Elliptic curves with everywhere good reduction over real quadratic fields

KAGAWA Takaaki

March, 1998

A dissertation submitted for the degree of
Doctor of Science at Waseda University

Acknowledgments

I would like to express my gratitude to Professor Norio Adachi who guided me to the theory of algebraic numbers and unceasingly encouraged me. His advice during the preparation of this thesis was very helpful.

I would also like to express my thanks to Professor Ki-ichiro Hashimoto for introducing me to the subject of this thesis and for his invaluable advice and comments.

I also wish to thank Kazumaro Aoki for his information about various computer packages for number theory, which were indispensable for this work. I also thank Yuji Hasegawa, Manabu Ozaki and Atsuki Umegaki for several useful discussions.

Finally, I am grateful to my parents Toshihiko and Yasuko, and my elder brother Hirotoshi. Without their patience and understanding, this thesis could never have been finished.

KAGAWA Takaaki
School of Science and Engineering
Waseda University
Tokyo 169–8555, Japan

Contents

Introduction

Let k be a number field. It is a fascinating problem to determine the elliptic curves with everywhere good reduction over k. It is well-known that there are no such curves over the field of rational numbers. When k is an imaginary quadratic field, Stroeker [41] showed that such a curve does not admit a global minimal model, and also that there is no such curve over k provided that the class number of k is prime to 6. Hence the problem is solved as far as we are concerned in this case.

It is natural that we next turn to the case where k is a real quadratic field. Another reason we are interested in this case is related to Shimura's elliptic curves obtained in the following way. Let N be a positive fundamental discriminant and let χ_N be the associated Dirichlet character. When the space $S_N = S_2(\Gamma_0(N), \chi_N)$ of cuspforms of Neben-type of weight two has a 2-dimensional $\mathbb{Q}$-simple factor, Shimura [36] constructed a certain abelian surface A defined over $\mathbb{Q}$. Over the real quadratic field $k = \mathbb{Q}(\sqrt{N})$, A splits as $B \times B'$, where B is an elliptic curve defined over k and B' is the conjugate of B. We call B Shimura's elliptic curve over k. It is known that B is isogenous to B' over k ([36]), and that B has everywhere good reduction over k (cf. [3], [12], [18]). Conversely, an elliptic curve E over a real quadratic field k with the properties stated above is conjectured to be isogenous over k to Shimura's elliptic curve (cf. Pinch [27]).

Hence the case of a real quadratic field is especially interesting. In this case, the following are known:

- Several examples are known ([8], [17], [35], [37], etc.).
- There is a method of constructing $\mathbb{Q}$-curves with everywhere good reduction over real quadratic fields ([44]). Recall that a $\mathbb{Q}$-*curve* is an elliptic curve defined over $\overline{\mathbb{Q}}$ which is isogenous over $\overline{\mathbb{Q}}$ to any of its Galois conjugates.
- There are no elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{5})$ or $\mathbb{Q}(\sqrt{13})$ ([17], [27]).

- A defining equation of Shimura's elliptic curve is obtained for many fields ([10], [37]. See also [26]).

- Determination of such curves has been made under certain conditions ([8], [19]).

However, there has been known no result determining all elliptic curves with everywhere good reduction over a real quadratic field.

In this thesis, we shall determine all elliptic curves with everywhere good reduction over many real quadratic fields. More precisely, we prove

Theorem. (1) *There are no elliptic curves with everywhere good reduction over* $\mathbb{Q}(\sqrt{m})$ *if* $m = 2$, 3, 5, 10, 13, 15, 17, 21, 30, 34, 39, 42, 47, 53, 58, 66, 69, 70, 73, 74, 85, 89, 94 *or* 97.

(2) *The elliptic curves with everywhere good reduction over* $k = \mathbb{Q}(\sqrt{m})$ *are determined for* $m = 6, 7, 14, 29, 33, 37, 41$ *and* 65. *All such curves are tabulated in Appendix B. The number of* k*-isogeny classes is* 2 *if* $m = 65$, 1 *otherwise.*

Kida [20] independently gives the same result for $m = 2, 3, 6, 7, 14, 47, 94$.

Here we should mention the relation of this theorem to the above mentioned conjecture.

Let $d(m)$ be the discriminant of a quadratic field $\mathbb{Q}(\sqrt{m})$. Then the structure of the space $S_{d(m)}$ is known. For the values of m in Theorem (1), $S_{d(m)}$ has no 2-dimensional $\mathbb{Q}$-simple factor. For $m = 6, 7, 29, 33, 37$ and 41, $S_{d(m)}$ is 2-dimensional and $\mathbb{Q}$-simple; $S_{d(14)}$ is a direct product of a 2-dimensional $\mathbb{Q}$-simple subspace and a 4-dimensional $\mathbb{Q}$-simple subspace; $S_{d(65)}$ 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. For prime m, see also [36].) Hence for these 32 values of m in the theorem, the conjecture is true. In particular, our curves are all modular. It is worth remarking that, for $m = 29, 37, 41$ and 65, the curves have no complex multiplication. (For $m = 6, 7, 14$ and 33, the curves over $\mathbb{Q}(\sqrt{m})$ have complex multiplication.) For related topics concerning the modularity of elliptic curves over number fields, see [14].

This thesis is organized as follows. In Chapter 1, we investigate elliptic curves admitting a 3-isogeny defined over k and obtain a characterization of 6A1, 6A1′, 33A1 and 33A1′ (Proposition 1.7), and of 29A1, 29A1′, 29A2 and 29A2′ (Proposition 1.10). In Chapter 2, we give criteria for every elliptic curve with everywhere good reduction over a real quadratic field k to have a k-rational point of order 2 (Corollary 2.3), to admit a 3-isogeny defined over k (Propositions 2.6 and 2.8), or to have cubic discriminant (Proposition 2.12). To

obtain these criteria, the ramification properties of the field of n-division points ($n = 2, 3$) are important. In Chapter 3, we show the nonexistence of elliptic curves with everywhere good reduction for 24 real quadratic fields, or determine such curves over 8 real quadratic fields. In the determination, the results obtained in Chapters 1 and 2 are used to reduce the amount of computation. In Chapter 4, we solve some diophantine equations which are used to determine the elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{37})$, but are not solved in Chapter 3. In Appendix A, we give an algebraic proof of Proposition 3.5, which is crucial for the determination for the curves over $\mathbb{Q}(\sqrt{29})$ and whose proof given in Chapter 3 are heavily relies on computer calculation. In Appendix B, we present tables of the elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{m})$ ($m = 6, 7, 14, 29, 33, 37, 41, 65$).

Now we introduce some notation used throughout this thesis. For an algebraic number field k, we denote by $\mathcal{O}_k$, $\mathcal{O}_k^\times$ and h_k its ring of integers, its group of units and its class number, respectively. If $\mathfrak{m}$ is a divisor of k (that is, a formal product of a fractional ideal of k and some infinite primes of k), $h_k(\mathfrak{m})$ denotes the ray class number modulo $\mathfrak{m}$; write $h_k^{(2)}$ instead if $\mathfrak{m} = \prod_{\mathfrak{p}|2} \mathfrak{p}$. If k is a real quadratic field, then ε is the fundamental unit greater than 1, and, for $x \in k$, we denote its conjugate by x'. If $k = \mathbb{Q}(\sqrt{m})$ with $m \equiv 1 \pmod 4$, then let $\omega = (1 + \sqrt{m})/2$.

For an elliptic curve E given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

we define the associated quantities $b_2, b_4, b_6, b_8, c_4, c_6, \Delta$ and j as usual. To specify the curve, we denote $b_2(E), \ldots, j(E)$ instead. (Note that these quantities except $j(E)$ depends on the choice of a model. Thus the meaning of $b_2(E)$ and so on are the corresponding quantities of a model of E.) Let $E[n]$ be the kernel of multiplication by n. When E is defined over a field k, let $E(k)$ be the group of k-rational points of E, $E(k)_{\mathrm{tors}}$ the torsion subgroup of $E(k)$, and let $E(k)[n] = E(k) \cap E[n]$. Also let $k(E[n])$ the extension of k generated by the coordinates of all points in $E[n]$. When k is an algebraic number field and $\mathfrak{p}$ is a prime ideal of k, let $E_\mathfrak{p}$ be the reduction of E modulo $\mathfrak{p}$.

Chapter 1

Curves with 3-isogeny

Let k be a real quadratic field. In this chapter, we investigate elliptic curves having everywhere good reduction over k and admitting a 3-isogeny defined over k. Throughout this chapter, we assume that h_k is prime to 6. This assumption will make our arguments simple in several situations. For example,

Lemma 1.1 (Setzer [34])**.** *Let k be a number field whose class number is prime to 6. Then every elliptic curve with everywhere good reduction over k admits a global minimal model.*

Let E_1 and E_2 be elliptic curves defined over k which are 3-isogenous over k. We define a rational function $J(x)$ by

$$J(x) = \frac{(x+27)(x+3)^3}{x}.$$

Then, by Pinch [28], the j-invariants of E_1 and E_2 can be written as

$$j(E_1) = J(t_1),\ j(E_2) = J(t_2),\ t_1, t_2 \in k,\ t_1 t_2 = 3^6.$$

(This is nothing but a parametrization of the modular curve $Y_0(3)$.) Suppose further that E_1 and E_2 have everywhere good reduction over k. Then $j(E_1)$ and $j(E_2) \in \mathcal{O}_k$ and hence t_1 and $t_2 \in \mathcal{O}_k$. We also have

Lemma 1.2 (Setzer [35])**.** *Let E be an elliptic curve with everywhere good reduction over a quadratic field. Then $j(E) \neq 0, 1728$.*

From the relations

$$j(E_1) = \frac{c_4(E_1)^3}{\Delta(E_1)} = \frac{(t_1+27)(t_1+3)^3}{t_1}, \tag{1.1}$$

$$j(E_1) - 1728 = \frac{c_6(E_1)^2}{\Delta(E_1)} = \frac{(t_1^2+18t_1-27)^2}{t_1}, \tag{1.2}$$

the principal ideals $((t_i+27)/t_i)$ and (t_i) $(i=1,2)$ are a cube and a square, respectively, since the principal ideal $(\Delta(E_i))$ is a 12-th power. From these we easily see that, for $i=1,2$,

$$(t_i)=\begin{cases}(1),\ (729) & \text{if 3 is inert,}\\ (1),\ (27),\ (729) & \text{if 3 ramifies,}\\ (1),\ \mathfrak{p}^6,\ \mathfrak{p}'^6,\ (729) & \text{if } (3)=\mathfrak{p}\mathfrak{p}',\ \mathfrak{p} \text{ and } \mathfrak{p}' \text{ are distinct prime ideals of } k.\end{cases}$$

Since $j(E_1)\neq 0$ by Lemma 1.2, we see from (1.1) that

$$\left(\frac{c_4(E_1)}{t_1+3}\right)^3=\Delta(E_1)\left(1+\frac{27}{t_1}\right)\ (\neq 0).$$

If $(t_1)=(1)$, then

$$\left(\frac{c_4(E_1)}{t_1+3}\right)^3=\Delta(E_1)(1+27u),\qquad u=\frac{1}{t_1}\in\mathcal{O}_k^\times.$$

If $(t_1)=(729)$, then

$$\left(\frac{3c_4(E_1)}{t_1+3}\right)^3=\Delta(E_1)(u+27),\qquad u=\frac{729}{t_1}\in\mathcal{O}_k^\times.$$

If 3 ramifies in k and $(t_1)=(27)$, then

$$\left(\frac{c_4(E_1)}{t_1+3}\right)^3=\Delta(E_1)(1+u),\qquad u=\frac{27}{t_1}\in\mathcal{O}_k^\times.$$

Suppose that 3 splits and $(t_1)=\mathfrak{p}^6$, where $\mathfrak{p}$ is a prime ideal dividing 3. Since $(h_k,6)=1$, $\mathfrak{p}$ is principal, say $\mathfrak{p}=(\pi)$, $\pi\in\mathcal{O}_k$. Hence

$$\left(\frac{\pi c_4(E_1)}{t_1+3}\right)^3=\Delta(E_1)(\pi^3\pm\pi'^3u),\quad u=\frac{\pi^6}{t_1}\in\mathcal{O}_k^\times.$$

Hence to investigate curves with 3-isogeny, we need to study the equations

$$X^3=u+27v,\quad X^3=u+v,\quad X^3=\pi^3u+\pi'^3v,$$

where $X\in\mathcal{O}_k$, $u,v\in\mathcal{O}_k^\times$, $3=\pm\pi\pi'$. Though to solve these equations is difficult in general, we can solve them under certain condition, for example either u or v is a cube in k. We first treat the case.

Lemma 1.3. *Let k be a quadratic field having class number prime to 6. The equation*

$$X^3=1+27u,\quad X\in\mathcal{O}_k,\quad u\in\mathcal{O}_k^\times \tag{1.3}$$

has no solutions unless $k = \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{33})$*, when the only solutions are*

$$(X, u) = (4 \pm \sqrt{6}, 5 \pm 2\sqrt{6}),\ (-(5 \pm \sqrt{33}), -(23 \pm 4\sqrt{33})),$$

respectively. Note that $5 + 2\sqrt{6}$ *(resp.* $23 + 4\sqrt{33}$*) is a fundamental unit of* $\mathbb{Q}(\sqrt{6})$ *(resp.* $\mathbb{Q}(\sqrt{33})$*).*

Proof. First we consider the case where 3 is ramified. Since h_k is odd, we have $(3) = (\pi^2)$, $\pi \in \mathcal{O}_k$. Writing (1.3) as

$$27u = (X - 1)(X^2 + X + 1),$$

we have

$$X - 1 = \pi^a v, \quad X^2 + X + 1 = \pi^{6-a} w, \quad v, w \in \mathcal{O}_k^\times, \quad a \in \mathbb{Z}, \quad 0 \leq a \leq 6,$$

whence

$$\pi^{2a} v^2 + 3\pi^a v + 3 = \pi^{6-a} w. \tag{1.4}$$

The cases $a = 0, 2, 3, 5, 6$ immediately lead to contradictions. If $a = 1$, then

$$\Pi^2 + 3\Pi + 3 = \pi^5 w,$$

where $\Pi = \pi v$. Taking the norms of both sides, we have

$$\mathrm{Tr}_{k/\mathbb{Q}}(\Pi)^2 + (N_{k/\mathbb{Q}}(\Pi) + 3)\,\mathrm{Tr}_{k/\mathbb{Q}}(\Pi) + (N_{k/\mathbb{Q}}(\Pi) + 6) = \pm 3^4.$$

If $N_{k/\mathbb{Q}}(\Pi) = -3$, then $\mathrm{Tr}_{k/\mathbb{Q}}(\Pi)$ cannot be rational. If $N_{k/\mathbb{Q}}(\Pi) = 3$, then $\mathrm{Tr}_{k/\mathbb{Q}}(\Pi) = -12$ or 6. The former corresponds to $\Pi = -6 \pm \sqrt{33}$, $X = -5 \pm \sqrt{33}$, the latter to $\Pi = 3 \pm \sqrt{6}$, $X = 4 \pm \sqrt{6}$.

If $a = 4$, then we similarly obtain

$$\mathrm{Tr}_{k/\mathbb{Q}}(\Pi)^2 + (N_{k/\mathbb{Q}}(\Pi) + 3)\,\mathrm{Tr}_{k/\mathbb{Q}}(\Pi) + (N_{k/\mathbb{Q}}(\Pi) + 3 + 3^7) = \pm 3,$$

where $\Pi = \pi^4 v$. For all possibilities, $\mathrm{Tr}_{k/\mathbb{Q}}(\Pi)$ cannot be rational.

In the case where 3 is inert, a similar argument works and we can show that there are no solutions in this case.

Finally, we consider the case $3 = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}$ and $\mathfrak{p}'$ are distinct prime ideals of k. Then, for some $a, a' \in \mathbb{Z}$, $0 \leq a, a' \leq 3$, $(X - 1) = \mathfrak{p}^a \mathfrak{p}'^{a'}$, $(X^2 + X + 1) = \mathfrak{p}^{3-a} \mathfrak{p}'^{3-a'}$. If $a = a'$, then $(X - 1) = (3)^a$, $(X^2 + X + 1) = (3)^{3-a}$. Hence a similar argument works also in this case. If $a \neq a'$, then, using $(h_k, 6) = 1$, we can deduce that $\mathfrak{p}$, $\mathfrak{p}'$ are principal. For example, if $a = 1$, $a' = 3$ (the remaining cases are similar), then $(X - 1) = \mathfrak{p}\mathfrak{p}'^3 = (3)\mathfrak{p}'^2$.

Hence $\mathfrak{p}'^2$ is principal. Since $(h_k, 6) = 1$, we see that $\mathfrak{p}' = (\pi')$, $\mathfrak{p} = (\pi)$ for some $\pi \in \mathcal{O}_k$. Hence $(X-1) = (3\pi'^2), (X^2+X+1) = (\pi^2)$, and we can treat this case analogously and conclude that there are no solutions in the case where 3 splits. □

The following three lemmas can be proved similarly.

Lemma 1.4. *Let k be a quadratic field. Then the equation*

$$X^3 = 1 + u, \quad X \in \mathcal{O}_k, \quad u \in \mathcal{O}_k^\times$$

has only the solution $X = 0, u = -1$.

Lemma 1.5. *Let k be a real quadratic field in which 3 splits as $3 = \pm\pi\pi'$, $\pi, \pi' \in \mathcal{O}_k$, $(\pi) \neq (\pi')$. Then the equation*

$$X^3 = \pi^3 + \pi'^3 u, \quad X \in \mathcal{O}_k, \quad u \in \mathcal{O}_k^\times$$

has no solutions.

Lemma 1.6. *Let k be a quadratic field. Then the equation*

$$X^3 = u + 27, \quad X \in \mathcal{O}_k, \quad u \in \mathcal{O}_k^\times$$

has no solutions.

Using these lemmas, we can prove the following characterization of 6A1, 6A1′, 33A1 and 33A1′:

Proposition 1.7. *Let k be a real quadratic field having class number prime to 6. Then* 6A1, 6A1′, 33A1 *and* 33A1′ *are the only elliptic curves having everywhere good reduction over k, having cubic discriminant, and admitting a 3-isogeny defined over k.*

Proof. Let E_1 be an elliptic curve satisfying the above properties and let E_2 be a 3-isogenous curve. Then $j(E_1) = J(t_1)$, $j(E_2) = J(t_2)$, $t_1, t_2 \in \mathcal{O}_k$, $t_1 t_2 = 3^6$. By Lemma 1.1, we can take $\Delta(E) = v^3$, $v \in \mathcal{O}_k^\times$. The argument given above shows that there exist $X \in \mathcal{O}_k \backslash \{0\}$ and $u \in \mathcal{O}_k^\times$ such that

$$X^3 = 1 + 27u \qquad \text{if } (t_1) = (1), \text{ or} \tag{1.5}$$

$$X^3 = u + 27 \qquad \text{if } (t_1) = (729), \text{ or} \tag{1.6}$$

$$X^3 = 1 + u \qquad \text{if 3 is ramified and } (t_1) = (27), \text{ or} \tag{1.7}$$

$$X^3 = \pi^3 + \pi'^3 u \quad \text{if } 3 = \pm\pi\pi' \text{ and } (t_1) \text{ is } (\pi^6) \text{ or } (\pi'^6). \tag{1.8}$$

Note that in equation (1.5), $X = c_4(E_1)/(t_1+3)v$, $u = 1/t_1$. By Lemmas 1.4, 1.5 and 1.6, no equations (1.6), (1.7) and (1.8) have solutions. From Lemma 1.3, only the units satisfying equation (1.5) are $u = 5 \pm 2\sqrt{6}$ and $-(23 \pm 4\sqrt{33})$. If $u = 5 \pm 2\sqrt{6}$, that is $t_1 = 5 \mp 2\sqrt{6}$, then $j(E_1) = J(t_1) = 8000$. If $u = -(23 \pm 4\sqrt{33})$, that is $t_1 = -(23 \mp 4\sqrt{33})$, then $j(E_1) = -32768$. We have two curves over $\mathbb{Q}(\sqrt{6})$ (resp. $\mathbb{Q}(\sqrt{33})$) having $j = 8000$ (resp. $j = -32768$), namely 6A1, 6A1′ (resp. 33A1, 33A1′). Since exactly two prime numbers ramify in $\mathbb{Q}(\sqrt{6})$ or $\mathbb{Q}(\sqrt{33})$, they are all such curves by Theorem 2 of [35]. □

In the rest of this chapter, the symbol □ stands for a square in a real quadratic field. To obtain a characterization of curves over $\mathbb{Q}(\sqrt{29})$, we solve $X^3 = u + 27v$ when $uv = \pm\square$

Lemma 1.8. (1) *The equation* $27Y^2 = X^3 - 676$ $(X, Y \in \mathbb{Z})$ *has no solutions.*
(2) *The equation* $27Y^2 = X^3 + 784$ $(X, Y \in \mathbb{Z})$ *has no solutions.*
(3) *The only* $X, Y \in \mathbb{Z}$ *satisfying* $27Y^2 = X^3 + 676$ *are* $(X, Y) = (-1, \pm 5), (26, \pm 26)$.
(4) *The only* $X, Y \in \mathbb{Z}$ *satisfying* $27Y^2 = X^3 - 784$ *are* $(X, Y) = (19, \pm 15), (28, \pm 28)$.

Proof. Let A be one of $\pm 676, \pm 784$. If $X, Y \in \mathbb{Z}$ satisfy $27Y^2 = X^3 + A$, then $(3X, 27Y)$ is an integral point of the elliptic curve

$$E_A : y^2 = x^3 + 27A.$$

If $A = 784$ or -676, then $E_A(\mathbb{Q}) = \{O\}$ is shown by 2-descent. (Cremona's program `mrank` took only a few second to compute $E_A(\mathbb{Q})$ on Sparc station SS4, CPU110MHZ.) The only integral points (x, y) on E_{676} are

$$(78, \pm 702), (13, \pm 143), (-3, \pm 135), (-26, \pm 26), (22, \pm 170), (1573, \pm 62387),$$

among which $(78, \pm 702) = (3 \cdot 26, \pm 27 \cdot 26)$ and $(-3, \pm 135) = (3 \cdot (-1), \pm 27 \cdot 5)$ satisfy $3 \mid x$, $27 \mid y$. The only integral points (x, y) on E_{-784} are

$$(84, \pm 756), (28, \pm 28), (57, \pm 405), (1708, \pm 70588),$$

among which $(84, \pm 756) = (3 \cdot 28, \pm 27 \cdot 27)$ and $(57, \pm 405) = (3 \cdot 19, \pm 27 \cdot 15)$ satisfy $3 \mid x$, $27 \mid y$. The computations of the integral points of E_{676} and E_{-784} are done using KASH version 1.8 and took about 28 seconds and 18 seconds, respectively. □

Remark. Using Cremona's program `mwrank`, we see that $E_{-784}(\mathbb{Q}) = \langle (84, 756) \rangle \cong \mathbb{Z}$ and $E_{676}(\mathbb{Q}) = \langle (78, 702) \rangle \oplus \langle (-26, 26) \rangle \cong \mathbb{Z} \oplus \mathbb{Z}$.

Lemma 1.9. *Let k be a real quadratic field. If there exists $u, v \in \mathcal{O}_k^\times$, $X \in \mathcal{O}_k$ such that $X^3 = u + 27v$, $uv = \pm\square$, then $k = \mathbb{Q}(\sqrt{29})$ and $(u, v, X) = (\pm\varepsilon^{3n+1}, \mp\varepsilon^{3n-1}, \mp\varepsilon^{n-1})$, $(\pm\varepsilon^{3n-1}, \mp\varepsilon^{3n+1}, \mp\varepsilon^{n+1})$ $(n \in \mathbb{Z})$. Here $\varepsilon = (5 + \sqrt{29})/2$ is a fundamental unit of k.*

Proof. Let $X \in \mathcal{O}_k$, $u, v \in \mathcal{O}_k^\times$ such that $X^3 = u + 27v$, $uv = \pm\square$. We may suppose that $N_{k/\mathbb{Q}}(u) = N_{k/\mathbb{Q}}(v) = 1$ by changing, if necessary, u, v, X to $\varepsilon^3 u$, $\varepsilon^3 v$, εX, respectively. Taking the norms of both sides, we have

$$N_{k/\mathbb{Q}}(X)^3 = 730 + 27\,\mathrm{Tr}_{k/\mathbb{Q}}(uv').$$

Since $uv = \pm\square$, we have $uv' = uv/v^2 = \pm w^2$ for some $w \in \mathcal{O}_k^\times$. Hence $N_{k/\mathbb{Q}}(X)^3 = 730 \pm 27\,\mathrm{Tr}_{k/\mathbb{Q}}(w^2) = 730 \pm 27(\mathrm{Tr}_{k/\mathbb{Q}}(w)^2 - 2N_{k/\mathbb{Q}}(w))$. If the sign is $+$, then

$$\begin{aligned} 27\,\mathrm{Tr}_{k/\mathbb{Q}}(w)^2 &= N_{k/\mathbb{Q}}(X)^3 - 730 + 54N_{k/\mathbb{Q}}(w) \\ &= \begin{cases} N_{k/\mathbb{Q}}(X)^3 - 676 & \text{if } N_{k/\mathbb{Q}}(w) = 1, \\ N_{k/\mathbb{Q}}(X)^3 - 784 & \text{if } N_{k/\mathbb{Q}}(w) = -1. \end{cases} \end{aligned}$$

It follows from Lemma 1.8 that $N_{k/\mathbb{Q}}(w) = -1$ and $\mathrm{Tr}_{k/\mathbb{Q}}(w) = \pm 15$ or ± 28, that is, $w = \pm(15 \pm \sqrt{229})/2$ or $\pm(14 \pm \sqrt{197})$. If $w = \pm(15 \pm \sqrt{229})/2$, then $(u + 27v) = \mathfrak{p}^3$, where $\mathfrak{p}$ is a prime ideal of $\mathbb{Q}(\sqrt{229})$ dividing 19. Since the class number of $\mathbb{Q}(\sqrt{229})$ is 3 and $\mathfrak{p}$ is not principal, we see that $u + 27v$ is not a cube in $\mathbb{Q}(\sqrt{229})$. If $w = \pm(14 \pm \sqrt{197})$, then $u + 27v = v \cdot 2^3 \cdot 7(15 \pm \sqrt{197})/2$. Since $7 = \pi\pi'$, $\pi = (15 + \sqrt{197})/2$, we see that $\pi^2 \,||\, (u + 27v)$ or $\pi'^2 \,||\, (u + 27v)$, and hence $u + 27v$ is not a cube in $\mathbb{Q}(\sqrt{197})$.

If the sign is $-$, then

$$\begin{aligned} 27\,\mathrm{Tr}_{k/\mathbb{Q}}(w)^2 &= (-N_{k/\mathbb{Q}}(X))^3 + 730 + 54N_{k/\mathbb{Q}}(w) \\ &= \begin{cases} (-N_{k/\mathbb{Q}}(X))^3 + 784 & \text{if } N_{k/\mathbb{Q}}(w) = 1, \\ (-N_{k/\mathbb{Q}}(X))^3 + 676 & \text{if } N_{k/\mathbb{Q}}(w) = -1. \end{cases} \end{aligned}$$

By Lemma 1.8, $N_{k/\mathbb{Q}}(w) = -1$ and $\mathrm{Tr}_{k/\mathbb{Q}}(w) = \pm 5$ or ± 26, that is, $w = \pm(13 \pm \sqrt{170})$ or $\pm(5 \pm \sqrt{29})/2$. If $w = \pm(13 \pm \sqrt{170})$, then $(u + 27v) = (26(12 \pm \sqrt{170})) = \mathfrak{p}_2^3\mathfrak{p}_{13}^2\mathfrak{p}'_{13}$, where $(2) = \mathfrak{p}_2^3$, $(13) = \mathfrak{p}_{13}\mathfrak{p}'_{13}$. Thus $u + 27v$ is not a cube in $\mathbb{Q}(\sqrt{170})$. If $w = \pm(5 \pm \sqrt{29})/2$, then $u + 27v = v\varepsilon^{\pm 2}$ $(\varepsilon = (5 + \sqrt{29})/2)$. Thus, if $X^3 = u + 27v$, then we must have $v = \pm\varepsilon^{3n-1}$, $X = \pm\varepsilon^{n-1}$, or $v = \pm\varepsilon^{3n+1}$, $X = \pm\varepsilon^{n+1}$ for some $n \in \mathbb{Z}$. □

Remark. In his paper [26], Nakamura proves that the only $m \in \mathbb{Z}$ and $x \in \mathcal{O}_k$ satisfying $x^3 = \varepsilon^{4+12m} - 27\varepsilon^2$ are $m = 0$ and $x = -1$. This result readily follows from Lemma 1.9.

Using Lemma 1.9, we can prove the following.

Proposition 1.10. *Let k be a real quadratic field. If there exists an elliptic curve E with everywhere good reduction over k given by a global minimal model with $j(E) = J(t)$ ($t \in \mathcal{O}_k$, $(t) = (1)$ or (729)) and $\Delta(E) = \pm\square$, then $k = \mathbb{Q}(\sqrt{29})$ and E is isomorphic over k to* 29A1, 29A1′, 29A2 *or* 29A2′.

Proof. Suppose that there exists such a curve E. Let

$$X = \begin{cases} c_4(E)/(t+3) & \text{if } (t) = (1), \\ 3c_4(E)/(t+3) & \text{if } (t) = (729), \end{cases}$$

$$u = \begin{cases} \Delta(E) & \text{if } (t) = (1), \\ 729\Delta(E)/t & \text{if } (t) = (729), \end{cases} \qquad v = \begin{cases} \Delta(E)/t & \text{if } (t) = (1), \\ \Delta(E) & \text{if } (t) = (729). \end{cases}$$

Since $t_1/\Delta(E_1)$ is a square from (1.2),

$$X^3 = u + 27v,\ X \in \mathcal{O}_k,\ u, v \in \mathcal{O}_k^\times,\ uv = \pm\square.$$

Hence, by Lemma 1.9, $k = \mathbb{Q}(\sqrt{29})$, $u/v = -\varepsilon^{\pm 2}$, where $\varepsilon = (5+\sqrt{29})/2$ is the fundamental unit of $\mathbb{Q}(\sqrt{29})$ greater than 1. If $(t) = (1)$, then $t = u/v = -\varepsilon^2, -\varepsilon'^2$, and $j(E)$ is equal to $J(-\varepsilon^2) = (5\varepsilon - 2)^3/\varepsilon^4$ or $J(-\varepsilon'^2) = (5\varepsilon' - 2)^3\varepsilon^4$. If $(t) = (729)$, then $t = 729v/u = -729\varepsilon^2$, $-729\varepsilon'^2$, and $j(E)$ is equal to $J(-729\varepsilon^2) = -(1 + 216\varepsilon'^2)^3\varepsilon^{14}$ or $J(-729\varepsilon'^2) = -(1 + 216\varepsilon^2)^3\varepsilon'^{14}$. The values of j-invariant obtained above are those of 29A1, 29A1′, 29A2 and 29A2′. Hence a result of Ishii (see [37], Lemma 1.5) implies our assertion. □

Chapter 2

Some criteria

In this chapter, we give criteria for every elliptic curve with everywhere good reduction over a real quadratic field k to have a k-rational point of order 2 (Corollary 2.3), to admit a 3-isogeny defined over k (Propositions 2.6 and 2.8), or to have a cubic discriminant (Proposition 2.12). To obtain these criteria, the study of ramification properties of the field of n-division points ($n = 2, 3$) is important.

2.1 Fields of 2-division points

We recall the following well-known fact (see [38], p. 184):

Lemma 2.1 (Criterion of Néron-Ogg-Shafarevich)**.** *For a natural number n and an elliptic curve E defined over a number field k, the primes that can ramify in $k(E[n])/k$ are primes of bad reduction, prime divisors of n and infinite primes.* □

Let E be an elliptic curve defined over a number field k. It is easy to see that $k(E[2])$ is the splitting field of $f(x) = 4x^3+b_2(E)x^2+2b_4(E)x+b_6(E)$, and $k(\sqrt{\mathrm{disc}(f)}) = k(\sqrt{\Delta(E)})$. Hence, together with Lemma 2.1, we obtain:

Proposition 2.2. *Let E be an elliptic curve defined over a number field k. If E has good reduction outside 2 and has no k-rational point of order 2, then $k(E[2])/k(\sqrt{\Delta(E)})$ is a cyclic cubic extension unramified outside 2. In particular, $h^{(2)}_{k(\sqrt{\Delta(E)})}$ is a multiple of 3.* □

Using this, we can prove a criterion for every elliptic curve defined over a real quadratic field k to be admissible. Recall that an elliptic curve defined over a number field k is called *admissible* if it satisfies the conditions below:

(1) it has everywhere good reduction over k;

(2) it has a k-rational point of order 2;

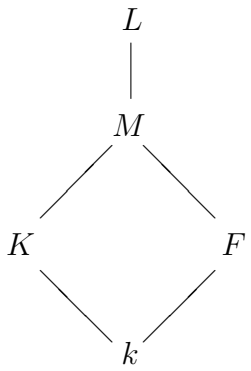
Let k be a real quadratic field and E an elliptic curve with everywhere good reduction over k. Then the principal ideal $(\Delta(E))$ is a 12-th power, say $(\Delta(E)) = \mathfrak{a}^{12}$. Assume first that the class number of k is prime to 6. Then $\mathfrak{a} = (\alpha)$ for some $\alpha \in k^\times$, and thus $k(\sqrt{\Delta(E)})$ is one of the field k, $k(\sqrt{-1})$ or $k(\sqrt{\pm\varepsilon})$ (see also Lemma 1.1). Assume next that $h_k = 2$. Then $(\Delta(E)) = (\mathfrak{a}^2)^6 = (\alpha)^6$ for some $\alpha \in k^\times$. Hence in this case, we also see that $k(\sqrt{\Delta(E)})$ is one of the fields k, $k(\sqrt{-1})$ or $k(\sqrt{\pm\varepsilon})$.

Combining the above argument with Proposition 2.2, the following immediately follows:

Corollary 2.3. *If the class number of k is prime to 6 or is equal to 2, $h_k^{(2)}$, $h_{k(\sqrt{-1})}^{(2)}$ and $h_{k(\sqrt{\pm\varepsilon})}^{(2)}$ are all prime to 3, then each elliptic curve with everywhere good reduction over k is admissible.* □

2.2 Fields of 3-division points, I

Let $L = k(E[3])$, $F = k(\sqrt{-3})$, $K = k(\sqrt[3]{\Delta(E)})$, $M = FK = k(\sqrt[3]{\Delta(E)}, \sqrt{-3})$, $G = \mathrm{Gal}(L/k)$. It is known that L contains F and K ([33], p. 305, [38], p. 98).



By a faithful representation on $E[3]$, we regard G as a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ whose order is $48 = 2^4 \cdot 3$. We know when G is a 2-group:

Lemma 2.4. *G is a 2-group (that is, $[k(E[3]) : k]$ is not divisible by 3) if and only if $\Delta(E)$ is not a cube in k.*

Proof. See [33], § 5.3. □

Let

$$\sigma = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \tau = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \quad g = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Then $\langle\sigma,\tau\rangle$, $g\langle\sigma,\tau\rangle g^{-1}$ and $g^{-1}\langle\sigma,\tau\rangle g$ are the 2-Sylow subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$. They are isomorphic to SD_{16}, the semi-dihedral group of order 16:

$$SD_{16} = \langle\sigma,\tau \mid \sigma^2 = 1,\ \tau^8 = 1,\ \sigma\tau\sigma = \tau^3\rangle. \tag{2.1}$$

Lemma 2.5. *Let k be a real quadratic field and $\mathfrak{p}_\infty^{(1)}$, $\mathfrak{p}_\infty^{(2)}$ the real primes of k. Assume that the ray class number of k modulo $(3)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}$ is not divisible by 4. If E is an elliptic curve having everywhere good reduction over k and admitting no 3-isogeny defined over k, then the 3-division polynomial of E is irreducible over k.*

Proof. Let x_i $(i = 1, 2, 3, 4)$ be the x-coordinate of the point of order 3, that is, the roots of the 3-division polynomial $\psi_3(x) = 3x^4 + b_2(E)x^3 + 3b_4(E)x^2 + 3b_6(E)x + b_8(E) \in k[x]$. By assumption, $\psi_3(x)$ has no roots in k. Suppose that $\psi_3(x)$ is a product of two irreducible quadratic polynomials. Then $k(x_1, x_2, x_3, x_4)$ is an abelian extension of k of degree 2 or 4 unramified outside $\{3, \mathfrak{p}_\infty^{(1)}, \mathfrak{p}_\infty^{(2)}\}$. Thus, by assumption, it follows that $k(x_1, x_2, x_3, x_4) = k(\sqrt{-3})$. Since the maximal real subfield of $k(\sqrt{-3})$ is k, none of x_1, x_2, x_3, x_4 are real, This contradicts $E(\mathbb{R})[3]$ is a cyclic group of order 3 ([39], Chapter V, Corollary 2.3.1, or [40], Chapter II). □

Proposition 2.6. *Let k be as in Lemma 2.5 and let E be an elliptic curve with everywhere good reduction over k. If $\Delta(E)$ is a cube in k, then E admits a 3-isogeny defined over k.*

Proof. Suppose that E admits no 3-isogeny defined over k. Then, by Lemmas 2.4 and 2.5, the order of G is 4, 8 or 16. In any case, G has a normal subgroup of N such that G/N is of order 4, in other words, the ray class number of k modulo $(3)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}$ is divisible by 4 in all cases. In fact, if $\#G = 4$ or 8, it is clear. If $\#G = 16$, then $G = \langle\sigma,\tau\rangle$ is a 2-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$, where σ, τ are as in (2.1). The group $\langle\tau^2\rangle$ is a normal subgroup of G and $G/\langle\tau^2\rangle$ is isomorphic to the Klein 4-group. This contradicts our assumption. □

Here we give a simple criterion for $\mathrm{Gal}(k(E[3])/k) = \mathrm{GL}_2(\mathbb{F}_3)$:

Lemma 2.7. *Let E be an elliptic curve defined over an algebraic number field k. If k does not contain $\sqrt{-3}$, $\sqrt[3]{\Delta(E)}$, and E does not admit a 3-isogeny defined over k, then $\mathrm{Gal}(k(E[3])/k) = \mathrm{GL}_2(\mathbb{F}_3)$, $\mathrm{Gal}(k(E[3])/k(\sqrt{-3})) = \mathrm{SL}_2(\mathbb{F}_3)$.*

Proof. By Lemma 2.4, the order of $G = \mathrm{Gal}(k(E[3])/k)$ is divisible by 3. Hence, by Proposition 15 of [33], G contains $\mathrm{SL}_2(\mathbb{F}_3)$ or is conjugate to a subgroup of $\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$. Since the

latter means that E admits a 3-isogeny defined over k and is excluded by the assumption, we have $G \supset \mathrm{SL}_2(\mathbb{F}_3)$. Since $\sqrt{-3} \notin k$, we see from the commutative diagram below that $\det : G \to \mathbb{F}_3^\times$ is surjective.

$$\begin{array}{ccc} \mathrm{Gal}(k(E[3])/k) & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_3) \\ {\scriptstyle \mathrm{Res}}\downarrow & & \downarrow{\scriptstyle \det} \\ \mathrm{Gal}(k(\sqrt{-3})/k) & \xrightarrow{\cong} & \mathbb{F}_3^\times \end{array}$$

Hence $G = \mathrm{GL}_2(\mathbb{F}_3)$. The diagram also shows that $\mathrm{Gal}(k(E[3])/k(\sqrt{-3})) = \mathrm{SL}_2(\mathbb{F}_3)$. □

Proposition 2.8. *Let k be a real quadratic field. Let E be an elliptic curve with everywhere good reduction over k given by a global minimal equation whose discriminant $\Delta(E) \in \mathcal{O}_k^\times$ is not a cube in k. If the ray class number modulo (3) of the field $k(\sqrt[3]{\varepsilon}, \sqrt{-3})$ is odd, then $\mathrm{Gal}(k(E[3])/k)$ is conjugate to the group $\begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix}$ or $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$. In particular, there is a basis (P_1, P_2) of $E[3]$ such that either P_1 is a k-rational point of order 3 on E, or $\langle P_1 \rangle$ is a k-rational subgroup of order 3 and the image of P_2 in the 3-isogenous curve $E/\langle P_1 \rangle$ is a k-rational point of order 3.*

Proof. Since $\Delta(E)$ is not a cube, we have $M = k(\sqrt[3]{\varepsilon}, \sqrt{-3})$, $K = k(\sqrt[3]{\varepsilon})$. Since L contains M which is a Galois extension of k with Galois group isomorphic to the symmetric group of degree 3, G is not a commutative groups of order at least 6. Suppose E admits no 3-isogeny defined over k. Then $G = \mathrm{GL}_2(\mathbb{F}_3)$ by Lemma 2.7, and hence $H := \mathrm{Gal}(L/K)$ is a 2-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. Let σ, τ be generators of H as in (2.1). Since σ and τ has determinant -1, we have $\mathrm{Gal}(L/M) = H \cap \mathrm{SL}_2(\mathbb{F}_3) = \langle \sigma\tau, \tau^2 \rangle$. Hence the fixed field of $\langle \tau^2 \rangle$ is a quadratic extension of M unramified outside 3, a contradiction. Hence E admits a 3-isogeny defined over k, that is, G is conjugate to a subgroup of $B = \begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$. Supposing $G = B$, we see that L/M is a quadratic extension unramified outside 3. This is again a contradiction. Hence G is non-commutative group of order 6. Such a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ is conjugate to one of the groups stated in the lemma. □

2.3 Fields of 3-division points, II

If 3 is unramified in k, we can obtain detailed information for the ramification of 3:

Lemma 2.9 (Serre [33])**.** *Let k be an algebraic number field in which a prime number p is unramified. Let $\mathfrak{p}$ be a prime ideal of k dividing p. Let E be an elliptic curve defined*

over k and let $Z_{\mathfrak{p}}$, $T_{\mathfrak{p}} \subset \mathrm{Gal}(k(E[3])/k)$ be the decomposition group and inertia group of $\mathfrak{p}$, respectively.

(1) *If E has ordinary reduction at $\mathfrak{p}$, then $T_{\mathfrak{p}}$ is conjugate to $\begin{bmatrix} * & 0 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$.*

(2) *If E has supersingular reduction at $\mathfrak{p}$, then $T_{\mathfrak{p}}$ is isomorphic to $\mathbb{F}_{p^2}^{\times}$, hence is a cyclic group of order p^2-1, and*

$$Z_{\mathfrak{p}} = \begin{cases} T_{\mathfrak{p}} & \text{if } \mathcal{O}_k/\mathfrak{p} \supset \mathbb{F}_{p^2}, \\ N(T_{\mathfrak{p}}) & \text{if } \mathcal{O}_k/\mathfrak{p} \not\supset \mathbb{F}_{p^2}, \end{cases}$$

where $N(T_{\mathfrak{p}})$ is the normalizer of $T_{\mathfrak{p}}$ in $\mathrm{GL}_2(\mathbb{F}_p)$. The order of $N(T_{\mathfrak{p}})$ is $2(p^2-1)$. □

Using this, we will obtain a criterion for E to have cubic discriminant (Proposition 2.12 below). Note that the discriminant being a cube or not is independent of the choice of a model.

Let L, F, K, M and G as in the previous section.

Lemma 2.10. *Let k be a real quadratic field. Assume that 3 is unramified in k and the class number of F is prime to 3. Let E be an elliptic curve with everywhere good reduction over k given by a global minimal equation whose discriminant $\Delta(E) \in \mathcal{O}_k^{\times}$ is not a cube in k. (Hence $K = k(\sqrt[3]{\varepsilon})$, $M = k(\sqrt[3]{\varepsilon}, \sqrt{-3})$.) Then E has ordinary good reduction at all primes of k lying above 3.*

Proof. (The essential part of the following proof is due to M. Kida.) Let $\mathfrak{p}$ be a prime ideal of k dividing 3. Note that $\mathfrak{p}$ is ramified in K and F: $\mathfrak{p}\mathcal{O}_F = \mathfrak{P}_F^2$. Suppose that E has supersingular reduction at $\mathfrak{p}$. Then, by Lemma 2.9, the decomposition group of $\mathfrak{p}$ is a 2-group. Hence $\mathfrak{p}$ cannot be totally ramified in K/M. Therefore $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_K^2\mathfrak{P}'_K$, where $\mathfrak{P}_K$ and $\mathfrak{P}'_K$ are distinct prime ideals of K. Since M/k is a Galois extension, we have $\mathfrak{p}\mathcal{O}_M = (\mathfrak{P}\mathfrak{P}'\mathfrak{P}'')^2$ with three distinct prime ideals $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}''$ of M. It follows that $\mathfrak{P}_F$ splits completely in M.

Hence, if 3 remains prime in k, then M/F is an unramified cyclic extension of degree three. This is a contradiction.

Next consider the case where 3 decomposes in k: $3\mathcal{O}_k = \mathfrak{p}\mathfrak{p}'$, $3\mathcal{O}_F = (\mathfrak{P}_F\mathfrak{P}'_F)^2$. Since $M = F(\sqrt[3]{\varepsilon})$ is a Kummer extension of degree 3 over F, we see, by Theorem 119 of [16], that $\mathfrak{P}_F$ splits completely in M if and only if the congruence

$$X^3 \equiv \varepsilon \pmod{\mathfrak{P}_F^4} \tag{2.2}$$

is solvable in $\mathcal{O}_F$. Let σ be an element of $\mathrm{Gal}(F/\mathbb{Q})$ such that $\sigma|_k$ is the non-trivial element of $\mathrm{Gal}(k/\mathbb{Q})$. Applying σ to the congruence (2.2), we have a solution $N_{k/\mathbb{Q}}(\varepsilon)X^{\sigma}$ of the

congruence

$$Y^3 \equiv \varepsilon^{-1} \pmod{\mathfrak{P}_F'^4}.$$

This means that $\mathfrak{P}'_F$ also decomposes in M. Hence M/F is again an unramified cyclic extension of degree three. □

Lemma 2.11. *Let k and E be as in Lemma 2.10. If the class number of $K = k(\sqrt[3]{\varepsilon})$ is odd, then E admits a 3-isogeny defined over k.*

Proof. Since $\Delta(E)$ is not a cube, the order of G is divisible by 3 by Lemma 2.4. Suppose that E does not admit any 3-isogeny defined over k. Then $G = \mathrm{GL}_2(\mathbb{F}_3)$ by Lemma 2.7. Hence $\mathrm{Gal}(L/K) = \langle \sigma, \tau \rangle$ is a 2-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$, where σ, τ are as in (2.1). Since, by Lemma 2.10, E has ordinary good reduction at any primes of k lying above 3, we can apply the argument in the proof of Proposition 5.6 of [2] to this case and we see that the fixed field of $\langle \sigma, \tau^2 \rangle$ is an unramified quadratic extension of K. □

Proposition 2.12. *Let k be a real quadratic field. Then the discriminant of every elliptic curve with everywhere good reduction over k is a cube in k if the following conditions hold:*

(1) *The class number of k is prime to 6;*
(2) *3 is unramified in k;*
(3) *The class number of $k(\sqrt{-3})$ is prime to 3;*
(4) *The class number of $k(\sqrt[3]{\varepsilon})$ is odd;*
(5) *For some prime ideal $\mathfrak{p}$ of k dividing 3, the congruence $X^3 \equiv \varepsilon \pmod{\mathfrak{p}^2}$ does not have a solutions $X \in \mathcal{O}_k$.*

Proof. Suppose that there exists an elliptic curve E whose discriminant is not a cube in k. By (1) and Lemma 1.1, E admits a global minimal model. By (2), (3), (4) and Lemma 2.11, E admits a 3-isogeny $f : E \to \bar{E}$ defined over k. Let, as in Chapter 1, $j(E) = J(\tau)$, $j(\bar{E}) = J(\bar{\tau})$, $\tau, \bar{\tau} \in \mathcal{O}_k$, $\tau\bar{\tau} = 3^6$. Since $\bar{E}$ admits a 3-isogeny over k and $k \neq \mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{33})$, $\Delta(\bar{E})$ is not a cube (Proposition 1.7). Hence, by considering the dual of f if necessary, we may assume that $(\tau) = (1)$ if (3) is a prime ideal, that $(\tau) = (1)$ or $\mathfrak{p}^6$ if $(3) = \mathfrak{p}\mathfrak{p}'$. If $(\tau) = (1)$, then $X^3 = u + 27v$, $X \in \mathcal{O}_k$, $u, v \in \mathcal{O}_k^\times$, $u \notin k^{\times 3}$. Without loss of generality, we may assume that $u = \varepsilon^{\pm 1}$. If $u = \varepsilon$, then $X^3 = \varepsilon + 27v \equiv \varepsilon \pmod{\mathfrak{p}^2}$. If $u = \varepsilon^{-1}$, then $(N_{k/\mathbb{Q}}(\varepsilon)X')^3 = \varepsilon + 27v' \equiv \varepsilon \pmod{\mathfrak{p}^2}$. In case $(\tau_1) = \mathfrak{p}^6$, we can prove similarly. □

Chapter 3

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

In this chapter, we show the nonexistence of elliptic curves with everywhere good reduction over 24 real quadratic fields, and determine such curves over 8 real quadratic fields.

3.1 Admissible curves

Let k be a real quadratic field and E an elliptic curve with everywhere good reduction over k. To check the assumptions of Corollary 2.3, we compute $h_k^{(2)}$, $h_{k(\sqrt{-1})}^{(2)}$ and $h_{k(\sqrt{\pm\varepsilon})}^{(2)}$ (Table 3.1). The bold-faced numbers in the table are the ones divisible by 3. We exclude $m = 79$ and 82, because $h_{\mathbb{Q}(\sqrt{79})} = 3$, $h_{\mathbb{Q}(\sqrt{82})} = 4$.

m	k	$k(\sqrt{-1})$	$k(\sqrt{\varepsilon})$	$k(\sqrt{-\varepsilon})$	m	k	$k(\sqrt{-1})$	$k(\sqrt{\varepsilon})$	$k(\sqrt{-\varepsilon})$
2	1	1	1	1	3	1	1	1	2
5	1	1	1	1	6	1	2	1	1
7	1	1	1	4	10	2	2	2	2
11	1	**3**	1	2	13	1	1	1	1
14	1	4	1	1	15	2	2	2	8
17	1	2	1	1	19	1	**3**	1	**6**
21	1	2	1	1	22	1	2	1	**3**
23	1	**3**	1	4	26	2	**6**	2	2
29	1	**3**	1	1	30	2	4	1	8
31	1	**3**	1	8	33	1	2	1	**3**
34	2	8	1	8	35	2	**6**	2	16
37	**3**	**3**	**3**	**3**	38	1	**6**	1	**3**
39	2	4	1	4	41	1	4	1	1

m	k	$k(\sqrt{-1})$	$k(\sqrt{\varepsilon})$	$k(\sqrt{-\varepsilon})$	m	k	$k(\sqrt{-1})$	$k(\sqrt{\varepsilon})$	$k(\sqrt{-\varepsilon})$
42	2	4	2	4	43	1	**3**	1	10
46	1	4	1	**3**	47	1	5	1	8
51	2	**12**	4	8	53	1	**3**	1	1
55	2	4	1	**12**	57	1	2	1	**3**
58	2	2	2	2	59	1	**9**	1	**6**
61	1	**3**	1	1	62	1	8	1	**3**
65	2	8	2	2	66	2	16	1	8
67	1	**3**	1	14	69	1	4	1	**3**
70	2	4	1	16	71	1	7	**3**	4
73	1	2	1	1	74	2	10	2	2
77	1	4	1	**3**	78	2	4	2	**12**
83	1	**9**	1	10	85	2	4	4	4
86	1	10	1	**3**	87	2	**6**	2	8
89	1	**6**	1	1	91	2	**6**	2	**48**
93	1	2	1	**3**	94	1	8	1	5
95	2	8	1	**12**	97	1	2	1	1

Table 3.1: $h_K^{(2)}$ $(K = k, k(\sqrt{-1}), k(\sqrt{\pm\varepsilon}))$

We thus obtain

Proposition 3.1. *Every elliptic curve with everywhere good reduction over* $\mathbb{Q}(\sqrt{m})$ *is admissible if* m *is one of* 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 21, 30, 34, 39, 41, 42, 47, 58, 65, 66, 70, 73, 74, 85, 94, 97.

In his paper [8], Comalada characterizes real quadratic fields admitting an admissible curve by means of some diophantine equations. Solving the diophantine equations explicitly, he showed that there exists an admissible elliptic curve over $k = \mathbb{Q}(\sqrt{m})$ $(1 < m < 100)$ if and only if $m = 6, 7, 14, 22, 38, 41, 65, 77$ or 86. Moreover, for these m, the k-isomorphism classes of such curves are determined and listed in [8], § 5.

Combining this and Proposition 3.1 we obtain:

Theorem 3.2. (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* $\mathbb{Q}(\sqrt{m})$ *is admissible. Thus the curves* E_i $(1 \leq i \leq 18, 23 \leq i \leq 40)$ *listed in* § 5 *of* [8]*, and thus the curves in the table in Appendix B are all curves having everywhere good reduction over these fields.*

Combining Comalada's result, Proposition 2.2 and the computation $h_K(\mathfrak{m}_2)$, we also obtain the following:

Lemma 3.3. (1) *If $m = 29, 53$ or 89, then every elliptic curve with everywhere good reduction over $\mathbb{Q}(\sqrt{m})$ has a global minimal model whose discriminant is of the form $-\varepsilon^{2n}$ $(n \in \mathbb{Z})$.*

(2) *If $m = 33$ or 69, every elliptic curve with everywhere good reduction over $\mathbb{Q}(\sqrt{m})$ has a global minimal model whose discriminant is of the form $-\varepsilon^{2n+1}$ $(n \in \mathbb{Z})$.*

For curves over $\mathbb{Q}(\sqrt{37})$, we cannot get any information on the sign and the parity of the exponent of the discriminant, since $h_k^{(2)} = h_{k(\sqrt{-1})}^{(2)} = h_{k(\sqrt{\pm\varepsilon})}^{(2)} = 3$.

3.2 The cases $m = 29, 33$ or 69

Let $k = \mathbb{Q}(\sqrt{m})$, $1 < m < 100$ be square-free. Suppose that $(h_k, 6) = 1$ and m is not appeared in Theorem 3.2. That is, $m = 11$, 19, 22, 23, 29, 31, 33, 37, 38, 43, 46, 53, 57, 59, 61, 62, 67, 69, 71, 77, 83, 86, 89 or 93. Then $h_k = 1$.

First, we consider the case of cubic discriminant. Since

$$h_k((3)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}) = \begin{cases} 2 & \text{if } m = 29, 33, 53, 89, \\ 6 & \text{if } m = 69, \\ 8 & \text{if } m = 59, \\ 12 & \text{if } m = 93, \\ 16 & \text{if } m = 11, 38, 83, 86, \\ 4 & \text{otherwise,} \end{cases}$$

Propositions 1.7 and 2.6 imply the following:

Proposition 3.4. (1) *If $m = 29, 53, 69$ or 89, then there are no elliptic curves with everywhere good reduction over $k = \mathbb{Q}(\sqrt{m})$ whose discriminant is not a cube in k.*

(2) *If E is an elliptic curve with everywhere good reduction over $k = \mathbb{Q}(\sqrt{33})$ whose discriminant is a cube in k, then E is isomorphic over k to* 33A1 *or* 33A1$'$.

Next, we consider the case of non-cubic discriminant. To use Proposition 2.8, we compute $h_M((3))$ using KASH, where $M = k(\sqrt[3]{\varepsilon}, \sqrt{-3})$. For $m = 29, 33, 69$, we have

$$h_M((3)) = \begin{cases} 3 & \text{if } m = 29, \\ 243 & \text{if } m = 33, \\ 9 & \text{if } m = 69. \end{cases}$$

(The computation of $h_M((3))$ took about 1 minutes, 20 minutes and 1 minutes, respectively, on a Sparc station SS4, CPU 110MHZ. For $m = 53, 89$, we did not compute $h_M((3))$, because it seems that the computation would take too much time.) Thus

Proposition 3.5. *Let $k = \mathbb{Q}(\sqrt{m})$ $(m = 29, 33, 69)$. If E has everywhere good reduction over k with $\Delta(E) \notin k^{\times 3}$, then E admits a 3-isogeny $f : E \to \bar{E}$ defined over k, and either E or $\bar{E}$ has a k-rational point of order 3.*

In the following, we determine the elliptic curves having good reduction over $k = \mathbb{Q}(\sqrt{m})$ $(m = 29, 33, 69)$, having non-cubic discriminant and admitting a 3-isogeny defined over k (we do not need the fact that either of the pair of 3-isogenous curves has a k-rational point of order 3).

Let E be such a curve. First consider the case $m = 29$. By Lemma 3.3, $\Delta(E) = -\varepsilon^{2n}$ for some $n \in \mathbb{Z}$. The curves with such properties are already determined (Proposition 1.10). Note that in [26], the curves having properties $\Delta(E) \notin k^{\times 3}$ and $E(k)[3] \neq \{O\}$ are already determined.

Next consider the cases $m = 33$ or 69. By Lemma 3.3, $\Delta(E) = -\varepsilon^{2n+1}$ ($n \in \mathbb{Z}$, $2n + 1 \not\equiv 0 \pmod 3$). In view of the formulae for the admissible change of variables, we may assume that $\Delta(E) = -\varepsilon^{\pm n}$ ($n = 1, 5$). By considering the conjugate, we may assume that $\Delta(E) = -\varepsilon^{6n+1}$ ($n = 0, -1$). Let $j(E) = J(t)$ ($t \in \mathcal{O}_k$) as in Chapter 1. Suppose first that $(t) = (1)$. By a similar argument as in Chapter 1

$$X^3 = \varepsilon + 27u, \quad X = \frac{-c_4(E)}{(t+3)\varepsilon^{2n}} \in \mathcal{O}_k \backslash \{0\}, \quad u = \varepsilon/t \in \mathcal{O}_k^{\times}.$$

This equation is shown to be impossible by reducing modulo 9.

Suppose $(t) = (27)$. Then similarly,

$$X^3 = \varepsilon + \varepsilon u, \quad X = \frac{-c_4(E)}{(t+3)\varepsilon^{2n}} \in \mathcal{O}_k \backslash \{0\}, \quad u = 27/t \in \mathcal{O}_k^{\times}.$$

Let

$$\pi = \begin{cases} 6 + \sqrt{33}, \\ (9 + \sqrt{69})/2 \end{cases}$$

be a prime element of k dividing 3. Since $\pi^2 = 3\varepsilon$ and, from (1.2), $t/\Delta(E) = -\pi^6/(\varepsilon^{6n+4}u)$ is a square, we have $u = -\varepsilon^{2l}$, $l \in \mathbb{Z}$, whence

$$X^3 = \varepsilon - \varepsilon^{-2l+1}, \ X \neq 0.$$

Taking the norm of both sides and noting $\mathrm{Tr}_{k/\mathbb{Q}}(w^2) = \mathrm{Tr}_{k/\mathbb{Q}}(w)^2 - 2$ for $w \in \mathcal{O}_k^{\times}$, we obtain

$$\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon^l)^2 = \{-N_{k/\mathbb{Q}}(X)\}^3 + 4.$$

Since the only (affine) $\mathbb{Q}$-rational point of the elliptic curve $y^2 = x^3 + 4$, which is the curve 108A1 in the table in [11], are $(0, \pm 2)$, we see that $X = 0$, a contradiction.

Finally suppose $(t) = (729)$. Then

$$X^3 = -\varepsilon(u + 27), \quad X = \frac{3c_4(E)}{(t+3)\varepsilon^{2n}} \in \mathcal{O}_k \backslash \{0\}, \quad u = 729/t \in \mathcal{O}_k^{\times}.$$

Since, by (1.2), $t/\Delta(E) = -3^6/(u\varepsilon^{6n+1})$ is a square, we have $u = -\varepsilon^{2s-1}$, $s \in \mathbb{Z}$. By reducing modulo 9, we see that $s \equiv 0 \pmod 3$, say $s = 3t$, $t \in \mathbb{Z}$. Hence

$$(X/\varepsilon^{2t})^3 = 1 - 27\varepsilon^{1-6t}.$$

Thus, by Lemma 1.3, we must have $k = \mathbb{Q}(\sqrt{33})$, $t = 0$, $u = -\varepsilon^{-1}$, $t = -729\varepsilon$ and $j(E) = -(5+\sqrt{33})^3(5588+972\sqrt{33})^3\varepsilon^{-1}$. Since $\Delta(E) = -\varepsilon^{6n+1}$ $(n = 0, -1)$, we have 4 candidates (C_4, C_6) for $(c_4(E), c_6(E))$ of an elliptic curve E:

$$(C_4, C_6) = \big((5+\sqrt{33})(5588+972\sqrt{33})\varepsilon^{2n}, \pm(20793752+3619728\sqrt{33})\varepsilon^{3n}\big) \quad (n = 0, -1).$$

To determine which of them occur as c_4, c_6 of an elliptic curve, we use the following Kraus' result:

Lemma 3.6 (Kraus [21])**.** *Let K be a finite unramified extension of $\mathbb{Q}_2$. Let C_4, C_6 be integers of K such that $(C_4^3 - C_6^2)/1728$ is a nonzero integer of K. In order for there to exist a Weierstrass equation with coeficients a_i $(i = 1, 2, 3, 4, 6)$ in integers of K satisfiyng $c_4 = C_4$, $c_6 = C_6$, it is necessary and sufficient that*

(1) *C_4 is a unit of K and and there exeists an interger x of K such that $-C_6 \equiv x^2 \pmod 4$*

or,

(2) *$C_4 \equiv 0 \pmod{16}$ and there exists an integer x of K such that $C_6 \equiv 8x^2 \pmod{32}$.*

Remark. Kraus gives similar conditions also when $K/\mathbb{Q}_2$ is a finite ramified extension or $K/\mathbb{Q}_3$ is any finite extension.

In our cases, the following two pairs satisfy the condition of Lemma 3.6:

$$\big((5+\sqrt{33})(5588+972\sqrt{33}), 20793752+3619728\sqrt{33}\big),$$
$$\big((5+\sqrt{33})(5588+972\sqrt{33})\varepsilon^{-2}, -(20793752+3619728\sqrt{33})\varepsilon^{-3}\big),$$

since $(5+\sqrt{33})(5588+972\sqrt{33})\varepsilon^{2n}$ is divisible by 16, $(207935752+3619728\sqrt{33})/8 \equiv 1 \pmod 4$, $\varepsilon^{-3} \equiv -1 \pmod 4$ and -1 is not a square modulo 4. The curve E satisfying $c_4(E) = (5+\sqrt{33})(5588+972\sqrt{33})$ and $c_6(E) = 20793752+3619728\sqrt{33}$ (resp. $c_4(E) = (5+\sqrt{33})(5588+972\sqrt{33})\varepsilon^{-2}$ and $c_6(E) = -(20793752+3619728\sqrt{33})\varepsilon^{-3}$) is 33A2 (resp. 33A3′).

Instead of using Lemma 3.6, computing the conductor over k of the elliptic curve

$$Y^2 = X^3 - 27C_4X - 54C_6$$

by Tate's algorithm ([42]. See also [39]) also gives the result. In fact, the curves corresponding to

$$(C_4, C_6) = \big((5+\sqrt{33})(5588+972\sqrt{33}), -(20793752+3619728\sqrt{33})\big),$$
$$\big((5+\sqrt{33})(5588+972\sqrt{33})\varepsilon^{-2}, (20793752+3619728\sqrt{33})\varepsilon^{-3}\big)$$

have conductor (2^4). Tate's algorithm over quadratic fields is implemented by A. Umegaki on Sparc work station using PARI/GP Version 1.39.

We now have proved

Theorem 3.7. (1) *The only elliptic curves with everywhere good reduction over* $\mathbb{Q}(\sqrt{29})$ *are* 29A1, 29A1′, 29A2 *and* 29A2′.

(2) *The only elliptic curves with everywhere good reduction over* $\mathbb{Q}(\sqrt{33})$ *are* 33A1, 33A1′, 33A2, 33A2′, 33A3 *and* 33A3′.

(3) *There are no elliptic curves with everywhere good reduction over* $\mathbb{Q}(\sqrt{69})$.

3.3 The cases $m = 53$ or 89

We verify the conditions of Proposition 2.12 for the values of m appeared in the top of the previous section except $m = 29, 33, 69$.

As mentioned above, the class number of $k = \mathbb{Q}(\sqrt{m})$ is 1 for these m. Hence $m \neq 57, 93$ satisfy the condition (1) and (2).

The class numbers of $k(\sqrt{-3})$ and $k(\sqrt[3]{\varepsilon})$ are as in Table 3.2. The bold-faced numbers are those that do not satisfy the assumption. The following 13 m's satisfy the assumptions (3) and (4).

$$m = 11, 19, 22, 23, 31, 37, 38, 46, 53, 59, 61, 86, 89.$$

For the assumption (5), see Tables 3.3, 3.4. Note that if $3 = \mathfrak{p}\mathfrak{p}'$ $(\mathfrak{p} \neq \mathfrak{p}')$, then $\mathcal{O}_k/\mathfrak{p}^2 \cong \mathbb{Z}/9\mathbb{Z}$, and hence (5) is equivalent to $\varepsilon \not\equiv \pm 1 \pmod{\mathfrak{p}^2}$.

m	$k(\sqrt{-3})$	$k(\sqrt[3]{\varepsilon})$	m	$k(\sqrt{-3})$	$k(\sqrt[3]{\varepsilon})$
11	2	1	59	2	1
19	2	1	61	4	1
22	4	1	62	**6**	1
23	4	1	67	**6**	1
31	2	1	71	4	**2**
37	4	1	77	**6**	1
38	4	1	83	**6**	1
43	**6**	1	86	4	1
46	4	1	89	1	1
53	5	1			

Table 3.2: Class numbers of $k(\sqrt{-3})$ and $k(\sqrt[3]{\varepsilon})$

m	$\mathfrak{p}$	ε	$\varepsilon \bmod \mathfrak{p}^2$
19	$(4+\sqrt{19})$	$170+39\sqrt{19}$	-4
22	$(5+\sqrt{22})$	$197+42\sqrt{22}$	-4
31	$(11+2\sqrt{31})$	$1520+273\sqrt{31}$	-4
37	$(3+\omega)$	$5+2\omega$	-4
46	$(7+\sqrt{46})$	$24335+3588\sqrt{46}$	2
61	$(3+\omega)$	$17+5\omega$	-4

Table 3.3: $\varepsilon \bmod \mathfrak{p}^2$ $(3=\mathfrak{p}\mathfrak{p}')$

m	$(\mathcal{O}_k/9\mathcal{O}_k)^{\times 3}$	ε	$\varepsilon \bmod 9$
11	± 1, $\pm 2\sqrt{11}$, $\pm(2\pm 4\sqrt{11})$	$10+3\sqrt{11}$	$1+3\sqrt{11}$
23	± 1, $\pm 4\sqrt{23}$, $\pm(2\pm\sqrt{23})$	$24+5\sqrt{23}$	$-3-4\sqrt{23}$
38	± 1, $\pm 2\sqrt{38}$, $\pm(2\pm 4\sqrt{38})$	$37+6\sqrt{38}$	$1-3\sqrt{38}$
53	± 1, $\pm 4\omega$, $\pm(4-4\omega)$, $\pm(1-2\omega)$	$3+\omega$	$3+\omega$
59	± 1, $\pm 4\sqrt{59}$, $\pm(2\pm\sqrt{59})$	$530+69\sqrt{59}$	$-1-3\sqrt{59}$
86	± 1, $\pm 4\sqrt{86}$, $\pm(2\pm\sqrt{86})$	$10405+1122\sqrt{86}$	$1-3\sqrt{86}$
89	± 1, $\pm 4\omega$, $\pm(4-4\omega)$, $\pm(1-2\omega)$	$447+106\omega$	$-3-2\omega$

Table 3.4: $\varepsilon \bmod 9$ (3 is inert in k)

Summing up the preceding computations, we have

Proposition 3.8. *If $m = 11, 19, 22, 23, 31, 37, 38, 46, 53, 59, 61, 86$ or 89, then every elliptic curve with everywhere good reduction over $k=\mathbb{Q}(\sqrt{m})$ has a global minimal model with discriminant $\Delta(E) \in \mathcal{O}_k^{\times 3}$.*

Among these m, we treat $m = 53, 89$ in this section and $m = 37$ in the next section. The case of other m's will be treated in a forthcoming article.

Theorem 3.9. *There are no elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{m})$ $(m = 53, 89)$.*

Proof. This is clear from Propositions 3.4 and 3.8. □

We can prove Proposition 3.4 for $m = 29, 53, 89$ as follows.

Suppose that there is an elliptic curve E having cubic discriminant and everywhere good reduction over $k=\mathbb{Q}(\sqrt{m})$ ($m = 29, 53$ or 89). By Lemma 3.3, $\Delta(E) = -\varepsilon^{6n}$ for some $n \in \mathbb{Z}$. Hence $(c_4(E)/\varepsilon^{2n}, c_6(E)/\varepsilon^{3n})$ is an $\mathcal{O}_k$-integral point of $y^2 = x^3 + 1728$.

Lemma 3.10. *Let D be a nonzero rational integer all of whose prime divisors other than 3 are congruent to 5 modulo 12, and let E be the elliptic curve defined over $\mathbb{Q}$ by the equation $y^2 = x^3 + D^3$. Then* $\operatorname{rank} E(\mathbb{Q}) = 0$.

Proof. (The following proof is taken from [9].) Letting $X = x + D$, we have $E : y^2 = X^3 - 3DX^2 + 3D^2X$. The rank r of $E(\mathbb{Q})$ is computed from the following formula (see [40], Chapter III):

$$2^r = \frac{\#\alpha(E) \cdot \#\bar{\alpha}(\bar{E})}{4},$$

where $\alpha(E)$ and $\bar{\alpha}(\bar{E})$ are subgroups of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ defined by

$$\begin{aligned}
\alpha(E) = &\{1\mathbb{Q}^{\times 2},\ 3\mathbb{Q}^{\times 2}\} \\
&\cup \left\{ b_1\mathbb{Q}^{\times 2} \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \;\middle|\; \begin{array}{l} b_1 \mid 3D^2,\ b_1M^4 - 3DM^2e^2 + (3D^2/b_1)e^4 = N^2 \\ \text{has a solution } M, N, e \in \mathbb{Z} \text{ with } Me \neq 0 \end{array} \right\}, \\
\bar{\alpha}(\bar{E}) = &\{1\mathbb{Q}^{\times 2},\ -3\mathbb{Q}^{\times 2}\} \\
&\cup \left\{ b_1\mathbb{Q}^{\times 2} \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \;\middle|\; \begin{array}{l} b_1 \mid 3D^2,\ b_1M^4 + 6DM^2e^2 - (3D^2/b_1)e^4 = N^2 \\ \text{has a solution } M, N, e \in \mathbb{Z} \text{ with } Me \neq 0 \end{array} \right\}.
\end{aligned}$$

Thus it is enough to prove $\#\alpha(E) = \#\bar{\alpha}(\bar{E}) = 2$.

For a prime p, let $(*,*)_p$ the Hilbert symbol correspondig to the prime number p. Let b_1 be a square-free divisor of $3D^2$ other than $1, 3$. If $b_1M^4 - 3DM^2e^2 + (3D^2/b_1)e^4 = N^2$, then $b_1(M^2 - 3De^2/(2b_1))^2 + (3D^2)/(4b_1)e^2 - N^2 = 0$, $e \neq 0$, and hence $(b_1, 3D^2/4b_1)_p = (b_1, -3)_p = 1$ for any prime p. Thus if $(b_1, -3)_p = -1$ for some prime p, then $b_1\mathbb{Q}^{\times 2} \notin \alpha(E)$. If $b_1 = -1$ or -3, then $(b_1, -3)_p = (-1/3) = -1$. If $b_1 \neq -1, -3$, then, for any prime divisor $p \neq 3$ of b_1, we have $(b_1, -3)_p = (p, -3)_p = (-3/p) = -1$, since $p \equiv 5 \pmod{12}$. Hence $\alpha(E) = \{1\mathbb{Q}^{\times 2}, 3\mathbb{Q}^{\times 2}\}$.

For $\bar{\alpha}(\bar{E})$, similar computation involving $(b_1, 3)_p$ yields $\bar{\alpha}(\bar{E}) = \{1\mathbb{Q}^{\times 2}, -3\mathbb{Q}^{\times 2}\}$. □

Lemma 3.11. *If E is an elliptic curve defined over $\mathbb{Q}$, then*

$$\operatorname{rank} E(\mathbb{Q}(\sqrt{m})) = \operatorname{rank} E(\mathbb{Q}) + \operatorname{rank} E^{(m)}(\mathbb{Q}),$$

where m is a square-free rational integer and $E^{(m)}$ is the quadratic twist of E by m.

Proof. See [30]. □

Lemma 3.12. *Let E be an elliptic curve defined over a number field k. Let $\mathfrak{p}$ be a prime ideal of k and let p be the prime number such that $\mathfrak{p} \cap \mathbb{Z} = (p)$. If $\mathfrak{p}$ is a prime of good reduction and the ramification index of $\mathfrak{p}$ is less than $p - 1$, then the reduction map $E(k)_{\text{tors}} \to E_{\mathfrak{p}}(\mathcal{O}_k/\mathfrak{p})$ is injective.*

Proof. Use Propositions 2.1 and 2.2 in [38], Chapter VII. See also Theorem 1 of [25]. □

Corollary 3.13. *Let* $C : y^2 = x^3 + 1728$. *Then* $C(k) = \langle(-12, 0)\rangle \cong \mathbb{Z}/2\mathbb{Z}$ *if* $k = \mathbb{Q}(\sqrt{p})$, $p = 29, 53$ *or* 89.

Proof. We first show that $\operatorname{rank} C(k) = 0$. It follows from Lemma 3.10 that $\operatorname{rank} C(\mathbb{Q}) = \operatorname{rank} C^{(p)}(\mathbb{Q}) = 0$, since C and $C^{(p)}$ have a model $y^2 = x^3 + 3^3$ and $y^2 = x^3 + (3p)^3$, respectively which satisfy the assumption of Lemma 3.10. Hence the assertion follows from Lemma 3.11.

We next show that $\#C(k)_{\mathrm{tors}} \leq 2$. For a prime ideal $\mathfrak{p}$ of k,

$$\#C_{\mathfrak{p}}(\mathcal{O}_k/\mathfrak{p}) = \begin{cases} 2 \cdot 3 & \text{if } p = 29 \text{ or } 89, \text{ and } \mathfrak{p} \mid 5, \\ 2^2 & \text{if } p = 29 \text{ or } 53, \text{ and } \mathfrak{p} \mid 7, \\ 2 \cdot 3^2 & \text{if } p = 53 \text{ and } \mathfrak{p} \mid 17, \\ 2^2 \cdot 13 & \text{if } p = 89 \text{ and } \mathfrak{p} \mid 67. \end{cases}$$

Hence the assertion follows from Lemma 3.12. □.

Hence $c_6(E) = 0$, that is $j(E) = 1728$. This contradicts Lemma 1.2 and completes the proof.

3.4 The case $m = 37$

In his paper [19], Kida showed that if E is an elliptic curve having everywhere good reduction over $k = \mathbb{Q}(\sqrt{37})$ and rational j-invariant, then E is isomorphic over k to 37A1 or 37A2. In this section we show that the same conclusion holds without any restriction on j-invariant, namely

Theorem 3.14. *The only elliptic curves with everywhere good reduction over* $\mathbb{Q}(\sqrt{37})$ *are* 37A1 *and* 37A2.

The rest of this section is devoted to the proof of this theorem.

Let $k = \mathbb{Q}(\sqrt{37})$ and $\varepsilon = 6 + \sqrt{37}$. By Proposition 3.8, $\Delta(E) = \pm\varepsilon^{3n}$ for some $n \in \mathbb{Z}$. (As remarked in section 3.1, we do not know the parity of n and the sign of $\Delta(E)$ at present.) Hence $(c_4(E), c_6(E))$ is an $\mathcal{O}_k$-integral point of the elliptic curve

$$E_{3n}^{\pm} : y^2 = x^3 \pm 1728\varepsilon^{3n}.$$

In view of the formulae for an admissible change of variables, we may assume that $-2 \leq n < 2$. Thus to determine the elliptic curves with everywhere good reduction over k, we

first determine the sets

$$E_{3n}^{\pm}(\mathcal{O}_k) = \left\{(x,y) \in \mathcal{O}_k \times \mathcal{O}_k \mid y^2 = x^3 \pm 1728\varepsilon^{3n}\right\}, \quad n = -2,-1,0,1;$$

It is enough to determine the following three sets:

$$E_0^{\pm}(\mathcal{O}_k), \quad E_3^{+}(\mathcal{O}_k),$$

because the maps

$$\begin{aligned} E_{3n}^{\pm}(\mathcal{O}_k) &\to E_{3n+6}^{\pm}(\mathcal{O}_k), \quad (x,y) \mapsto (x\varepsilon^2, y\varepsilon^3), \\ E_3^{+}(\mathcal{O}_k) &\to E_3^{-}(\mathcal{O}_k), \qquad (x,y) \mapsto (x'\varepsilon^2, y'\varepsilon^3) \end{aligned}$$

are bijections.

Proposition 3.15. *$E_0^+(k) = \langle(-12,0)\rangle \cong \mathbb{Z}/2\mathbb{Z}$. In particular, $E_0^+(\mathcal{O}_k) = \left\{(-12,0)\right\}$.*

Proof. We first calculate the rank. Since E_0^+ is isomorphic over $\mathbb{Q}$ to $y^2 = x^3 + 27$, which is 144A3 in [11], we have $\operatorname{rank} E_0^+(\mathbb{Q}) = 0$. (See also Lemma 3.10.) Let $L((E_0^+)^{(37)}/\mathbb{Q}, s)$ be the Hasse-Weil L-function of $(E_0^+)^{(37)}$. Since $(E_0^+)^{(37)}$ has complex multiplication by $\mathbb{Z}[(1+\sqrt{-3})/2]$ and $L((E_0^+)^{(37)}/\mathbb{Q}, 1) = 3.1941\ldots$ (which is calculated by Upecs Version 1.4), we have, by Theorem 1 of Coates-Wiles [4], $\operatorname{rank} (E_0^+)^{(37)}(\mathbb{Q}) = 0$. Therefore $\operatorname{rank} E_0^+(k) = 0$ by Lemma 3.11.

Next, we compute the torsion subgroup. Since, for a prime $\mathfrak{p}$ of k,

$$\#(E_0^+)_{\mathfrak{p}}(\mathcal{O}_k/\mathfrak{p}) = \begin{cases} 2^2 & \text{if } \mathfrak{p} \mid 7, \\ 2 \cdot 3 \cdot 7 & \text{if } \mathfrak{p} \mid 41, \end{cases}$$

we have, by Lemma 3.12, $\#E_0^+(k)_{\mathrm{tors}} \leq 2$. This completes the proof. □

Remark. The rank of $E_0^+(\mathbb{Q})$ is easily computed by 2-descent, whereas it is hard to compute the rank of $(E_0^+)^{(37)}(\mathbb{Q})$ by the same method, since the (conjectural) order of the Shafarevich-Tate group Ш of $(E_0^+)^{(37)}/\mathbb{Q}$ is 4. This is why the author resorts to L-functions.

Remark. $\operatorname{rank} (E_0^+)^{(37)}(\mathbb{Q}) = 0$ follows from a result in [32] without using the L-function. By other results in the same paper, we know that the 3-primary part of Ш is trivial. Hence, combining this with the main result of Rubin ([31]), in which the above value of the L-function appears, we see that the order of Ш is exactly 4.

Lemma 3.16. *For $n, x \in \mathbb{Z}$, $\operatorname{Tr}_{k/\mathbb{Q}}(\varepsilon^n) = x^2$ holds if and only if $n = 3$, $x = \pm 42$.*

Proof. This will be proved in Chapter 4. □

Lemma 3.17. *Let u_1, u_2 stand for units in k and A for an integer in k. Then*
(a) The equation $64u_1 + u_2 = A^2$ has no solution.
(b) The solutions of the equation $8u_1 + u_2 = A^2$ are

$$(u_1, u_2, A) = (w^2, w^2, \pm 3w) \ (w \in \mathcal{O}_k^\times).$$

(c) The equation $16u_1 + 2u_2 = A^2$ has no solution.
(d) The solutions of the equation $u_1 + u_2 = A^2$ are

$$(u_1, u_2, A) = (w, -w, 0), \ (w^2\varepsilon^3, w^2\varepsilon'^3, \pm 42w), \ (w^2\varepsilon'^3, w^2\varepsilon^3, \pm 42w) \ (w \in \mathcal{O}_k^\times).$$

Proof. (a) is a special case of Lemma 2.1 of Ishii [17]. A key point of his proof is that 64 is divisible by 4. Hence (b) can be proved similarly to (a). The assertion (c) is clear since $8u_1 + u_2$ is prime to 2.

(d) If $A \neq 0$, then Proposition 2 of [8] implies that

$$u_1 = w^2 u_0, \ u_2 = w^2 u_0', \ w, u_0 \in \mathcal{O}_k^\times, \ \mathrm{Tr}_{k/\mathbb{Q}}(u_0) = x^2, \ x \in \mathbb{Z}.$$

We may suppose that u_1 is positive, and hence $u_0 = \varepsilon^n$ for some $n \in \mathbb{Z}$. By Lemma 3.16, $u_0 = \varepsilon^3$, $u_0' = \varepsilon'^3$. □

In the rest of this section, we let $\pi = (7 + \sqrt{37})/2$ be a prime element dividing 3. Observe that $N_{k/\mathbb{Q}}(\pi) = 3$.

Lemma 3.18. *The map $x + y\omega \mapsto x$ $(x, y \in \mathbb{Z})$ gives rise to a canonical isomorphism $\mathcal{O}_k/\pi^2 \cong \mathbb{Z}/9\mathbb{Z}$. In particular, $\varepsilon \equiv 5 \pmod{\pi^2}$ and hence ε is not a cube modulo π^2.*

Proposition 3.19.

$$E_3^+(\mathcal{O}_k) = \left\{(-12\varepsilon, 0), (17640 - 1740\sqrt{37}, \pm(2074464 - 438480\sqrt{37}))\right\}.$$

Proof. Factorizing $x^3 = y^2 - 1728\varepsilon^3$ in $L = k(\sqrt{3\varepsilon})$, we have

$$x^3 = (y + 24\varepsilon\sqrt{3\varepsilon})(y - 24\varepsilon\sqrt{3\varepsilon}).$$

Hence, to determine $E_3^+(\mathcal{O}_k)$, we use the following data for L:
(a) $\mathcal{O}_L = \mathcal{O}_k \oplus \mathcal{O}_k\sqrt{3\varepsilon}$.
(b) A system of fundamental units of L is $\varepsilon, \ \varepsilon_1 = \varepsilon + 2\sqrt{3\varepsilon}$. Note that $N_{L/k}(\varepsilon_1) = 1$.
(c) 2, π and π' decompose as $(2) = \mathfrak{P}_2^2$, $(\pi) = \mathfrak{P}_3^2$, $(\pi') = \mathfrak{P}_3'^2$, respectively.

(d) The class number of L is 2.

We denote the conjugation of L over k by $^-$. Let $(y+24\varepsilon\sqrt{3\varepsilon}) = \mathfrak{A}\mathfrak{C}^3$, $(y-24\varepsilon\sqrt{3\varepsilon}) = \mathfrak{B}\mathfrak{D}^3$, where $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ are integral ideals in L such that $\mathfrak{A}, \mathfrak{B}$ are cube-free, $\mathfrak{A}\mathfrak{B}$ is a cube and $\overline{\mathfrak{A}} = \mathfrak{B}$. If a prime ideal $\mathfrak{P}$ in L divides $\mathfrak{A}$, then it divides both of $(y \pm 24\varepsilon\sqrt{3\varepsilon})$. Thus $\mathfrak{P} \mid 48\varepsilon\sqrt{3\varepsilon}$ and we can write

$$\mathfrak{A} = \mathfrak{P}_2^{a_2}\mathfrak{P}_3^{a_3}\mathfrak{P}_3'^{a_3'},\ 0 \le a_2, a_3, a_3' < 3.$$

Since $\overline{\mathfrak{A}} = \mathfrak{B}$ and (c), we see that $\mathfrak{A} = \mathfrak{B}$. Moreover, since $\mathfrak{A}\mathfrak{B}$ is a cube, we have $a_2 = a_3 = a_3' = 0$, and thus

$$(y + 24\varepsilon\sqrt{3\varepsilon}) = \mathfrak{C}^3.$$

By (a) and (d), we can write $\mathfrak{C} = (a + b\sqrt{3\varepsilon})$ with $a, b \in \mathcal{O}_k$, and hence $y + 24\varepsilon\sqrt{3\varepsilon} = \eta(a + b\sqrt{3\varepsilon})^3$ with $\eta \in \mathcal{O}_L^\times$. We may write $\eta = \varepsilon^l\varepsilon_1^m$ $(-1 \le l, m \le 1)$ since -1, ε^3 and ε_1^3 can be absorbed in the cube. By (b), taking the norm from L to k yields

$$x^3 = \varepsilon^{2l}\big\{(a + b\sqrt{3\varepsilon})(a - b\sqrt{3\varepsilon})\big\}^3,$$

whence $l = 0$ and

$$y + 24\varepsilon\sqrt{3\varepsilon} = \varepsilon_1^m(a + b\sqrt{3\varepsilon})^3,\ m = 0, \pm 1.$$

If $m = -1$, then taking conjugation yields

$$-y + 24\varepsilon\sqrt{3\varepsilon} = \varepsilon_1(-a + b\sqrt{3\varepsilon})^3.$$

Therefore it is sufficient to solve the following:

$$\pm y + 24\varepsilon\sqrt{3\varepsilon} = \varepsilon_1^m(a + b\sqrt{3\varepsilon})^3,\ a, b, y \in \mathcal{O}_k,\ m = 0, 1.$$

Case 1: $m = 1$. Equating the coefficients of $\sqrt{3\varepsilon}$ yields

$$2a^3 + 3\varepsilon a^2 b + 18\varepsilon ab^2 + 3\varepsilon^2 b^3 = 24\varepsilon.$$

We see that a is divisible by 3. Letting $A = a/3 \in \mathcal{O}_k$ yields $\varepsilon b^3 \equiv -1 \pmod{\pi^2}$, which is impossible by Lemma 3.18.

Case 2: $m = 0$. Equating the coefficients yields

$$8\varepsilon = b(a^2 + \varepsilon b^2), \quad \pm y = a(a^2 + 9\varepsilon b^2). \tag{3.1}$$

From the first equation of (3.1), we have $b = u, 2u, 4u$ or $8u$ for some positive unit u of k (note that 2 is prime in k). If $b = 8u$, then $a^2 = \varepsilon u^{-1} - 64\varepsilon u^2$, which has no solutions by

Lemma 3.17 (a). If $b = u$, then Lemma 3.17 (b) implies that $u^3 = -1$, which contradicts $u > 0$. If $b = 4u$, then $a^2 = -16\varepsilon u^2 + 2\varepsilon u^{-1}$, which has no solutions by Lemma 3.17 (c). If $b = 2u$, then

$$\left(\frac{a}{2}\right)^2 = \varepsilon u^{-1} - \varepsilon u^2. \tag{3.2}$$

By Lemma 3.17 (d), we see that (3.2) holds only for $u = 1, \varepsilon^{-2}$, from which we obtain $(a, b) = (0, 2), (\pm 84, 2\varepsilon^{-2})$. From the second equation of (3.1), the corresponding values of y are $\pm y = 0$, $2074464 - 438480\sqrt{37}$, respectively. □

Proposition 3.20. *The set $E_0^-(\mathcal{O}_k)$ consists of the following 15 elements:*

$$(12, 0),\ (16, \pm 8\sqrt{37}),\ (120, \pm 216\sqrt{37}),\ (3376, \pm 32248\sqrt{37}),$$
$$\big(44 + 4\sqrt{37}, \pm(320 + 40\sqrt{37})\big),\ \big(44 - 4\sqrt{37}, \pm(320 - 40\sqrt{37})\big),$$
$$\big(572 + 92\sqrt{37}, \pm(19040 + 3128\sqrt{37})\big),\ \big(572 - 92\sqrt{37}, \pm(19040 - 3128\sqrt{37})\big).$$

Proof. Let $L = k(\sqrt{-3})$. To prove the proposition, we use the following data for L:
(a) $\mathcal{O}_L = \mathcal{O}_k \oplus \mathcal{O}_k\zeta$, where $\zeta = (1 + \sqrt{-3})/2$.
(b) $\mathcal{O}_L^\times = \langle\varepsilon\rangle \times \langle\zeta\rangle \cong \mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.
(c) 2, π and π' decompose as $(2) = \mathfrak{P}_2\overline{\mathfrak{P}}_2$ $(\mathfrak{P}_2 \neq \overline{\mathfrak{P}}_2)$, $(\pi) = \mathfrak{P}_3^2$, $(\pi') = \mathfrak{P}_3'^2$, respectively.
(d) The ideal class group is a cyclic group of order 4 generated by the class of $\mathfrak{P}_2$.
(e) $\mathfrak{P}_2^4 = (1 + \omega - 3\zeta)$.
Arguing similarly to Proposition 3.19 over the field L, we see that it suffices to solve

$$(\pm y + 24\sqrt{-3}) = \mathfrak{P}_2^{a_2}\overline{\mathfrak{P}}_2^{\overline{a}_2}\mathfrak{C}^3$$

for $(a_2, \overline{a}_2) = (0, 0), (2, 1)$, $y \in \mathcal{O}_k$ and an integral ideal $\mathfrak{C}$ of L.

Case 1:$(a_2, \overline{a}_2) = (0, 0)$. Since $(\pm y + 24\sqrt{-3}) = \mathfrak{C}^3$ and, by (d), the class number of L is prime to 3, we see that $\mathfrak{C}$ is a principal ideal. Hence, by (a) and (b), $\pm y + 24\sqrt{-3} = \varepsilon^m\zeta^n(a + b\zeta)^3$, $a, b \in \mathcal{O}_k$, $m = 0, \pm 1$ and $n = 0, \pm 1$. Taking the norm from L to k of both sides, we obtain $m = 0$; and considering the conjugate, we may suppose that $n = 0$ or 1.

If $n = 0$, equating the coefficients gives

$$\pm y = \frac{1}{2}(a - b)(2a + b)(a + 2b), \tag{3.3}$$
$$16 = ab(a + b). \tag{3.4}$$

From (3.4) we obtain

$$(a + b, ab) = (u, 16u^{-1}), (2u, 8u^{-1}), (4u, 4u^{-1}), (8u, 2u^{-1}), (16u, u^{-1})$$

for some unit u of k. If $(a+b, ab) = (4u, 4u^{-1})$, then a and b are the roots of the quadratic polynomial

$$X^2 - 4uX + 4u^{-1}.$$

The discriminant of the polynomial is $16(u^2 - u^{-1})$, which must be a square in k. By Lemma 3.17 (d), $(u^2, -u^{-1}) = (w, -w), (w^2\varepsilon^3, w^2\varepsilon'^3)$ for some unit w of k. The first case leads to $u = 1$, $a = b = 2$, and we get $y = 0$ by (3.3). The second case leads to $w^2 = \varepsilon$, a contradiction. If $(a+b, ab) = (2u, 8u^{-1})$, then the quadratic polynomial satisfied by a and b is

$$X^2 - 2uX + 8u^{-1},$$

whose discriminant $4(u^2 - 8u^{-1})$ must be a square in k. By Lemma 3.17 (b), we obtain $u = -1$, $(a, b) = (2, -4), (-4, 2)$, and, by (3.3), $y = 0$. For $(a, b) = (u, 16u^{-1}), (8u, 2u^{-1})$ or $(16u, u^{-1})$, the discriminant of the quadratic polynomials which a, b satisfy are

$$u^2 + 64u^{-1}, \quad 4(16u^2 - 2u^{-1}), \quad 4(64u^2 - u^{-1}),$$

respectively, none of which is a square by Lemma 3.17 (a), (c).

If $n = 1$, then we obtain

$$a^3 + 3a^2b - b^3 = 48.$$

We see that $a \equiv b \pmod 3$. Letting $a = 3A + b, A \in \mathcal{O}_k$ and taking modulo π^2, we obtain $b^3 \equiv 7 \pmod{\pi^2}$, which contradicts Lemma 3.18.

Case 2:$(a_2, \overline{a}_2) = (2, 1)$. Multiplying both sides by $(4) = (\mathfrak{P}_2\overline{\mathfrak{P}}_2)^2$ and considering (e) yields

$$(4)(\pm y + 24\sqrt{-3}) = \mathfrak{P}_2^4(\overline{\mathfrak{P}}_2\mathfrak{C})^3 = (1 + \omega - 3\zeta)(\overline{\mathfrak{P}}_2\mathfrak{C})^3,$$

whence, by (d),

$$4(\pm y + 24\sqrt{-3}) = \zeta^n(1 + \omega - 3\zeta)(a + b\zeta)^3, \ a, b \in \mathcal{O}_k, \ n = 0, \pm 1.$$

If $n = 0$, then equating the coefficients yields

$$-64 = a^3 - (\omega - 2)a^2b - (\omega + 1)ab^2 - b^3, \tag{3.5}$$

$$\pm 4y - 96 = (\omega + 1)a^3 + 9a^2b - 3(\omega - 2)ab^2 - (\omega + 1)b^3. \tag{3.6}$$

Let $(a, b) \in \mathcal{O}_k \times \mathcal{O}_k$ be a solution of (3.5). Putting $A = -a - (\omega + 2)b$ we have

$$A^3 + (4\omega + 4)A^2b + (16\omega + 48)Ab^2 + (32\omega + 80)b^3 = 64.$$

It is easy to see that $4 \mid A$ and $2 \mid b$. By putting $A = 4X, b = 2Y$ $(X, Y \in \mathcal{O}_k)$, we have

$$X^3 + 2(\omega+1)X^2Y + 4(\omega+3)XY^2 + 2(2\omega+5)Y^3 = 1. \tag{3.7}$$

We will determine $X, Y \in \mathcal{O}_k$ satisfying (3.7) in Chapter 4. Substituting them in $a = 4X - 2(\omega+2)Y$, $b = 2Y$, we obtain the solutions of (3.5):

$$\begin{aligned}
&(4,-4),\ (0,4),\ (-4,0),\\
&(-3+\sqrt{37}, -2\sqrt{37}),\ (-2\sqrt{37}, 3+\sqrt{37}),\ (3+\sqrt{37}, -3+\sqrt{37}),\\
&(-40-4\sqrt{37}, 8\sqrt{37}),\ (8\sqrt{37}, 40-4\sqrt{37}),\ (40-4\sqrt{37}, -40-4\sqrt{37}),\\
&(-2, 3+\sqrt{37}),\ (-1-\sqrt{37}, -2),\ (3+\sqrt{37}, -1-\sqrt{37}),\\
&(-3+\sqrt{37}, 2),\ (1-\sqrt{37}, -3+\sqrt{37}),\ (2, 1-\sqrt{37}),\\
&(-19-3\sqrt{37}, 16+2\sqrt{37}),\ (16+2\sqrt{37}, 3+\sqrt{37}),\ (3+\sqrt{37}, -19-3\sqrt{37}),\\
&(-16+2\sqrt{37}, 19-3\sqrt{37}),\ (-3+\sqrt{37}, -16+2\sqrt{37}),\ (19-3\sqrt{37}, -3+\sqrt{37}).
\end{aligned}$$

Substituting them in (3.6), we get the above values of y other than 0.

If $n = 1$ or $n = -1$, then we obtain

$$\begin{aligned}
192 &= (-2+\omega)a^3 + 3(1+\omega)a^2b + 9ab^2 + (2-\omega)b^3,\\
-192 &= (1+\omega)a^3 + 9a^2b + 3(1+\omega)ab^2 - (2-\omega)b^3,
\end{aligned}$$

respectively. They are shown to be impossible similarly as in the case $n = 1$ in Case 1. □

Remark. $\operatorname{rank} E_0^-(k) = \operatorname{rank} (E_0^-)^{(37)}(\mathbb{Q}) = 2$, which is easily seen by 2-descent.

Now we have determined $E_{3n}^{\pm}(\mathcal{O}_k)$ $(n = -2, -1, 0, 1)$. It turns out that the only $(x, y) \in E_{3n}^{\pm}(\mathcal{O}_k)$ satisfying the conditions of Lemma 3.6 are

$$(16\varepsilon^{-2},\ -8\sqrt{37}\varepsilon^{-3})\ ,\ (3376\varepsilon^{-2},\ 32248\sqrt{37}\varepsilon^{-3}) \in E_{-6}^-(\mathcal{O}_k). \tag{3.8}$$

The former corresponds to Shimura's elliptic curve C_1 and the latter to C_2.

As before, instead of using Kraus' results, computing the conductor over k of the elliptic curve

$$Y^2 = X^3 - 27xX - 54y$$

by Tate's algorithm also gives the result. (Each $(x, y) \in E_{3n}^{\pm}(\mathcal{O}_k)$ other than the ones in (3.8) gives an elliptic curve with good reduction outside 2.)

Chapter 4

Some diophantine equations

In Chapter 3, we needed to solve certain diophantine equations, but some of them remain unsolved. In this chapter we solve them, completing the proof of Theorem 3.14.

4.1 A Thue equation over $\mathbb{Q}(\sqrt{37})$

Let $k = \mathbb{Q}(\sqrt{37})$, $\omega = (1+\sqrt{37})/2$ and let $\varepsilon = 6+\sqrt{37}$ be the fundamental unit of k greater than 1. In section 3.4, we needed to solve the equation

$$X^3 + 2(\omega+1)X^2Y + 4(\omega+3)XY^2 + 2(2\omega+5)Y^3 = 1 \tag{3.7.bis}$$

in $X, Y \in \mathcal{O}_k$. In [48], de Weger solves a equation of this kind:

$$x^3 + (9+2\sqrt{13})x^2y - (12+\sqrt{13})xy^2 - \frac{11+3\sqrt{13}}{2}y^3 = \left(\frac{3+\sqrt{13}}{2}\right)^n \qquad (x, y \in \mathcal{O}_{\mathbb{Q}(\sqrt{13})},\quad n \in \mathbb{Z}).$$

To the author's knowledge, this is the only example in the literaturea where a Thue equation over a real quadratic field is solved completely. Following his argument, we can prove the following:

Proposition 4.1. *The only* $(X, Y) \in \mathcal{O}_k \times \mathcal{O}_k$ *satisfying* (3.7) *are*

$$(-2-9\omega, 22-4\omega),\ (-23-8\omega, -4+8\omega),\ (25+17\omega, -18-4\omega),$$
$$(21+8\omega, -8-3\omega),\ (-9-3\omega, 1+\omega),\ (-12-5\omega, 7+2\omega),$$
$$(9+2\omega, 1-2\omega),\ (-3-\omega, -2+\omega),\ (-6-\omega, 1+\omega),$$
$$(-5-2\omega, 1+\omega),\ (1+\omega, -1),\ (4+\omega, -\omega),$$
$$(-2-\omega, 2),\ (1, 0),\ (1+\omega, -2),$$
$$(3+\omega, 1-\omega),\ (-\omega, 1),\ (-3, -2+\omega),$$
$$(7-2\omega, 11-3\omega),\ (1+\omega, -9+2\omega),\ (-8+\omega, -2+\omega).$$

4.1.1 Number field associated with equation (3.7)

Let $F(X,Y)$ be the left hand side of (3.7), θ a root of the polynomial $F(X,1)$ and let $L=\mathbb{Q}(\theta)$. Then $k\subset L$, $[L:\mathbb{Q}]=6$ and $\mathcal{O}_L=\mathbb{Z}[\xi]$,where $\xi=(12+18\theta-4\theta^3-\theta^4)/20$. In particular, $\theta=4\xi-5\xi^2-4\xi^3+4\xi^4+\xi^5$ and $\sqrt{37}=3-12\xi-8\xi^2+8\xi^3+2\xi^4$. The extension $L/\mathbb{Q}$ is Galois with Galois group $\langle\sigma,\tau\rangle$, where σ and τ are given by

$$\begin{aligned}\sigma(\xi)&=-14-6\xi+49\xi^2+9\xi^3-28\xi^4-6\xi^5,\\ \tau(\xi)&=-1-3\xi+5\xi^2+4\xi^3-4\xi^4-\xi^5,\end{aligned}$$

and they satisfy $\sigma^3=1,\tau^2=1$ and $\sigma\tau=\tau\sigma^2$. Thus $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to the symmetric group of degree 3. The conjugates of ξ in L are numbered as follows:

$$\begin{array}{rcrcl}\xi^{(1)}&=&\xi&=&-4.6017164\ldots,\\ \xi^{(2)}&=&\sigma(\xi)&=&-0.5284180\ldots,\\ \xi^{(3)}&=&\sigma^2(\xi)&=&-0.4112467\ldots,\\ \xi^{(4)}&=&\tau(\xi)&=&-1.2776453\ldots,\\ \xi^{(5)}&=&\tau\sigma(\xi)&=&0.6985045\ldots,\\ \xi^{(6)}&=&\tau\sigma^2(\xi)&=&1.1205221\ldots.\end{array}$$

The conjugates of θ are numbered in accordance with the numbering of the conjugates of ξ. A system of fundamental units of L is given by

$$\begin{aligned}\varepsilon_1&=-\xi,\\ \varepsilon_2&=-5-4\xi+18\xi^2+5\xi^3-9\xi^4-2\xi^5,\\ \varepsilon_3&=-6-8\xi+23\xi^2+9\xi^3-13\xi^4-3\xi^5,\\ \varepsilon_4&=1+3\xi-5\xi^2-4\xi^3+4\xi^4+\xi^5,\\ \varepsilon_5&=-16-15\xi+63\xi^2+18\xi^3-36\xi^4-8\xi^5.\end{aligned}$$

The actions of σ and τ on the units are as follows:

$$\sigma(\varepsilon_i)=\begin{cases}\varepsilon_3^{-1} & \text{if } i=1,\\ \varepsilon_4^{-1} & \text{if } i=2,\\ \varepsilon_1\varepsilon_3^{-1} & \text{if } i=3,\\ \varepsilon_2\varepsilon_4^{-1} & \text{if } i=4,\\ \varepsilon_1\varepsilon_2^{-1}\varepsilon_3^{-1}\varepsilon_4\varepsilon_5 & \text{if } i=5,\end{cases}\qquad \tau(\varepsilon_i)=\begin{cases}\varepsilon_4 & \text{if } i=1,\\ \varepsilon_3 & \text{if } i=2,\\ \varepsilon_2 & \text{if } i=3,\\ \varepsilon_1 & \text{if } i=4,\\ -\varepsilon_1^{-1}\varepsilon_2\varepsilon_3\varepsilon_4^{-1}\varepsilon_5^{-1} & \text{if } i=5.\end{cases}$$

We see that $N_{L/k}(\varepsilon_i)=1$ $(i=1,2,3,4)$ and $N_{L/k}(\varepsilon_5)=\varepsilon_1\varepsilon_2^{-1}\varepsilon_3^{-2}\varepsilon_4^2\varepsilon_5^3=\varepsilon$.

4.1.2 An upper bound for the solutions

Since (3.7) is equivalent to $N_{L/k}(X - Y\theta) = 1$, we have $\eta := X - Y\theta = \varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\varepsilon_4^{a_4}$ for some $a_1, a_2, a_3, a_4 \in \mathbb{Z}$. Eliminating X, Y we obtain

$$\big(\sigma(\theta) - \sigma^2(\theta)\big)\eta + \big(\sigma^2(\theta) - \theta\big)\sigma(\eta) + \big(\theta - \sigma(\theta)\big)\sigma^2(\eta) = 0,$$

hence

$$\frac{\theta - \sigma^2(\theta)}{\theta - \sigma(\theta)} \cdot \frac{\sigma(\eta)}{\sigma^2(\eta)} - 1 = -\frac{\sigma(\theta) - \sigma^2(\theta)}{\sigma(\theta) - \theta} \cdot \frac{\eta}{\sigma^2(\eta)},$$

or equivalently

$$-\varepsilon_1^{b_1}\varepsilon_2^{b_2}\varepsilon_3^{b_3}\varepsilon_4^{b_4} - 1 = \varepsilon_1^{d_1}\varepsilon_2^{d_2}\varepsilon_3^{d_3}\varepsilon_4^{d_4}, \tag{4.1}$$

where

$$b_1 = a_1 + 2a_3, \quad b_2 = a_2 + 2a_4 - 1, \quad b_3 = -2a_1 - a_3 + 1, \quad b_4 = -2a_2 - a_4,$$
$$d_1 = -b_3, \quad d_2 = -b_4, \quad d_3 = b_1 + b_3, \quad d_4 = b_2 + b_4.$$

As in [19], [43], [47] or [48], we estimate linear forms in the logarithms

$$\Lambda_i = \sum_{j=1}^{4} b_j \log|\varepsilon_j^{(i)}| = \begin{cases} \log\left|\dfrac{\theta^{(i)} - \sigma^2(\theta^{(i)})}{\theta^{(i)} - \sigma(\theta^{(i)})} \cdot \dfrac{\sigma(\eta^{(i)})}{\sigma^2(\eta^{(i)})}\right| & (1 \le i \le 3), \\ \log\left|\dfrac{\theta^{(i)} - \sigma(\theta^{(i)})}{\theta^{(i)} - \sigma^2(\theta^{(i)})} \cdot \dfrac{\sigma^2(\eta^{(i)})}{\sigma(\eta^{(i)})}\right| & (4 \le i \le 6). \end{cases}$$

Put

$$T = \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \\ -2 & 0 & -1 & 0 \\ 0 & -2 & 0 & -1 \end{bmatrix}, \quad \mathbf{a} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}, \quad \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}, \quad \mathbf{c} = \begin{bmatrix} 0 \\ -1 \\ 1 \\ 0 \end{bmatrix}.$$

Then $\mathbf{b} = T\mathbf{a} + \mathbf{c}$. For $I = \{h_1, h_2, h_3, h_4\} \subset \{1, 2, 3, 4, 5, 6\}$, put

$$U_I = \begin{bmatrix} \log|\varepsilon_1^{(h_1)}| & \dots & \log|\varepsilon_4^{(h_1)}| \\ \vdots & & \vdots \\ \log|\varepsilon_1^{(h_4)}| & \dots & \log|\varepsilon_4^{(h_4)}| \end{bmatrix}.$$

If U_I is invertible, then

$$\mathbf{b} = \mathbf{c} + U_I^{-1} \begin{bmatrix} \pm(\log|\sigma(\eta^{(h_1)})| - \log|\sigma^2(\eta^{(h_1)})|) \\ \dots \\ \pm(\log|\sigma(\eta^{(h_4)})| - \log|\sigma^2(\eta^{(h_4)})|) \end{bmatrix}.$$

Let $i_1 \in \{1, \dots, 6\}$ such that $\max\limits_{1 \le i \le 6}\big|\log|\eta^{(i)}|\big| = \big|\log|\eta^{(i_1)}|\big|$. Then

$$B := \max\big\{|b_1|, |b_2|, |b_3|, |b_4|\big\} \le 1 + 2N[U_I^{-1}]\big|\log|\eta^{(i_1)}|\big|.$$

Here, for a matrix $A = [a_{ij}]_{1\le i,j\le n}$, we put $N[A] := \max_{1\le i\le n} \sum_{j=1}^{n} |a_{ij}|$. We claim that $\det U_I \neq 0$ is equivalent to $\#(I \cap \{1,2,3\}) = \#(I \cap \{4,5,6\}) = 2$. In fact, if this is the case, $|\det(U_I)| = 2.7633\ldots$; if $\{h_1, h_2, h_3\} = \{1,2,3\}$ or $\{4,5,6\}$, then, since $N_{k/\mathbb{Q}}(\varepsilon_i) = 1$ $(i = 1,2,3,4)$ the row vectors $\mathbf{u}_j = \left[\log|\varepsilon_1^{(h_j)}|, \log|\varepsilon_2^{(h_j)}|, \log|\varepsilon_3^{(h_j)}|, \log|\varepsilon_4^{(h_j)}|\right]$ $(j = 1,2,3)$ of U_I satisfy $\mathbf{u}_1 + \mathbf{u}_2 + \mathbf{u}_3 = 0$, whence $\det U_I = 0$. Since

$$N[U_I^{-1}] = \begin{cases} 1.5178097\ldots & \text{if } I = \{1,2,4,6\}, \\ 1.6686180\ldots & \text{if } I = \{1,2,4,5\}, \{2,3,5,6\} \text{ or } \{1,3,4,6\}, \\ 1.7370728\ldots & \text{if } I = \{1,3,5,6\} \text{ or } \{2,3,4,5\}, \\ 1.8160123\ldots & \text{if } I = \{1,3,4,5\} \text{ or } \{2,3,4,6\}, \end{cases}$$

taking $I = \{1,2,4,6\}$ yields $B < 1 + 3.0357\left|\log|\eta^{(i_1)}|\right|$. Hence either

$$|\eta^{(i_1)}| > \exp\left(\frac{B-1}{3.0357}\right)$$

or

$$|\eta^{(i_1)}| < \exp\left(-\frac{B-1}{3.0357}\right)$$

holds. Let $i_0 \in \{1,\ldots,6\}$ such that $|\eta^{(i_0)}| = \min_{1\le i\le 6} |\eta^{(i)}|$. If $B \ge 100$ then

$$|\eta^{(i_0)}| < \exp(-0.16305B). \tag{4.2}$$

In fact, if this is false, then

$$\exp\left(\frac{B-1}{3.0357}\right) < |\eta^{(i_1)}| = \frac{1}{|\sigma(\eta^{(i_1)})||\sigma^2(\eta^{(i_1)})|} \le |\eta^{(i_0)}|^{-2} \le \exp(0.32610B),$$

which implies $B < 99.5$, or

$$\exp\left(-\frac{B-1}{3.0357}\right) > |\eta^{(i_1)}| \ge |\eta^{(i_0)}| \ge \exp(-0.16305B),$$

which implies $B < 2$. Similarly, if $B \ge 50$ then

$$|\eta^{(i_0)}| < \exp(-0.16141B). \tag{4.3}$$

Let

$$\alpha_{i_0} = \frac{\theta^{(i_0)} - \sigma^2(\theta^{(i_0)})}{\theta^{(i_0)} - \sigma(\theta^{(i_0)})} \cdot \frac{\sigma(\eta^{(i_0)})}{\sigma^2(\eta^{(i_0)})}.$$

We claim that $\alpha_{i_0} > 0$ provided $B \ge 50$. To prove this, we show that either

$$\alpha_{i_0} - 1 = -\frac{\sigma(\theta^{(i_0)}) - \sigma^2(\theta^{(i_0)})}{\sigma(\theta^{(i_0)}) - \theta^{(i_0)}} \cdot \frac{\eta^{(i_0)}}{\sigma^2(\eta^{(i_0)})},$$

or

$$\alpha_{i_0}^{-1} - 1 = -\frac{\sigma^2(\theta^{(i_0)}) - \sigma(\theta^{(i_0)})}{\sigma^2(\theta^{(i_0)}) - \theta^{(i_0)}} \cdot \frac{\eta^{(i_0)}}{\sigma(\eta^{(i_0)})}.$$

is extremely small. From the minimality of i_0, we have

$$\max\bigl\{|\sigma(\eta^{(i_0)})|, |\sigma^2(\eta^{(i_0)})|\bigr\} \geq |\sigma(\eta^{(i_0)})|^{1/2} |\sigma^2(\eta^{(i_0)})|^{1/2} = |\eta^{(i_0)}|^{-1/2},$$

thus

$$\begin{aligned} &\min\bigl\{|\alpha_{i_0} - 1|, |\alpha_{i_0}^{-1} - 1|\bigr\} \\ &\leq \max_i \max \left\{ \frac{\sigma(\theta^{(i)}) - \sigma^2(\theta^{(i)})}{\sigma(\theta^{(i)}) - \theta^{(i)}}, \frac{\sigma^2(\theta^{(i)}) - \sigma(\theta^{(i)})}{\sigma^2(\theta^{(i)}) - \theta^{(i)}} \right\} |\eta^{(i_0)}|^{3/2} \\ &< 4.1068\, |\eta^{(i_0)}|^{3/2}. \end{aligned}$$

Combining this, (4.2) and (4.3), we obtain

$$\min\bigl\{|\alpha_{i_0} - 1|, |\alpha_{i_0}^{-1} - 1|\bigr\} \leq \begin{cases} 4.1068 \exp(-0.24457B) < 9.82 \times 10^{-11} & \text{if } B \geq 100, \\ 4.1068 \exp(-0.24211B) < 2.28 \times 10^{-5} & \text{if } B \geq 50, \end{cases}$$

as claimed. We therefore have $\alpha_{i_0} = \exp(\pm \Lambda_{i_0})$ and

$$\begin{aligned} &\min\bigl\{|\exp(\Lambda_{i_0}) - 1|, |\exp(-\Lambda_{i_0}) - 1|\bigr\} \\ &\qquad < \begin{cases} 4.1068 \exp(-0.24457B) < 9.82 \times 10^{-11} & \text{if } B \geq 100, \\ 4.1068 \exp(-0.24211B) < 2.28 \times 10^{-5} & \text{if } B \geq 50. \end{cases} \end{aligned}$$

Lemma 4.2. *Let C_1, C_2, B and B_0 be given positive numbers. If*

$$\min\bigl\{|e^x - 1|, |e^{-x} - 1|\bigr\} < C_1 \exp(-C_2 B), \quad B \geq B_0,$$

then $|x| < aC_1 \exp(-C_2 B)/(1 - \exp(-a))$, where $a = -\log(1 - C_1 \exp(-C_2 B_0))$ (> 0).

Hence we find that

$$|\Lambda_{i_0}| < 4.1069 \exp(-0.24457B) \quad \text{if } B \geq 100, \tag{4.4}$$

$$|\Lambda_{i_0}| < 4.1069 \exp(-0.24211B) \quad \text{if } B \geq 50. \tag{4.5}$$

To obtain a lower bound for $|\Lambda_{i_0}|$, we use the main result of Baker-Wüstholz [1]:

Lemma 4.3. *Let $\alpha_1, \ldots \alpha_n$ be nonzero algebraic number and $b_1, \ldots, b_n$ rational integers, not all 0. Also let $d = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$, $h'(\alpha_i) = \max\bigl\{h(\alpha_i), |\log \alpha_i|/d, 1/d\bigr\}$, where $h(\alpha_i)$ is the absolute logarithmic height of α_i and* log *is a fixed determination of the logarithm. If $\Lambda := b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n \neq 0$ and $B := \max\bigl\{|b_1|, \ldots, |b_n|\bigr\} \geq 3$, then*

$$\log |\Lambda| > -C(n, d) h'(\alpha_1) \ldots h'(\alpha_n) \log B,$$

where $C(n, d) = 18(n + 1)!\, n^{n+1} (32d)^{n+2} \log(2nd)$.

Note that $\Lambda_i \neq 0$; otherwise $b_1 = \cdots = b_4 = 0$, whence $a_1 = 2/3$, a contradiction. Thus we can apply Lemma 4.3 with $\alpha_i = |\varepsilon_j^{(i)}|$. As explained in [47], § 3.2, we may suppose that $i_0 = 1$. In our case, $d = [\mathbb{Q}(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) : \mathbb{Q}] = 6$, since $\mathbb{Q}(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) = L$. Since $\varepsilon_4 = \varepsilon_1^{(4)}$, $\varepsilon_2 = 1/\varepsilon_1^{(5)}$ and $\varepsilon_3 = 1/\varepsilon_1^{(2)}$, and ε_1 is a root of $x^6 - 5x^5 + 9x^3 - 2x^2 - 3x + 1$, we see that $h(\varepsilon_i) = 0.314207\ldots$ for $i = 1, 2, 3, 4$. Since $1/d = 0.166\ldots$ and

$$\frac{\left|\log|\varepsilon^{(i)}|\right|}{d} = \begin{cases} 0.22544\ldots & \text{if } i = 1, \\ 0.05980\ldots & \text{if } i = 2, \\ 0.10631\ldots & \text{if } i = 3, \\ 0.04083\ldots & \text{if } i = 4, \end{cases}$$

we see that $h'(\varepsilon_i) = 0.314207\cdots < 0.31421$ $(i = 1, 2, 3, 4)$. Hence by Lemma 4.3, we find

$$\log|\Lambda_1| > -4.1810 \times 10^{18} \log(B). \tag{4.6}$$

Combining (4.4) and (4.6) we have $B \leq 1.5142 \times 10^{21}$.

4.1.3 Reduction of the upper bound

We reduce the large upper bound obtained above to the manageable one. To do this, we use the the following lemma (Proposition 3.1 of [43]).

Lemma 4.4. *Let $\mu_1, \ldots, \mu_n$ be given real numbers. Let $b_1, \ldots, b_n \in \mathbb{Z}$ and let $\Lambda = \sum_{i=1}^{n} b_i\mu_i$. Let K_1, K_2, K_3 be given positive numbers. Let $b_1, \ldots, b_n$ be solutions of*

$$|\Lambda| < K_1 \exp(-K_2 B), \quad B := \max\bigl\{|b_1|, \ldots, |b_n|\bigr\} < K_3. \tag{4.7}$$

For a sufficiently large real number c_0, consider the lattice Γ generated by the columns of the matrix

$$\mathcal{A} = \begin{bmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \\ [c_0\mu_1] & \ldots & [c_0\mu_{n-1}] & [c_0\mu_n] \end{bmatrix},$$

where

$$[x] = \begin{cases} \lfloor x \rfloor & \text{if } x \geq 0, \\ \lceil x \rceil & \text{if } x < 0, \end{cases}$$

in other words, $[\cdot]$ means rounding off towards zero. Let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be the LLL-reduced basis of Γ. If $|\mathbf{b}_1| > \sqrt{(n^2 + n - 1)2^{n-1}}K_3$, then every solution of (4.7) satisfies

$$B < \frac{\log(c_0 K_1) - \log(\sqrt{2^{1-n}|\mathbf{b}_1|^2 - (n-1)K_3^2} - nK_3)}{K_2}.$$

In our case, $n = 4$, $K_1 = 4.1069$, $K_2 = 0.24457$ and $K_3 = 1.5142 \times 10^{21}$. Take $c_0 = 10^{100}$. Applying LLL-reduction algorithm using PARI/GP to the matrix $\mathcal{A}$, we get

$$\mathcal{B} = \big[\mathbf{b}_1\ \mathbf{b}_2\ \mathbf{b}_3\ \mathbf{b}_4\big],$$

where

$$\mathbf{b}_1 = \begin{bmatrix} 525766899856084740716174 \\ 384638986832445610427342 7 \\ -124418666451172811371813 1 \\ -395108746616005504770747 \end{bmatrix},\ \mathbf{b}_2 = \begin{bmatrix} -358052285081368813529910 4 \\ -341447815688279270973156 \\ 172781386077326034251467 5 \\ 324672105193753478335587 3 \end{bmatrix},$$

$$\mathbf{b}_3 = \begin{bmatrix} 407267427999956449527312 7 \\ 269244207052729576352184 4 \\ 782025387667325633997448 6 \\ -285101950383064823043109 4 \end{bmatrix},\ \mathbf{b}_4 = \begin{bmatrix} -782540284530375014759499 4 \\ -154731239896422989358345 9 \\ -529196120215387679117837 \\ -106205987118553569141892 51 \end{bmatrix}.$$

Since $|\mathbf{b}_1| = 4.096 \cdots \times 10^{24} > \sqrt{(n^2+n-1)2^{n-1}}K_3 = 1.866 \times 10^{22}$, Lemma 4.4 implies that a new upper bound K_3 for B is 719.

Take $c_0 = 10^{18}$. We again apply LLL-reduction to $\mathcal{A}$. Then

$$\mathcal{B} = \begin{bmatrix} -291 & -1300 & 23101 & 13586 \\ 2046 & 2852 & 6305 & -24467 \\ 19892 & 7913 & 5062 & -1315 \\ 285 & -18603 & -7284 & -5310 \end{bmatrix}.$$

Since $|\mathbf{b}_1| = 2.000 \cdots \times 10^4 > \sqrt{(n^2+n-1)2^{n-1}}K_3 = 8.874 \times 10^3$, we obtain $B \le 141$.

4.1.4 Completion of the proof

We search the range $B \le 141$ for solutions of (4.1). First consider the case $100 \le B \le 141$ or $50 \le B < 100$. In these cases, it is enough to find the solutions of (4.4) or (4.5), respectively. Note that, since $|\Lambda_1|/\big|\log|\varepsilon_4|\big| < 0.5$ provided $B \ge 50$, the value of $b_4 \in \mathbb{Z}$ is determined uniquely by b_1, b_2 and b_3. Hence for $100 \le B \le 141$ (resp. $50 \le B < 100$), there are $(2{\cdot}141{+}1)^3 - (2{\cdot}99{+}1)^3 \approx 1.5 \times 10^7$ possibilities (resp. $(2{\cdot}99{+}1)^3 - (2{\cdot}49{+}1)^3 \approx 6.9 \times 10^6$ possibilities) to be checked. No solutions of (4.4) are found, and 14 solutions of (4.5) are found, none of which give integral (a_1, a_2, a_3, a_4). If $B < 50$, we check about 10^8 possibilities directly to be the solutions of (4.1). From this, we find 39 solutions, 21 of which give integral (a_1, a_2, a_3, a_4). The search took less than 15 minutes on Sparc station SS4 with a C-program. For each (a_1, a_2, a_3, a_4), we see with KASH that the unit $\varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\varepsilon_4^{a_4}$ is of the form $X - Y\theta$. We list the solutions in Table 4.1.

a_1	a_2	a_3	a_4	b_1	b_2	b_3	b_4	X	Y
-3	-4	-1	5	-5	5	8	3	$-2-9\omega$	$22-4\omega$
0	4	4	0	8	3	-3	-8	$-23-8\omega$	$-4+8\omega$
5	-1	-4	-3	-3	-8	-5	5	$25+17\omega$	$-18-4\omega$
4	-1	-4	1	-4	0	-3	1	$21+8\omega$	$-8-3\omega$
-3	0	0	1	-3	1	7	-1	$-9-3\omega$	$1+\omega$
1	0	3	0	7	-1	-4	0	$-12-5\omega$	$7+2\omega$
3	-3	-3	3	-3	2	-2	3	$9+2\omega$	$1-2\omega$
-2	2	0	1	-2	3	5	-5	$-3-\omega$	$-2+\omega$
1	0	2	-2	5	-5	-3	2	$-6-\omega$	$1+\omega$
2	0	-2	1	-2	1	-1	-1	$-5-2\omega$	$1+\omega$
-1	0	0	0	-1	-1	3	0	$1+\omega$	-1
1	-1	1	1	3	0	-2	1	$4+\omega$	$-\omega$
1	0	-1	1	-1	1	0	-1	$-2-\omega$	2
0	0	0	0	0	-1	1	0	1	0
1	-1	0	1	1	0	-1	1	$1+\omega$	-2
1	1	-1	1	-1	2	0	-3	$3+\omega$	$1-\omega$
0	0	0	-1	0	-3	1	1	$-\omega$	1
1	-2	0	2	1	1	-1	2	-3	$-2+\omega$
1	-4	-1	4	-1	3	0	4	$7-2\omega$	$11-3\omega$
0	3	0	1	0	4	1	-7	$1+\omega$	$-9+2\omega$
1	0	0	-3	1	-7	-1	3	$-8+\omega$	$-2+\omega$

Table 4.1: The solutions of (3.7) and (4.1)

4.2 Squares in Lucas sequences and some diophantine equations

Let $k = \mathbb{Q}(\sqrt{37})$. In section 3.4, we needed to know when $\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon^n)$ is a square in $\mathbb{Z}$ (Lemma 3.16). In this section, we investigate the following problem which is related to the above one.

Let t be an even rational integer. The sequences $\{v_n\}$, $\{u_n\}$ are defined by

$$\begin{cases} v_0 = 1, & v_1 = t, & v_{n+2} = 2tv_{n+1} + v_n, \\ u_0 = 0, & u_1 = 1, & u_{n+2} = 2tu_{n+1} + u_n. \end{cases} \tag{4.8}$$

Problem. When is v_n, $2v_n$, u_n or $2u_n$ a square ?

Our result is as follows:

Theorem 4.5. *Let $t > 2$ be an even integer such that $\mathrm{ord}_p(t)$ is odd for $p = 3, 5$ or 7. Define the sequences $\{v_n\}, \{u_n\}$ by (4.8).*

(1) *The equation $v_n = 2x^2$ $(n, x \in \mathbb{Z})$ has no solutions unless $t = 6$, $D = 37$, when the only solution is $n = 3$, $x = \pm 21$.*

(2) *The equation $v_n = x^2$ $(n, x \in \mathbb{Z}, 2 \not| \ n)$ has no solutions.*

(3) *The equation $u_n = 2x^2$ $(n, x \in \mathbb{Z})$ has only the solution $n = x = 0$.*

(4) *The equation $u_n = x^2$ $(n, x \in \mathbb{Z}, 2 \mid n)$ has only the solution $n = x = 0$.*

Though Cohn ([5], [6]), Ribenboim and McDaniel ([29]), and others investigate the problem of similar types, our result is not covered by theirs.

4.2.1 Preliminaries

We easily find from (4.8) that

$$v_n \text{ is even } \iff n \text{ is odd}, \quad u_n \text{ is even } \iff n \text{ is even}.$$

We also have the following relations:

$$v_n^2 - Du_n^2 = (-1)^n, \quad v_{-n} = (-1)^n v_n, \quad u_{-n} = (-1)^{n+1} u_n, \tag{4.9}$$

$$v_{m+n} = v_m v_n + Du_m u_n, \quad u_{m+n} = v_m u_n + v_n u_m, \tag{4.10}$$

$$v_{2n} = 2v_n^2 + (-1)^{n+1}, \quad u_{2n} = 2v_n u_n, \tag{4.11}$$

$$\begin{cases} v_{3n} = v_n(4v_n^2 + 3(-1)^{n+1}), \\ u_{3n} = u_n(4v_n^2 + (-1)^{n+1}), \end{cases} \tag{4.12}$$

$$\begin{cases} v_{5n} = v_n\{16v_n^4 + (-1)^{n+1}20v_n^2 + 5\}, \\ u_{5n} = u_n\{16v_n^4 + (-1)^{n+1}12v_n^2 + 1\}, \end{cases} \tag{4.13}$$

$$\begin{cases} v_{7n} = v_n\{64v_n^6 + (-1)^{n+1}112v_n^4 + 56v_n^2 + (-1)^{n+1} \cdot 7\}, \\ u_{7n} = u_n\{64v_n^6 + (-1)^{n+1}80v_n^4 + 24v_n^2 + (-1)^{n+1}\}. \end{cases} \tag{4.14}$$

It is clear from (4.8) that if $n > 0$, then v_n, $u_n > 0$. Thus from (4.9) if $n < 0$, then

$$v_n > 0 \iff n \text{ is even}, \qquad u_n > 0 \iff n \text{ is odd}.$$

We need the following diophantine lemmas which will be used in the proof of the theorem.

Lemma 4.6 (Ljunggren [24])**.** *The only $x, y \in \mathbb{Z}$ satisfying*

$$x^2 - 3y^4 = 1$$

are $(|x|, |y|) = (1, 0), (2, 1), (7, 2)$.

Lemma 4.7. *The only $x, y \in \mathbb{Z}$ satisfying*

$$x^2 - Dy^4 = 1 \quad (D = 12, 111, 444)$$

are $(|x|, |y|) = (1, 0)$.

Proof. See Cohn [7]. □

4.2.2 Proof of Theorem 4.5

(1) Let $v_n = 2x^2$ $(n, x \in \mathbb{Z})$. Since v_n is even, we see that n is odd. Thus if $n < 0$, then $v_n < 0$. Hence we may suppose that $n > 0$.

The proof is divided into two cases: $n \equiv 0 \pmod{p}$ and $n \not\equiv 0 \pmod{p}$ with $p = 3, 5$ or 7.

Case 1: $n \equiv 0 \pmod{p}$. Then let $n = pk$. Note that k is odd.

(i) If $p = 3$, then from (4.12) we have $v_{3k} = v_k(4v_k^2 + 3) = 2x^2$. Since k is odd and $t \equiv 0 \pmod 3$, we see from (4.8) that $v_k \equiv 0 \pmod 3$, whence $\gcd(v_k, 4v_k^2 + 3) = 3$. Thus we have

$$v_k = 2 \cdot 3x_1^2 \text{ and } 4v_k^2 + 3 = 3x_2^2, \quad x_1, x_2 \in \mathbb{N},$$

thus

$$3(2x_1)^4 + 1 = x_2^2.$$

It follows from Lemma 4.6 that $x_1 = 1, x_2 = 7, v_k = 6$. Hence from (4.9) we obtain $D = 37, t = 6, k = 1, n = 3$.

(ii) If $p = 5$, then from (4.13) we have $v_{5k} = v_k(16v_k^4 + 20v_k^2 + 5) = 2x^2$. Since k is odd and $t \equiv 0 \pmod 5$, we see that $\gcd(v_k, 16v_k^4 + 20v_k^2 + 5)$ is 5. Thus we have

$$v_k = 2 \cdot 5x_1^2 \text{ and } 16v_k^4 + 20v_k^2 + 5 = 5x_2^2,$$

thus

$$(2^2 \cdot 5x_1^2)^4 + 5(2^2 \cdot 5x_1^2)^2 + 5 = 5x_2^2.$$

Hence we obtain the elliptic curve

$$E : Y^2 = X^3 + 5^2X^2 + 5^3X$$

with $x_3 = 2^2 \cdot 5x_1^2$, $X = 5x_3^2$, $Y = 5^2x_3x_2$. The substitution $X = X' - 8$, $Y = Y'$ yields the elliptic curve

$$E' : Y'^2 = X'^3 + X'^2 - 83X' + 88,$$

which is the curve 400F1 in Cremona's table [11]. We see that $E'(\mathbb{Q}) = \langle (8, 0) \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Therefore we have $E(\mathbb{Q}) = \{O, (0, 0)\}, x_1 = 0$, hence $v_k = 0$, which contradicts $v_k > 0$.

(iii) If $p = 7$, then we similarly have from (4.14)

$$v_k = 2 \cdot 7x_1^2 \text{ and } 64v_k^6 + 112v_k^4 + 56v_k^2 + 7 = 7x_2^2,$$

so the elliptic curve

$$E : Y^2 = X^3 + 7^2X^2 + 2 \cdot 7^3X + 7^4$$

with $x_3 = (2^2 \cdot 7x_1^2)^2$, $X = 7x_3$, $Y = 7^2x_2$. The substitution $X = X' - 16$, $Y = Y'$ yields

$$E' : Y'^2 = X'^3 + X'^2 - 114X' - 127,$$

which is the curve 196B1 in Cremona's table [11]. We see that $E'(\mathbb{Q}) = \langle (16, 49) \rangle \cong \mathbb{Z}/3\mathbb{Z}$. We therefore have $E(\mathbb{Q}) = \{O, (0, \pm 49)\}$, $x_3 = 0, x_1 = 0$, whence $v_k = 0$, which contradicts $v_k > 0$.

Case 2: $n \not\equiv 0 \pmod p$. Then we can put $n = pk \pm l$, where k is even and l is odd with $1 \leq l < p$.

Now suppose that $d = \mathrm{ord}_p(t)$ is odd. From (4.9) and (4.10), we have $v_{pk \pm l} = \pm v_{pk}v_l + Du_{pk}u_l = 2x^2$. Then the following claim holds:

Claim. (a) $\mathrm{ord}_p(v_l) = d$, $\mathrm{ord}_p(u_l) = 0$.

(b) $\mathrm{ord}_p(v_{pk}) = 0$, $\mathrm{ord}_p(u_{pk}) \geq d+1$.

The claim above implies that $\mathrm{ord}_p(v_{pk\pm l}) = d$, which is impossible, since d is odd and $v_{pk\pm l} = 2x^2$. Thus to prove (1), it suffices to show the claim.

Proof of claim. (a) Since l is odd ($< p \leq 7$), we have $l = 1, 3, 5$. Then $v_1 = t$, $v_3 = t(4t^2+3)$, $v_5 = t(16t^4+20t^2+5)$. These imply that $\mathrm{ord}_p(v_l) = d$ for each l, p with $1 \leq l < p \leq 7$. From $(v_l, u_l) = 1$, we have $\mathrm{ord}_p(u_l) = 0$.

(b) Since k is even, we have $u_k \equiv 0 \pmod{t}$, whence $\mathrm{ord}_p(u_k) \geq d$, $\mathrm{ord}_p(v_k) = 0$. Since $v_{pk} + u_{pk}\sqrt{D} = (v_k + u_k\sqrt{D})^p$, we have

$$u_{pk} = u_k \sum_{j=0}^{(p-1)/2} \binom{p}{2j} v_k^{2j} (u_k^2 D)^{\frac{p-1}{2}-j} := u_k \sum_{j=0}^{(p-1)/2} a_j.$$

Then $\mathrm{ord}_p(u_{pk}) \geq d+1$. Indeed, if $j < (p-1)/2$, then $\mathrm{ord}_p(a_j) \geq d(p-1-2j) > 1$. If $j = (p-1)/2$, then $\mathrm{ord}_p(a_j) = 1$. Thus $\mathrm{ord}_p(\sum_{j=0}^{(p-1)/2} a_j) = 1$. From $(v_{pk}, u_{pk}) = 1$, we have $\mathrm{ord}_p(v_{pk}) = 0$. This completes the proof of the claim and hence of (1).

(2) Let $v_n = x^2$ ($n, x \in \mathbb{Z}$, $2 \nmid n$). Case 1: $n \equiv 0 \pmod{p}$. In the same way as in the proof of Theorem 4.5, we obtain the following, respectively.

(i) If $p = 3$, then we have the equation

$$12x_1^4 + 1 = x_2^2,$$

which has no non-trivial solutions by Lemma 4.7.

(ii) If $p = 5$, then we have the elliptic curve defined by

$$Y^2 = X^3 + 5^2X^2 + 5^3X,$$

which implies $X = 0$, whence $v_k = 0$, as above.

(iii) If $p = 7$, then we have the elliptic curve defined by

$$Y^2 = X^3 + 7^2X^2 + 2 \cdot 7^3X + 7^4,$$

which implies $X = 0$, whence $v_k = 0$, as above.

Case 2: $n \not\equiv 0 \pmod{p}$. Similarly, comparing p-adic values of both sides of $v_n = x^2$ leads to a contradiction.

In order to prove (3), (4), we need the following two propositions:

Proposition 4.8. *If the equation $u_n = x^2$ or $2x^2$ with n even > 0 has any solutions, then we have $D = 37$, $n = 2^e \cdot 3$ with $e \geq 1$.*

Proof. Let $n = 2^e s$, where $e \geq 1$ and s is odd. Then applying (4.11) e times yields

$$u_n = 2v_{n/2}u_{n/2} = 2^2 v_{n/2}v_{n/4}u_{n/4} = \cdots = 2^e \left(\prod_{j=1}^{e} v_{n/2^j} \right) u_s.$$

Since $v_{n/2^j}$ $(1 \leq j \leq e)$, u_s are pairwise relatively prime, we have $v_s = x_1^2$ or $2x_1^2$ $(x_1 \in \mathbb{N})$. By (2), the first equation has no solutions, since s is odd. By (1), the second equation has only the solution $s = 3$, $t = 6$, $D = 37$, $n = 2^e \cdot 3$ with $e \geq 1$. □

Proposition 4.9. *Let $D = 37$ and $n = 2^e \cdot 3$ with $e \geq 1$. Then neither $u_n = x^2$ nor $u_n = 2x^2$ has solutions.*

Proof. Write $n = 3k$, where $k = 2^e$. Then by (4.9) and (4.12), we have $u_{3k} = u_k(4 \cdot 37u_k^2 + 3)$, since k is even. We see that $u_k \equiv 0 \pmod 3$. Otherwise, $u_n = x^2$ or $2x^2$ implies $4 \cdot 37u_k^2 + 3 = x_1^2$ $(x_1 \in \mathbb{N})$, which is found impossible by taking modulo 4. Hence it follows from $u_n = x^2$ that

$$u_k = 3x_1^2, \quad 4 \cdot 37u_k^2 + 3 = 3x_2^2, \quad x_1, x_2 \in \mathbb{N},$$

thus

$$444x_1^4 + 1 = x_2^2,$$

which has no non-trivial solution by Lemma 4.7. It also follows from $u_n = 2x^2$ that

$$u_k = 3 \cdot 2 \cdot x_1^2, \quad 4 \cdot 37u_k^2 + 3 = 3x_2^2, \quad x_1, x_2 \in \mathbb{N},$$

thus

$$111(2x_1)^4 + 1 = x_2^2,$$

which has no non-trivial solutions by Lemma 4.7. □

We now prove (3). Let $u_n = 2x^2$, $x \in \mathbb{Z}$. Since u_n is even, we see that n is even and hence $n \geq 0$. Thus by (4.11), we have

$$v_{n/2} = x_1^2, \quad u_{n/2} = x_2^2 \ (x_1, x_2 \in \mathbb{Z}).$$

If $n/2$ is odd, then the first equation has no solution by (2). If $n/2$ is even, then the second equation has only the solution $n = 0$ by Propositions 4.8, 4.9.

The assertion (4) is clear from Propositions 4.8, 4.9.

4.2.3 Corollaries

Let $t > 2$ be even and $D = t^2+1$. It is easy to see that D is not a square. The fundamental solution of the Pell equation $X^2 - DY^2 = \pm 4$ is $(2t, 2)$, and the general solution (X, Y) is $(X + Y\sqrt{D})/2 = v_n + u_n\sqrt{D}$. Thus rephrasing Theorem 4.5 in terms of Pell's equation and quadratic fields yields the following two corollaries.

Corollary 4.10. *Let t be as in Theorem 4.5 and let $D = t^2 + 1$.*

(1) *The equation $4x^4 - Dy^2 = \pm 1$ in $x, y \in \mathbb{Z}$ has no solutions unless $t = 6, D = 37$, when only the solutions are $x = \pm 21$, $y = \pm 145$.*

(2) *The equation $x^4 - Dy^2 = -1$ in $x, y \in \mathbb{Z}$ has no solutions.*

(3) *The equation $x^2 - 4Dy^4 = \pm 1$ in $x, y \in \mathbb{Z}$ has only the solution $x = \pm 1$, $y = 0$.*

(4) *The equation $x^2 - Dy^4 = 1$ in $x, y \in \mathbb{Z}$ has only the solution $x = \pm 1$, $y = 0$.*

Remark. The curve $4x^4 - 37y^2 = -1$ is birationally equivalent over $\mathbb{Q}$ to the elliptic curve $y^2 = x^3 - 37^2x$, whose Mordell-Weil group is $\langle(-1764/145^2, 32672766/145^3)\rangle \oplus \langle(-37, 0)\rangle \oplus \langle(0, 0)\rangle \cong \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$.

Corollary 4.11. *Let t be as in Theorem 4.5. Assume that $D = t^2+1$ is square-free, and let $k = \mathbb{Q}(\sqrt{D})$. Then the fundamental unit ε of k is $t+\sqrt{D}$. The equation $\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon^n) = x^2$ $(n, x \in \mathbb{Z})$ has no solutions except $t = 6$, $D = 37$, when the only solutions are $n = 3$, $x = \pm 42$.*

Remark. Let D be a square-free integer such that $D \equiv 5 \pmod 8$, $1 < D < 200$. Let ε be a fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{D})$. Then the equation $\mathrm{Tr}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\varepsilon^n) = x^2$ $(x, n \in \mathbb{Z})$ has no solutions except $D = 5$, 13, 37, 69, 77, 85, when the only solutions are the following:

$$(n, x) = \begin{cases} (1,1), (3,2) & \text{if } D = 5, \\ (3,6) & \text{if } D = 13, \\ (3,42) & \text{if } D = 37, \\ (\pm 1, 5) & \text{if } D = 69, \\ (\pm 1, 3) & \text{if } D = 77, \\ (1,3) & \text{if } D = 85. \end{cases}$$

Indeed, if $D \neq 37, 101, 141, 197$, then $\varepsilon = (a + b\sqrt{D})/2$ for some odd a, b, and the assertion follows from Theorem 1 of [5] and Theorem 1 of [6]; if $D = 37, 101$ or 197, the assertion follows from Corollary 4.11. The remaining D is 141. In this case, $\varepsilon = 95 + 8\sqrt{141}$,

$N_{\mathbb{Q}(\sqrt{141})/\mathbb{Q}}(\varepsilon) = 1$. Thus it is sufficient to show that $4x^4 - 141y^2 = 1$ has no solution. But this readily follows by reducing modulo 4.

Table 4.2 below gives all values of $t < 100$ satisfying the condition of Theorem 4.5 and corresponding $D = t^2 + 1$.

t	$D = t^2 + 1$
$6 = 2 \times 3$	37
$10 = 2 \times 5$	101
$12 = 2^2 \times 3$	$145 = 5 \times 29$
$14 = 2 \times 7$	197
$20 = 2^2 \times 5$	401
$24 = 2^3 \times 3$	577
$28 = 2^2 \times 7$	$785 = 5 \times 157$
$30 = 2 \times 3 \times 5$	$901 = 17 \times 53$
$40 = 2^3 \times 5$	1601
$42 = 2 \times 3 \times 7$	$1765 = 5 \times 353$
$48 = 2^4 \times 3$	$2305 = 5 \times 461$
$54 = 2 \times 3^3$	2917
$56 = 2^3 \times 7$	3137
$60 = 2^2 \times 3 \times 5$	$3601 = 13 \times 277$
$66 = 2 \times 3 \times 11$	4357
$70 = 2 \times 5 \times 7$	$4901 = 13^2 \times 29$
$78 = 2 \times 3 \times 13$	$6085 = 5 \times 1217$
$80 = 2^4 \times 5$	$6401 = 37 \times 173$
$84 = 2^2 \times 3 \times 7$	7057
$90 = 2 \times 3^2 \times 5$	8101
$96 = 2^5 \times 3$	$9217 = 13 \times 709$

Table 4.2: $t < 100$ satisfying the condition

Appendix A

Another proof of Proposition 3.5 for $\mathbb{Q}(\sqrt{29})$

In Chapter 3, we determined the elliptic curves with everywhere good reduction over $k = \mathbb{Q}(\sqrt{29})$ (Theorem 3.7 (1)). An important part of the proof is the following proposition (cf. Proposition 3.5):

Proposition A.1. *Let E be an elliptic curve with everywhere good reduction over k with $\Delta(E) \notin k^{\times 3}$. Then E admits a 3-isogeny $f : E \to \bar{E}$ defined over k and either E or $\bar{E}$ has a k-rational point of order 3.*

The proof given in Chapter 3 is heavily relies on computer calculation, in particular, the calculation of the ray class number of $k(\sqrt[3]{\varepsilon}, \sqrt{-3})$ modulo (3). Since 3 is unramified in k, we can apply Lemma 2.9 and we know more about the decomposition of 3 in $k(E[3])$. Using this, we give an algebraic proof of Proposition A.1 in the following.

Let $\varepsilon = (5 + \sqrt{29})/2$. Let E be an elliptic curve with everywhere good reduction over k with $\Delta(E) \notin k^{\times 3}$. By assumption and Lemmas 1.1 and 3.3, we may assume that $\Delta(E) = -\varepsilon^{2n}$, $n \in \mathbb{Z}$, $3 \nmid n$.

We first prove

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

Let $L = k(E[3])$, $G = \mathrm{Gal}(L/k)$. Moreover, we set $F = k(\sqrt{-3})$, $K = k(\sqrt[3]{\Delta(E)}) = k(\alpha) = \mathbb{Q}(\alpha)$ and $M = FK = \mathbb{Q}(\alpha, \sqrt{-3})$, where $\alpha = \sqrt[3]{\varepsilon}$. To prove Proposition A.2, suppose that the assertion is false. Then $G = \mathrm{GL}_2(\mathbb{F}_3)$ by Lemma 2.7.

We quote some results which are proved in [26] or easily deduced from results in the paper.

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

(1) *$\mathcal{O}_N = \mathbb{Z}[\eta]$. The discriminant of N is $-3 \cdot 29$. $\mathcal{O}_K = \mathcal{O}_N[\alpha]$. The discriminant of K is $3^2 29^3$.*

(2) *$h_N = 1$*

(3) *The prime 3 decomposes in N and M as $\mathfrak{p}_3\mathfrak{p}_3'^2$ and $(\mathfrak{P}_3\mathfrak{P}_3'\mathfrak{P}_3'')^2$, respectively, where $\mathfrak{p}_3 = (\eta - 1)$ and $\mathfrak{p}_3' = (\eta + 1)$ are distinct prime ideals of N, and $\mathfrak{P}_3, \mathfrak{P}_3'$ and $\mathfrak{P}_3''$ are distinct prime ideals of M. The primes $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ are inert in K.*

(4) *The prime 29 decomposes in N and K as $\mathfrak{p}_{29}^2\mathfrak{p}_{29}'$ and $(\mathfrak{P}_{29}\mathfrak{P}_{29}')^2$, respectively, where $\mathfrak{p}_{29}$ and $\mathfrak{p}_{29}'$ are distinct prime ideals and $\mathfrak{P}_{29}$ and $\mathfrak{P}_{29}'$ are distinct prime ideals of K.*

(5) *$K = kN$. In particular, the real prime of N is unramified in K.*

(6) *$\eta \mapsto -1$ induces an isomorphism $\mathcal{O}_K/\mathfrak{p}_3' \cong \mathbb{F}_9 = \mathbb{F}_3(\bar{\alpha})$, where $\bar{\alpha} = \alpha + \mathfrak{p}_3'$.*

(7) *M is the Hilbert class field of $\mathbb{Q}(\sqrt{-87})$.*

Let $\mathfrak{p} = 3\mathcal{O}_k$. Assume first that E has ordinary reduction at $\mathfrak{p}$. Then, Lemma 2.9 and Lemma A.3 (3) imply that the ramification index of $\mathfrak{p}$ in L/k is 2. It follows from Lemma A.3 (3) and (7) that L/M is an unramified extension of degree 8, which assertion contradicts the fact that M is the maximal unramified extension of $\mathbb{Q}(\sqrt{-87})$ (see [49]).

Suppose next that E has supersingular reduction at $\mathfrak{p}$. Then by Lemma 2.9, the inertia group in L/k of a prime ideal of L 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 $\tau = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$, $g = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Let $\mathfrak{P}$ be a prime ideal of L dividing $\mathfrak{p}$ with inertia group $\langle\tau\rangle$. By Lemma A.3 (3), we must have $\mathfrak{P} \cap K = \mathfrak{p}_3$ and the fixed field of L 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 A.4. *$h_K(\mathfrak{p}_3'\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)})$ is odd.*

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

$$K_{\mathfrak{m}} = \big\{x \in K^\times \;\big|\; (x, \mathfrak{m}) = 1\big\}, \quad K_{\mathfrak{m},1} = \big\{x \in K_{\mathfrak{m}} \;\big|\; x \equiv 1 \pmod{\mathfrak{m}}\big\}.$$

The following three units generate the group $K_{\mathfrak{m}}/K_{\mathfrak{m},1} \cong (\mathcal{O}_K/\mathfrak{p}_3')^\times \times \langle -1\rangle \times \langle -1\rangle$:

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

In fact, $u_1 \equiv \alpha$, $u_2 \equiv u_3 \equiv 1 \pmod{\mathfrak{p}_3'}$ by Lemma A.3 (6), and

$$u_1^{(1)} = \quad 3.124\ldots\ , \quad u_1^{(2)} = \quad 0.815\ldots\ ,$$

$$u_2^{(1)} = \quad 0.554\ldots\ , \quad u_2^{(2)} = -0.708\ldots\ ,$$
$$u_3^{(1)} = -1.411\ldots\ , \quad u_3^{(2)} = \quad 1.804\ldots\ ,$$

where $^{(i)}$ $(i = 1, 2)$ means the conjugacy corresponding to $\mathfrak{p}_\infty^{(i)}$. Hence, it follows from the formula for the ray class number ([23], p. 127) that $h_K(\mathfrak{m}) = h_K$. Thus it is enough to prove that h_K is odd. Let F be as in Lemma A.3. By Lemma A.3 (3), (4) and (5), the only prime of F ramifying in K is $\mathfrak{p}'_{29}$. Hence h_K is odd by Lemma A.3 (2) above and Theorem 10.4 (a) of [46]. □

Remark. Using KASH, we see that $h_K = h_K(\mathfrak{p}'_3\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}) = 1$.

Again we have a contradiction. This completes the proof of Proposition A.2.

What is remaining to prove Proposition A.1 is that either E or the 3-isogenous curve has a k-rational point of order 3. This assertion is a special case of the following result.

Lemma A.5. *Let k be a real quadratic field with narrow class number 1 and let p be a prime number which is inert in k. Then for semistable elliptic curves $E, \bar{E}$ defined over k which are p-isogenous over k, either E or $\bar{E}$ has a k-rational point of order p.*

Proof. See p. 248 of the paper of Kraus [22]. His proof is similar to that of a result of Serre which states that at least one of a pair of semi-stable p-isogenous curves defined over $\mathbb{Q}$ must have a $\mathbb{Q}$-rational point of order p. □

Remark. The condition of the theorem that p is inert is necessary. In fact if p ramifies, we cannot use Lemma 2.9 which Kraus used to prove Lemma A.5; if p splits in k, the conclusion does not hold in general (for example, our curves 29A1 and 29A1′ are 5-isogenous over $\mathbb{Q}(\sqrt{29})$ but none of the two curves have $\mathbb{Q}(\sqrt{29})$-rational points of order 5).

Hence the proof of Proposition A.1 is complete.

Appendix B

Tables of elliptic curves

So far we have determined the elliptic curves with everywhere good reduction over $k = \mathbb{Q}(\sqrt{m})$ for $m = 6, 7, 14, 29, 33, 37, 41$ and 65. Here we give all these curves and divided them into k-isogeny classes. The columns of the tables give the following data for each curve E:

(1) The code of the form mXi, where m means that the curve is defined over $k = \mathbb{Q}(\sqrt{m})$, X denotes the k-isogeny class, and i is the ordinal number of the curve in its class. When $m = 6, 7, 14, 41, 65$, we also give the code of each curve as given in Comalada's paper [8].

(2) The coefficients a_1, a_2, a_3, a_4 and a_6.

(3) The discriminant of E.

(4) The j-invariant of E.

(5) The structure of the torsion subgroup, in which C_n is a cyclic group of order n.

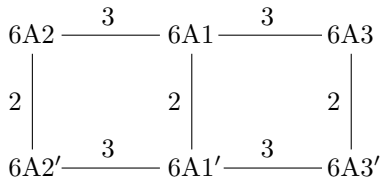
(6) The isogeny graph of related curves. For elliptic curves E and $\bar{E}$ defined over k and a rational prime p, the graph

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

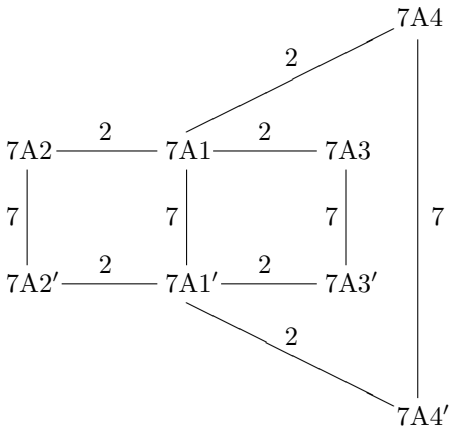
means that E and $\bar{E}$ are p-isogenous over k.

To compute the torsion subgroup, Lemma 3.12 and the main result of [25] were used. To divide into k-isogeny classes, Vélu's formula ([45]) and results concerning $\mathbb{Q}$-curves ([13], [15]) were used.

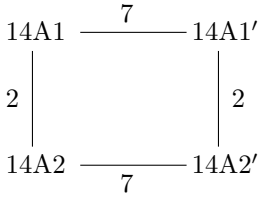
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
6A1 (E_1)	$\sqrt{6}$	$-2-\sqrt{6}$	-1	0	0	ε^3	8000	C_6
6A1′ (E_2)	$-\sqrt{6}$	$-2+\sqrt{6}$	-1	0	0	ε'^3	8000	C_6
6A2 (E_3)	$\sqrt{6}$	$1-\sqrt{6}$	$1+\sqrt{6}$	$9-34\varepsilon$	$-1122-459\sqrt{6}$	ε	$64(4\varepsilon^4+1)^3\varepsilon'^4$	C_2
6A2′ (E_4)	$-\sqrt{6}$	$1+\sqrt{6}$	$1-\sqrt{6}$	$9-34\varepsilon'$	$-1122+459\sqrt{6}$	ε'	$64(4\varepsilon'^4+1)^3\varepsilon^4$	C_2
6A3 (E_5)	$\sqrt{6}$	$2+\varepsilon'$	$3-\sqrt{6}$	$-7+3\sqrt{6}$	0	ε'^5	$64(4\varepsilon^4+1)^3\varepsilon'^4$	C_6
6A3′ (E_6)	$-\sqrt{6}$	$2+\varepsilon$	$3+\sqrt{6}$	$-7-3\sqrt{6}$	0	ε^5	$64(4\varepsilon'^4+1)^3\varepsilon^4$	C_6



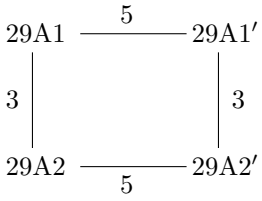
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
7A1 (E_7)	1	4ε	0	ε	0	ε^6	255^3	$C_2\times C_2$
7A1′ (E_8)	1	$4\varepsilon'$	0	ε'	0	ε'^6	255^3	$C_2\times C_2$
7A2 (E_9)	1	4ε	0	$6\varepsilon-80\varepsilon^2$	$-3044+48513\varepsilon$	ε^3	$(256\varepsilon^2+\varepsilon')^3$	C_4
7A2′ (E_{10})	1	$4\varepsilon'$	0	$6\varepsilon'-80\varepsilon'^2$	$-3044+48513\varepsilon'$	ε^{-3}	$(256\varepsilon'^2+\varepsilon)^3$	C_4
7A3 (E_{14})	ε'	$-2\varepsilon'$	0	ε'^2	0	$-\varepsilon'^6$	-15^3	C_4
7A3′ (E_{13})	ε	-2ε	0	ε^2	0	$-\varepsilon^6$	-15^3	C_4
7A4 (E_{12})	1	4ε	0	-4ε	$-\varepsilon^3-2\varepsilon$	ε'^9	$(256\varepsilon'^2+\varepsilon)^3$	C_2
7A4′ (E_{11})	1	$4\varepsilon'$	0	$-4\varepsilon'$	$-\varepsilon'^3-2\varepsilon'$	ε^9	$(256\varepsilon^2+\varepsilon')^3$	C_2



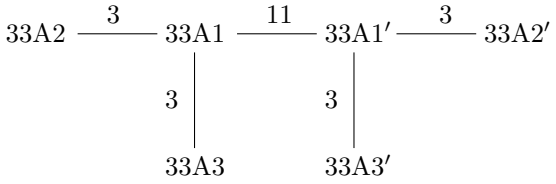
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
14A1 (E_{15})	$1+\sqrt{14}$	$-9-2\sqrt{14}$	0	ε	0	$-\varepsilon^3$	-15^3	C_2
14A1′ (E_{16})	$1-\sqrt{14}$	$-9+2\sqrt{14}$	0	ε'	0	$-\varepsilon'^3$	-15^3	C_2
14A2 (E_{17})	$1+\sqrt{14}$	$-9-2\sqrt{14}$	0	-4ε	$651+174\sqrt{14}$	ε^3	255^3	C_2
14A2′ (E_{18})	$1-\sqrt{14}$	$-9+2\sqrt{14}$	0	$-4\varepsilon'$	$651-174\sqrt{14}$	ε'^3	255^3	C_2



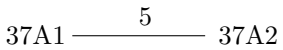
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
29A1	1	0	ε^2	0	0	$-\varepsilon^{10}$	$(5\varepsilon-2)^3\varepsilon'^4$	C_3
29A1′	1	0	ε^{-2}	0	0	$-\varepsilon'^{10}$	$(5\varepsilon'-2)^3\varepsilon^4$	C_3
29A2	1	0	ε^2	$-5\varepsilon^2$	$-(\varepsilon^2+7\varepsilon^4)$	$-\varepsilon^{14}$	$-(1+216\varepsilon^2)^3\varepsilon'^{14}$	1
29A2′	1	0	ε'^2	$-5\varepsilon'^2$	$-(\varepsilon'^2+7\varepsilon'^4)$	$-\varepsilon'^{14}$	$-(1+216\varepsilon'^2)^3\varepsilon^{14}$	1



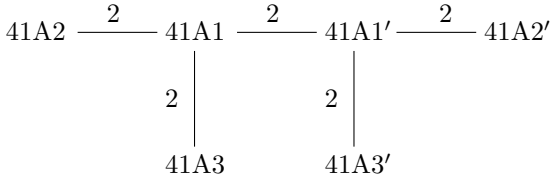
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
33A1	$(\varepsilon-3)/4$	0	ε	0	0	$-\varepsilon^3$	-2^{15}	C_3
33A1′	$(\varepsilon'-3)/4$	0	ε'	0	0	$-\varepsilon'^3$	-2^{15}	C_3
33A2	$(\varepsilon-3)/4$	0	ε	$(5-215\varepsilon)/4$	$34-1563\varepsilon$	$-\varepsilon$	$-(5+\sqrt{33})^3(243\varepsilon-1)^3\varepsilon'$	1
33A2′	$(\varepsilon'-3)/4$	0	ε'	$(5-215\varepsilon')/4$	$34-1563\varepsilon'$	$-\varepsilon'$	$-(5-\sqrt{33})^3(243\varepsilon'-1)^3\varepsilon$	1
33A3	$(\varepsilon-3)/4$	0	ε	$(15\varepsilon-5)/4$	$(127\varepsilon-1)/4$	$-\varepsilon^5$	$-(5-\sqrt{33})^3(243\varepsilon'-1)^3\varepsilon$	1
33A3′	$(\varepsilon'-3)/4$	0	ε'	$(15\varepsilon'-5)/4$	$(127\varepsilon'-1)/4$	$-\varepsilon'^5$	$-(5+\sqrt{33})^3(243\varepsilon-1)^3\varepsilon'$	1



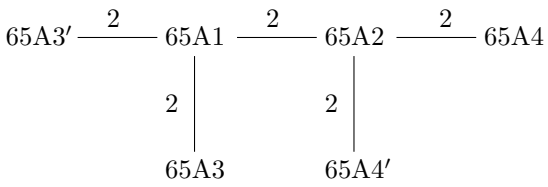
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
37A1	0	$(3\varepsilon+1)/2$	$-\varepsilon$	$(11\varepsilon+1)/2$	0	ε^6	2^{12}	C_5
37A2	0	$(3\varepsilon+1)/2$	$-\varepsilon$	$-(1669\varepsilon+139)/2$	$-7(5449\varepsilon+451)$	ε^6	3376^3	1



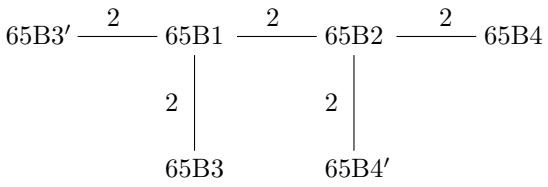
Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
41A1 (E_{23})	1	0	0	$-\varepsilon$	0	ε^4	$-(\varepsilon-16)^3\varepsilon'$	$C_2\times C_2$
41A1′ (E_{24})	1	0	0	$-\varepsilon'$	0	ε'^4	$-(\varepsilon'-16)^3\varepsilon$	$C_2\times C_2$
41A2 (E_{26})	1	$(7-\sqrt{41})/2$	$(7-\sqrt{41})/2$	$6-\sqrt{41}$	0	$-\varepsilon'$	$17^3\varepsilon$	C_4
41A2′ (E_{25})	1	$(7+\sqrt{41})/2$	$(7+\sqrt{41})/2$	$6+\sqrt{41}$	0	$-\varepsilon$	$17^3\varepsilon'$	C_4
41A3 (E_{28})	1	0	0	4ε	ε	$-\varepsilon^5$	$-(256\varepsilon'+1)^3\varepsilon$	C_2
41A3′ (E_{27})	1	0	0	$4\varepsilon'$	ε'	$-\varepsilon'^5$	$-(256\varepsilon+1)^3\varepsilon'$	C_2



Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
65A1 (E_{29})	1	-4ε	0	$-\varepsilon$	0	ε^6	257^3	$C_2 \times C_2$
65A2 (E_{31})	1	2ε	0	ε^2	0	ε^6	17^3	$C_4 \times C_2$
65A3 (E_{38})	1	-4ε	0	4ε	$2\varepsilon - \varepsilon^3$	ε'^3	$(256\varepsilon'^2 - \varepsilon)^3$	C_2
65A3′ (E_{37})	1	$-4\varepsilon'$	0	$4\varepsilon'$	$2\varepsilon' - \varepsilon'^3$	ε^3	$(256\varepsilon^2 - \varepsilon')^3$	C_2
65A4 (E_{35})	1	$-\omega$	ω	$6 + 4\varepsilon$	$-(431 + 53\sqrt{65})/2$	$-5^6\varepsilon^3$	$(8 + \varepsilon')^3$	C_4
65A4′ (E_{36})	1	$-\omega'$	ω'	$6 + 4\varepsilon'$	$-(431 - 53\sqrt{65})/2$	$-5^6\varepsilon'^3$	$(8 + \varepsilon)^3$	C_4



Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors
65B1 (E_{30})	1	$1 - 20\varepsilon$	0	-25ε	0	$(5\varepsilon)^6$	257^3	$C_2 \times C_2$
65B2 (E_{32})	1	$1 + 10\varepsilon$	0	$25\varepsilon^2$	0	$(5\varepsilon)^6$	17^3	$C_2 \times C_2$
65B3 (E_{40})	1	$1 - 20\varepsilon$	0	100ε	$-125(2\varepsilon - \varepsilon^3)$	$-5^6\varepsilon^9$	$(256\varepsilon'^2 - \varepsilon)^3$	C_2
65B3′ (E_{39})	1	$1 - 20\varepsilon'$	0	$100\varepsilon'$	$-125(2\varepsilon' - \varepsilon'^3)$	$-5^6\varepsilon'^9$	$(256\varepsilon^2 - \varepsilon')^3$	C_2
65B4 (E_{33})	1	$1 + \omega$	ω	$7 + \omega$	ω	$-\varepsilon^3$	$(8 + \varepsilon')^3$	C_2
65B4′ (E_{34})	1	$1 + \omega'$	ω'	$7 + \omega'$	ω'	$-\varepsilon'^3$	$(8 + \varepsilon)^3$	C_2



Bibliography

[1] A. Baker and G. Wüstholz, Logarithmic forms and group varieties, *J. Reine angew. Math.* **442** (1993), 19–62.

[2] A. Brumer and K. Kramer, The rank of elliptic curves, *Duke Math. J.* **44** (1977), 715–743.

[3] W. Casselman, On abelian varieties with many endomorphisms, and a conjecture of Shimura's, *Invent. Math.* **12** (1971), 225–236.

[4] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (1977), 223–251.

[5] J. H. E. Cohn, Eight Diophantine equations, *Proc. London Math. Soc.* **16** (1966), 153–166. Addendum, ibid. **17** (1967), 381.

[6] ———, Five Diophantine equations, *Math. Scand.* **21** (1967), 61–70.

[7] ———, The Diophantine equation $y^2 = Dx^4+1$, Ш, *Math. Scand.* **42** (1978), 180–188.

[8] S. Comalada, Elliptic curves with trivial conductor over quadratic fields, *Pacific J. Math.* **144** (1990), 237–258.

[9] I. Connell, Elliptic curve handbook, available from `http://`.

[10] J. E. Cremona, Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction, *Math. Proc. Cambridge Phil. Soc.* **111** (1992), 199–218.

[11] ———, *Algorithms for modular elliptic curves* (2nd ed.), Cambridge Univ. Press, 1997.

[12] P. Deligne et M. Rapoport, Les schémas de modules des courbes elliptiques, in *Modular Functions of One Variable II*, Lecture Notes in Math. no. 349, Springer, 1973, 143–316.

[13] Y. Hasegawa, $\mathbb{Q}$-curves over quadratic fields, *Manuscripta Math.*, to appear.

[14] Y. Hasegawa, K. Hashimoto and F. Momose, Modular conjecture for $\mathbb{Q}$-curves and QM-curves, *preprint.*

[15] K. Hashimoto, $\mathbb{Q}$-curves of degree 5 and jacobian surfaces of GL_2-type, *preprint.*

[16] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, GTM 77, Springer, 1981.

[17] H. Ishii, The non-existence of elliptic curves with everywhere good reduction over certain quadratic fields, *Japan. J. Math.* **12** (1986), 45–52.

[18] N. Katz and B. Mazur, *The Arithmetic Moduli of Elliptic Curves*, Princeton University Press, 1985.

[19] M. Kida, On a characterization of Shimura's elliptic curve over $\mathbb{Q}(\sqrt{37})$, *Acta Arith.* **77** (1996), 157–171.

[20] ———, Reduction of elliptic curves over real quadratic number fields, *preprint.*

[21] A. Kraus, Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique, *Acta Arith.* **54** (1989), 75–80.

[22] ———, Courbes elliptiques semi-stable et corps quadratiques, *J. Number Theory* **60** (1996), 245–253.

[23] S. Lang, *Algebraic Number Theory*, Addison-Wesley, 1970.

[24] W. Ljunggren, Einige Eigenschaften der Einheiten reeller quadratischer und reinbiquadratischer Zahlkörper, *Oslo Vid.-Akad. Skrifter* **1** (1936), Nr. 12.

[25] H. H. Müller, H. Ströher and H. G. Zimmer, Torsion groups of elliptic curves with integral j-invariant over quadratic fields, *J. Reine angew. Math.* **397** (1989), 100–161.

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

[27] R. G. E. Pinch, Elliptic curves over number fields, Ph. D. thesis, Oxford, 1982.

[28] ———, Elliptic curves with good reduction away from 3, *Math. Proc. Cambridge Phil. Soc.* **101** (1987), 451–459.

[29] P. Ribenboim and W. L. McDaniel, The square terms in Lucas sequences, *J. Number Theory* **58** (1996), 104–123.

[30] M. I. Rosen, Some confirming instances of the Birch–Swinnerton-Dyer conjecture over biquadratic fields, in *Number Theory* (R. A. Mollin ed.), Walter de Gruyter, 1990, 493–499.

[31] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **103** (1991), 25–68.

[32] P. Satgé, Groupes de Selmer et corps cubiques, *J. Number Theory* **23** (1986), 294–317.

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

[34] B. Setzer, Elliptic curves over complex quadratic fields, *Pacific J. Math.* **74** (1978), 235–250.

[35] ———, Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invariant, *Illinois J. Math.* **25** (1981), 233–245.

[36] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan, no. 11, Iwanami Shoten, Publishers and Princeton University Press, 1971.

[37] K. Shiota, On the explicit models of Shimura's elliptic curves, *J. Math. Soc. Japan* **38** (1986), 649–659.

[38] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer, 1986.

[39] ———, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer, 1994.

[40] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, UTM, Springer, 1992.

[41] R. J. Stroeker, Reduction of elliptic curves over imaginary quadratic number fields, *Pacific J. Math.* **108** (1983), 451–463.

[42] J. Tate, Algorithm for determining the type of a singular fibre in an elliptic pencil, in *Modular Functions of One Variable IV*, Lecture Notes in Math. no. 476, Springer, 1975, 33–52.

[43] N. Tzanakis and B. M. M. de Weger, On the practical solution of the Thue equation, *J. Number Theory* **31** (1989), 99–132.

[44] A. Umegaki, A construction of everywhere good $\mathbb{Q}$-curves with p-isogeny, *preprint*.

[45] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sc. Paris* **273** (1971), 238–241.

[46] L. C. Washington, Introduction to cyclotomic fields, GTM 83, Springer (1982).

[47] B. M. M. de Weger, A hyperelliptic diophantine equation related to imaginary quadratic number fields with class number 2, *J. Reine angew. Math.* **427** (1992), 137–156; Correction, ibid. **441** (1993), 217–218.

[48] ———, A Thue equation with quadratic integers as variables, *Math. Comp.* **64** (1995), 855–861.

[49] K. Yamamura, Maximal unramified extensions of imaginary quadratic number fields of small conductor, *Journal de Théorie des Nombres de Bordeaux* **9** (1997), 405–448.

List of Papers by Takaaki KAGAWA

[1] The Hasse norm principle for the maximal real subfields of cyclotomic fields, *Tokyo Journal of Mathematics* **18** (1995), 221–229.

[2] (with M. Kida) Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields, *J. Number Theory* **66** (1997), 201–210.

[3] Determination of elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{37})$, *Acta Arith.*, to appear.

[4] (with N. Terai) Squares in Lucas sequences and some Diophantine equations, *Manuscripta Math.*, to appear.

[5] Determination of elliptic curves with everywhere good reduction over real quadratic fields, submitted to *Arch. Math.*

[6] Determination of elliptic curves with everywhere good reduction over real quadratic fields, II, *preprint*.