J. Math. Soc. Japan
Vol. 36, No. 4, 1984

On Shimura's elliptic curve over $\boldsymbol{Q}(\sqrt{29})$

By Tetsuo NAKAMURA

(Received Dec. 5, 1983)

Let k be the real quadratic field $\boldsymbol{Q}(\sqrt{29})$. Then the class number of k is 1 and $\varepsilon=(5+\sqrt{29})/2$ is a fundamental unit of k. Let E_0 be an elliptic curve over k defined by the equation:

$$y^2+xy+\varepsilon^2 y=x^3 .$$

Let B be the elliptic curve over k which is obtained from the space $S_2\left(\Gamma_0(29), \left(\frac{}{29}\right)\right)$ of cusp forms of "Neben"-type of weight 2 (see Shimura [**4**, §7.5, §7.7]). It is conjectured that B is isogenous to E_0 over k (see Serre [**3**, p. 323] and Shimura [**5**, p. 184]). It will be shown here that this is so, by reducing the problem to the solution of a certain diophantine equation over k.

§1. Let σ be the non-trivial automorphism of k and O_k the integer ring of k. Let E be an elliptic curve over k. For a natural number n, we denote by E_n the group of elements x of $E(\bar{k})$ with $nx=0$.

THEOREM. *Let E be an elliptic curve over k. Assume that E satisfies the following conditions:*

(i) *E has everywhere good reduction over k.*

(ii) *E has an isogeny onto E^σ over k whose degree is prime to* 6.

(iii) *E has a k-rational point of order* 3.

(iv) *$[k(E_2):k]$ is divisible by* 2.

(v) *$[k(E_3):k]$ is divisible by* 3.

Then E is k-isomorphic to either E_0 or E_0^σ.

REMARK. The condition (ii) of Theorem implies that $k(E_2)$ and $k(E_3)$ are Galois over $\boldsymbol{Q}$.

COROLLARY. *Shimura's elliptic curve B is isogenous to E_0 over k.*

PROOF OF COROLLARY. By Casselman [**1**], B has everywhere good reduction. It is known that B has an isogeny onto B^σ of degree 5. Since the number of the $\boldsymbol{F}_{p^2}$-rational points of the reduction of B at $p=3$ is $1-(2p+a_p^2)+p^2=9$ ($a_p=-\sqrt{-5}$, cf. Yamauchi [**6**]), we have $k(B_2)\neq k$. By (i), $k(B_2)/k$ is unramified

This research was partially supported by Grant-in-Aid for Scientific Research (No. 59540008), Ministry of Education.

outside 2. Now the order of the ray class group of k of conductor 2 is prime to 3, so that we see that $[k(B_2):k]\neq 3$. Therefore $[k(B_2):k]$ is divisible by 2, since $[k(B_2):k]$ is a divisor of 6. Let $\varphi_3:\mathrm{Gal}(\bar{k}/k)\to \mathrm{Aut}(B_3)\cong GL_2(F_3)$ be the representation of $\mathrm{Gal}(\bar{k}/k)$ on B_3. By Yamauchi [**6**], $\varphi_3(\mathrm{Gal}(\bar{k}/k))$ is a half Borel subgroup. Therefore if B has a k-rational point of order 3, B satisfies all the conditions of Theorem. If B has no k-rational point of order 3, then B_3 contains a subgroup X of order 3 which is stable under $\mathrm{Gal}(\bar{k}/k)$. Let $B'=B/X$. Then B' is an elliptic curve over k with a k-rational point of order 3. We see that B' has an isogeny onto B'^{σ} of degree 5. Since B and B' are isogenous over k, B' satisfies all the conditions of Theorem (cf. Serre [**2**, IV, 2.3]). Noting that E_0 and E_0^{σ} are isogenous by Serre [**3**, p. 323], Theorem shows that B is isogenous to E_0.

Now admitting Proposition 2.3 in § 2, we will give a proof of Theorem.

PROOF OF THEOREM. Let E be an elliptic curve which satisfies the conditions (i)~(v) of Theorem. Let Δ be the discriminant of a global minimal model of E over k. By (iv) and (v), we see that $\sqrt{\Delta}$, $\sqrt[3]{\Delta}\notin k$ (cf. Serre [**3**, p. 305]). Since $k(\sqrt{\Delta})$ is the unique quadratic extension of k contained in $k(E_2)$, it follows that $k(\sqrt{\Delta})/\boldsymbol{Q}$ is Galois. By (i), Δ is a unit of k, so that we must have that $k(\sqrt{\Delta})=k(\sqrt{-1})$, $k(\sqrt{\varepsilon})$ or $k(\sqrt{-\varepsilon})$. As $k(\sqrt{\varepsilon})$ and $k(\sqrt{-\varepsilon})$ are not Galois over $\boldsymbol{Q}$, we have $k(\sqrt{\Delta})=k(\sqrt{-1})$. Therefore we may assume that $\Delta=-\varepsilon^2$, $-\varepsilon^4$, $-\varepsilon^8$ or $-\varepsilon^{10}$. If $\Delta=-\varepsilon^{10}$ (resp. $-\varepsilon^4$), then E^{σ} has a global minimal model with discriminant $-\varepsilon^2$ (resp. $-\varepsilon^8$). We see that E^{σ} satisfies all the conditions of Theorem, and hence we may assume that $\Delta=-\varepsilon^{10}$ or $-\varepsilon^4$. Now we can choose a model

$$y^2=x^3+b_2x^2+8b_4x+16b_6$$

of E, where b_2, b_4, b_6 are in O_k and $(0, b)$ for some b in O_k is a point of order 3. The x-coordinates of the points of order 3 are the roots of the equation

$$3x^4+4b_2x^3+3\cdot 2^4b_4x^2+3\cdot 2^6b_6x+2^8b_8=0$$

where $b_8=(b_2b_6-b_4^2)/4$ (cf. Serre [**3**, p. 305]). Then, since $b_8=0$ and $b^2=16b_6$, the curve E can be written in the form

$$y^2=x^3+c^2x^2+2bcx+b^2$$

where $c\in O_k$ with $c^2=b_2=b_4^2/b_6$. As $4^2b^3(4c^3-27b)=2^{12}\Delta$, we can write $b=4d$ with $d\in O_k$, and then $d^3(c^3-27d)=\Delta$. Hence d is a unit and $c^3=27d+\Delta d^{-3}$. Write $d=\pm\varepsilon^m$. If $c\equiv 0 \bmod 2$, then we have $m\equiv 1 \bmod 3$, since $\Delta\equiv\varepsilon \bmod 2$. Putting $m=1+3n$, we have $(\pm\varepsilon^{-n}c)^3=27\varepsilon+\varepsilon^{-3-12n}\Delta$. In case $\Delta=-\varepsilon^{10}$, we have $(\pm\varepsilon^{-n}c)^3=27\varepsilon-\varepsilon^{7-12n}$. Let $\mathfrak{p}_{13}$ be the prime divisor of 13 such that $\varepsilon\equiv 11 \bmod \mathfrak{p}_{13}$. Then $(\pm\varepsilon^{-n}c)^3\equiv 9 \bmod \mathfrak{p}_{13}$, but this is impossible for $c\in O_k$. In case $\Delta=-\varepsilon^4$, let $\mathfrak{p}_7$ be the prime divisor of 7 such that $\varepsilon\equiv 2 \bmod \mathfrak{p}_7$. Then $(\pm\varepsilon^{-n}c)^3\equiv 3 \bmod \mathfrak{p}_7$, but this is also impossible. Therefore $c\not\equiv 0 \bmod 2$. Then $c^3\equiv 1 \bmod 2$, so that we have $m\equiv 2 \bmod 3$. Put $m=2+3n$ and $C=\pm\varepsilon^{-n}c$. If $\Delta=-\varepsilon^4$, we have $C^3=27\varepsilon^2-\varepsilon^{-2-12n}$. Let $\mathfrak{q}_{13}$ be the prime divisor of 13 such that $\varepsilon\equiv 7 \bmod \mathfrak{q}_{13}$. Then $C^3\equiv 6 \bmod \mathfrak{q}_{13}$, but this is impossible. It follows that $\Delta=-\varepsilon^{10}$ and

$$C^3=27\varepsilon^2-\varepsilon^{4-12n}.$$

It will be shown in §2 (Proposition 2.3) that for $C\in O_k$ and an integer n, the above equation has a unique solution $C=1$, $n=0$. Therefore the curve E takes the form

$$y^2=x^3+x^2+8\varepsilon^2x+16\varepsilon^4,$$

which is clearly isomorphic to E_0 over k. This completes the proof of Theorem.

§ **2.** 2.1. Let $\alpha=\sqrt[3]{\varepsilon}$ and $K=k(\alpha)$. Let η be the real root of $X^3=2X^2+X+1$. Then we have $\alpha^{-1}-\alpha=\eta(\eta-3)$ and $\eta=(-2\alpha^5+\alpha^4+11\alpha^2-3\alpha+2)/3$. Therefore $K=k\cdot F$, where $F=\boldsymbol{Q}(\eta)$. The discriminant of F is -87 and η is a fundamental unit of F. Let D_K be the discriminant of K. Since $|D_K|=29^3|N_k(D_{K/k})|=(-87)^2|N_F(D_{K/F})|$, D_K is divisible by $9\cdot 29^3$. The discriminant of $\{1, \eta, \eta^2, \alpha, \alpha\eta, \alpha\eta^2\}$ is $9\cdot 29^3$. Hence $|D_K|=9\cdot 29^3$ and $\{1, \eta, \eta^2, \alpha, \alpha\eta, \alpha\eta^2\}$ is an integral basis of K over $\boldsymbol{Q}$. Let $L=K(\zeta)$ where $\zeta^2+\zeta+1=0$. Then $L/\boldsymbol{Q}$ is Galois. Let ρ, τ, σ be the automorphisms of L such that ρ is the complex conjugation, $\alpha^\tau=\alpha\zeta$, $\zeta^\tau=\zeta$, $\alpha^\sigma=-\alpha^{-1}$, $\zeta^\sigma=\zeta^2$. We see that $\eta^\sigma=\eta$, $\rho\tau=\tau^2\rho$, $\rho^2=\sigma^2=\tau^3=1$ and $\mathrm{Gal}(L/\boldsymbol{Q})=\langle\sigma\rangle\times\langle\rho, \tau\rangle$. The different imbeddings of K into $\bar{\boldsymbol{Q}}$ are $\sigma_1=1$, $\sigma_2=\sigma$, $\sigma_3=\tau$, $\sigma_4=\tau^2$, $\sigma_5=\sigma\tau$ and $\sigma_6=\sigma\tau^2$. Clearly the unit group U_K of K has rank 3 over $\boldsymbol{Z}$. Let $\beta=1+(\alpha\eta)^{-1}$. Then $\beta\in U_K$ and $N_{K/k}(\beta)=1$, $N_{K/F}(\beta)=\eta^{-1}$.

LEMMA 1. $W=\{u\in U_K \mid N_{K/k}(u)=N_{K/F}(u)=1\}=\langle\eta\beta^2\rangle$.

PROOF. We see easily that W is $\boldsymbol{Z}$-free of rank 1 and $\eta\beta^2\in W$. First we note that η is not a square in K. In fact, let $\eta=(A+B\alpha)^2$, with $A, B\in O_F$; this means that $\eta=A^2+B^2$ and $(2A-\eta(\eta-3)B)B=0$. Since η is a fundamental unit of F, we have $B\neq 0$; hence $2A=\eta(\eta-3)B$. Then $\eta(2\eta-3)B^2=4\eta$. As $2\eta-3$ is prime to 4, this is a contradiction. Therefore in order to prove Lemma 1, it suffices to show that there exists no $\gamma\in W$ such that $\eta\beta^2=\gamma^n$ for $n\geqq 3$. Let $\theta_1=\alpha\eta^2$, $\theta_2=\alpha\eta$, $\theta_3=\alpha$, $\theta_4=\eta^2$, $\theta_5=\eta$, $\theta_6=1$. Write $x^{(i)}=x^{\sigma_i}$ $(1\leqq i\leqq 6)$ for $x\in K$ and let $D=\det(\theta_i^{(j)})$. Then $D^2=9\cdot 29^3$. We denote by $D_{i,j}$ the cofactor of $\theta_i^{(j)}$ of D. Let $\gamma=\sum_{i=1}^{6} a_i\theta_i$ with $a_i\in\boldsymbol{Z}$ be such that $\gamma^n=\eta\beta^2$ for $n\geqq 3$. By the simultaneous linear equations $\gamma^{(j)}=\sum_{i=1}^{6} a_i\theta_i^{(j)}$ $(1\leqq j\leqq 6)$, we have

$$|a_i|\leqq|D^{-1}|\sum_{j=1}^{6}|\gamma^{(j)}||D_{i,j}| \qquad (i=1, \cdots, 6).$$

Put $v=\eta\beta^2$. Then $N_{K/F}(v)=v^{(1)}v^{(2)}=1$, $|v^{(3)}|^2=v^{(3)}v^{(4)}=v^{-1}$ and $|v^{(5)}|^2=v^{(5)}v^{(6)}=v$. Some computations give the following inequalities:

$$1.73<\alpha<1.74\,,\quad 2.54<\eta<2.55\,,\quad v<3.99\,,$$

$$|\gamma^{(1)}|\leqq v^{1/3}<1.59\,,\quad |\gamma^{(2)}|<1\,,\quad |\gamma^{(3)}|=|\gamma^{(4)}|<1\,,$$

$$|\gamma^{(5)}|=|\gamma^{(6)}|\leqq v^{1/6}<1.26\,,\quad |D_{1,1}|=|D_{1,2}|<25.88\,,$$

$$|D_{1,3}|=|D_{1,4}|=|D_{1,5}|=|D_{1,6}|<96.34\,,$$

$$|D_{2,1}|=|D_{2,2}|<14.23\,,\quad |D_{2,3}|=\cdots=|D_{2,6}|<226.39\,,$$

$$|D_{3,1}|=|D_{3,2}|<10.35\,,\quad |D_{3,3}|=\cdots=|D_{3,6}|<157.23\,.$$

Then we get $|a_1|<1.08$, $|a_2|<2.27$ and $|a_3|<1.58$. Since $\gamma^n-(\gamma^\sigma)^n=\eta(\beta^2-(\beta^\sigma)^2)$ $=(\eta-1)(\alpha^{-1}+\alpha)$, we see that $a_1\eta^2+a_2\eta+a_3=(\gamma-\gamma^\sigma)(\alpha^{-1}+\alpha)^{-1}$ is a divisor of $\eta-1$. It is easily seen that the divisors $A=a_1\eta^2+a_2\eta+a_3$ of $\eta-1$ such that $|a_1|\leqq 1$, $|a_2|\leqq 2$ and $|a_3|\leqq 1$ are the followings: $\pm A=1$, η, η^2, $\eta^{-1}(=\eta^2-2\eta-1)$, $\eta-1$, $\eta(\eta-1)$, $\eta^2(\eta-1)$. Noticing that $N_{K/F}(\gamma)=B^2-\eta(\eta-3)BA-A^2=1$ where $B=a_4\eta^2+a_5\eta+a_6$, we get, after some calculations, $A=\pm(\eta-1)$ and $\gamma=\pm v$, $\pm v^{-1}$. However this is a contradiction. Thus our lemma is proved.

LEMMA 2. $V=\{u\in U_K\,|\,N_{K/k}(u)=1\}=\langle\eta,\,\beta\rangle$.

PROOF. Clearly V is $\boldsymbol{Z}$-free of rank 2 and $\eta,\,\beta\in V$. Now assume that $u^n=\eta$ $(n\geqq 2)$ for some $u\in V$. Let $N_{K/F}(u)=\eta^e$. Then $\eta^{en}=\eta^2$ and therefore $n=2$. This shows that η is not a power of another unit in V, since η is not a square in K. Then we can choose a basis $\{\eta,\,\delta\}$ of V such that $N_{K/F}(\delta)=\eta^{-1}$. Since $\delta/\beta\in W$, we have $\delta\in\langle\eta,\,\beta\rangle$ by Lemma 1. Therefore $V=\langle\eta,\,\beta\rangle$.

2.2. We describe here the decomposition of 3 in L, which can be checked by simple calculations. Obviously 3 remains prime in k. Since $3=\eta^{-2}(\eta-1)(\eta+1)^2$, 3 decomposes in F as $\mathfrak{p}\mathfrak{q}^2$ where $\mathfrak{p}=(\eta-1)$ and $\mathfrak{q}=(\eta+1)$. We see that $\mathfrak{p}$ and $\mathfrak{q}$ remain prime in K. Let P_i $(i=1, 2, 3)$ be ideals of L such that $P_3=(\eta+1,\,\eta^\tau+1)$, $P_1=P_3^\tau$ and $P_2=P_1^\tau$. Then P_i $(i=1, 2, 3)$ are prime ideals and we have the following relations:

$$P_i^\sigma=P_i\ (i=1,\,2,\,3)\,,\quad P_1^\rho=P_1\,,\quad P_2^\rho=P_3\,,$$

$$\mathfrak{p}=P_1^2\,,\quad \mathfrak{q}=P_2P_3\,,\quad (3)=(P_1P_2P_3)^2\,.$$

2.3. PROPOSITION. *The equation* $\varepsilon^{4+12m}-x^3=27\varepsilon^2$ *for* $m\in\boldsymbol{Z}$ *has exactly one solution in* k, *namely* $x=-1$ *and* $m=0$.

PROOF. Let $A=\varepsilon^{1+4m}\alpha-x$ for $x\in k$. Then we easily have the following relations:

(1) $A+\zeta A^\tau+(\zeta A^\tau)^\rho=0$.

(2) $(A-A^\tau)(A-A^\tau)^\sigma=3$.

Now $N_{K/k}(A)=\varepsilon^{4+12m}-x^3=27\varepsilon^2$ implies that the ideal (A) of K is either $\mathfrak{p}^3$, $\mathfrak{p}^2\mathfrak{q}$, $\mathfrak{p}\mathfrak{q}^2$ or $\mathfrak{q}^3$. In view of (2) we must have $(A)=\mathfrak{p}^2\mathfrak{q}=(\alpha^2+\alpha^{-2})$. Then, by Lemma 2, A can be written as $(\alpha^2+\alpha^{-2})\alpha^2\eta^p\beta^q=(1+\alpha^4)\eta^p\beta^q$ with $p, q\in \boldsymbol{Z}$. In order to complete the proof, it suffices to show that $p=q=0$, i.e., $A=1+\varepsilon\alpha$.

Step I. Since $A^\tau\equiv 0 \bmod P_2^4$, (2) implies $AA^\sigma\equiv 3 \bmod P_2^4$. Now $AA^\sigma=3\{1-3(\eta+1)^2+18\eta\}\eta^{2p-q}$ and this shows that $\eta^{2p-q}\equiv 1 \bmod P_2^2$. Noticing $\eta\equiv -1 \bmod P_2$ and $\eta\not\equiv -1 \bmod P_2^2$, we see that q is even and $2p-q\equiv 0 \bmod 3$. We put $\pi=\eta^\tau+1$ and $J=\zeta(1+\zeta\alpha^4)$. It is easily shown that $\zeta\equiv 1 \bmod P_1$ and $\beta^\tau\equiv -\alpha^\tau(1-\alpha^\tau\pi) \bmod P_1^2$. Then we have $\zeta A^\tau=J(\eta^\tau)^p(\beta^\tau)^q\equiv(-1)^{p+q}\alpha^q\{\zeta^q J-pJ\pi-q\alpha J\pi\} \bmod P_1^3$. Since $\zeta A^\tau+(\zeta A^\tau)^\rho\equiv 0 \bmod P_1^3$ by (1), this shows $\zeta^q J+(\zeta^q J)^\rho\equiv(p+q\alpha)(J\pi+(J\pi)^\rho) \bmod P_1^3$. Now we have $J\pi+(J\pi)^\rho=3(-\eta^2+\eta+4)-3(4\eta^2-11\eta+2)\alpha\equiv 3(1-\alpha) \bmod P_1^3$. Since $\alpha-1\equiv\varepsilon^2 \bmod P_1^2$ and $q\equiv 2p \bmod 3$, we see $(p+q\alpha)(J\pi+(J\pi)^\rho)\equiv -3q\varepsilon^4\equiv 3q \bmod P_1^3$. On the other hand, we get easily $\zeta^q J+(\zeta^q J)^\rho\equiv -3q \bmod P_1^3$. Therefore we must have $q\equiv 0 \bmod 3$, hence $p\equiv 0 \bmod 3$.

Step II. By Step I, A can be written as $(1+\alpha^4)\eta^{3p}\beta^{6q}$, where $p, q\in\boldsymbol{Z}$. We have easily $3=(\eta-1)+\eta^{-1}(\eta-1)^3=(\eta+1)^2+(\eta+1)^4(\eta^2-\eta-4)$ and $1+\alpha^4=-\alpha^2\{(\eta-1)^2-(\eta-1)^4\}$. The following congruences are checked by some calculations:

$$3\equiv\pi^2+\pi^4-\pi^7,\quad 1+\alpha^4\equiv-\alpha^2\pi^4(1-\pi^2) \qquad \bmod P_1^8,$$

$$(1+\zeta\alpha^4)(1+\zeta^2\alpha^{-4})\equiv 3(1-\pi^3+\pi^6) \qquad \bmod P_1^9,$$

$$\varepsilon^4(=27\varepsilon^2-1)\equiv -1 \quad \bmod P_1^6, \qquad (\eta\eta^\tau)^3\equiv-(1+\pi^3) \quad \bmod P_1^4,$$

$$\beta^6\equiv -1,\quad (\beta^\tau)^6\equiv\varepsilon^2(1-\pi^3) \qquad \bmod P_1^4.$$

Putting $r=2(p-q)$, we get $AA^\sigma=(1+\alpha^4)(1+\alpha^{-4})\eta^{3r}\equiv\pi^8 \bmod P_1^9$ and $(AA^\sigma)^\tau=(1+\zeta\alpha^4)(1+\zeta^2\alpha^{-4})(\eta^\tau)^{3r}\equiv 3(1-\pi^3+\pi^6)\left(1+rs+\binom{r}{2}s^2\right) \bmod P_1^9$ where $s=-(\pi-1)^3-1\equiv\pi^3+\pi^4+\pi^5+\pi^6 \bmod P_1^7$. Further we have $AA^{\tau\sigma}+A^\sigma A^\tau=(1+\alpha^4)(1+\zeta^2\alpha^{-4})(\eta\eta^\tau)^{3p}\Phi$, where $\Phi=(\beta\beta^{\tau\sigma})^{6q}+\zeta(\beta^\sigma\beta^\tau)^{6q}\equiv(-1)^q(1-q\pi^3)(\varepsilon^{-2q}+\zeta\varepsilon^{2q}) \bmod P_1^4$. If q is odd, then $\Phi\equiv(1-\zeta)\varepsilon^{2q} \bmod P_1^4$. This gives $AA^{\tau\sigma}+A^\sigma A^\tau\equiv(-1)^p\alpha^{6q+2}3\pi^4(1-\pi^2)\equiv\pm\pi^6 \bmod P_1^9$. Then by (2), we have $3(1-\pi^3+\pi^6)\left(1+rs+\binom{r}{2}s^2\right)\pm\pi^6+\pi^8\equiv 3 \bmod P_1^9$. In particular, we have $3(1-\pi^3)(1+rs)\equiv 3 \bmod P_1^6$ and this implies $r\equiv 1 \bmod 3$; then $\binom{r}{2}s^2\equiv 0 \bmod P_1^9$. Putting $r=1+3r'$, we obtain $\pi^6+\pi^7+\pi^7(1+\pi)r'\pm\pi^6\equiv 0 \bmod P_1^9$. However this last congruence is impossible for $r'\in\boldsymbol{Z}$. Therefore q must be even. Then we have $\Phi\equiv(1-q\pi^3)\varepsilon^{2q}(1+\zeta) \bmod P_1^4$, so that $AA^{\tau\sigma}+A^\sigma A^\tau\equiv(-1)^{p+q'}(\zeta\alpha^4+\zeta^2\alpha^{-4}-1) \bmod P_1^7$ where $q=2q'$. Now we want to prove that $p+q'\equiv 0 \bmod 6$. Assume $p+q'$ is odd. By (2), we have $(1+\zeta\alpha^4)(1+\zeta^2\alpha^{-4})(1+s)^r+(\zeta\alpha^4+\zeta^2\alpha^{-4}-1)\equiv 3 \bmod P_1^7$ and this implies $-2\pi^5+\pi^5(1+\pi)r\equiv 0 \bmod P_1^7$. This congruence is also impossible for $r\in\boldsymbol{Z}$. Therefore $p+q'$ is even and then we have by (2) that $(1+\zeta\alpha^4)(1+\zeta^2\alpha^{-4})sr\equiv 0 \bmod P_1^7$; this implies that $r=2(p-2q')\equiv 0 \bmod 3$. Then obviously we have $p+q'\equiv 0 \bmod 6$.

Step III. We easily see that $\alpha^4\beta^4\eta^{-1}=3\alpha^2-1$. As $A=(1+\alpha^4)\eta^{3p}\beta^{12q'} =(1+\alpha^4)\eta^{3(p+q')}(\alpha^4\beta^4\eta^{-1})^{3q'}\alpha^{-12q'}$, by Step II we can write A as $\varepsilon^{-4y}(1+\alpha^4)\eta^{18x} \cdot(3\alpha^2-1)^{3y}$ where $x, y\in \boldsymbol{Z}$. Put $\eta^6(=33\eta^2+18\eta+13)=1+3M$. Then $M=30+(13\varepsilon-50)\alpha+(-15\varepsilon+88)\alpha^2$. Putting $\eta^{18}=1+9\phi$, we get

$$\phi=M+3M^2+3M^3\equiv(4-2\varepsilon)\alpha+(6\varepsilon+4)\alpha^2 \qquad \bmod 9O_k[\alpha]\,.$$

We have $(1-3\alpha^2)^3=1+9\psi$, where $\psi=-3\varepsilon^2+3\varepsilon\alpha-\alpha^2$. For $G=a+b\alpha+c\alpha^2$ $(a, b, c\in O_k)$, let

$$T(G)=(1+\alpha^4)G+\zeta((1+\alpha^4)G)^\tau+\zeta^2((1+\alpha^4)G)^{\tau\rho}\,.$$

Then $T(G)=3\alpha^2(b\varepsilon+c)$. By (1), we have $T(\eta^{18x}(1-3\alpha^2)^{3y})=0$. Now consider the following 9-adic expansion:

$$\begin{aligned}\eta^{18x}(1-3\alpha^2)^{3y}&=(1+9\phi)^x(1+9\psi)^y\\&=\left(1+9x\phi+9^2\binom{x}{2}\phi^2+\cdots\right)\left(1+9y\psi+9^2\binom{y}{2}\psi^2+\cdots\right)\\&=1+9(x\phi+y\psi)+9^2\left(\binom{x}{2}\phi^2+\binom{y}{2}\psi^2+xy\phi\psi\right)+\cdots.\end{aligned}$$

Then we have

$$9(xT(\phi)+yT(\psi))+9^2\left(\binom{x}{2}T(\phi^2)+\binom{y}{2}T(\psi^2)+xyT(\phi\psi)\right)+\cdots=0\,.$$

If either x or y is not zero, then we can put $x=3^e m$, $y=3^e n$, $(m, n, 3)=1$ $(e\geqq 0)$. Since $9^i\binom{x}{i}T(\phi^i)$, $9^i\binom{y}{i}T(\psi^i)$ $(i\geqq 2)$ are divisible by $9^2\cdot 3^{e+1}$, we obtain

$$9(xT(\phi)+yT(\psi))\equiv 0 \qquad \bmod 9^2\cdot 3^{e+1}$$

or

$$mT(\phi)+nT(\psi)\equiv 0 \qquad \bmod 27\,.$$

Noticing $T(\phi)\equiv 6\alpha^2 \bmod 27$ and $T(\psi)=3(2+15\varepsilon)\alpha^2$, we have $2(m+n)+15\varepsilon n\equiv 0 \bmod 9$, and this implies $m+n\equiv 0$, $15n\equiv 0 \bmod 9$, so that $m\equiv n\equiv 0 \bmod 3$, which is a contradiction. Therefore $x=y=0$ and this completes the proof.

References

[1] W. Casselman, On abelian varieties with many endomorphisms and a conjecture of Shimura, Invent. Math., **12** (1971), 225-236.
[2] J.-P. Serre, Abelian l-adic representations and elliptic curves, Benjamin, New York, 1968.
[3] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math., **15** (1972), 259-331.

[4] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten and Princeton Univ. Press, 1971.
[5] G. Shimura, Class fields over real quadratic fields and Hecke operators, Ann. of Math., **95** (1972), 130-190.
[6] M. Yamauchi, On the fields generated by certain points of finite order on Shimura's elliptic curves, J. Math. Kyoto univ., **14** (1974), 243-255.

Tetsuo NAKAMURA
Department of Mathematics
College of General Education
Tohoku University
Kawauchi, Sendai 980
Japan