Pacific Journal of Mathematics

ELLIPTIC CURVES WITH TRIVIAL CONDUCTOR OVER QUADRATIC FIELDS

SALVADOR COMALADA

Vol. 144, No. 2 June 1990

PACIFIC JOURNAL OF MATHEMATICS
Vol. 144, No. 2, 1990

ELLIPTIC CURVES WITH TRIVIAL CONDUCTOR OVER QUADRATIC FIELDS

SALVADOR COMALADA

This paper concerns elliptic curves defined over quadratic fields and having good reduction at all primes. All those real fields admitting such curves having a 2-division point defined over the field and a global minimal model are characterized. The number of isomorphism classes, over the ground field, of these curves is also determined. If the number of divisor classes of the field is odd, all the mentioned curves without a global minimal model are classified and counted as well. It is shown that there are only eight elliptic curves defined over a quadratic field having good reduction everywhere and four 2-division points defined over the field.

Introduction. The existence of elliptic curves with good reduction everywhere over quadratic fields was first observed by Tate, by the way of his result about the non-existence of such curves over $\mathbf{Q}$. As far as the classification of these curves is concerned we can mention the following works:

1. Stroeker in [**6**] proves that there is no such curve admitting a global minimal model over an imaginary quadratic field.

2. Setzer in [**4**] characterizes all the admissible elliptic curves defined over imaginary quadratic fields. We recall that an admissible elliptic curve over a number field K is an elliptic curve defined over K, having good reduction everywhere and with a non-trivial 2-division point rational over K.

3. Setzer in [**5**] characterizes all elliptic curves over a quadratic field with good reduction everywhere and having a rational j-invariant.

In this paper, we extend some of those results to the case of a real quadratic field and without any assumptions on the j-invariant. Like the referred authors we follow the way of diophantine approach to classify all elliptic curves with a given conductor. In our case, we shall deal with certain diophantine equations in units of the real quadratic field.

Let K be a quadratic field. An elliptic curve defined over K will be called "g-admissible" if it is admissible and has a global minimal

model. By a result of Setzer [**4**], if 6 does not divide the number of divisor classes of K all admissible curves are g-admissible.

In §1 we characterize the real quadratic fields admitting g-admissible curves in terms of the solvability of certain diophantine equations over $\mathbf{Z}$. We also give an effective procedure for finding them all explicitly for each given K. The number of such curves is determined in §3. The set of j-invariants of these curves is seen to be infinite (Corollary of Theorem 3) unlike the case with rational j-invariant [**5**, Th. 4]. In §2 we prove that there are only eight elliptic curves defined over a quadratic field K having good reduction everywhere and four 2-division K-rational points. There is no such curve if K is imaginary and there are two curves in $\mathbf{Q}(\sqrt{7})$ and in $\mathbf{Q}(\sqrt{41})$ and four curves in $\mathbf{Q}(\sqrt{65})$. These curves are explicitly given in Theorem 2. In §4 we characterize the real quadratic fields with odd number of divisor classes admitting admissible curves. Finally in §5 we give a table containing models of all admissible curves defined over $K = \mathbf{Q}(\sqrt{d})$ for $2 \leq d < 100$.

1. g-admissible elliptic curves. Throughout this paper—except in §2—K will stand for the real quadratic field $\mathbf{Q}(\sqrt{d})$, where d is a square-free positive integer. The symbols $\mathfrak{O}_K$, $\mathfrak{U}_K$, h_K, N, tr will always denote the ring of integers, the group of units, the number of divisor classes, the norm and trace, respectively. We shall also use the notation $\bar{x}$ for the conjugate of $x \in K$. The aim of this section is to determine all the quadratic fields K admitting a g-admissible elliptic curve. They are characterized in the following way:

THEOREM 1. *The following conditions are equivalent*:

(i) *There exists a g-admissible elliptic curve defined over* K.

(ii) *Either of the following equations has a solution in integers* $u, v \in \mathfrak{U}_K$, $X, Y \in \mathfrak{O}_K$:

(1.1) $u + 64v = X^2$, X *a square* (*modulo* 4),

(1.2) $u + v = X^2$, $u \equiv v \equiv 1 + 2\sqrt{d} \pmod 4$ *and* $d \equiv 2 \pmod 4$,

(1.3) $4Y + u\overline{Y}^2 = X^2$, $2 \nmid Y$, $N(Y) = \pm 16$, $N(X) \equiv -2 \pmod 8$ *and* $d \equiv 1 \pmod 8$.

(iii) $d = 1023$ *or either of these sets of diophantine equations has a solution*:

(1.4) $x^2 - 4dy^2 = -7$, $7 \mid d$,

(1.5) $x^2 - 4dy^2 = 65$, $65 \mid d$,

(1.6) $x^2 - dy^2 = -2$, $d \equiv -2 \pmod 8$,

(1.7)

$$\left.\begin{aligned} x^2 - dy^2 &= -8 \\ r^4 - ds^2 &= \pm 256 \end{aligned}\right\} \qquad r \text{ odd}, \quad d \equiv 1 \pmod 8,$$

(1.8)

$$\left.\begin{aligned} r^4 - ds^2 &= -16384 \\ m^2 - dn^2 &= 8r \end{aligned}\right\} \qquad \begin{aligned} &r \equiv 3 \pmod 4, (m, r) = 1 \\ &128n \equiv sm \pmod r, \quad d \equiv 1 \pmod 8. \end{aligned}$$

Every g-admissible curve E has a model:

$$(1.9) \quad y^2 = x^3 + Ax^2 + Bx, \quad \Delta = 2^{12}w, \quad A, B \in \mathfrak{O}_K, \quad w \in \mathfrak{U}_K.$$

For primes $\mathfrak{P}$ dividing 2, we shall make constant use of the criterion for good reduction given in [4]. For quadratic fields, these conditions can be reformulated as follows:

LEMMA (*Setzer*). (a) *Let* $\mathfrak{P}$ *be an unramified prime dividing* 2. *Then an elliptic curve with model* (1.9) *has good reduction at* $\mathfrak{P}$ *if and only if* A *and* B *satisfy either of these sets of congruences*:

$$A \equiv -2\alpha^2 \pmod{\mathfrak{P}^3}, \quad B \equiv \alpha^4 \pmod{\mathfrak{P}^3},$$
$$A \equiv \alpha^2 \pmod{\mathfrak{P}^2}, \quad B \equiv 0 \pmod{\mathfrak{P}^4}$$

α *is integral and prime to* $\mathfrak{P}$.

(b) *An elliptic curve with model* (1.9) *has good reduction at a ramified prime dividing* 2 *if and only if* A *and* B *satisfy either the congruences of* (a) *with* $\mathfrak{P} = 2$ *or they satisfy*:

$$A = 4(a_1 + a_2\sqrt{d}), \quad a_1 \equiv 0 \pmod 2,$$
$$B = 4(b_1 + b_2\sqrt{d}), \quad b_1 \equiv 1 \pmod 4, \quad b_2 \equiv 2 \pmod 4$$

and

$$d \equiv 2 \pmod 4, \quad a_2 \equiv 1 \pmod 2,$$
$$b_1 - b_2 + 1 \equiv d(a_1 - a_2 - 1) \pmod 8,$$

or

$$d \equiv 3 \pmod 4, \quad a_2 \equiv 0 \pmod 2,$$
$$2a_2 - b_1 \equiv d \pmod 8.$$

Let E be an elliptic curve defined over K and having a model (1.9). Then, if Setzer's conditions are satisfied, we can find a suitable transformation to obtain a global minimal model for E. More

precisely,

LEMMA 1. *Let E be an admissible elliptic curve defined over K. Then E is g-admissible if and only if it has a model* (1.9).

Proof. If E has such a model we shall be able to obtain a global minimal equation for it by means of a transformation:

$$(1.10)\quad x = U^2x' + R, \quad y = U^3y' + U^2Sx' + T, \qquad R, S, T \in K, U \in K^*.$$

The reader can check [7] for the explicit transformation formulae for the coefficients of an elliptic curve having a Weierstrass normal form. If A, B satisfy (a) of Setzer's lemma, we set in (1.10): $U = 2$, $S = \alpha$, $T = B/2$, $R = -A/2$, 0 depending on whether the first or the second congruences are respectively satisfied by $\mathfrak{P} = 2$. Otherwise, we set: $U = 2$, $S = 1$, $R = A - 1$, $T = 4(m + n\omega)$ where

$$m = \begin{cases} 0 & \text{if } v_{\mathfrak{P}}(A+2) = 3, \\ 1 & \text{if } v_{\mathfrak{P}}(A+2) > 3, \end{cases}$$

$$n = \begin{cases} 0 & \text{if } v_{\overline{\mathfrak{P}}}(A-1) = 2 \text{ and } m = 1 \\ & \text{or } v_{\overline{\mathfrak{P}}}(A-1) > 2 \text{ and } m = 0, \\ 1 & \text{if } v_{\overline{\mathfrak{P}}}(A-1) = 2 \text{ and } m = 0 \\ & \text{or } v_{\overline{\mathfrak{P}}}(A-1) > 2 \text{ and } m = 1. \end{cases}$$

$\mathfrak{P}$ is a prime dividing 2 such that $\mathfrak{P}|(A+2, \omega)$, $\omega = (1 \pm \sqrt{d})/2$. Finally, if the congruences of (b) are satisfied, we set:

$$U = 2, \quad T = 4, \quad S = \pi,$$

$$R = \begin{cases} -\pi^2 & \text{if } \pi^2 A - B \equiv \pi^4 + \pi^4 \pmod{32} \\ -(4+\pi^2) & \text{if } \pi^2 A - B \equiv 5\pi^4 + 4\pi^5 + \pi^6 \pmod{32} \end{cases}$$

where $\pi = \sqrt{d}$, $1 + \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$, respectively. □

Before the proof of Theorem 1 we solve the diophantine equations of (ii).

PROPOSITION 1. *Let $\varepsilon \in \mathfrak{U}_K$ denote either the fundamental unit of K or its conjugate. The equation:*

$$(1.11)\qquad u + 64v = X^2, \qquad u, v \in \mathfrak{U}_K, \quad X \in \mathfrak{O}_K,$$

has a solution if and only if $u = \pm v$ *and* $X^2\mathfrak{O}_K = 63\mathfrak{O}_K$ *or* $65\mathfrak{O}_K$, *respectively, or in the following exceptional cases*:

$$\begin{aligned}
&d = 7, && u \in \mathfrak{U}_K^2, && v = \varepsilon^2 u, && X = (2\varepsilon^2 + 1)\sqrt{u},\\
&d = 41, && u \in \mathfrak{U}_K^2, && v = \varepsilon u, && X = \varepsilon\sqrt{u},\\
&d = 65, && u = \mathfrak{U}_K^2, && v = \varepsilon^3 u, && X = (2\varepsilon^2 - 1)\sqrt{u},\\
&d = 1023, && -u \in \mathfrak{U}_K^2, && v = -\varepsilon u, && X = \varepsilon\sqrt{-u}.
\end{aligned}$$

Proof. We consider first the cases $u = \pm 1$ or $v = \pm 1$. If $X^2 = u + 64$ then we have that $X - 8$, $X + 8 \in \mathfrak{U}_K$, and taking norms we get the solutions:

$$d = 7,\ X = \pm 3\sqrt{7},\ u = -1 \quad \text{and} \quad d = 65,\ X = \pm\sqrt{65},\ u = 1.$$

Similarly, from $X^2 = 1 + 64v$ we have:

$$\{(X-1)\mathfrak{O}_K, (X+1)\mathfrak{O}_K\} = \{2\mathfrak{O}_K, 2^5\mathfrak{O}_K\} \quad \text{or} \quad \{\mathfrak{P}\cdot\overline{\mathfrak{P}}^5, \mathfrak{P}^5\cdot\overline{\mathfrak{P}}\},$$

where $2\mathfrak{O}_K = \mathfrak{P}\cdot\overline{\mathfrak{P}}$ in the last case. Taking norms we get the solutions:

$$d = 7,\ X = \pm(2\varepsilon^2 + 1),\ v = \varepsilon^3; \quad d = 41,\ X = \pm\varepsilon,\ v = \varepsilon,$$

$$d = 65,\ X = \pm\sqrt{65},\ v = 1; \quad d = 65,\ X = \pm(2\varepsilon^2 - 1),\ v = \varepsilon^3.$$

In the case $X^2 + 1 = 64v$ setting $X = (r + s\sqrt{d})/2$, $r \equiv s \pmod 2$, $a = s^2 d$, and taking norms we get:

$$a^2 + 2(4 - r^2)a + (4 + r^2)^2 - 16N(64v) = 0.$$

Let $64b^2$ be the discriminant of this quadratic equation. From the equality $N(64v) = b^2 + r^2$, we find that all the solutions of $X^2 + 1 = 64v$ are:

$$d = 7,\ X = \pm 3\sqrt{7},\ v = 1; \quad d = 1023,\ X = \pm\varepsilon,\ v = \varepsilon.$$

In the case $X^2 + 64 = u$, proceeding as above we find that there are no solutions. Since every solution of (1.11) with $\pm u$ or $\pm v \in \mathfrak{U}_K^2$ leads up to the preceding cases, we can assume that $\pm u$, $\pm v \notin \mathfrak{U}_K^2$. In this case we have that $uv = \pm w^2$, $w \in \mathfrak{U}_K$. Setting $u\bar{w} = (r + s\sqrt{d})/2$, $r \equiv s \pmod 2$, taking norms and having in mind that $N(u) = N(v)$ we have:

$$\begin{aligned}
N(X)^2 &= N(u)(1 + 2^{12} \pm 2^6 \operatorname{tr}((u\bar{w})^2))\\
&= N(u)(1 + 2^{12} \mp 2^7 N(w) \pm 2^6 r^2).
\end{aligned}$$

Taking into account all possible signs for $N(u)$ and $N(w)$ we find in any case a finite number of possibilities for r and $N(X)$, from which only the following ones provide effective solutions to (1.11):

$$r = \pm 2, \quad N(X) = \pm 63 \quad \text{or} \quad \pm 65,$$

and they lead to $X^2\mathfrak{O}_K = 63\mathfrak{O}_K$ or $65\mathfrak{O}_K$, respectively. On the other hand, it is clear that this last condition ensures the existence of a solution to (1.11). □

PROPOSITION 2. *Let $\varepsilon \in \mathfrak{U}_K$ denote either the fundamental unit of K or its conjugate. The equation:*

$$u + v = X^2, \quad u, v \in \mathfrak{U}_K, \quad X \in \mathfrak{O}_K, \quad X \neq 0, \tag{1.12}$$

has a solution if and only if $u = v$ and $2\mathfrak{O}_K = X^2\mathfrak{O}_K$ or $u = w^2u_0$, $v = w^2\bar{u}_0$, $u_0, w \in \mathfrak{U}_K$, $\mathrm{tr}(u_0)$ a square or in the following exceptional cases:

$$\begin{array}{llll} d = 2, & u \notin \mathfrak{U}_K^2, & u\varepsilon < 0, v = -\varepsilon^2 u, & X = \sqrt{-2\varepsilon u}, \\ d = 5, & u \in \mathfrak{U}_K^2, & v = \varepsilon u, & X = \varepsilon\sqrt{u}, \\ d = 6, & 0 < u \notin \mathfrak{U}_K^2, & v = \varepsilon^4 u, & X = 7\varepsilon\sqrt{2}u. \end{array}$$

Proof. Let $u, v \in \mathfrak{U}_K$ be a solution of (1.12) and let us assume first that $N(uv) = 1$. Multiplying by $\overline{uv}$ both sides of (1.12) we get:

$$\overline{X}^2 = \bar{u} + \bar{v} = N(u)X^2\overline{uv}.$$

Hence, $N(u)\overline{uv} = w^2$, $w \in \mathfrak{U}_K w > 0$. From (1.12) we have:

$$X^2 w = uw + vw = uw + N(w)\overline{uw} = \mathrm{tr}(uw),$$

since $N(w) = -1$ would lead to a contradiction. Now, every odd prime dividing $\mathrm{tr}(uw)$ is unramified in K; hence, either $\mathrm{tr}(uw)$ or $\frac{1}{2}\mathrm{tr}(uw)$ is a rational square. In the first case, taking $u_0 = uw$ we have $u = w^{-1}u_0$, $v = w^{-1}\bar{u}_0$ and $w^{-1} \in \mathfrak{U}_K^2$. If $\frac{1}{2}\mathrm{tr}(uw) = r^2$, $r \in \mathbf{Z}$, then the prime 2 is ramified in K and the prime ideal dividing 2 is principal. If $N(u) = N(v) = 1$ we have a solution to $r^4 - ds^2 = 1$ and by a theorem of Cohn [**1**] we have $uw = \pm 1$, that is $u = v$, with the exceptional case $d = 6$, when there is the possibility $uw = \pm\varepsilon^2$, leading to $v = \varepsilon^4 u$. If $N(u) = N(v) = -1$, w is a square; hence, $2 \in \mathfrak{O}_K^2$ and $d = 2$. Now, the equation $r^4 - 2s^2 = -1$ has only one solution in positive integers, namely $r = s = 1$ [**3**, D24-31]; hence we have $uw = \varepsilon$, $v = -\varepsilon^2 u$.

If $N(u) = 1$ and $N(v) = -1$, then $u > 0$; otherwise either of the sums $u + v$, $\bar{u} + \bar{v}$ would be negative and (1.12) would lead to a contradiction. Hence, $u \in \mathfrak{U}_K^2$ and (1.12) furnishes an integer $Y \in \mathfrak{O}_K$ such that $Y - 1$, $Y + 1 \in \mathfrak{U}_K$. Taking norms we easily see that $d = 5$ and the solutions to (1.12) must be those given in the statement. □

PROPOSITION 3. *Let* $\varepsilon \in \mathfrak{U}_K$ *denote either the fundamental unit of* $K = \mathbf{Q}(\sqrt{d})$, $d \equiv 1 \pmod 8$, *or its conjugate, and let* $\mathfrak{P}$ *be a prime dividing* 2 *such that* $\mathfrak{P}^4$ *is principal.*

Then, the equation:

$$4Y + u\overline{Y}^2 = X^2 \tag{1.13}$$

has a solution with $X, Y \in \mathfrak{O}_K$, $u \in \mathfrak{U}_K$, $Y\mathfrak{O}_K = \mathfrak{P}^4$, *if and only if*:

(i) $\mathfrak{P}$ *is principal and there exists a generator of* $\mathfrak{P}^6$ *whose trace is a square. In this case, if* $\mathfrak{P} = H\mathfrak{O}_K$, *the solutions of* (1.13) *are*:

$$X = r\overline{H}, \quad Y = vH^4, \quad u = vN(v),$$

where $r \in \mathbf{Z}$, $v \in \mathfrak{U}_K$ *satisfy* $\operatorname{tr}(vH^6) = r^2$.

(ii) $\mathfrak{P}^2$ *is not principal and the following equations have an integral solution*:

$$\begin{cases} r^4 - ds^2 = -16384, & r \text{ odd} \\ m^2 - dn^2 = 8r; \quad (m, r) = 1, & 128n \equiv sm \pmod r. \end{cases} \tag{1.14}$$

In this case, the solutions of (1.13) *are*: $X = (m + n\sqrt{d})/2$, Y, u *such that* $u\overline{Y}^3 = (r^2 + s\sqrt{d})/2$, *where* m, n, r, s *are a solution of* (1.14).

We have the following exceptional cases:

$$\begin{aligned}
&d = 41, \quad X = \left(\frac{\varepsilon - 3}{2}\right)\sqrt{v}, && Y = \left(\frac{\varepsilon + 3}{10}\right)^4 \bar{\varepsilon} v, && u = v, && v \in \mathfrak{U}_K^2, \\
&d = 41, \quad X = \left(\frac{43\varepsilon - 1}{10}\right)\sqrt{v}, && Y = \left(\frac{\varepsilon + 3}{10}\right)^4 v, && u = \varepsilon^5 v, && v \in \mathfrak{U}_K^2, \\
&d = 65, \quad X = \left(\frac{\bar{\varepsilon} - 5}{2}\right)\sqrt{v}, && Y = \left(\frac{\varepsilon - 1}{2}\right)^2 \bar{\varepsilon} v, && u = v, && v \in \mathfrak{U}_K^2, \\
&d = 65, \quad X = \left(\frac{3\varepsilon - 1}{2}\right)\sqrt{v}, && Y = \left(\frac{\varepsilon - 1}{2}\right)^2 v, && u = \varepsilon^3 v, && v \in \mathfrak{U}_K^2.
\end{aligned}$$

Proof. Suppose that there exists a solution to (1.13) with $N(uY) = 16$. Multiplying by $\bar{u}Y$ both sides of the equation we get:

$$X^2 \bar{u} Y = 4\bar{u} Y^2 + 16\overline{Y} = 4\overline{X}^2.$$

Hence, $\mathfrak{P}^2$ is principal generated by $G = 2\overline{X}/X$. Replacing $Y = N(u)uG^2$ in (1.13) we obtain:

$$X^2 = 4N(u)uG^2 + u\bar{u}^2\overline{G}^4 = N(u)\overline{G}\operatorname{tr}(uG^3).$$

Since $(d, \operatorname{tr}(uG^3)) = 1$ we conclude that $\overline{G}$ is a square in $\mathfrak{O}_K$ and $\operatorname{tr}(N(u)uG^3)$ is a square in $\mathbf{Z}$. Thus, (i) is satisfied. If we have a

solution of (1.13) with $N(uY) = -16$, taking norms directly from (1.13) we get:

$$N(X)^2 = 4\,\mathrm{tr}(u\overline{Y}^3).$$

Hence, if $C = u\overline{Y}^3$, we have:

$$N(C) = -2^{12}, \quad \mathrm{tr}(C) = r^2, \quad N(X) = 2r, \quad r \in \mathbf{Z},$$

so that the equations of (1.14) are satisfied, and from:

$$C - 64N(u) = u\overline{Y}^3 + 4Y\overline{Y} = \overline{Y}X^2,$$

we have that X divides $C \pm 64$ in $\mathfrak{O}_K$, which is equivalent to the congruence, $128n \equiv sm \pmod{r}$. To see that the solutions given in (ii) do satisfy (1.13) we write:

$$(C + 64)\mathfrak{O}_K = \overline{\mathfrak{P}}^6\mathfrak{A}, \quad N(\mathfrak{A}) = r^2,$$

since $N(C + 64) = 64r^2$. If $r = p_1^{a_1} \cdots p_k^{a_k}$, from the first equation in (1.14) we have that all p_i decompose in $\mathbf{Q}(\sqrt{d})$ and $\mathfrak{A} = \mathfrak{P}_1^{2a1} \cdots \mathfrak{P}_k^{2ak}$ where each $\mathfrak{P}_i$ is one of the two prime ideals dividing p_i. Now, since X divides $C + 64$, we deduce that $X^2\mathfrak{O}_k = \overline{\mathfrak{P}}^2\mathfrak{A}$. Hence, $C + 64 = \overline{Y}X^2w$, $w \in \mathfrak{U}_K$ and equation (1.13) is easily obtained. We have only to check that if $\mathfrak{P}^2$ is principal then we fall in the exceptional cases. We set $\mathfrak{P}^2 = G\mathfrak{O}_K$ and $Y = G^2v$, $v \in \mathfrak{U}_K$. If $N(u) = 1$, $N(Y) = -16$, we have $N(v) = -1$. Hence, $u = \pm w^2$, $w \in \mathfrak{U}_K$; but $u = -w^2$ never occurs since we would have from (1.13) the congruence $X^2 \equiv -1 \pmod{\mathfrak{P}^2}$, which is impossible. Thus, the equation becomes:

$$4Y = (X - w\overline{Y})(X + w\overline{Y}),$$

and

$$\{(X - w\overline{Y})\mathfrak{O}_K, (X + w\overline{Y})\mathfrak{O}_K\} = \{2\mathfrak{O}_K, (2\mathfrak{O}_K)\mathfrak{P}^4\}.$$

Taking norms it can easily be deduced that $d = 41$ or 65 and the first and the third exceptional cases can be obtained. If $N(u) = -1$, $N(Y) = 16$, we have that $v = \pm w^2$, $w \in \mathfrak{U}_K$, but $Y < 0$ implies $u > 0$, so that $\overline{Y} < 0$, $\bar{u} < 0$ which is impossible since $4\overline{Y} + \bar{u}Y^2 = \overline{X}^2$. Hence, Y is a square and setting $Y = H^2$, the equation becomes:

$$u\overline{H}^4 = (X - 2H)(X + 2H),$$

and we proceed as above to get the two remaining exceptional cases. □

Proof of Theorem 1. Let's see first the equivalence between (i) and (ii): If E is a g-admissible elliptic curve defined over K, having a model (1.9), then from the equation of the discriminant:

$$B^2(A^2 - 4B) = 2^8 w,$$

and the conditions of Setzer's lemma, we have the following possibilities:

(1.15) $B = 2^4 u$, $A^2 - 2^6 u = v$, $u, v \in \mathfrak{U}_K$ and $A \equiv \alpha^2 \pmod 4$,

(1.16) $B = u$, $A^2 - 4u = 2^8 v$, $u, v \in \mathfrak{U}_K$ and $A \equiv -2\alpha^2 \pmod 8$,

(1.17) $B = 4u$, $A^2 - 2^4 u = 2^4 v$, $u, v \in \mathfrak{U}_K$ and $A \equiv 4\sqrt{d} \pmod 8$, $B \equiv 4 + 8\sqrt{d} \pmod{16}$ if $d \equiv 2 \pmod 4$,

(1.18) $B = 4u$, $A^2 - 2^4 u = 2^4 v$, $u, v \in \mathfrak{U}_K$ and $A \equiv 0 \pmod 8$, $B \equiv 4 + 8\sqrt{d} \pmod{16}$ if $d \equiv 3 \pmod 4$,

(1.19) $B\mathfrak{O}_K = \mathfrak{P}^4$, $\mathfrak{P}$ a prime dividing 2, $A^2 - 4B = u\overline{B}^2$, $u \in \mathfrak{U}_K$ and

$$\begin{cases} A \equiv -2 \pmod{\overline{\mathfrak{P}}^3} \\ A \equiv 1 \pmod{\mathfrak{P}^2} \end{cases}$$

if $d \equiv 1 \pmod 8$.

The equation (1.1) follows immediately from (1.15) and (1.16). Possibility (1.18) never holds because it would imply the existence of a unit $u \equiv 1 + 2\sqrt{d} \pmod 4$, which is impossible if $d \equiv 3 \pmod 4$. The equation (1.2) can be easily deduced from (1.17) and so does equation (1.3) from (1.19) together with the fact that the set of congruences in (1.19) is seen to be equivalent to:

$$N(A) \equiv -2 \pmod 8, \quad \mathrm{tr}(A) \equiv 3 \pmod 4,$$

as it can be easily checked by taking norms. Conversely, if we are given a solution of either (1.1) (1.2) or (1.3), following the possibilities listed above, we can clearly construct an elliptic curve E with a model (1.9) satisfying the conditions of Setzer's lemma, so that, by Lemma 1, E is g-admissible.

To prove the equivalence between (ii) and (iii), we first apply Proposition 1 to equation (1.1). Hence, we may have $N(X/3) = \pm 7$, $7 \mid d$ or $N(X) = \pm 65$, $65 \mid d$. The condition of $X\mathfrak{O}_K$ being a square (mod 4) is seen to be equivalent in this case to $Xw \equiv \overline{Xw} \pmod 4$, $w \in \mathfrak{U}_K$. Thus, equations (1.4) and (1.5) are obtained. For $d = 7$, 65 these last equations are respectively satisfied. For $d = 41$ equations (1.7) and (1.8) are solvable and, finally, in the case $d = 1023$ a solution to (1.1) can be found taking, for instance, $u = -\varepsilon^2$, $v = \varepsilon$, $X = 1$, ε as in Proposition 1.

Applying Proposition 2 to equation (1.2) we have that: $X^2 = 2u$, $u \equiv 1 + 2\sqrt{d} \pmod 4$, so that (1.6) is seen to be satisfied. For the exceptional case $d = 6$, this last equation has also a solution. At last, Proposition 3 gives us the equivalence between the existence of solutions to (1.3) and the solvability of (1.7) or (1.8). Condition $N(X) \equiv -2 \pmod 8$ is clearly equivalent to $N(H) = -2$, $r \equiv 3 \pmod 4$, respectively. Hence, Theorem 1 is proved. □

REMARKS. (1) We can find solutions to all the diophantine equations of (iii) taking, for example, $d = 7$, $d = 65$, $d = 6$, $d = 41$ or $d = 17867009$, respectively.

(2) It is not difficult to check that every pair of diophantine equations of (iii) is not simultaneously solvable except for (1.7) and (1.8), which can only have $d = 41, 65$ in common and (1.5) and (1.8), which are both solvable for $d = 65$. I believe that this is the only common d but I am not able to prove it.

(3) The proofs of Theorem 1 and Propositions 1, 2, 3 give, in fact, a procedure for effectively constructing all g-admissible curves for a given K. This will be treated even more explicitly in Theorem 3 below.

2. Admissible elliptic curves with four 2-division K-rational points. In this section, the set of the elliptic curves defined over any quadratic field $K = \mathbf{Q}(\sqrt{d})$, with good reduction everywhere and all 2-division points rational over K is completely determined (see [2]).

Let σ be the non-trivial $\mathbf{Q}$-automorphism of K. We have:

THEOREM 2. *Let $K = \mathbf{Q}(\sqrt{d})$. Let E be an elliptic curve defined over K with good reduction everywhere and having four 2-division K-rational points. Then we must have $d = 7$, 41 or 65 and E is isomorphic to one of the following eight curves:*

$$E_i\colon y^2 = x^3 + Ax^2 + Bx, \quad \Delta = 2^{12}D, \quad 1 \le i \le 8,$$

	d	A	B	D	j
E_1	7	$-(1+2\varepsilon^2)$	$16\varepsilon^3$	ε^6	$(255)^3$
E_3	41	$(3\varepsilon-1)/2$	$\varepsilon(\varepsilon-1)/2$	ε^4	$(\varepsilon-16)^3/\varepsilon$
E_5	65	$2\varepsilon^2-1$	$16\varepsilon^3$	ε^6	$(257)^3$
E_6	65	$10\varepsilon^2-5$	$400\varepsilon^3$	$(5\varepsilon)^6$	$(257)^3$
E_7	65	$8\varepsilon+1$	$16\varepsilon^2$	ε^6	$(17)^3$
E_8	65	$40\varepsilon+5$	$400\varepsilon^2$	$(5\varepsilon)^6$	$(17)^3$

$E_2 = E_1^\sigma$, $E_4 = E_3^\sigma$. In each case, ε stands for the fundamental unit, i.e., $\varepsilon = 8 + 3\sqrt{7}$, $32 + 5\sqrt{41}$ or $8 + \sqrt{65}$, respectively.

Proof. Let E an elliptic curve with good reduction everywhere and four 2-division K-rational points. Then E has a model:

$$E: y^2 = x^3 + Ax^2 + Bx, \qquad A, B \in \mathfrak{O}_K, \tag{2.1}$$

with discriminant:

$$\Delta = 16B^2(A^2 - 4B) = 2^{12}D, \qquad D \in \mathfrak{O}_K^2, \ (D, 2) = 1. \tag{2.2}$$

By Setzer's conditions, given in [**4**], we have:

$$A\mathfrak{O}_K = \mathfrak{D}^2\mathfrak{A}, \quad B\mathfrak{O}_K = \mathfrak{D}^4\mathfrak{B}, \quad D\mathfrak{O}_K = \mathfrak{D}^{12},$$

where $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{D}$ are ideals of $\mathfrak{O}_K$ and $\mathfrak{B} = \mathfrak{O}_K$, $16\mathfrak{O}_K$, $4\mathfrak{O}_K$ or $\mathfrak{P}^4$, the two last cases being only considered when $2 = \mathfrak{P}^2$ or $\mathfrak{P}\overline{\mathfrak{P}}$ respectively. Let's assume $\mathfrak{B} = \mathfrak{P}^4$. Since $B^3\mathfrak{O}_K = \mathfrak{D}^{12}\mathfrak{P}^{12}$ we have that $\mathfrak{P}^{12}$ is principal and from (2.2) we get the equation

$$N(X^2 - 64) = \pm 2^{12}, \qquad X \in \mathfrak{O}_K, \quad 2 \nmid X,$$

which ensures the principality of $\mathfrak{B}$. In any case, since $\mathfrak{B}$ is always principal, we conclude that $\mathfrak{D}^2$ and $\mathfrak{A}$ must be principal, too. Thus, we may set:

$$\mathfrak{A} = a\mathfrak{O}_K, \quad \mathfrak{B} = b\mathfrak{O}_K, \quad \mathfrak{D}^2 = c\mathfrak{O}_K, \qquad a, b, c \in \mathfrak{O}_K,$$

$$A = cau_1, \quad B = c^2bu_2, \quad D = c^6u_3^2, \qquad u_1, u_2, u_3 \in \mathfrak{U}_K. \tag{2.3}$$

From (2.2) we have:

$$b^2(a^2u_1^2 - 4bu_2) = 2^8u_3^2u_2^{-2}.$$

If $b = 1$ or 16, this last equality leads to a solution of

$$X^2 = u + 64v, \qquad X \in \mathfrak{O}_K, \quad u, v \in \mathfrak{U}_K, \tag{2.4}$$

with $v \in \mathfrak{U}_K^2$ or $u \in \mathfrak{U}_K^2$, respectively. If $b = 4$ we have:

$$X^2 = u + v, \qquad X \in \mathfrak{O}_K, \quad u, v \in \mathfrak{U}_K, \tag{2.5}$$

with $u \in \mathfrak{U}_K^2$. If $b\mathfrak{O}_K = \mathfrak{P}^4$ we obtain:

$$X^2 = 4Y + u\overline{Y}^2, \quad 2 \nmid Y, \ N(Y) = \pm 16, \qquad X, Y \in \mathfrak{O}_K, \quad u \in \mathfrak{U}_K, \tag{2.6}$$

with $u \in \mathfrak{U}_K^2$. Equations (2.4), (2.5) and (2.6) are completely studied in Propositions 1, 2 and 3, respectively. In our particular case, where one of the units u, v is a square, it is easy to see that equation (2.4) implies $d = -7$, 7, 41 or 65, equation (2.5) implies $d = 2$ and from

equation (2.6) we have $d = -7$, 41 or 65. Finally, from its finite number of solutions, we can construct all the desired curves. Notice that for $d = -7$, by Stroeker's result in [6], no elliptic curves with good reduction everywhere can be found. Also, for $d = 2$ we have already shown in Theorem 1 that no admissible curves exist.

Clearly, by Lemma 1, all the curves obtained have a global minimal model except for E_6 and E_8, which cannot have it. Notice that these last curves have been obtained by setting $c = 5$ in (2.3). In fact, following Setzer in [4], it can be easily shown that two admissible curves over $\mathbf{Q}(\sqrt{65})$ attached to a solution of (2.4) or (2.6) with c_1, c_2 respectively, are isomorphic if and only if $\mathfrak{D}_1$, $\mathfrak{D}_2$ are equivalent ideals. □

3. Counting g-admissible curves.

THEOREM 3. *Let* $K = \mathbf{Q}(\sqrt{d})$, $d \neq 7$, 41, 65, 1023 *satisfy the conditions of Theorem* 1. *Then the number of* g*-admissible elliptic curves over* K *(up to isomorphism) is*:

2	*if* (1.6) *is solvable,* $d \neq 6$,
6	*if* $d = 6$
8	*if either* (1.4) *or* (1.5) *is solvable and* $d \equiv 3 \pmod 4$,
4	*if either* (1.4) *or* (1.5) *is solvable,* (1.8) *is unsolvable and* $d \not\equiv 3 \pmod 4$,
$2^f N$	*if* (1.8) *is solvable and* (1.5) *is unsolvable,*
$4 + 2^f N$	*if both* (1.5) *and* (1.8) *are solvable,*
$2^{f+1} M$	*if* (1.7) *is solvable*,

where M *is the number of solutions in positive integers* (r, s) *of the equation* $r^4 - ds^2 = \pm 256$, $2 \nmid r$. N *is the number of solutions in integers* (r, s) *of the equation* $r^4 - ds^2 = -16384$, $r \equiv 3 \pmod 4$ *for which the whole set of equations* (1.8) *has also a solution. Let* $f = 0, 1$ *according to whether the norm of the fundamental unit is* -1 *or* 1, *respectively. For* $d = 7$, 41, 65, 1023, *the number of* g*-admissible elliptic curves is* 8, 6, 6, 8 *respectively.*

Proof. Let $\mathfrak{G}$ be the set of classes of isomorphic g-admissible elliptic curves. In each case, we shall consider different sets $\mathfrak{H}$ and we shall establish a mapping $\Phi: \mathfrak{G} \to \mathfrak{H}$ of $\mathfrak{G}$ onto $\mathfrak{H}$. We shall obtain the result about the cardinal of $\mathfrak{G}$ in terms of the cardinal of $\mathfrak{H}$ and the fibres of Φ. Notice that two models: $y^2 = x^3 + A_1 x^2 + B_1 x$, $y^2 = x^3 + A_2 x^2 + B_2 x$, belong to isomorphic elliptic curves if and

only if they are related by a dilation:

$$A_2 = A_1 U^2, \quad B_2 = B_1 U^4, \qquad U \in \mathfrak{U}_k.$$

In fact, if a transformation (1.15) changes one model into the other we must have $S = T = 0$ and $R^3 + A_1 R^2 + B_1 R = 0$, $R \in \mathfrak{O}_K$ and since $d \neq 7, 41, 65$ (see Th. 2), $R = 0$. Using this argument we shall have, in any case, that Φ does not depend on the particular choice of the model.

Assume that (1.6) is solvable. We define:

$$\mathfrak{H} = \{u \in \mathfrak{U}_K ; \operatorname{tr}(u) = 2r^2, \ r \in \mathbf{Z}\},$$

$$\Phi(E) := \Phi(A, B) = \left(\frac{A^2}{4B} - 1\right)^{1/2}, \qquad E \in \mathfrak{G}.$$

If $A = 4C$, $B = 4u$, $C \in \mathfrak{O}_K$, $u \in \mathfrak{U}_K$ then $C^2 = u + v$, $v \in \mathfrak{U}_K$ and $\Phi^2(E) = \bar{u}v$. By Proposition 2, $\bar{u}v \in \mathfrak{U}_K^2$ and $\Phi(E) \in \mathfrak{H}$. Let us show that Φ is onto: Setting $u = r^2 + s\sqrt{d}$ and taking $C \in \mathfrak{O}_K$ such that $N(C) = -2$ we have:

$C^2 = 2v$, $v \in \mathfrak{U}_K$, $v \equiv 1 + 2\sqrt{d} \pmod 4$, $u + \bar{u} = 2r^2 = C^2 \bar{v} r^2$; hence $uv + \bar{u}v = (Cr)^2$ with $uv \equiv 1 + 2\sqrt{d} \pmod 4$.

Thus, uv, $\bar{u}v$, Cr is a solution of equation (1.2) and a g-admissible curve E can be obtained by taking: $A = \pm 4rC$ (sign determined by (b) of Setzer's lemma), $B = 4\bar{u}v$, so that $\Phi(E) = u$. Finally, $\Phi(A_1, B_1) = \Phi(A_2, B_2)$ if and only if $(A_1/A_2)^2 = B_1/B_2$ and since $B_1/B_2 \in \mathfrak{U}_K$ this is equivalent to: $A_2 = A_1 u$; $B_2 = B_1 u^2$, $u \in \mathfrak{U}_K$, if $u \in \mathfrak{U}_K^2$ the curves are isomorphic and if $u \notin \mathfrak{U}_K^2$ we obtain two non-isomorphic curves such that all curves with the same image by Φ must be isomorphic to one of them. Therefore, in this case, the number of g-admissible elliptic curves defined over K (up to isomorphism) is just twice the number of units in $\mathfrak{H}$, i.e., the number of integral solutions (r, s) of the diophantine equation:

$$r^4 - ds^2 = 1.$$

Applying a theorem of Cohn ([1]), we get the first two cases ($d \neq 6$, $d = 6$).

If (1.4) is solvable and $E \in \mathfrak{G}$ has a model (1.9) then we have:

$A^2 = 2^{8-2e}v + 2^{e+2}u$, $B = 2^e u$, $u, v \in \mathfrak{U}_K$, with $e = 0$ or 4. Let $\mathfrak{H}$ be the set of classes [C] of elements of the set: $\{C \in \mathfrak{O}_K$, $N(C) = -7$, C is a square (mod 4)$\}$, classified by the relation:

$$B \sim C \quad \text{iff} \quad CB^{-1} \in \mathfrak{U}_K^2.$$

In this case we set:

$$\Phi(A, B) = [-A/3] \quad \text{if } e = 4,$$
$$\Phi(A, B) = [A/6] \quad \text{if } e = 0.$$

By Proposition 1 together with (1.15), (1.16) we get that $\Phi(A, B) \in \mathfrak{H}$. Also, let us see that there are exactly two elements of $\mathfrak{G}$ which map to every class of $\mathfrak{H}$: Let $I \in \mathfrak{H}$, $I = [C]$, $C \in \mathfrak{O}_K$. From $C^2 = 7u$, $u \in \mathfrak{U}_K$, we can take the g-admissible curves E_1, E_2 given by:

$$A_1 = -3C, \quad B_1 = 16u, \quad A_2 = 6C, \quad B_2 = -u.$$

Clearly, $\Phi(E_1) = \Phi(E_2) = I$. It is also clear that E_1, E_2 are not isomorphic and they are the only elements of $\mathfrak{G}$ which map to I, for if $\Phi(A_1, B_1) = \Phi(A_2, B_2)$, either $A_2 \in [A_1]$ or $-2A_2 \in [A_1]$ and, in any case, B_1, B_2 are uniquely determined by equations:

$$\left(\frac{A}{3}\right)^2 = 7\frac{B}{16} \quad \text{or} \quad \left(\frac{A}{6}\right)^2 = -7B.$$

Therefore, the cardinal of $\mathfrak{G}$ is twice the cardinal of $\mathfrak{H}$ and this is four if $d \equiv 4 \pmod 4$, being $[C]$, $[-C]$, $[\overline{C}]$, $[-\overline{C}]$ all the classes, and two if $d \not\equiv 3 \pmod 4$ being $[C]$, $[\overline{C}]$ all the classes.

If (1.5) is solvable and (1.8) is unsolvable we take $\mathfrak{H}$ to be the set of classes $[C]$ of elements of the set:

$$\{C \in \mathfrak{O}_K, N(C) = 65, C \text{ is a square } (\mathrm{mod}\, 4)\}$$

classified as above. Now, we set:

$$\Phi(A, B) = [A] \quad \text{if } e = 4,$$
$$\Phi(A, B) = [-A/2] \quad \text{if } e = 0.$$

Arguing as in the preceding case we can show that $\Phi(A, B) \in \mathfrak{H}$. Moreover, the proof of the existence of two elements of $\mathfrak{G}$ mapping to every $I \in \mathfrak{H}$ is practically the same, but now, the curves E_1, E_2 are given by:

$$A_1 = C, \quad B_1 = 16u, \quad A_2 = -2C, \quad B_2 = u,$$

where $I = [C]$, $C \in \mathfrak{O}_K$ and $C^2 = 65u$, $u \in \mathfrak{U}_K$. Finally, the cardinal of $\mathfrak{H}$ is the same as before. If (1.8) is solvable and (1.5) is unsolvable then we take: $\mathfrak{H} = \{C \in \mathfrak{O}_K, C = (r^2 + s\sqrt{d})/2, r, s \in \mathbf{Z}$ where (r, s, m, n) satisfy (1.8) for $m, n \in \mathbf{Z}\}$, and $\Phi(A, B) = A^2\overline{B} - 4N(B)$. From (1.19) and the fact that the primes dividing 2 are not principal we get that A, B must satisfy equation (1.3) with

$N(uB) = -16$ (see Prop. 3). Now, multiplying by $\overline{B}$ both sides of this equation we get:

$$A^2\overline{B} = 4N(B) + u\overline{B}^3,$$

so that $\Phi(A, B) = u\overline{B}^3$, $\Phi(A, B) \in \mathfrak{H}$. We show that either one or two elements of $\mathfrak{G}$ map to every $C \in \mathfrak{H}$ depending on whether the norm of the fundamental unit is -1 or 1, respectively. If $C \in \mathfrak{H}$, then from Proposition 3 and the last equality we have that:

$$A^2\overline{B} = 4N(\overline{B}) + C,$$

where $A = (m + n\sqrt{d})/2$, $2 \nmid B$, $N(B) = \pm 16$, so that B can be found and the elliptic curve with coefficients, A, B is g-admissible. Clearly, $\Phi(A, B) = C$. If $\Phi(A_1, B_1) = \Phi(A_2, B_2)$ from $N(B_1) = N(B_2) = \pm 16$ we get that $B_2/B_1 = (A_2/A_1)^2$. Now, since $B_2/B_1 \in \mathfrak{U}_K$ we have:

$$A_2 = A_1 u, \quad B_2 = B_1 u^2, \qquad u \in \mathfrak{U}_K.$$

Hence, if $u \in \mathfrak{U}_K^2$ the curves are isomorphic, and if $u \notin \mathfrak{U}_K^2$ we obtain two non-isomorphic curves only when $N(u) = 1$, i.e., when the norm of the fundamental unit is 1, as we must have $N(A_1) \equiv N(A_2) \equiv -2 \pmod 8$. If both (1.5) and (1.8) are solvable we fall simultaneously in the two last cases, but, clearly, curves coming from different cases are non-isomorphic, so that the cardinal is the sum of the two last cardinals and the result follows.

If, at last, we assume that (1.7) is solvable we consider:

$$\mathfrak{H} = \{C \in \mathfrak{O}_K ; N(C) = \pm 256, \operatorname{tr}(C) = r^2, r \in \mathbf{Z}, (r, 2) = 1\}$$

and $\Phi(A, B) = -2\overline{A}B/A$. To show that $\Phi(E) \in \mathfrak{H}$ we put by Proposition 3: $A = r\overline{H}$, $B = uH^4$, where $u \in \mathfrak{U}_K$, $N(H) = -2$, $\operatorname{tr}(uH^6) = r^2$. Hence, $-2\overline{A}B/A = -2\overline{A}^2B/N(A) = uH^6$. Now we show that either one or two elements of $\mathfrak{G}$ map to every $C \in \mathfrak{H}$ depending on whether the norm of the fundamental unit is -1 or 1, respectively. If $C \in \mathfrak{H}$ with $\operatorname{tr}(C) = r^2$, then from:

$$C = uH^6, \quad u \in \mathfrak{U}_K, \quad N(H) = 2, \qquad H \in \mathfrak{O}_K,$$

we have that the elliptic curve given by: $A = \pm r\overline{H}$ ($\operatorname{tr} A \equiv -1 \pmod 4$), $B = uH^4$, is g-admissible and $\Phi(A, B) = C$. If $\Phi(A_1, B_1) = \Phi(A_2, B_2)$ since $N(A_1) = N(A_2)$ we get

$$B_1/B_2 = (A_1/A_2)^2, \quad B_1/B_2 \in \mathfrak{U}_K.$$

Thus,

$$A_2 = A_1 u, \quad B_2 = B_1 u^2, \qquad u \in \mathfrak{U}_k,$$

and we argue as in the preceding case to get the result. For $d = 7, 41, 65$ and 1023 we construct all the g-admissible curves directly from the solutions of the diophantine equations in (iii) of Theorem 1. It is straightforward to check that there are 8, 6, 6, 8 curves respectively. In §5 we give explicit models for all these curves with $d = 7, 41$ and 65. □

REMARK. Assume that (1.7) is solvable. Then if the norm of the fundamental unit is 1 we must have:

$$r^4 - ds^2 = 256, \qquad (r, 2) = 1.$$

Otherwise, from $(r^2 + s\sqrt{d})/2 = uH^6$, $N(H) = -2$, we should have $N(u) = -1$. Also, if the norm of the fundamental unit is -1 and $d \neq 41$ we must have:

$$r^4 - ds^2 = -256, \quad (r, 2) = 1.$$

Otherwise, proceeding as above we would have $N(u) = 1$ and, hence, $u \in \mathfrak{U}_K^2$ so that the g-admissible curve given by: $A = r\overline{H}$, $B = uH^4$, should have all the 2-division points rational over K, and Theorem 2 would lead to contradiction.

Let J_i, J_r be the sets of j-invariants of all g-admissible elliptic curves defined over imaginary or real quadratic fields, respectively. Setzer ([4], [5]) has proved that J_i and $J_r \cap \mathbf{Z}$ are both finite. In fact,

$$J_i = \{17^3, 257^3\},$$
$$J_r \cap \mathbf{Z} = \{17^3, 257^3, -15^3, 255^3, 20^3\}.$$

On the other hand, as a consequence of Theorems 1 and 3, we can state the following:

COROLLARY. *J_r is not finite.*

Proof. For any integer $m \equiv 13 \pmod{32}$ let d_m be the square-free positive integer determined by:

$$7m^6 + 1 = 16d_m n^2. \tag{3.1}$$

Taking $x = 7m^3$, $y = 2n$, $d = 7d_m$ we obtain a solution to (1.4) with $d \equiv 3 \pmod 4$. Since, (3.1) has only a finite number of solutions for a given d_m, we get in this way an infinite number of real quadratic fields $K = \mathbf{Q}(\sqrt{d})$ admitting g-admissible elliptic curves. By Theorem 3, there are exactly 8 such curves for each K and by [5, Th. 3] not all of them can have a rational j-invariant. □

4. Admissible curves. It seems very difficult to characterize all the admissible curves defined over K by means of this diophantine approach. Nevertheless, in the case $2 \nmid h_k$ it is still possible to solve it completely. In fact, under this assumption on h_k, almost all the admissible curves turn out to be g-admissible and they are already characterized by Theorem 1. More precisely,

THEOREM 4. *Assume* $2 \nmid h_k$. *All admissible elliptic curves defined over* K *are* g*-admissible except for the case*:

d *prime,* $d \equiv 1 \pmod{16}$ *and* $\mathfrak{P}$ *not principal, where* $\mathfrak{P}$ *is a prime dividing* 2. *In this latter case, the following conditions are equivalent*:

(i) *There exists an admissible elliptic curve defined over* K.

(ii) *The equation*:

$$uY^4 + 64v = X^2, \quad 2 \nmid Y, \ N(Y) = \pm 8, \tag{4.1}$$

has a solution in integers $u, v \in \mathfrak{U}_K$, $X, Y \in \mathfrak{O}_K$.

(iii) *The following equation has an integral solution*:

$$r^4 - ds^2 = -256, \quad r \text{ odd}. \tag{4.2}$$

When these conditions are satisfied, the number of admissible elliptic curves is twice the number of positive integral solutions of (4.2). *None of these curves is* g*-admissible.*

Proceeding as in §1, we solve the equation (4.1) before the proof of the theorem.

PROPOSITION 4. *Let* $\varepsilon \in \mathfrak{U}_K$ *denote either the fundamental unit of* $K = \mathbf{Q}(\sqrt{d})$, $d \equiv 1 \pmod 8$, *or its conjugate, and let* $\mathfrak{P}$ *be a prime dividing* 2 *such that* $\mathfrak{P}^3$ *is principal. Then, the equation*:

$$uY^4 + 64v = X^2 \tag{4.3}$$

has a solution with $X, Y \in \mathfrak{O}_K$, $u, v \in \mathfrak{U}_K$, $Y\mathfrak{O}_K = \mathfrak{P}^3$ *if and only if there exists a generator of* $\mathfrak{P}^6$ *whose trace is a square. The solution is then given by*: $X = rY$, $v = \bar{u}$, *where* $\operatorname{tr}(Y^2 u) = r^2$, $r \in \mathbf{Z}$, *except for* $d = 41$, *when there are also the solutions*:

$$X = \frac{11\varepsilon - 27}{20}\sqrt{u}, \quad v = \varepsilon u, \quad Y = \frac{\varepsilon - 17}{10}, \quad u \in \mathfrak{U}_K^2,$$

$$X = \frac{\varepsilon - 15}{2}\sqrt{v}, \quad u = \varepsilon v, \quad Y = \frac{\bar{\varepsilon} - 17}{10}, \quad v \in \mathfrak{U}_K^2.$$

Proof. Let us assume that (4.3) has a solution. Then, multiplying both sides of the equation by $\overline{Y}^2$ we get:

$$uY^2 + v\overline{Y} = \left(\frac{X\overline{Y}}{8}\right)^2. \tag{4.4}$$

If $N(uv) = 1$, multiplying both sides of (4.4) by $\overline{uv}$ we have:

$$(\overline{X}Y/8)^2 = \bar{v}Y^2 + \bar{u}\overline{Y}^2 = (X\overline{Y}/8)\overline{uv}N(u).$$

Hence, $\pm\overline{uv} \in \mathfrak{U}_K^2$. Setting $\pm\overline{uv} = w^2$, $w \in \mathfrak{U}_K$ and multiplying again (4.4) by w, we get:

$$\operatorname{tr}(uwY^2) = uwY^2 + N(w)\overline{uw}\overline{Y}^2 = (X\overline{Y}/8)^2 w,$$

for we must have $N(w) = 1$. Now, since $(d, \operatorname{tr}(uwY^2)) = 1$, we conclude that $\operatorname{tr}(uwY^2)$ must be a square in $\mathbf{Z}$. Setting $Y' = Y\sqrt{w^{-1}}$, $u' = uw^2$ we have:

$$X = rY', \quad v = \bar{u}', \quad \text{where } \operatorname{tr}((Y')^2u') = r^2, \ r \in \mathbf{Z}.$$

If $N(uv) = -1$, we may assume $N(u) = -1$ so that $N(v) = 1$ and $\pm v \in \mathfrak{U}_K^2$. But from (4.4) $v \equiv 1 \pmod{\mathfrak{P}^2}$. Thus, $v \in \mathfrak{U}_K^2$ and we may write:

$$\left(\frac{X\overline{Y}}{8} - \sqrt{v\overline{Y}}\right)\left(\frac{X\overline{Y}}{8} + \sqrt{v\overline{Y}}\right) = uY^2 \quad \text{and}$$

$$\left\{\left(\frac{X\overline{Y}}{8} - \sqrt{v\overline{Y}}\right)\mathfrak{O}_K, \left(\frac{X\overline{Y}}{8} + \sqrt{v\overline{Y}}\right)\mathfrak{O}_K\right\} = \{\mathfrak{P}, \mathfrak{P}^5\}.$$

Taking norms we have $d = 41$ and the two exceptional solutions are obtained. □

Proof of Theorem 4. Let E be an admissible elliptic curve with model (2.1) and discriminant (2.2). Then, we also have:

$$A\mathfrak{O}_K = \mathfrak{D}^2\mathfrak{A}, \quad B\mathfrak{O}_K = \mathfrak{D}^4\mathfrak{B}, \quad D\mathfrak{O}_K = \mathfrak{D}^{12},$$

where $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{D}$ are ideals of $\mathfrak{O}_K$ and $\mathfrak{B} = \mathfrak{O}_K$, $16\mathfrak{O}_K$, $4\mathfrak{O}_K$ or $\mathfrak{P}^4$. Since $\mathfrak{D}^{12}$ is principal and $2 \nmid h_k$ we conclude that $\mathfrak{D}^3$ and, consequently, $\mathfrak{D}\mathfrak{B}$ are principal. If $\mathfrak{D}$ is principal then by a dilation we get an admissible curve isomorphic to E with a model (1.9) so that by Lemma 1 a global minimal model for it can be obtained. Otherwise,

the non-principality of $\mathfrak{D}$ is equivalent to the non-principality of $\mathfrak{P}$, where $\mathfrak{B} = \mathfrak{P}^4$. In this latter case we may set:

$$\mathfrak{P}^3 = a\mathfrak{O}_k, \quad \mathfrak{D}^3 = b\mathfrak{O}_K, \quad a, b \in \mathfrak{O}_K,$$
$$B^3 = ua^4b^4, \quad D = vb^4, \quad u, v \in \mathfrak{U}_K.$$

From the discriminant we have:

$$\left(\frac{AB}{2b^2}\right)^2 = ua^4 + 64v.$$

Hence, equation (4.1) is satisfied. Now it suffices to apply Proposition 4 to get the equivalence between (ii) and (iii). It is well known that for $d \equiv 1 \pmod 4$ condition $2 \nmid h_k$ is equivalent to ([**8**]):

$$d \text{ prime or}$$

$$d = qq', \quad q \equiv q' \equiv 3 \pmod 4.$$

In the last case, the norm of the fundamental unit is 1 and, by the Remark at the end of §3, we have that only the plus sign is possible in (4.2). Now, it is easy to see that this equation is not solvable for these values of d. Hence, d must be a prime. In this case, the fundamental unit has norm -1 and only the minus sign is possible in (4.2). It is clear that the solvability of (4.2) implies $d \equiv 1 \pmod{16}$ so that the first assertion of Theorem 4 is proved. Let's assume a solution X, Y, u, v, of (4.1) such that $N(Xu) \equiv -8 \pmod{32}$. Let $F \in \mathfrak{O}_K$ be a uniformizing element for $\mathfrak{P}$, where $Y\mathfrak{O}_K = \mathfrak{P}^3$ and let us set $G = F^3/uY$. Then, the elliptic curve given by:

$$B = u^{-1}F^4, \quad AB = 2XG^2, \quad D = vG^4,$$

is admissible. It is not difficult to check Setzer's conditions (a) on A, B, which are equivalent to the following ones:

$$N(A) \equiv -2 \pmod 8, \quad \operatorname{tr}(A) \equiv 3 \pmod 4,$$
$$N(B-1) \equiv 0 \pmod 8.$$

To prove the last assertion of the theorem we count the number of admissible curves proceeding as in §3. Now, $\mathfrak{G}$ will stand for the set of the isomorphic admissible elliptic curves. Notice that since d is a prime, $d \equiv 1 \pmod{16}$ and $\mathfrak{P}$ is not principal, none of the conditions of Theorem 1 is satisfied. Hence, $\mathfrak{G}$ will have no g-admissible curves.

Assuming (4.2) solvable, we define:

$$\mathfrak{H} = \{C \in \mathfrak{O}_K\,;\ C > 0\,,\ N(C) = -256\,,\quad \operatorname{tr}(C) = \pm r^2\,,\ r \in \mathbf{Z}\,,\ (r\,,\ 2) = 1\}\,,$$

$$\Phi(E) = \Phi(A\,,\ B) = \left|\frac{B^3}{D}\right|^{1/2}.$$

We may set:

$$B^3 = uY^4G^4\,,\quad AB = 2XG^2\,,\quad D = vG^4\,, \tag{4.5}$$

where X, Y, u, v is a solution of (4.1) and $G\mathfrak{O}_K = \mathfrak{A}^3$, $\mathfrak{A}$ an ideal prime to 2 such that $\mathfrak{P}\mathfrak{A}$ is principal. Hence,

$$\frac{B^3}{D} = uv^{-1}Y^4 = N(v)u\bar{v}Y^4. \tag{4.6}$$

By Proposition 4, $u\bar{v}Y^4 = (uwY^2)^2$, $\operatorname{tr}(uwY^2) = r^2$, $r \in \mathbf{Z}$, $w \in \mathfrak{U}_K$, so that $\Phi(E) \in \mathfrak{H}$. To see that Φ is onto let's set $C = (\pm r^2 + s\sqrt{d})/2$. Then, $C = uP^2$ where $P\mathfrak{O}_K = \mathfrak{P}^3$, $N(P) = 8$, $u \in \mathfrak{U}_K^2$. We get an admissible elliptic curve by taking: $B = u^{-1}F^4$, $AB = \pm 2rPG^2$, (sign determined by $\operatorname{tr}(A) \equiv -1 \pmod 4$), where F, G are taken as above. Thus,

$$\Phi(E) = \left|\frac{uP^4G^4}{\bar{u}G^4}\right|^{1/2} = C.$$

Finally, $\Phi(A_1\,,\ B_1) = \Phi(A_2\,,\ B_2)$ iff $D_1/D_2 = (B_1/B_2)^3$. Assume that E_i is attached to the solution of (4.1) X_i, Y_i, u_i, v_i, $i = 1\,,\ 2$, in the way of (4.5). Clearly, we may assume by (4.6) that $Y_1 = Y_2$. Then we have $u_1/u_2 = v_1/v_2$ and since $Y_i^4u_i + 64v_i \in \mathfrak{O}_K^2$ for $i = 1\,,\ 2$ we conclude that $u_2 = u_1w^2$, $v_2 = v_1w^2$, $w \in \mathfrak{U}_K$. Hence, E_2 is attached to the solution $\pm 2wX_1$, Y, U_1w^2, v_1w^2. If $w \in \mathfrak{U}_K^2$, we have from (4.5) and the fact that $\mathfrak{A}_1$, $\mathfrak{A}_2$ are equivalent, the relation:

$$\frac{G_1}{G_2} = U^3\,,\quad U \in K^*$$

Hence, $B_1 = B_2U^4$ and from $A_1B_1/A_2B_2 = (G_1/G_2)^2$ we get $A_1 = A_2U^2$, so that E_1 and E_2 are isomorphic. The possibility $w \notin \mathfrak{U}_K^2$ never occurs since we must have $N(A_1) \equiv N(A_2) \equiv -2 \pmod 8$. □

REMARKS. (1) $d = 257$ is the first one to satisfy the conditions of Theorem 4.

(2) In case $2 \nmid h_k$, the diophantine conditions (iii) of Theorem 1 for the existence of g-admissible models can be reformulated as follows.

$d = 7$, 41 or $d = 7q$, $q \equiv 3 \pmod 4$, $x^2 - 4dy^2 = -7$ solvable,

$d = 2q$, $q \equiv 3 \pmod 4$, $x^2 - dy^2 = -2$ solvable,

d prime, $d \equiv 1 \pmod{16}$, $\mathfrak{P}$ *principal*, $r^4 - ds^2 = -256$ solvable.

We get solutions to all these equations taking, for instance, $d = 77$, $d = 6, 22, 38$, $d = 337$, respectively.

5. A table of all admissible curves defined over $K = \mathbf{Q}(\sqrt{d})$, $0 < d < 100$. Let E be an admissible curve defined over $K = \mathbf{Q}(\sqrt{d})$ $0 < d < 100$. Then we must have $d = 6, 7, 14, 22, 38, 41, 65, 77$ or 86 and E is isomorphic to one of the following curves:

$$E_i\colon y^2 = x^3 + Ax^2 + Bx, \quad \Delta = 2^{12}D, \quad 1 \le i \le 46$$

	d	A	B	D	j
E_1	6	$-2(\varepsilon - 1)$	4ε	ε^3	$(20)^3$
E_3	6	$-14(\varepsilon - 1)$	$4\bar{\varepsilon}$	ε	$64(4\varepsilon^4 + 1)^3/\varepsilon^4$
E_5	6	$14(\varepsilon - 1)\varepsilon$	4ε	ε^7	$64(4\varepsilon^4 + 1)^3/\varepsilon^4$
E_7	7	$-(1 + 2\varepsilon^2)$	$16\varepsilon^3$	ε^6	$(255)^3$
E_9	7	$2(1 + 2\varepsilon^2)$	1	ε^3	$(256\varepsilon^2 + \bar{\varepsilon})^3$
E_{11}	7	$-2(1 + 2\varepsilon^2)$	1	ε^3	$(256\varepsilon^2 + \bar{\varepsilon})^3$
E_{13}	7	$8\varepsilon - 1$	$16\varepsilon^2$	$-\varepsilon^6$	$(-15)^3$
E_{14}	7	$-(8\varepsilon - 1)$	$16\varepsilon^2$	$-\varepsilon^6$	$(-15)^3$
E_{15}	14	$-3(\varepsilon - 1)/2$	16ε	$-\varepsilon^3$	$(-15)^3$
E_{17}	14	$3(\varepsilon - 1)$	$-\varepsilon$	ε^3	$(255)^3$
E_{19}	22	$-2(\varepsilon - 1)/7$	4ε	ε^3	$(20)^3$
E_{21}	38	$2(\varepsilon - 1)/3$	4ε	ε^3	$(20)^3$
E_{23}	41	$(3\varepsilon - 1)/2$	$\varepsilon(\varepsilon - 1)/2$	ε^4	$(\varepsilon - 16)^3/\varepsilon$
E_{25}	41	$(\varepsilon + 43)/10$	$(\varepsilon + 1)/2$	$-\varepsilon$	$(17)^3\bar{\varepsilon}$
E_{27}	41	$-2\varepsilon^2$	ε^2	ε^7	$(256\varepsilon + 1)^3/\varepsilon$
E_{29}	65	$2\varepsilon^2 - 1$	$16\varepsilon^3$	ε^6	$(257)^3$
E_{30}	65	$10\varepsilon^2 - 5$	$400\varepsilon^3$	$(5\varepsilon)^6$	$(257)^3$
E_{31}	65	$8\varepsilon + 1$	$16\varepsilon^2$	ε^6	$(17)^3$
E_{32}	65	$40\varepsilon + 5$	$400\varepsilon^2$	$(5\varepsilon)^6$	$(17)^3$
E_{33}	65	$(\varepsilon + 3)/2$	$(\varepsilon + 1)^2/4$	$-\varepsilon^3$	$(8 + \bar{\varepsilon})^2$
E_{35}	65	$5(\varepsilon + 3)/2$	$25(\varepsilon + 1)^2/4$	$-5^6\varepsilon^3$	$(8 + \bar{\varepsilon})^2$
E_{37}	65	$-2(2\varepsilon^2 - 1)$	1	ε^3	$(256\varepsilon^2 - \bar{\varepsilon})^3$
E_{39}	65	$-10(2\varepsilon^2 - 1)$	25	$5^6\varepsilon^3$	$(256\varepsilon^2 - \bar{\varepsilon})^3$
E_{41}	77	$3(\varepsilon^3 - 1)/10$	$16\varepsilon^3$	$-\varepsilon^9$	$(-15)^3$
E_{43}	77	$-3(\varepsilon^3 - 1)/5$	$-\varepsilon^3$	ε^9	$(255)^3$
E_{45}	86	$2(\varepsilon - 1)/51$	4ε	ε^3	$(20)^3$

$E_i = E_{i-1}^{\sigma}$ for every missing i, $0 \leq i \leq 46$, where σ is the non-trivial automorphism of K. In each case, ε stands for the fundamental unit of the respective field.

All the curves listed above are g-admissible except for $d = 65$, where E_{30}, E_{32}, E_{35}, E_{36}, E_{39} and E_{40} clearly cannot have a global minimal model. This table has been computed using the results given in this paper. Fields having an even number of divisor classes have been treated in a straightforward way. None of them (excepting $d = 65$) supplies admissible elliptic curves.

Acknowledgment. The author wishes to express his gratitude to Enric Nart for his help, especially in the conception of Theorem 2.

References

[1] J. H. E. Cohn, *The diophantine equation* $x^4 - Dy^2 = 1$, Quart. J. Math. Oxford, **26** (3) (1975), 279–281.

[2] S. Comalada and E. Nart, *Courbes elliptiques avec bonne réduction partout*, C. R. Acad. Sci. Paris Sér. I Math., **305** (1987), 223–224.

[3] W. LeVeque, *Reviews in Number Theory*, Amer. Math. Soc., **2** (1974).

[4] B. Setzer, *Elliptic curves over complex quadratic fields*, Pacific J. Math., **74** (1) (1978), 235–250.

[5] ——, *Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invariant*, Illinois J. Math., **25** (2) (1981), 233–245.

[6] R. J. Stroeker, *Reduction of elliptic curves over imaginary quadratic number fields*, Pacific J. Math., **108** (2) (1983), 451–463.

[7] J. T. Tate, *The arithmetic of elliptic curves*, Invent. Math., **23** (1974), 179–206.

[8] D. B. Zagier, *Zetafuncktionen und Quadratische Körper*, Springer-Verlag, 1981.

Received September 17, 1987 and in revised form July 17, 1989.

Universitat Autonoma de Barcelona
Bellaterra, Barcelona 08193 Spain

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph must be capable of being used separately as a synopsis of the entire paper. In particular it should contain no bibliographic references. Please propose a heading for the odd numbered pages of less than 35 characters. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the 1980 *Mathematics Subject Classification* (1985 *Revision*) scheme which can be found in the December index volumes of *Mathematical Reviews*. Supply name and address of author to whom proofs should be sent. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California 90024-1555-05.

There are page-charges associated with articles appearing in the Pacific Journal of Mathematics. These charges are expected to be paid by the author's University, Government Agency or Company. If the author or authors do not have access to such Institutional support these charges are waived. Single authors will receive 50 free reprints; joint authors will receive a total of 100 free reprints. Additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* (ISSN 0030-8730) is published monthly. Regular subscription rate: $190.00 a year (12 issues). Special rate: $95.00 a year to individual members of supporting institutions.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address should be sent to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924, U.S.A. Old back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

The Pacific Journal of Mathematics at P.O. Box 969, Carmel Valley, CA 93924 (ISSN 0030-8730) is published monthly. Second-class postage paid at Carmel Valley, California 93924, and additional mailing offices. Postmaster: send address changes to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Pacific Journal of Mathematics
Vol. 144, No. 2 June, 1990