Nonexistence of elliptic curves having everywhere good reduction and cubic discriminant

By Takaaki Kagawa

Department of Mathematics, Ritsumeikan University, 1-1-1, Nojihigashi, Kusatsu, Shiga 525-8577
(Communicated by Heisuke Hironaka, M. J. A., Nov. 13, 2000)

Abstract: In this paper, it is proved that, over certain real quadratic fields, there are no elliptic curves having everywhere good reduction and cubic discriminant.

Key words: Elliptic curves; everywhere good reduction.

1. Result. In [2], we showed that there are, up to isomorphism over $\mathbf{Q}(\sqrt{33})$, exactly six elliptic curves with everywhere good reduction over $\mathbf{Q}(\sqrt{33})$, two of which have cubic discriminant, and that there are no such curves over $\mathbf{Q}(\sqrt{3p})$ if $p = 19, 23$ or 31. In this paper, we refine some results in [2], and using them, we prove the following:

Theorem. *If p is a prime number such that $p \equiv 3 \pmod 4$ and $p \neq 3, 11$, then there is no elliptic curve which has everywhere good reduction over $k = \mathbf{Q}(\sqrt{3p})$ and whose discriminant is a cube in k.*

2. Proof of Theorem. Theorem follows from the following two propositions:

Proposition 1. *Let k be a quadratic field in which 3 does not split. If there is an elliptic curve which has everywhere good reduction over k and admits a 3-isogeny defined over k, and whose discriminant is a cube in k, then k is $\mathbf{Q}(\sqrt{6})$ or $\mathbf{Q}(\sqrt{33})$.*

Proposition 2. *Let p be a prime number such that $p \neq 3$ and $p \equiv 3 \pmod 4$ and let $k = \mathbf{Q}(\sqrt{3p})$. Then every elliptic curve with everywhere good reduction over k whose discriminant is a cube in k admits a 3-isogeny defined over k.*

2.1. Proof of Proposition 1. For a number field k, we denote by h_k, $\mathcal{O}_k$ and $\mathcal{O}_k^\times$ the class number, the ring of integers and the group of units of k, respectively.

Let k be as in Proposition 1. In [2], Proposition 1 is proved under the assumption that $(h_k, 6) = 1$, but without the requirement that 3 does not split in k. The condition $(h_k, 6) = 1$ is used, when 3 does not split, only in solving the equation

$$(1) \qquad X^3 = 1 + 27v, \quad X \in \mathcal{O}_k, \quad v \in \mathcal{O}_k^\times.$$

Hence, to prove Proposition 1, it is enough to prove the following:

Lemma 1. *Let k be a quadratic field. Then equation (1) has a solution only when $k = \mathbf{Q}(\sqrt{6})$ or $\mathbf{Q}(\sqrt{33})$, in which cases, the only solutions are $(X, v) = (4 \pm \sqrt{6}, 5 \pm 2\sqrt{6})$, $(-(5 \pm \sqrt{33}), -(23 \pm 4\sqrt{33}))$, respectively. Note that $5 + 2\sqrt{6}$ (resp. $23 + 4\sqrt{33}$) is the fundamental unit of $\mathbf{Q}(\sqrt{6})$ (resp. $\mathbf{Q}(\sqrt{33})$).*

Proof. Taking the norm of (1), we have

$$\begin{aligned} & x^3 - y^3 + 3xy + 1 \\ &= (x - y + 1)(x^2 + y^2 + 1 + xy + y - x) \\ &= 729 N_{k/\mathbf{Q}}(v), \end{aligned}$$

where $x = N_{k/\mathbf{Q}}(X)$, $y = \mathrm{Tr}_{k/\mathbf{Q}}(X) \in \mathbf{Z}$. Reducing modulo 4, we see that $N_{k/\mathbf{Q}}(v) = 1$, whence we have

$$\begin{aligned} x - y + 1 &= 3^a e, \\ x^2 + y^2 + 1 + xy + y - x &= 3^{6-a} e \end{aligned}$$

for some $a \in \mathbf{Z}$ with $0 \leq a \leq 6$ and $e = \pm 1$. Eliminating x, we have

$$3y^2 + (3^{a+1}e - 3)y + (3^{2a} + 3 - 3^{a+1}e - 3^{6-a}e) = 0.$$

This is possible only when $e = 1$, $a = 1$, and $y = 8$ or -10. Thus $(\mathrm{Tr}_{k/\mathbf{Q}}(X), N_{k/\mathbf{Q}}(X)) = (8, 10)$, that is $X = 4 \pm \sqrt{6}$, or $(\mathrm{Tr}_{k/\mathbf{Q}}(X), N_{k/\mathbf{Q}}(X)) = (-10, -8)$, that is $X = -(5 \pm \sqrt{33})$. □

2.2. Proof of Proposition 2. The following is proved in [2]:

Proposition 3. *Let k be a real quadratic field. Assume that the ray class number of $k(\sqrt{-3})$ modulo $(\sqrt{-3})$ is not a multiple of 4. Then every elliptic curve which has everywhere good reduction over k and whose discriminant is a cube in k admits a 3-isogeny defined over k.*

1991 Mathematics Subject Classification. 11G05.

Thus, to prove Proposition 2, we prove that a real quadratic field as in Proposition 2 satisfies the assumption of Proposition 3. (Corollary 1 below.) Note that, in [2], we checked this assumption using the computer software KASH when $p = 11, 19, 23$ or 31.

Lemma 2. *Let p and q be distinct primes such that $p \equiv q \equiv 3 \pmod 4$ and let $k = \mathbf{Q}(\sqrt{pq})$. Let ε be the fundamental unit of k greater than 1 and let $\mathfrak{q}$ be the prime ideal of k dividing q. Then*

(i) *h_k is odd.*
(ii) *$k(\sqrt{-\varepsilon}) = \mathbf{Q}(\sqrt{-p}, \sqrt{-q})$.*
(iii) *$\varepsilon \equiv (p/q) \pmod{\mathfrak{q}}$, where $(\cdot/\cdot)$ is the Legendre symbol. In particular, $\varepsilon \equiv p \pmod{\mathfrak{q}}$ if $q = 3$.*

Proof. (i) This is well-known (see Theorems 39 and 41 of [1] for example).
(ii) By (i), $\mathfrak{q}$ is principal. Let $\pi \in \mathcal{O}_k$ be a generator of $\mathfrak{q}$. Since $\varepsilon > 1$, k is real and $k \neq \mathbf{Q}(\sqrt{q})$, we have $q = \pi^2\varepsilon^{2n+1}$ for some $n \in \mathbf{Z}$, whence $k(\sqrt{-q}) = k(\sqrt{-\varepsilon})$.
(iii) We first show that $\varepsilon \equiv \pm 1 \pmod{\mathfrak{q}}$, which is equivalent to $\mathrm{Tr}_{k/\mathbf{Q}}(\varepsilon)^2 \equiv 4 \pmod q$ since $N_{k/\mathbf{Q}}(\varepsilon \pm 1) = 2 \pm \mathrm{Tr}_{k/\mathbf{Q}}(\varepsilon)$. But this readily follows on writing ε as $\varepsilon = (\mathrm{Tr}_{k/\mathbf{Q}}(\varepsilon) + b\sqrt{pq})/2$, $b \in \mathbf{Z}$.

Let $K = k(\sqrt{-\varepsilon}) = \mathbf{Q}(\sqrt{-p}, \sqrt{-q})$. By Theorem 23 in [1], $\mathfrak{q}$ splits in K if and only if there exists an $X \in \mathcal{O}_k$ such that $X^2 \equiv -\varepsilon \pmod{\mathfrak{q}}$, which is equivalent to $\varepsilon \equiv -1 \pmod{\mathfrak{q}}$, since $\mathcal{O}_K/\mathfrak{q} \cong \mathbf{Z}/q\mathbf{Z}$ and $q \equiv 3 \pmod 4$. On the other hand, $\mathfrak{q}$ splits in K if and only if q splits in $\mathbf{Q}(\sqrt{-p})$, which is equivalent to $(p/q) = -1$. □

Corollary 1. *Let p be a prime number such that $p \equiv 3 \pmod 4$ and $p \neq 3$. Let $k = \mathbf{Q}(\sqrt{3p})$ and $K = k(\sqrt{-3})$. Then*

(i) *h_K is odd.*
(ii) *The ray class number $h_K(\sqrt{-3})$ of K modulo $(\sqrt{-3})$ is $2h_K$ or h_K according as $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. In particular, $h_K(\sqrt{-3})$ is not a multiple of 4.*

Proof. (i) From [1], Corollary 3 to Theorem 74, it follows that $h_K = h_k h_{\mathbf{Q}(\sqrt{-p})} h_{\mathbf{Q}(\sqrt{-3})} = h_k h_{\mathbf{Q}(\sqrt{-p})}$, which is odd by Lemma 2 (i).
(ii) Let $G := (\mathcal{O}_K/\sqrt{-3}\mathcal{O}_K)^\times$ and $H := \{x + \sqrt{-3}\mathcal{O}_K \mid x \in \mathcal{O}_K^\times\} \subset G$. From the formula for the ray class number (Theorem 1 of Chapter VI in [3]), it follows that $h_K(\sqrt{-3}) = h_K(G : H)$. Thus it is enough to show that

$$(G : H) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 3, \\ 1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Let $\zeta_6 = (1 + \sqrt{-3})/2$ be a primitive sixth root of unity and $\varepsilon > 1$ the fundamental unit of k. Since $K = k(\sqrt{-\varepsilon})$ by Lemma 2 (ii) and $\zeta_6 \in K$, we have $\mathcal{O}_K^\times = \langle \zeta_6 \rangle \times \langle \sqrt{-\varepsilon} \rangle$ (cf. [1], pp. 194, 195), and hence $H = \langle \sqrt{-\varepsilon} + \sqrt{-3}\mathcal{O}_K,\ \zeta_6 + \sqrt{-3}\mathcal{O}_K \rangle$. Let $\mathfrak{q}$ be the prime ideal of k dividing 3.

Assume that $p \equiv 1 \pmod 3$. Then, since $(-p/3) = -1$, $\mathfrak{q}\mathcal{O}_K = \sqrt{-3}O_K$ is a prime ideal of K and hence G is a cyclic group of order 8. Lemma 2 (iii) and the formulas

$$\zeta_6 - 1 = \zeta_6^2, \quad \zeta_6^2 - 1 = \sqrt{-3}\zeta_6 \tag{2}$$

imply that $H = \langle \sqrt{-\varepsilon} + \sqrt{-3}\mathcal{O}_K \rangle \cong \mathbf{Z}/4\mathbf{Z}$. Thus $(G : H) = 2$.

Assume that $p \equiv 2 \pmod 3$. By Lemma 2 (iii), we have $X^2 + \varepsilon \equiv (X - 1)(X + 1) \pmod{\mathfrak{q}}$. Hence by letting $\mathfrak{Q}_1 = (\mathfrak{q}, \sqrt{-\varepsilon} - 1)$, $\mathfrak{Q}_2 = (\mathfrak{q}, \sqrt{-\varepsilon} + 1)$, it follows from [1], Theorem 23 that

$$\begin{aligned} \sqrt{-3}\mathcal{O}_K &= \mathfrak{q}\mathcal{O}_K = \mathfrak{Q}_1\mathfrak{Q}_2, \\ G &\cong (\mathcal{O}_K/\mathfrak{Q}_1)^\times \times (\mathcal{O}_K/\mathfrak{Q}_2)^\times \\ &\cong (\mathbf{Z}/3\mathbf{Z})^\times \times (\mathbf{Z}/3\mathbf{Z})^\times. \end{aligned}$$

The definition of $\mathfrak{Q}_i$ $(i = 1, 2)$ implies that $\sqrt{-\varepsilon} \equiv 1 \pmod{\mathfrak{Q}_1}$ and $\sqrt{-\varepsilon} \equiv -1 \pmod{\mathfrak{Q}_2}$. Further, (2) means that $\zeta_6 \equiv -1 \pmod{\mathfrak{Q}_i}$ $(i = 1,\ 2)$. Thus $H \cong (\mathbf{Z}/3\mathbf{Z})^\times \times (\mathbf{Z}/3\mathbf{Z})^\times$, whence $(G : H) = 1$. □

References

[1] Fröhlich, A., and Taylor, M. J.: Algebraic number theory. Cambridge Stud. Adv. Math., **27**, Cambridge Univ. Press, Cambridge (1991).

[2] Kagawa, T.: Determination of elliptic curves with everywhere good reduction over real quadratic fields $\mathbf{Q}(\sqrt{3p})$. Acta Arith. (to appear).

[3] Lang, S.: Algebraic Number Theory. 2nd ed., Grad. Texts in Math., **110**, Springer, Berlin-Heidelberg-New York (1994).