J. Math. Soc. Japan
Vol. 38, No. 4, 1986

On the explicit models of Shimura's elliptic curves

By Ken-ichi SHIOTA

(Received April 1, 1985)

Introduction.

In Shimura [**11**], an abelian variety A over $\boldsymbol{Q}$ is constructed from a "Neben"-type eigen cusp form in $S_2\left(\Gamma_0(N), \left(\frac{\cdot}{N}\right)\right)$ for a prime number N such that $N\equiv 1 \bmod 4$. There is an abelian subvariety B of A rational over $k_N=\boldsymbol{Q}(\sqrt{N})$; they are closely related with the construction of class fields over k_N (Shimura [**10**]). Moreover, it is known that they have everywhere good reduction over k_N as one of their interesting properties (Deligne-Rapoport [**1**]). When $N=29$, 37 or 41, they are uniquely determined (so we denote them by A_N and B_N), and B_N is an elliptic curve. On the other hand, some explicit models of elliptic curves with everywhere good reduction over k_N are known (see 1.2). Recently, T. Nakamura has shown that B_{29} is actually isogenous to one of such models ([**5**], Corollary).

The purpose of this paper is to determine the isomorphism class over k_N of B_N for $N=29$, 37 and 41 (see Theorem 1.3). This can be achieved by calculating the period lattice and the j-invariant of B_N. As a Corollary, we can show the existence of a $\boldsymbol{Q}$-rational point of certain order on A_N (see Corollary 1.4). In Appendix, we shall give a characterization of B_{37}.

The author would like to express his sincere thanks to Prof. H. Yoshida and Prof. H. Ishii for their valuable suggestion and encouragement, and to Prof. M. Yamauchi who computed the eigen-values of Hecke operators for this paper.

§ 1. Main theorem.

1.1. NOTATION. Let N be a prime number 29, 37 or 41, $\chi(\ )=\left(\frac{\cdot}{N}\right)$ the Legendre symbol, and

$$\Gamma=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix}\in\Gamma_0(N) \;\middle|\; \chi(a)=1\right\}.$$

Denote by X_0 (resp. X) the modular curve which corresponds to $\Gamma_0(N)$ (resp. Γ), and by J_0 (resp. J) its Jacobian variety; X_0, X, J_0, J and the natural homomorphism $J_0\to J$ are all defined over $\boldsymbol{Q}$. Put $A_N=\mathrm{Coker}(J_0\to J)$. Then A_N is a 2-dimensional abelian variety defined over $\boldsymbol{Q}$ which is attached to the Neben-type

eigen cusp forms in $S_2(\Gamma_0(N), \chi)$ in the sense of [**11**], Theorem 1.

Further, let k_N be the real quadratic field $\boldsymbol{Q}(\sqrt{N})$ (embedded in $\boldsymbol{C}$), and σ the non-trivial automorphism of k_N. Note that in each case the narrow class number of k_N is 1. Put $H=\frac{1}{\sqrt{N}}\begin{bmatrix}0 & -1\\ N & 0\end{bmatrix}$. Then H induces an automorphism η of A_N rational over k_N. Now put $B_N=(1+\eta)A_N$. Then B_N is an elliptic curve defined over k_N and has the following properties:

$$B_N^\sigma = (1-\eta)A_N\,; \qquad A_N = B_N+B_N^\sigma\,;$$

(1) $B_N\cap B_N^\sigma$ is annihilated by 2 (cf. Shimura [**9**], §7.5, §7.7);

(2) A_N and B_N have everywhere good reduction over k_N ([**1**]).

For an elliptic curve E, let $j(E)$ denote the j-invariant of E.

1.2. We have some examples of elliptic curves with everywhere good reduction over k_N. (For the definition of Δ, see Appendix.)

E_{29} : $y^2+xy+\varepsilon^2 y = x^3$;
$\varepsilon = (5+\sqrt{29})/2$; $\quad \Delta = -\varepsilon^{10}$; $\quad j(E_{29}) = (5\varepsilon-2)^3\varepsilon^{-4}$;
$(0, 0)$ is a rational point of order 3.

E_{37} : $y^2-\varepsilon y = x^3+\left(\frac{3\varepsilon+1}{2}\right)x^2+\left(\frac{11\varepsilon+1}{2}\right)x$;
$\varepsilon = 6+\sqrt{37}$; $\quad \Delta=\varepsilon^6$; $\quad j(E_{37}) = 2^{12}$;
$(0, 0)$ is a rational point of order 5.

E_{41} : $y^2+xy+\alpha y = x^3+\alpha x^2+(2\alpha-1)x$;
$\alpha = (7-\sqrt{41})/2$; $\quad \varepsilon = 32+5\sqrt{41}$; $\quad \Delta = 1/\varepsilon$; $\quad j(E_{41}) = 17^3\varepsilon$;
$\left(\frac{1-\alpha}{4}, -\frac{1+3\alpha}{8}\right)$ is a rational point of order 2.

In each case, ε denotes the fundamental unit of k_N, and the equation of E_N is globally minimal. The example E_{29} is due to J. Tate (Serre [**7**], p. 320), E_{37} to B. Setzer [**8**], and E_{41} is 2-isogenous to the example of F. Oort: $y^2+xy=x^3-\varepsilon x$ (Stroeker [**12**]).

1.3. THEOREM. *B_N is isomorphic to E_N over k_N for N=29, 37 and 41.*

1.4. COROLLARY. *A_{29} (resp. A_{37}, A_{41}) has a $\boldsymbol{Q}$-rational point of order* 3 *(resp.* 5, 2).

PROOF. Let $d_{29}=3$, $d_{37}=5$ and $d_{41}=2$. By Theorem 1.3, B_N has a k_N-rational point b of order d_N. Put $a=b+b^\sigma\in A_N$. If $a\neq 0$, then a is a $\boldsymbol{Q}$-rational point of order d_N. Otherwise, in view of (1), d_N must be even, namely

$N=41$ and $d_N=2$; hence b itself is $\boldsymbol{Q}$-rational. q. e. d.

Theorem 1.3 follows from Lemmas 1.5 and 1.6 below.

1.5. LEMMA (Ishii). *Let B and E be two semi-stable elliptic curves over an algebraic number field k (of finite degree) whose narrow class number h_k is odd. Assume that $j(B)=j(E)$ and that $j(B)\neq 0$. Then B is isomorphic to E over k.*

PROOF. Let

$$B : y^2=4x^3-g_2x-g_3, \qquad E : Y^2=4X^3-G_2X-G_3$$

be Weierstrass models of B and E over k respectively. Since $j(B)=j(E)$, there exists an isomorphism $\lambda : B\simeq E$ which is written as

$$\lambda(x, y)=(\mu^2x, \mu^3y)$$

with an element μ such that $G_2=\mu^4g_2$ and $G_3=\mu^6g_3$. Note that $g_2\neq 0$ since $j(B)\neq 0$; hence $\mu^4\in k$. Now

$$\phi(b, e)=(0, \lambda(b))$$

defines an endomorphism of $B\times E$ rational over $k(\mu)$. Then Theorem 1.3 of Ribet [**6**] asserts that ϕ (hence λ) is defined over an unramified extension of k. Since h_k is odd, we see that k is the unique unramified extension of k contained in $k(\mu)$. This completes the proof.

1.6. LEMMA. *$j(B_N)=j(E_N)$ for $N=29$, 37 and 41.*

PROOF. By (2), $j(B_N)$ is an integer in k_N. Hence we can determine $j(B_N)$ by calculating the values of $j(B_N)$ and $j(B_N)^\sigma$ with sufficient accuracy. The calculation will be carried out in § 2.

§ 2. Calculation of $j(B_N)$.

2.1. *The Neben-type cusp forms.* Let ρ denote the complex conjugation, and

$$f(z)=\sum_{n=1}^{\infty}a_n\exp(2\pi inz), \qquad f_\rho(z)=\sum_{n=1}^{\infty}a_n^\rho\exp(2\pi inz)$$

be the Neben-type eigen cusp forms in $S_2(\Gamma_0(N), \chi)$ normalized as $a_1=1$. Recall that

$$f|[H]_2=\left(\frac{a_N^\rho}{\sqrt{N}}\right)f_\rho, \qquad \left|\frac{a_N^\rho}{\sqrt{N}}\right|=1 \tag{3}$$

(cf. Naganuma [**4**], Lemma 2).

In our calculation, we choose f so that $a_2=\sqrt{5}i$, $a_2=2i$, $a_3=2\sqrt{2}i$ accord-

ing as $N=29, 37, 41$; f is uniquely determined by this condition. The computation of a_n's is due to H. Wada and M. Yamauchi.

2.2. NOTATION. Let $\mathfrak{H}=\{z\in\boldsymbol{C} \mid \mathrm{Im}(z)>0\}$ the upper half plane and $\mathfrak{H}^*=\mathfrak{H}\cup\boldsymbol{Q}\cup\{i\infty\}$. The quotient space $\Gamma\backslash\mathfrak{H}^*$ is identified with $X(\boldsymbol{C})$, and $S_2(\Gamma)$ with the space of holomorphic 1-forms on $X(\boldsymbol{C})$, in the usual manner. For $a, b\in\mathfrak{H}^*$, denote by $\{a, b\}$ the element of $H_1(X(\boldsymbol{C}), \boldsymbol{R})$ which is represented by a path in $\mathfrak{H}^*$ from a to b. The group ring $\boldsymbol{R}[SL_2(\boldsymbol{R})]$ acts $\boldsymbol{R}$-linearly on $H_1(X(\boldsymbol{C}), \boldsymbol{R})$ by

$$\alpha\{a, b\} = \{\alpha(a), \alpha(b)\} \qquad (\alpha\in SL_2(\boldsymbol{R})).$$

Of course, the action of Γ is trivial. For $h\in S_2(\Gamma)$, put

$$[\{a, b\}, h] = \int_a^b h(z)dz,$$

and extend this map $\boldsymbol{R}$-linearly to $[\ ,\ ]: H_1(X(\boldsymbol{C}), \boldsymbol{R})\times S_2(\Gamma)\to\boldsymbol{C}$.

Further, let $S=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$, $T=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$, U be a fixed element of $\Gamma_0(N)$ not belonging to Γ, and

$$g_+ = f+f|[H]_2, \qquad g_- = f-f|[H]_2.$$

Note that g_+ and g_- span $S_2(\Gamma_0(N), \chi)$ and that

$$[H\delta, g_\pm] = \pm[\delta, g_\pm], \qquad [U\delta, g_\pm] = -[\delta, g_\pm] \tag{4}$$

for any $\delta\in H_1(X(\boldsymbol{C}), \boldsymbol{R})$. Finally, let $z_0=i/\sqrt{N}$ the fixed point of H in $\mathfrak{H}$.

2.3. *$B_N(\boldsymbol{C})$ and $B_N^\circ(\boldsymbol{C})$ as complex tori.* Put

$$L = \left\{\begin{bmatrix}[\delta, g_+]\\ [\delta, g_-]\end{bmatrix} \;\middle|\; \delta\in H_1(X(\boldsymbol{C}), \boldsymbol{Z})\right\} \subset \boldsymbol{C}^2.$$

Then Proposition 3 of [**11**] asserts that L is a lattice in $\boldsymbol{C}^2$ such that

$$A_N(\boldsymbol{C}) \simeq \boldsymbol{C}^2/L$$

as complex tori; furthermore, the composed map

$$\Phi : \mathfrak{H}^* \to X(\boldsymbol{C}) \to J(\boldsymbol{C}) \to A_N(\boldsymbol{C}) \to \boldsymbol{C}^2/L$$

can be written as

$$\Phi(z) = \begin{bmatrix}[\{z_0, z\}, g_+]\\ [\{z_0, z\}, g_-]\end{bmatrix} \mod L \qquad (z\in\mathfrak{H}^*)$$

with a suitable choice of the canonical map $X\to J$.

Denote by the same letter η the isomorphism of $\boldsymbol{C}^2/L$ induced from η. Then there exists an element $c\in\boldsymbol{C}^2/L$ such that

$$\eta(\Phi(z)) = \Phi(H(z))+c \qquad (z\in\mathfrak{H}^*)$$

(cf. [**9**], § 7.2). Since $\{z_0, H(z)\}=H\{z_0, z\}$, we have

$$\Phi(H(z)) = \begin{bmatrix} [\{z_0, z\}, g_+] \\ -[\{z_0, z\}, g_-] \end{bmatrix} \mod L$$

by (4). It follows that

$$B_N(\boldsymbol{C}) \simeq \boldsymbol{C}/L_+, \qquad B_N^{\sigma}(\boldsymbol{C}) \simeq \boldsymbol{C}/L_-$$

as complex tori where

$$L_+ = \{[\delta, g_+] \mid \delta \in H_1(X(\boldsymbol{C}), \boldsymbol{Z}) \text{ such that } [\delta, g_-]=0\},$$
$$L_- = \{[\delta, g_-] \mid \delta \in H_1(X(\boldsymbol{C}), \boldsymbol{Z}) \text{ such that } [\delta, g_+]=0\}.$$

2.4. In Table I, we list the basis $\langle \delta_j \rangle$ of $H_1(X(\boldsymbol{C}), \boldsymbol{Z})$ where $\zeta=(-1+\sqrt{3}i)/2$. The rank of $H_1(X(\boldsymbol{C}), \boldsymbol{Z})$ is 8, 8, 10 according as $N=29$, 37, 41.

Table I

N	$\langle \delta_j \rangle$
29	$\delta_1=T\{\zeta+5, \zeta+7\}$, $\delta_2=T\{\zeta-9, \zeta+14\}$, $\delta_3=T\{\zeta-4, \zeta+6\}$, $\delta_4=T\{\zeta+10, \zeta-13\}$, $\delta_5=U\delta_1$, $\delta_6=U\delta_2$, $\delta_7=U\delta_3$, $\delta_8=U\delta_4$
37	$\delta_1=T\{\zeta+13, \zeta+16\}+T\{\zeta-6, \zeta+3\}$, $\delta_2=T\{\zeta+5, \zeta+9\}$, $\delta_3=T\{\zeta-8, \zeta-4\}$, $\delta_4=T\{\zeta-16, \zeta+8\}$, $\delta_5=U\delta_1$, $\delta_6=U\delta_2$, $\delta_7=U\delta_3$, $\delta_8=U\delta_4$
41	$\delta_1=T\{\zeta+17, \zeta-18\}$, $\delta_2=T\{\zeta+3, \zeta+7\}+UT\{\zeta-7, \zeta-13\}$, $\delta_3=T\{\zeta+16, \zeta+19\}+T\{\zeta-16, \zeta-17\}$, $\delta_4=T\{\zeta+6, \zeta+8\}$, $\delta_5=T\{\zeta+11, \zeta+15\}+UT\{\zeta-10, \zeta-14\}$, $\delta_6=((1+U)T)(\{\zeta-2, \zeta+4\}+\{\zeta+11, \zeta+14\})$, $\delta_7=U\delta_1$, $\delta_8=U\delta_2$, $\delta_9=U\delta_3$, $\delta_{10}=U\delta_4$

2.5. REMARK. Put $M=(N-1)/2$ and

$$\mathfrak{R} = \{1, U, TS^m, UTS^m \ (m=-M, -M+1, \cdots, M)\}.$$

Then $\mathfrak{R}$ is a complete set of representatives of $\Gamma\backslash SL_2(\boldsymbol{Z})$. Let $\mathfrak{D}_0$ be the

standard fundamental domain for $SL_2(\boldsymbol{Z})\backslash\mathfrak{H}^*$, and put

$$\mathcal{D}=\bigcup_{\alpha\in\mathcal{R}}\alpha(\mathcal{D}_0)\,.$$

Then $\mathcal{D}$ is a fundamental domain for $\Gamma\backslash\mathfrak{H}^*$. Observing the correspondences between the sides of $\mathcal{D}$, we get Table I.

By elementary calculations, we obtain:

2.6. PROPOSITION. *The following formulas hold. In the case* $N=29$,

$$[\delta_1, g_+]=[\delta_2, g_-]=[\delta_3, g_+]=[\delta_4, g_-]=0\,.$$

In the case $N=37$,

$$[\delta_3, g_\pm]=\pm[\delta_2, g_\pm]\,,\qquad [\delta_1, g_\pm]=\pm[(\delta_2-\delta_4), g_\pm]\,.$$

In the case $N=41$,

$$[\delta_1, g_+]=[\delta_2, g_-]=[\delta_3, g_+]=[\delta_4, g_-]=[\delta_6, g_\pm]=0\,,$$

$$[\delta_5, g_\pm]=\mp[\delta_4, g_\pm]\,.$$

PROOF. We shall prove here only the formulas for the case $N=37$; the other cases can be dealt with similarly. By virtue of (4), it is sufficient to prove:

(i) $$H\delta_2=\delta_3\,,$$

(ii) $$(1-U)(\delta_1-H(\delta_2-\delta_4))=0\,.$$

Since $\begin{bmatrix}9 & -1\\ 37 & -4\end{bmatrix}$ $(\in\Gamma)$ sends $\dfrac{\zeta+5}{37}$ and $\dfrac{-1}{\zeta-8}$ to $\dfrac{\zeta+9}{37}$ and $\dfrac{-1}{\zeta-4}$ respectively, we have

$$H\delta_2-\delta_3=\left\{\frac{\zeta+5}{37}, \frac{-1}{\zeta-8}\right\}-\left\{\frac{\zeta+9}{37}, \frac{-1}{\zeta-4}\right\}=0$$

which is (i). As to (ii), for simplicity, put $\xi_m=T\{\zeta+m, \zeta+m+1\}$ for $m\in\boldsymbol{Z}$. If $1+mn\equiv 0 \bmod 37$, $\alpha=\begin{bmatrix}-m & -1\\ 1+mn & n\end{bmatrix}$ is an element of $\Gamma_0(37)$ such that $\alpha\xi_m=-\xi_n$. Especially,

$$\xi_{-8}=-U\xi_{14},\qquad \xi_{-7}=-\xi_{16},\qquad \xi_{13}=-U\xi_{17}\,.$$

Moreover,

$$H\delta_4=\begin{bmatrix}7 & 3\\ 37 & 16\end{bmatrix}\left\{\frac{\zeta-16}{37}, \frac{-1}{2}\right\}+\left\{\frac{-1}{2}, \frac{\zeta+8}{37}\right\}$$

$$=\left\{\frac{-1}{2}, \frac{1}{5}\right\}$$

$$= U\begin{bmatrix} 2 & 1 \\ -37 & -18 \end{bmatrix}\left\{\frac{-1}{2}, \frac{-1}{\zeta+3}\right\}+\left\{\frac{-1}{\zeta+3}, \frac{-1}{\zeta-4}\right\}+U\begin{bmatrix} -5 & 1 \\ 74 & -15 \end{bmatrix}\left\{\frac{-1}{\zeta-4}, \frac{1}{5}\right\}$$
$$= T\{\zeta+3, \zeta-4\}+UT\{\zeta+15, \zeta+18\}.$$

Therefore, together with (i), we get

$$\begin{aligned}\delta_1-H(\delta_2-\delta_4) &= T\{\zeta-6, \zeta-8\}+T\{\zeta+13, \zeta+16\}+UT\{\zeta+15, \zeta+18\} \\ &= -\xi_{-7}-\xi_{-8}+\xi_{13}+T\{\zeta+14, \zeta+16\}+UT\{\zeta+15, \zeta+17\}+U\xi_{17} \\ &= (1+U)T\{\zeta+14, \zeta+17\}.\end{aligned}$$

Since $U^2\in\Gamma$, this implies (ii). q. e. d.

2.7. PROPOSITION. *The lattice $L_\pm$ can be written as follows: In the case $N=29$,*

$$L_+ = \boldsymbol{Z}[\delta_2, g_+]+\boldsymbol{Z}[\delta_4, g_+], \qquad L_- = \boldsymbol{Z}[\delta_1, g_-]+\boldsymbol{Z}[\delta_3, g_-].$$

In the case $N=37$,

$$L_\pm = \boldsymbol{Z}(2[\delta_2, g_\pm])+\boldsymbol{Z}(2[\delta_4, g_\pm]).$$

In the case $N=41$,

$$L_+ = \boldsymbol{Z}[\delta_2, g_+]+\boldsymbol{Z}[\delta_4, g_+], \qquad L_- = \boldsymbol{Z}[\delta_1, g_-]+\boldsymbol{Z}[\delta_3, g_-].$$

PROOF. As in the above proof, we shall treat here only L_+ of the case $N=37$. By (4), we see that

$$L_+ \subset \{[\delta, g_+] \mid \delta\in\boldsymbol{Z}\delta_1+\boldsymbol{Z}\delta_2+\boldsymbol{Z}\delta_3+\boldsymbol{Z}\delta_4\}.$$

The right hand side is equal to

$$\{[\delta, g_+] \mid \delta\in\boldsymbol{Z}\delta_2+\boldsymbol{Z}\delta_4\}$$

by Proposition 2.6; hence $[\delta_2, g_+]$ and $[\delta_4, g_+]$ are linearly independent over $\boldsymbol{Q}$. Again by Proposition 2.6, we see that

$$[x_1\delta_1+x_2\delta_2+x_3\delta_3+x_4\delta_4, g_-] = 0$$

if and only if

$$x_1 = -x_4 \quad \text{and} \quad x_3 = x_2+x_4$$

for $x_j\in\boldsymbol{Z}$. Therefore, L_+ is generated by the following two elements:

$$\begin{cases} [\delta_2+\delta_3, g_+] = 2[\delta_2, g_+] & (x_2=1, x_4=0) \\ [-\delta_1+\delta_3+\delta_4, g_+] = 2[\delta_4, g_+] & (x_2=0, x_4=1). \end{cases}$$ q. e. d.

2.8. *The computation of $[\delta_j, g_\pm]$.* Put

$$b_{\pm}^{(n)} = \frac{1}{2\pi i n}\left\{a_n \pm \left(\frac{a_N^{\rho}}{\sqrt{N}}\right) a_n^{\rho}\right\} \qquad (n=1, 2, \cdots),$$

and

$$\begin{aligned} G_{\pm}(m) &= \sum_{n=1}^{\infty} b_{\pm}^{(n)} \exp\left\{2\pi i n\left(\frac{\zeta+m}{N}\right)\right\} \\ &= [HT\{i\infty, \zeta+m\}, g_{\pm}] \qquad (m \in \boldsymbol{Z}). \end{aligned}$$

Then $[\delta_j, g_{\pm}]$ can be represented as a sum of (at most four) $\pm G_{\pm}(m)$'s. For example, in the case $N=41$,

$$\begin{aligned} [\delta_2, g_+] &= [T\{\zeta+3, \zeta+7\}, g_+]+[UT\{\zeta-7, \zeta-13\}, g_+] \\ &= [HT\{\zeta+3, \zeta+7\}, g_+]-[HT\{\zeta-7, \zeta-13\}, g_+] \\ &= -G_+(3)+G_+(7)+G_+(-7)-G_+(-13) \end{aligned}$$

by (4). Note that $|b_{\pm}^{(n)}| \leqq \frac{|a_n|}{\pi n}$ by (3), and that $\mathrm{Re}\left(2\pi i\left(\frac{\zeta+m}{N}\right)\right) = -\frac{\pi\sqrt{3}}{N}$. Moreover, the Riemann hypothesis for function fields implies that $|a_n| \leqq 2n$ for all n. Hence we obtain the following estimation:

$$\begin{aligned} &\left|\sum_{n>n_0} b_{\pm}^{(n)} \exp\left\{2\pi i n\left(\frac{\zeta+m}{N}\right)\right\}\right| \\ &\leqq \frac{2}{\pi}\exp\left\{-(n_0+1)\frac{\pi\sqrt{3}}{N}\right\} \Big/ \left\{1-\exp\left(-\frac{\pi\sqrt{3}}{N}\right)\right\} \\ &< \begin{cases} 1.4\times 10^{-20} & \text{if } N=29 \text{ and } n_0=250, \\ 2.8\times 10^{-19} & \text{if } N=37 \text{ and } n_0=300, \\ 2.3\times 10^{-17} & \text{if } N=41 \text{ and } n_0=300. \end{cases} \end{aligned}$$

Therefore, taking the sum of the first n_0 terms of each $G_{\pm}(m)$, we can evaluate $[\delta_j, g_{\pm}]$ with the accuracy to the 15th decimal place (more precisely, to 15 digits, since the computation shows that $|[\delta_j, g_{\pm}]| > 0.4$ in each case). For example, in the case $N=37$,

$$\begin{aligned} [\delta_2, g_+] &= \ (0.266746435693009\cdots)-(0.314883609969508\cdots)i, \\ [\delta_4, g_+] &= -(0.139121620790886\cdots)-(0.658705434926393\cdots)i, \\ [\delta_2, g_-] &= \ (0.343821824956884\cdots)-(0.405868056483896\cdots)i, \\ [\delta_4, g_-] &= -(0.314883609969508\cdots)-(0.266746435693009\cdots)i. \end{aligned}$$

2.9. *The computation of* $j(B_N)$. Let $\tau_{\pm}$ be an element of $\mathfrak{H}$ which is given in Table II. Then $j(B_N)$ (resp. $j(B_N)^{\sigma}$) is the value of the j-function at τ_+ (resp. τ_-) which can be computed with the accuracy to 10 digits. In each case, we can conclude $j(B_N)=j(E_N)$ which is Lemma 1.6.

Table II

N	29	37	41
τ_+	$[\delta_4, g_+]/[\delta_2, g_+]$ $=(0.432604345936224\cdots)$ $+(0.901583872902068\cdots)i$	$[\delta_2-\delta_4, g_+]/[\delta_2, g_+]$ $=(0.000000000000000\cdots)$ $+(1.288946276127860\cdots)i$	$-[\delta_2, g_+]/[\delta_4, g_+]$ $=(0.000000000000000\cdots)$ $+(2.014328107645633\cdots)i$
τ_-	$[\delta_1-\delta_3, g_-]/[\delta_1, g_-]$ $=(0.500000000000000\cdots)$ $+(1.573330200099442\cdots)i$	$[\delta_2, g_-]/[\delta_4, g_-]$ $=(0.000000000000000\cdots)$ $+(1.288946276127860\cdots)i$	$[\delta_1, g_-]/[\delta_3, g_-]$ $=(0.500000000000000\cdots)$ $+(0.992886904774228\cdots)i$
$j(\tau_+)$	$18.92714854\cdots$	$4096.000000\cdots$	$314508.7469\cdots$
$j(\tau_-)$	$-18909.92715\cdots$	$4096.000000\cdots$	$-76.74689254\cdots$
$j(B_N)$	$(-18891+3515\sqrt{29})/2$	4096	$157216+24565\sqrt{41}$

§ Appendix.

A.1. Let E be an elliptic curve over an algebraic number field k of finite degree. Denote by $\mathfrak{o}_k$, D_k and h_k the maximal order, the discriminant and the class number of k respectively. Take a cubic model of E as

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6 \tag{5}$$

with $a_j\in\mathfrak{o}_k$. Put

$$b_2 = 4a_2+a_1^2, \qquad b_4 = 2a_4+a_1a_3, \qquad b_6 = 4a_6+a_3^2,$$

$$b_8 = b_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2 = (b_2b_6-b_4^2)/4,$$

$$\Delta = -b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6.$$

Further put

$$p(x) = 6x^2+b_2x+b_4, \qquad q(x) = 4x^3+b_2x^2+2b_4x+b_6,$$

$$r(x) = 3x^4+b_2x^3+3b_4x^2+3b_6x+b_8,$$

$$F(x) = q(x)^2\{p(x)r(x)-q(x)^2\}-r(x)^3.$$

Then any point $P=(x_0, y_0)$ on (5) of order 5 satisfies $F(x_0)=0$. Note that $F(x)$ has integral coefficients, and that

$$F(x)=5x^{12}+\cdots+\{b_6^2(b_4b_8-b_6^2)-b_8^3\}.$$

A.2. PROPOSITION (cf. Miyawaki [3], Theorem 4). *Assume that* $h_k=1$, $(D_k, 5)=1$ *and that* E *has a* k*-rational point* P *of order* 5. *Then there exists a global minimal model* (5) *of* E *such that*

$$b_2=\alpha^2+6\alpha\beta+\beta^2,\qquad b_4=\alpha^2\beta(\alpha+\beta),$$
$$b_6=\alpha^4\beta^2,\qquad b_8=\alpha^5\beta^3,\qquad \Delta=\alpha^5\beta^5(\alpha^2-11\alpha\beta-\beta^2) \tag{6}$$

with some $\alpha, \beta\in\mathfrak{o}_k$.

PROOF. Since 5 is unramified in k, it can easily be shown that P has integral coordinates in any model of E of the type (5). Hence there exists a global minimal model (5) of E such that $P=(0, 0)$. Then we have $a_6=0$, $b_6=a_3^2$ and $b_6^2(b_4b_8-b_6^2)-b_8^3=0$. From these equations, we see that b_6 divides b_8, and that there exist $u, v\in\mathfrak{o}_k$ such that $b_4=a_3u$, $b_8=a_3^2(b_2-u^2)/4$, $b_2=2u^2-v^2$ and $8a_3=(u-v)(u+v)^2$. Then we have $u+v\equiv u-v\equiv 0 \bmod 2$, so that $u=\alpha+\beta$ and $v=\alpha-\beta$ with some $\alpha, \beta\in\mathfrak{o}_k$. These integers satisfy (6). q. e. d.

A.3. PROPOSITION (cf. Ishii [2], Proposition 4.1). *Besides the assumptions of Proposition* A.2, *assume that* k *is a quadratic field, and that* E *has everywhere good reduction over* k. *Then* $k=\boldsymbol{Q}(\sqrt{37})$ *and* E *is isomorphic to* B_{37} *over* k.

PROOF. Take a global minimal model (5) of E and $\alpha, \beta\in\mathfrak{o}_k$ satisfying (6). Since Δ is a unit of k, so are $\frac{\alpha}{\beta}$ and $\left(\frac{\alpha}{\beta}\right)^2-11\left(\frac{\alpha}{\beta}\right)-1$. Then we see easily that $\frac{\alpha}{\beta}=6\pm\sqrt{37}$ and $j(E)=2^{12}$; hence our assertion by Lemma 1.5. q. e. d.

References

[1] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques, Lecture Notes in Math., **349**, Springer, 1973.

[2] H. Ishii, The non-existence of elliptic curves with everywhere good reduction over certain quadratic fields, preprint.

[3] I. Miyawaki, Elliptic curves of prime power conductor with $\boldsymbol{Q}$-rational points of finite order, Osaka J. Math., **10** (1973), 309-323.

[4] H. Naganuma, On the coincidence of two Dirichlet series associated with cusp forms of Hecke's "Neben"-type and Hilbert modular forms over a real quadratic field, J. Math. Soc. Japan, **25** (1973), 547-555.

[5] T. Nakamura, On Shimura's elliptic curve over $\boldsymbol{Q}(\sqrt{29})$, J. Math. Soc. Japan, **36** (1984), 701-707.

[6] K. A. Ribet, Endomorphisms of semi-stable abelian varieties over number fields, Ann. of Math., **101** (1975), 555-562.

[7] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math., **15** (1972), 259-331.

[8] B. Setzer, Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invariant, Illinois J. Math., **25** (1981), 233-245.
[9] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten and Princeton Univ. Press, 1971.
[10] G. Shimura, Class fields over real quadratic fields and Hecke operators, Ann. of Math., **95** (1972), 130-190.
[11] G. Shimura, On the factors of the jacobian variety of a modular function field, J. Math. Soc. Japan, **25** (1973), 523-544.
[12] R. J. Stroeker, Elliptic curves defined over imaginary quadratic number fields, Thesis, University of Amsterdam, 1975.

Ken-ichi SHIOTA
Department of Mathematics
Faculty of Science
Kyoto University
Kyoto 606
Japan