= \alpha(P_a)\alpha(Q_a)\alpha(R) \\ &= (1, (a^2 - \omega^2)(1 - \omega^2 a^2)(-b(1 + \omega)), (a^2 - \omega)(1 - \omega a^2)(-b(1 + \omega^2)))\,. \end{aligned}$$

But we see that

$$(a^2 - \omega^2)(1 - \omega^2 a^2)(-b(1 + \omega)) = (a^2 - \omega^2)(-\omega^2)(a^2 - \omega) \cdot \omega^2 \cdot b = -(a^2 + 1)$$

in $\boldsymbol{Q}(\omega)^*/\boldsymbol{Q}(\omega)^{*2}$. This implies that there exists $d \in \boldsymbol{Q}^*$ such that $3d^2 = a^2 + 1$. But this is easily checked to have no rational solution. Hence $P_a + Q_a + R$ is not divisible by two in $E_a(\boldsymbol{Q})$.

Combining the above (i)–(vii), we complete the proof of Proposition 3.2.1.

PART B

4. Generalization. In this section we formulate a generalization of Theorem 0.1. Let k be a field of arbitrary characteristic. Let $\pi: C \to C'$ be a morphism of degree two defined over k between non-singular projective curves over k. Assume that there exists a k-rational point, called ∞, of C where π ramifies. For any abelian variety A over k, we define a 1-cocycle $b = (b_s) \in Z^1(\mathrm{Gal}(k(C)/k(C')), \mathrm{Aut}\,A)$ by

$$b_{\mathrm{id}} = \mathrm{id}\,, \qquad b_\iota = -\mathrm{id}\,,$$

where ι denotes the involution associated to the double covering π. Let us denote by A_b the twist of $A \otimes k(C')$ by this 1-cocycle. Then we have the following:

THEOREM 4.1. *The notation being as above, there exists an isomorphism of abelian groups*

$$A_b(k(C)) \cong \mathrm{Hom}_k(J(C)/\pi^*(J(C')), A) \oplus A_2(k)\,.$$

REMARK 4.2. Theorem 0.1 is obtained from this by taking $C \to \boldsymbol{P}^1$ as the double covering in Theorem 4.1, since in this case $J(C') = J(\boldsymbol{P}^1)$ is trivial.

PROOF. We can argue similarly as in the hyperelliptic case (see [3]). The only difference about which we should be careful is that (in the notation of [loc. cit.]) $b_\iota \circ {}^\iota P(x)$ becomes equal to

$$\alpha[((x)-(\infty)) - \pi^*((\pi(x)) - (\pi(\infty)))] - c\,.$$

Therefore in order that $P \in A_b(k(C'))$ holds it is necessary and sufficient that α vanishes on the subgroup $\pi^*(J(C'))$ and that $c \in A_2(k)$. Hence we obtain our theorem.

Using this theorem we can construct an abelian variety A defined over the function field of a curve C over $\boldsymbol{Q}$ such that its Mordell-Weil group $A(\boldsymbol{Q}(C))$ has an arbitrarily high rank. In order to construct such an abelian variety, we must recall some facts about modular curves. Let N be a positive integer. Let $\Gamma_0(N)$ denote the congruence subgroup of level N of $SL_2(\boldsymbol{Z})$ defined by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\boldsymbol{Z});\ c \equiv 0 \pmod{N} \right\}.$$

This group acts on the upper half plane properly discontinuously and defines an affine curve $Y_0(N)$ as its quotient. It is well known that we can compactify it by adding some "cusps" (which correspond to the orbits of $\boldsymbol{Q} \cup \{\infty\}$ under the action of $\Gamma_0(N)$), and we obtain a non-singular projective curve $X_0(N)$ which is defined over $\boldsymbol{Q}$. About the rationality of its cusps the following fact is known:

PROPOSITION 4.3 (cf. [7, Prop. 2]). *If N or $N/2$ is square-free, then all the cusps of $X_0(N)$ are rational over $\boldsymbol{Q}$.*

Further we recall the following:

PROPOSITION 4.4 (cf. [8, Prop. 3]). *If $N = 4N'$ with $(4, N') = 1$, then there exists an involution w_2 (called the* Atkin-Lehner involution *associated to the prime factor* 2 *of* N) *such that it has at least one fixed point among the cusps of $X_0(N)$.*

In view of these, if we let C be $X_0(4N')$ where N' is an odd square-free integer and let C' be its quotient $X_0(4N')/\langle w_2 \rangle$, then we obtain the double covering $\pi: C \to C'$ defined over $\boldsymbol{Q}$ which satisfies all the conditions in Theorem 4.1. Hence for any abelian variety A defined over $\boldsymbol{Q}$, we have an isomorphism

$$A_b(\boldsymbol{Q}(C')) \cong \mathrm{Hom}_{\boldsymbol{Q}}(J(C)/\pi^*(J(C')), A) \oplus A_2(\boldsymbol{Q})\,.$$

Further, if $N' = 11 \cdot p_1 \cdots p_n$ where p_i $(i = 1, \ldots, n)$ are distinct odd primes different from 11, then we can check that the dimension of the (-1)-eigenspace of w_2 acting on the "old part" $\bigoplus_{d\,|\,4p_1\cdots p_n} B_d(\langle \Gamma_0(11), 2\rangle_0)$ (in the notation of [1]) is exactly equal to 2^n, by Lemma 26 of [loc. cit.]. This implies that the elliptic curve $X_0(11)$ appears at least 2^n times in the isogeny decomposition of $J(C)/\pi^*(J(C'))$ (see [4, p. 21] for the decomposition of $J(C)$). Hence we obtain the following:

THEOREM 4.5. *The notation being as above, the rank of the Mordell-Weil group* $X_0(11)_b(\mathbf{Q}(C'))$ *is greater than or equal to* 2^n.

REFERENCES

[1] A. O. L. ATKIN AND J. LEHNER, Hecke operators on $\Gamma_0(m)$, Math. Ann. 185 (1970), 134–169.

[2] B. J. BIRCH AND W. KUYK (eds.), Modular functions of one variable IV, Lect. Notes in Math. 476, Springer-Verlag, Berlin, Heidelberg, New York, 1975.

[3] F. HAZAMA, On the Mordell-Weil group of certain abelian varieties defined over the rational function field, J. Number Theory 37 (1991), 168–172.

[4] G. LIGOZAT, Courbes modulaires de genre 1, Bull. Soc. Math. France, Mémoire 43, 1975.

[5] L. J. MORDELL, Diophantine Equations, Academic Press, 1969.

[6] D. MUMFORD, Tata Lectures on Theta II, Progress in Math. 43, Birkhäuser, Boston, 1984.

[7] A. P. OGG, Rational points on certain elliptic modular curves, Proc. Symp. Pure Math. 24 (1973), 221–231.

[8] A. P. OGG, Hyperelliptic modular curves, Bull. Soc. Math. France 102 (1974), 449–462.

[9] T. ONO, Variations on a theme of Euler, (in Japanese), Jikkyo Shuppan, 1980.

[10] J.-P. SERRE, Lectures on the Mordell-Weil Theorem, Aspects of Mathematics 15, Vieweg, Braunschweig, 1989.

[11] J. H. SILVERMAN, The Arithmetic of Elliptic Curves, Graduate Texts in Math. 106, Springer-Verlag, Berlin, Heidelberg, New York, 1985.

DEPARTMENT OF INFORMATION SCIENCES
COLLEGE OF SCIENCE AND ENGINEERING
TOKYO DENKI UNIVERSITY
HATOYAMA-MACHI, HIKI-GUN, SAITAMA 350–03
JAPAN