Arch. Math. 73 (1999) 25–32
0003-889X/99/010025-08 $ 3.10/0

Archiv der Mathematik

Determination of elliptic curves with everywhere good reduction over real quadratic fields

By

Takaaki Kagawa

Abstract. All elliptic curves having everywhere good reduction over $\mathbb{Q}(\sqrt{29})$ are determined by studying the fields of 2- and 3-division points. As a byproduct of the argument, the elliptic curves over some real quadratic fields are determined. Though part of the result are already obtained in [2], [4], [5], [10], the proof given in the present paper is simpler.

1. Introduction. Let d be the discriminant of a real quadratic field and χ_d the associated Dirichlet character. Let $S_d = S_2(\Gamma_0(d), \chi_d)$ be the space of cuspforms of Neben-type of weight two. When S_d has a 2-dimensional $\mathbb{Q}$-simple factor, Shimura [14] constructed a certain abelian surface A defined over $\mathbb{Q}$ from the factor and showed that A splits over the field $\mathbb{Q}(\sqrt{d})$ as $B \times B'$, where B is an elliptic curve defined over $\mathbb{Q}(\sqrt{d})$ and B' is the conjugate of B. It is known that the curve B, which we call Shimura's elliptic curve over $\mathbb{Q}(\sqrt{d})$, has everywhere good reduction over $\mathbb{Q}(\sqrt{d})$, and is isogenous over $\mathbb{Q}(\sqrt{d})$ to B'. Conversely, it is conjectured by Pinch ([10]) that any elliptic curve with such properties should be isogenous over $\mathbb{Q}(\sqrt{d})$ to Shimura's elliptic curve. By Shimura [14], S_d is $\{0\}$ for $d = 5, 13, 17$, and 2-dimensional and $\mathbb{Q}$-simple for $d = 29, 37, 41$. Hence, assuming Pinch's conjecture, there are no such curves when $d = 5, 13, 17$, and there is only one isogeny class of such curves when $d = 29, 37, 41$. In [3], [4], it was proved that this conclusion is true without the conjecture for all these d except $d = 29$ (see also [2], [10]). In this paper, we prove that it is also true for $d = 29$ by determining all elliptic curves with everywhere good reduction over $k = \mathbb{Q}(\sqrt{29})$.

In his paper [9], Nakamura has proved the conjecture of Serre given in [11], p. 184, which states that Shimura's elliptic curve over k is isogenous over k to

$$E_1 : y^2 + xy + \varepsilon^2 y = x^3$$

with discriminant $-\varepsilon^{10}$, where $\varepsilon = (5 + \sqrt{29})/2$ is a fundamental unit of k; see also [15]. Nakamura's result concerning Serre's conjecture (Lemma 2 below) forms one of the vital steps for our determination of elliptic curves with everywhere good reduction over k in the present paper.

We also deal with many other fields in Appendix, where we use similar arguments given in section 3.1 in order to simplify the arguments in our previous papers [2], [4], [5], [10].

Mathematics Subject Classification (1991): 11G05.

2. Results. Let $k = \mathbb{Q}(\sqrt{29})$ and let ε, E_1 be as in Section 1. We have $E_1(k)_{\mathrm{tors}} = \langle (0,0) \rangle \cong \mathbb{Z}/3\mathbb{Z}$. This follows from the following three facts: $(0,0) \in E_1(k)$ is of order 3; $\#(E_1)_{\mathfrak{p}_5}(\mathcal{O}_k/\mathfrak{p}_5) = 9$ and $\#(E_1)_{\mathfrak{p}_7}(\mathcal{O}_k/\mathfrak{p}_7) = 6$, where $\mathcal{O}_k$ is the ring of integers of k, $\mathfrak{p}_5$ (resp. $\mathfrak{p}_7$) is a prime ideal lying above 5 (resp. 7); the reduction map $E_1(k)_{\mathrm{tors}} \to (E_1)_{\mathfrak{p}_p}(\mathcal{O}_k/\mathfrak{p}_p)$ is injective, where $(E_1)_{\mathfrak{p}_p}$ is the reduction of E_1 modulo $\mathfrak{p}_p$ ($p = 5, 7$). A defining equation of $E_2 := E_1/\langle (0,0) \rangle$ is calculated by Vélu's formula ([18]):

$$E_2 : y^2 + xy + \varepsilon^2 y = x^3 - 5\varepsilon^2 x - (\varepsilon^2 + 7\varepsilon^4),$$

whose discriminant is $-\varepsilon^{14}$. As will be shown, E_2 does not have a k-rational point of order 3, and hence $\#E_2(k)_{\mathrm{tors}} = 1$.

At present, we have some examples of elliptic curves with everywhere good reduction over k, namely E_1, E_1', E_2 and E_2', where E_1', E_2' denote the conjugates of E_1, E_2 over k, respectively. Our aim is to prove that there are no such curves other than these:

Theorem 1. *Up to isomorphism over $k = \mathbb{Q}(\sqrt{29})$, the four curves listed above are all the elliptic curves with everywhere good reduction over k.*

By definition, E_1 and E_2 are 3-isogenous over k. Moreover, E_1 and E_1' are 5-isogenous over k, because E_1 has a k-rational subgroup V defined by $x^2 - \varepsilon x - (4 + 21\varepsilon)/5$, and there is an isomorphism defined over k between E_1' and

$$E_1/V : Y^2 + XY + \varepsilon^2 Y = X^3 - (2 + 3\varepsilon)\varepsilon^3 X - 13\varepsilon^5$$

given by the substitution

$$X = (\varepsilon^2 + \varepsilon)^2 x + (3\varepsilon^2 + \varepsilon),\ Y = (\varepsilon^2 + \varepsilon)^3 y + 3\varepsilon(\varepsilon^2 + \varepsilon)^2 x + 4\varepsilon^3.$$

(The equation of E_1/V given above is also calculated by Vélu's formula.) Hence

Corollary 1. *All elliptic curves with everywhere good reduction over $k = \mathbb{Q}(\sqrt{29})$ are isogenous over k.*

3. Proof of Theorem 1.

Notation. For a number field K, we denote by $\mathcal{O}_K$ and h_K its ring of integers and its class number, respectively. If $\mathfrak{m}$ is a divisor of K, $h_K(\mathfrak{m})$ denotes the ray class number of K modulo $\mathfrak{m}$.

The following two lemmas are known:

Lemma 1. *Let k be a real quadratic field with narrow class number 1 and let l be a prime number which is inert in k. Then for any semi-stable elliptic curves $E, \bar{E}$ over k which are l-isogenous over k, either E or $\bar{E}$ has a k-rational point of order l.*

Proof. [6], p. 248. □

Remark. The condition of the lemma that l is inert in k is necessary, because the results of Serre [11] used in [6] require the assumption that l is unramified, and the conclusion of the lemma does not hold in general if l splits in k. For example, as was shown above, our curves

E_1 and E_1' are 5-isogenous over $\mathbb{Q}(\sqrt{29})$ but none of the two curves have any $\mathbb{Q}(\sqrt{29})$-rational points of order 5. (See also the arguments in pp. 248–249 of [6] and in pp. 320–323 of [11].)

Lemma 2. *Let E be an elliptic curve with everywhere good reduction over $\mathbb{Q}(\sqrt{29})$ with discriminant $\Delta = -\varepsilon^n$ $(n = 2, 4, 8, 10)$. If E has a $\mathbb{Q}(\sqrt{29})$-rational point of order 3, then E is isomorphic over $\mathbb{Q}(\sqrt{29})$ to E_1 given in Section 1 or to its conjugate E_1'.*

Proof. This was proved in the proof of the theorem of [9]. □

Let E be an elliptic curve with everywhere good reduction over $k = \mathbb{Q}(\sqrt{29})$ with discriminant $\Delta = \pm\varepsilon^n$ $(n \in \mathbb{Z})$, where $\varepsilon = (5 + \sqrt{29})/2$. In view of the formulae for an admissible change of variables, we may assume that $0 \leqq n < 12$. The following lemma and propositions, together with Lemmas 1 and 2, imply Theorem 1.

Lemma 3. *Let E_1 be as in Section 1. The only k-rational subgroup of E_1 of order 3 is $E_1(k)_{\mathrm{tors}} = \langle (0, 0) \rangle$.*

Proposition 1. *The discriminant of E is of the form $-\varepsilon^n$ $(n = 2, 4, 8, 10)$.*

Proposition 2. *E admits a 3-isogeny defined over k.*

The proof of Theorem 1 is as follows. If E has a k-rational point of order 3, then Lemma 2 and Proposition 1 imply that E is E_1 or E_1'. If E has no k-rational point of order 3, then take a curve $\bar{E}$ which is 3-isogenous over k to E; the existence of $\bar{E}$ is guaranteed by Proposition 2. By Lemmas 1, 2 and Proposition 1, $\bar{E}$ is E_1 or E_1' and, by Lemma 3, E is E_2 or E_2', which proves Theorem 1. Thus, to complete the proof of Theorem 1, all that remains is to prove Lemma 3 and Propositions 1, 2.

We can prove Lemma 3 easily. Indeed, the x-coordinate $x \in k$ of a point of a k-rational subgroup of E_1 of order 3 satisfies $x(3x^3 + x^2 + 3\varepsilon^2 x + 3\varepsilon^4) = 0$, and $3x^3 + x^2 + 3\varepsilon^2 x + 3\varepsilon^4$ is irreducible modulo the prime ideal $((1 + \sqrt{29})/2)$ whose norm is 7, as claimed.

We will prove Propositions 1 and 2 in the following sections.

3.1. Proof of Proposition 1. Let E and Δ be as in the preceding section and let $N = k(\sqrt{\Delta})$. Since $\Delta = \pm\varepsilon^n$, we have $N = k$, $k(\sqrt{-1})$ or $k(\sqrt{\pm\varepsilon})$. Note that, since the norm of ε is -1, $k(\sqrt{\varepsilon})$ and $k(\sqrt{-\varepsilon})$ are conjugate over $\mathbb{Q}$ and hence we may assume that $N = k$, $k(\sqrt{-1})$ or $k(\sqrt{\varepsilon})$. We first show that N must be $k(\sqrt{-1})$, that is, the sign of Δ is $-$ and n is even.

Let k_2 be the extension of k generated by the coordinates of all points of order 2. Since, by Proposition 2.2 of [2], E has no k-rational points of order 2, k_2/N is a cyclic cubic extension. Further k_2/N is unramified outside 2 by the criterion of Néron-Ogg-Shafarevich ([16], p. 184). Thus we have

Lemma 4. *$h_N^{(2)} := h_N(\prod_{\mathfrak{p}|2} \mathfrak{p})$ is divisible by 3, where the product is taken over all prime ideals of N dividing 2.*

We interpret the divisibility of $h_N^{(2)}$ by 3 in terms of class number.

The discriminant of $k(\sqrt{-1})$ is $2^4 \cdot 29^2$ (see Proposition 17 of Chapter III in [8]).

Lemma 5. *Let $m > 1$ be square-free and congruent to 5 modulo 8 and let $L = \mathbb{Q}(\sqrt{m})$. Supposing that the norm of the fundamental unit ε of L is -1, the discriminant of $L(\sqrt{\varepsilon})$ is $-16m^2$.*

Proof. Since the discriminant of the polynomial $X^2 - \varepsilon$ is 4ε, the relative discriminant $d_{L(\sqrt{\varepsilon})/L}$ of $L(\sqrt{\varepsilon})/L$ is a divisor of $4\mathcal{O}_L$. If $d_{L(\sqrt{\varepsilon})/L} = \mathcal{O}_L$, then we have $|d_{L(\sqrt{\varepsilon})}| = m^2$ by the formula

$$|d_{L(\sqrt{\varepsilon})}| = |d_L|^{[L(\sqrt{\varepsilon}):L]} N_L d_{L(\sqrt{\varepsilon})/L}$$

(see [8], pp. 60, 66, or [19], p. 44). Here $d_{L(\sqrt{\varepsilon})}$ (resp. $d_L = m$) is the discriminant of $L(\sqrt{\varepsilon})$ (resp. of L), and $N_L d_{L(\sqrt{\varepsilon})/L}$ is the norm of the ideal $d_{L(\sqrt{\varepsilon})/L}$. We must have $d_{L(\sqrt{\varepsilon})} = -m^2$, since $L(\sqrt{\varepsilon})$ is a quartic field having two real embeddings and a pair of complex embeddings (see [19], Lemma 2.2). This contradicts the fact that the discriminant of a number field must be congruent to 0 or 1 modulo 4 (see [8], p. 67). Hence 2 is wildly ramified in the extension $L(\sqrt{\varepsilon})/L$ and hence $d_{L(\sqrt{\varepsilon})/L} = 4\mathcal{O}_L$ by Proposition 8 of Chapter III in [8], whence $d_{L(\sqrt{\varepsilon})} = -16m^2$ by the above formula. □

Remark. Let L, ε be as in Lemma 5 and let $\omega = (1 + \sqrt{m})/2$. The ring of integers of $L(\sqrt{\varepsilon})$ is $\mathbb{Z} \oplus \mathbb{Z}\omega \oplus \mathbb{Z}\sqrt{\varepsilon} \oplus \mathbb{Z}\omega\sqrt{\varepsilon} = \mathcal{O}_L \oplus \mathcal{O}_L\sqrt{\varepsilon}$, since its discriminant is $-16m^2$.

Hence there is just one prime $\mathfrak{p}$ of N dividing 2 and the norm of $\mathfrak{p}$ is 4. By this and the formula for the ray class number (Theorem 1 of Chapter VI in [8]), we obtain the following:

Lemma 6. *The ray class number $h_N^{(2)} = h_N(\mathfrak{p})$ is equal to h_N, whence $h_N \equiv 0 \pmod 3$.*

Lemma 7. *$h_k = h_{k(\sqrt{\varepsilon})} = 1$ and $h_{k(\sqrt{-1})} = 3$.*

Proof. The assertion that $h_k = 1$ is clear. The assertion that $h_{k(\sqrt{\varepsilon})} = 1$ is proved by checking that all the prime ideals with norm less than or equal to 13 (= the integral part of the Minkowski bound for $k(\sqrt{\varepsilon})$) are principal. For $k(\sqrt{-1})$, we have $h_{k(\sqrt{-1})} = h_{\mathbb{Q}(\sqrt{-1})} h_{\mathbb{Q}(\sqrt{-29})} h_k/2 = 3$ (cf. [7]). □

From Lemmas 6 and 7 it follows that $N = k(\sqrt{-1})$ and Δ is of the form $-\varepsilon^{2n}$ $(0 \leqq n < 6)$.

Next we show that both of the cases $n = 0$ and $n = 3$ are impossible. The discriminant Δ and the quantities c_4, c_6 defined as usual satisfy $c_4^3 - c_6^2 = 1728\Delta$. Hence, if $\Delta = -\varepsilon^{2n}$ $(n = 0, 3)$, then $(c_4/\varepsilon^{2n/3}, c_6/\varepsilon^n)$ is a k-rational point of the elliptic curve $C : y^2 = x^3 + 1728$.

Lemma 8. *The Mordell-Weil group $C(k)$ of C over k is $\langle(-12, 0)\rangle \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. The rank of $C(k)$ is shown to be 0 by the well-known formula

$$\operatorname{rank} C(k) = \operatorname{rank} C(\mathbb{Q}) + \operatorname{rank} C^{(29)}(\mathbb{Q}),$$

where $C^{(29)}$ is the quadratic twist of C by 29, and also by 2-descent via 2-isogeny (cf. [16], [17]). Combining the injectivity of the reduction map $C(k)_{\text{tors}} \to C_{\mathfrak{p}_p}(\mathcal{O}_k/\mathfrak{p}_p)$, where $\mathfrak{p}_p$ $(p = 5, 7)$ is a prime ideal of k dividing p and $C_{\mathfrak{p}_p}$ is the reduction of C modulo $\mathfrak{p}_p$, with the facts that $\#C_{\mathfrak{p}_5}(\mathcal{O}_k/\mathfrak{p}_5) = 2 \cdot 3$, $\#C_{\mathfrak{p}_7}(\mathcal{O}_k/\mathfrak{p}_7) = 2^2$, and also with the fact that order of the point $(-12, 0)$ is 2, we see that $C(k)_{\text{tors}}$ is of order 2. The proof of the lemma is now complete. □

Hence, if $\Delta = -1$ or $\Delta = -\varepsilon^6$, then $c_6 = 0$, that is, the j-invariant of E is 1728. But this is impossible by Theorem 2 (a) in [13] (see also [10], Remark 2.1.4.1).

Now we have proved Proposition 1.

3.2. Proof of Proposition 2. We again let E and Δ be as above.

To prove Proposition 2, suppose that the assertion is false. Let k_3 be the extension of k generated by the 3-torsion points of E and let $M = k(\sqrt{-3})$ and $K = k(\sqrt[3]{\Delta}) = k(\alpha) = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt[3]{\varepsilon}$. We may regard $G = \mathrm{Gal}(k_3/k)$ as a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. Since k_3 contains K ([11], p. 305) and K is a cubic extension of k, the order of G is divisible by 3. Thus, by Proposition 15 of [11], G is contained in a Borel subgroup, or G contains $\mathrm{SL}_2(\mathbb{F}_3)$. The former case is equivalent to the assertion that E admits a 3-isogeny defined over k, being excluded by our assumption. Therefore $\mathrm{SL}_2(\mathbb{F}_3) \subset G$, which is equivalent to the assertion $G = \mathrm{GL}_2(\mathbb{F}_3)$, since the map $\det : G \to \mathbb{F}_3^\times$ is surjective by the commutativity of the diagram

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_3) \\ {\scriptstyle \mathrm{Res}}\downarrow & & \downarrow{\scriptstyle \det} \\ \mathrm{Gal}(M/k) & \xrightarrow{\sim} & \mathbb{F}_3^\times \end{array} .$$

Thus the Galois group $\mathrm{Gal}(k_3/K)$, whose order is 2^4, is a 2-Sylow subgroup of $G = \mathrm{GL}_2(\mathbb{F}_3)$, whose order is $2^4 \cdot 3$, and is isomorphic to

$$\langle \sigma, \tau \mid \sigma^2 = 1, \tau^8 = 1, \sigma\tau\sigma = \tau^3 \rangle,$$

the semi-dihedral group of order 16.

We quote some results which are proved in [9] or easily deduced from results in the paper.

Lemma 9. *Let K be as above and let $F = \mathbb{Q}(\eta)$, where $\eta^3 - 2\eta^2 - \eta - 1 = 0$. Then the fields F, K and M have the following properties:*

(1) $K = kF$. (*Note that* $\alpha^2 + \eta(\eta - 3)\alpha - 1 = 0$.)
(2) $\mathcal{O}_F = \mathbb{Z}[\eta]$, $\mathcal{O}_K = \mathcal{O}_F[\alpha]$. *Hence the discriminant of F (resp. K) is* $-3 \cdot 29$ (*resp.* $3^2 \cdot 29^3$).
(3) $h_F = 1$.
(4) *The prime 3 decomposes in F and MK as* $\mathfrak{p}_3\mathfrak{p}_3'^2$ *and* $(\mathfrak{P}_3\mathfrak{P}_3'\mathfrak{P}_3'')^2$, *respectively, where* $\mathfrak{p}_3 = (\eta - 1)$, $\mathfrak{p}_3' = (\eta + 1)$ *are distinct prime ideals of F, and* $\mathfrak{P}_3$, $\mathfrak{P}_3'$, $\mathfrak{P}_3''$ *are distinct prime ideals of MK. The primes* $\mathfrak{p}_3$, $\mathfrak{p}_3'$ *are inert in K.*
(5) *The prime 29 decomposes in F and K as* $\mathfrak{p}_{29}^2\mathfrak{p}_{29}'$ *and* $(\mathfrak{P}_{29}\mathfrak{P}_{29}')^2$, *respectively, where* $\mathfrak{p}_{29}$, $\mathfrak{p}_{29}'$ *are distinct prime ideals of F and* $\mathfrak{P}_{29}$, $\mathfrak{P}_{29}'$ *are distinct prime ideals of K.*
(6) *The real prime of F is unramified in K.*
(7) $\eta \mapsto -1$ *induces an isomorphism* $\mathcal{O}_K/\mathfrak{p}_3' \cong \mathbb{F}_9 = \mathbb{F}_3(\bar{\alpha})$, *where* $\bar{\alpha} = \alpha + \mathfrak{p}_3'$.
(8) *MK is the Hilbert class field of* $\mathbb{Q}(\sqrt{-87})$.

Let $\mathfrak{p}$ be the principal ideal $3\mathcal{O}_k$. Assume first that E has ordinary reduction at $\mathfrak{p}$. Then, by the corollary to Proposition 11 of [11] and (4) of Lemma 9, the ramification index of $\mathfrak{p}$ in k_3/k is 2. It follows from (4), (8) of Lemma 9 and the criterion of Néron-Ogg-Shafarevich that $k_3/\mathbb{Q}(\sqrt{-87})$ is an unramified extension. But it is impossible, since MK is the maximal unramified abelian extension of $\mathbb{Q}(\sqrt{-87})$ (see [20]).

Suppose next that E has supersingular reduction at $\mathfrak{p}$. Then by Proposition 12 of [11], the inertia group in k_3/k of a prime ideal of k_3 dividing $\mathfrak{p}$ is a cyclic group of order 8. There are

exactly three such subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$, namely $\langle\tau\rangle$, $g\langle\tau\rangle g^{-1}$, $g^2\langle\tau\rangle g^{-2}$, where τ is as above and $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is of order 3. Let $\mathfrak{P}$ be a prime ideal of k_3 dividing $\mathfrak{p}$ with inertia group $\langle\tau\rangle$. By (4) of Lemma 9, we must have $\mathfrak{P} \cap K = \mathfrak{p}_3$ and the fixed field of k_3 by the group $\langle\tau\rangle$ is a quadratic extension of K unramified outside $\mathfrak{p}_3'$ and the real primes $\mathfrak{p}_\infty^{(1)}$, $\mathfrak{p}_\infty^{(2)}$ of K. However, we have

Lemma 10. *$h_K(\mathfrak{p}_3'\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)})$ is odd.*

Proof. Let $\mathfrak{m} = \mathfrak{p}_3'\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}$ and let

$$K_\mathfrak{m} = \{x \in K^\times \mid (x, \mathfrak{m}) = 1\}, K_{\mathfrak{m},1} = \{x \in K_\mathfrak{m} \mid x \equiv 1 \,(\mathrm{mod})\, \mathfrak{m}\}.$$

The following three units generate the group $K_\mathfrak{m}/K_{\mathfrak{m},1} \cong \mathbb{F}_3(\bar{\alpha})^\times \times \langle -1\rangle \times \langle -1\rangle$:

$$u_1 = (\eta^2 - 2\eta) + \alpha, u_2 = -\eta^{-1} + (\eta - 2)\alpha, u_3 = 1 + (2\eta - \eta^2)\alpha\,.$$

Indeed, $u_1 \equiv \alpha$, $u_2 \equiv u_3 \equiv 1 \,(\mathrm{mod}\, \mathfrak{p}_3')$ by Lemma (7) of 9, and

$$\begin{aligned} u_1^{(1)} &= 3.124\ldots, \quad u_1^{(2)} = 0.815\ldots, \\ u_2^{(1)} &= 0.554\ldots, \quad u_2^{(2)} = -0.708\ldots, \\ u_3^{(1)} &= -1.411\ldots, \quad u_3^{(2)} = 1.804\ldots, \end{aligned}$$

where $^{(i)}$ $(i = 1, 2)$ means the conjugacy corresponding to $\mathfrak{p}_\infty^{(i)}$. (We normalize $^{(i)}$ as $\alpha^{(1)} = 1.731\ldots$, $\alpha^{(2)} = -0.5774\ldots$. Note that $\eta^{(1)} = \eta^{(2)} = 2.546\ldots$.) Hence $h_K(\mathfrak{m}) = h_K$ by the formula for the ray class number. Thus it is enough to prove that h_K is odd. Let F be as in Lemma 9. By (2), (4), (5) and (6) of Lemma 9, the only prime of F ramifying in K is $\mathfrak{p}_{29}'$. Hence h_K is odd by (3) of Lemma 9 and (a) of Theorem 10.4 in [19]. (In fact, we can check that $h_K = 1$ and thus $h_K(\mathfrak{p}_3'\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}) = 1$.) □

Again we have a contradiction. Hence E admits a 3-isogeny defined over k.

The proof of Theorem 1 is complete.

4. Appendix. Let k be a real quadratic field and let E be an elliptic curve with everywhere good reduction over k with discriminant Δ. If E has no k-rational points of order 2, then the ray class number $h^{(2)}_{k(\sqrt{\Delta})} = h_{k(\sqrt{\Delta})}\left(\prod_{\mathfrak{p}|2} \mathfrak{p}\right)$ is divisible by 3 (cf. Lemma 4).

Assume first that the class number of k is prime to 6. Then E has a global minimal model ([12], Corollary to Theorem 1), and hence we may take Δ to be a unit. Hence, if $h_k^{(2)}$, $h^{(2)}_{k(\sqrt{-1})}$ and $h^{(2)}_{k(\sqrt{\varepsilon})}$ are all prime to 3, then each elliptic curve with everywhere good reduction over k has a k-rational point of order 2.

Assume next that $h_k = 2$. Since E has everywhere good reduction over k, the principal ideal (Δ) is a 12-th power, say $(\Delta) = \mathfrak{a}^{12}$. Since $h_k = 2$, $(\Delta) = (\mathfrak{a}^2)^6 = (\alpha)^6$ for some $\alpha \in k^\times$. Therefore $k(\sqrt{\Delta})$ is one of the fields k, $k(\sqrt{-1})$, $k(\sqrt{\pm\varepsilon})$ and hence an argument similar to that given above can be applied.

Computing $h_k^{(2)}$, $h^{(2)}_{k(\sqrt{-1})}$ and $h^{(2)}_{k(\sqrt{\varepsilon})}$ (we omit the details, merely remarking that $h^{(2)}_{k(\sqrt{\Delta})} = h_{k(\sqrt{\Delta})}$ in many cases) and combining this with results in [1], we obtain:

Theorem 2. (1) *If $m = 2, 3, 5, 10, 13, 15, 17, 21, 30, 34, 39, 42, 47, 58, 66, 70, 73, 74, 85, 94$ or 97, then there are no elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{m})$.*

(2) *If* $m = 6, 7, 14, 41$ *or* 65, *then every elliptic curve with everywhere good reduction over* $k = \mathbb{Q}(\sqrt{m})$ *has a* k*-rational point of order* 2. *Thus the curves* E_i $(1 \leqq i \leqq 18, 23 \leqq i \leqq 40)$ *listed in Section* 5 *of* [1] *are all the elliptic curves having everywhere good reduction over these fields.*

For the values of m above such that the class number of $\mathbb{Q}(\sqrt{m})$ is prime to 6, that is, for $m = 2, 3, 5, 6, 7, 13, 14, 17, 21, 41, 47, 73, 94, 97$, the same results have already been obtained in [2], [4], [5], [10]. It is worth remarking that we use the class field theory only, whereas the authors of [2], [4] and [5] used Serre's results on Galois representation theory ([11]) or the ramification theory in Kummer extensions in addition.

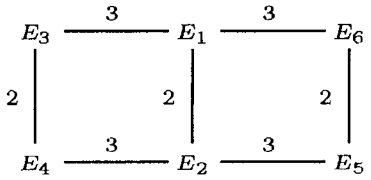
We can check that there is only one isogeny class for $m = 6, 7, 14, 41$ and that there are exactly two isogeny classes for $m = 65$. Below we show the isogeny graphs among the related elliptic curves. For elliptic curves E, E' defined over k and a rational prime p, the graph

$$E \overset{p}{\text{---}} E'$$

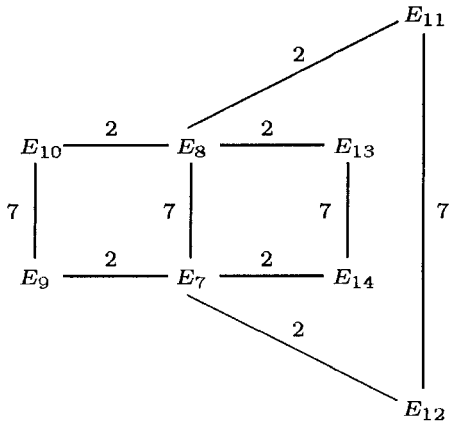
means that E and E' are p-isogenous over k.

Let $d(m)$ be the discriminant of a quadratic field $\mathbb{Q}(\sqrt{m})$. Then, on the other hand, the structure of the space $S_{d(m)}$ introduced in Section 1 is known. For the values of m stated in Theorem 2 (1), $S_{d(m)}$ has no 2-dimensional $\mathbb{Q}$-simple factor. For $m = 6, 7, 41$, $S_{d(m)}$ is 2-dimensional and $\mathbb{Q}$-simple; for $m = 14$, it is a direct product of a 2-dimensional $\mathbb{Q}$-simple subspace and a 4-dimensional $\mathbb{Q}$-simple subspace; for $m = 65$, it is a direct product of two $\mathbb{Q}$-simple subspaces of dimension 2 (the above calculations of $S_{d(m)}$ are done by Y. Hasegawa and T. Hibino independently). Hence, for the values of m in Theorem 2, the conjecture stated in Section 1 is true.

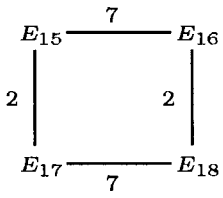
$\mathbb{Q}(\sqrt{6})$:



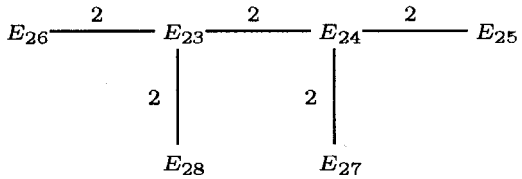
$\mathbb{Q}(\sqrt{7})$:



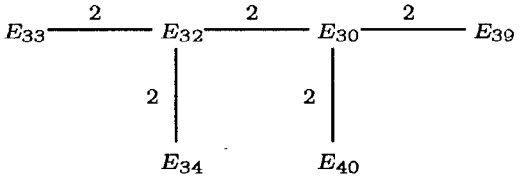
$\mathbb{Q}(\sqrt{14})$:

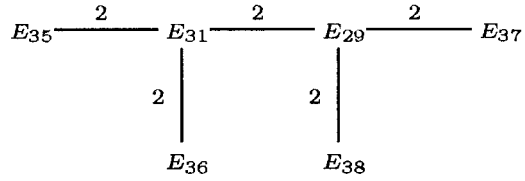


$\mathbb{Q}(\sqrt{41})$:



$\mathbb{Q}(\sqrt{65})$:





Acknowledgment. We would like to express our thanks to M. Ozaki and A. Umegaki for several useful discussions.

References

[1] S. COMALADA, Elliptic curves with trivial conductor over quadratic fields. Pacific J. Math. **144,** 233–258 (1990).
[2] H. ISHII, The non-existence of elliptic curves with everywhere good reduction over certain quadratic fields. Japan. J. Math. **12,** 45–52 (1986).
[3] T. KAGAWA, Determination of elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{37})$. Acta Arith. **83,** 253–269 (1998).
[4] M. KIDA and T. KAGAWA, Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields. J. Number Theory **66,** 201–210 (1997).
[5] M. KIDA, Reduction of elliptic curves over real quadratic number fields, to appear in Math. Comp.
[6] A. KRAUS, Courbes elliptiques semi-stable et corps quadratiques. J. Number Theory **60,** 245–253 (1996).
[7] T. KUBOTA, Über den bizyklischen biquadratischen Zahlkörper. Nagoya J. Math. **10,** 65–85 (1956).
[8] S. LANG, Algebraic Number Theory (2nd ed.). Grad. Texts in Math. **110** (1994).
[9] T. NAKAMURA, On Shimura's elliptic curve over $\mathbb{Q}(\sqrt{29})$. J. Math. Soc. Japan **36,** 701–707 (1984).
[10] R. G. E. PINCH, Elliptic curves over number fields. Ph. D. thesis, Oxford 1982.
[11] J.-P. SERRE, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15,** 259–331 (1972).
[12] B. SETZER, Elliptic curves over complex quadratic fields. Pacific J. Math. **74,** 235–250 (1978).
[13] B. SETZER, Elliptic curves with good reduction everywhere over quadratic fields and having rational *j*-invariant. Illinois J. Math. **25,** 233–245 (1981).
[14] G. SHIMURA, Introduction to the Arithmetic Theory of Automorphic Functions. Publ. Math. Soc. Japan **11** (1971).
[15] K. SHIOTA, On the explicit models of Shimura's elliptic curves. J. Math. Soc. Japan **38,** 649–659 (1986).
[16] J. H. SILVERMAN, The Arithmetic of Elliptic Curves. Grad. Texts in Math. **106** (1986).
[17] J. H. SILVERMAN and J. TATE, Rational Points on Elliptic Curves. Universitext Tracts. Math. (1992).
[18] J. VÉLU, Isogénies entre courbes elliptiques. C. R. Acad. Sc. Paris **273,** 238–241 (1971).
[19] L. C. WASHINGTON, Introduction to Cyclotomic Fields. Grad. Texts in Math. **83** (1982).
[20] K. YAMAMURA, Maximal unramified extensions of imaginary quadratic number fields of small conductors. J. Théor. Nombres de Bordeaux **9,** 405–448 (1997).

Eingegangen am 13. 3. 1998*)

Anschrift des Autors:

Takaaki Kagawa
Department of Mathematics
Ritsumeikan University
Kusatsu, Shiga, 525-8599
Japan

*) Eine überarbeitete Fassung ging am 4. 12. 1998 ein.