ILLINOIS JOURNAL OF MATHEMATICS
Volume 25, Number 2, Summer 1981

# ELLIPTIC CURVES WITH GOOD REDUCTION EVERYWHERE OVER QUADRATIC FIELDS AND HAVING RATIONAL $j$-INVARIANT

BY

BENNETT SETZER

The problem of determining elliptic curves over complex quadratic fields having good reduction everywhere has been discussed by Stroeker in [2] and the present author in [1]. In [1], such curves were constructed with $j$-invariants $17^3$ and $257^3$. In this paper, we determine those rational $j$ for which there is a quadratic field $k$ and an elliptic curve over $k$ having good reduction everywhere and such that the elliptic curve has $j$-invariant $j$. Given a suitable $j$, the fields $k$ and the elliptic curves are determined.

Throughout, we work with the elliptic curve $E_{A,u}$ defined by

$$\begin{aligned} &y^2 = x^3 - 3A(A^3 - 1728)u^2x - 2(A^3 - 1728)^2u^3 && \text{if } A \neq 0, 12, \\ &y^2 = x^3 + u && \text{if } A = 0, \\ &y^2 = x^3 + ux && \text{if } A = 12. \end{aligned}$$

The discriminants are, respectively,

$$\begin{aligned} &2^{12}3^6(A^3 - 1728)^3u^6, && A \neq 0, 12, \\ &-2^4 \cdot 3^3 \cdot u^2, && A = 0, \\ &-2^6 \cdot u^3, && A = 12. \end{aligned}$$

The $j$-invariant of $E_{A,u}$ is $A^3$. The curves $E_{A,u}$ are the candidates for good reduction everywhere as seen from the following theorem.

THEOREM 1. *Let $E$ be an elliptic curve over a quadratic field $k$ such that $E$ has good reduction everywhere, and the $j$-invariant, $j(E)$, of $E$ is rational. Then $j(E) = A^3$ for some rational integer $A$ and $E$ is isomorphic to $E_{A,u}$ for some $u \in k^*$.*

Throughout this paper, $k = Q[\sqrt{m}]$ will denote a quadratic field, $m$ a square-free rational integer. $N(x)$ and Tr $(x)$ will denote the norm and trace, respectively, of $x$ in $k$. $\bar{x}$ will denote the conjugate over $Q$ of $x$ in $k$. $[x]$ will denote the ideal generated by $x$, over the maximal order of $k$.

Received May 1, 1979.

For not all values of $A$ will there be a field $k$ and $u \in k^*$ such that $E_{A,u}$ has good reduction everywhere over $k$. Indeed, let

$$\mathscr{R} = \{A \in Z\text{: if 2 divides } A \text{ then 16 divides } A \text{ or } A - 4\text{; and}$$
$$\text{if 3 divides } A \text{ then 27 divides } A - 12\}.$$

THEOREM 2. (a) *Given a rational integer $A$, there is a quadratic field $k$ and $u \in k^*$ such that $E_{A,u}$ has good reduction everywhere over $k$ if and only if $A \in \mathscr{R}$.*

(b) *Let $A \in \mathscr{R}$ and let $D$ equal the square-free part of $A^3 - 1728$ (with the sign). For a quadratic field $k$, there is a $u \in k^*$ such that $E_{A,u}$ has good reduction everywhere over $k$ if and only if the following five conditions are true:*

(i) *$D$ divides the discriminant of $k$.*

(ii) *If $D$ is odd, then $\varepsilon D$ is a rational norm from $k$ where $\varepsilon = \pm 1$ and $\varepsilon D \equiv 1 \pmod 4$.*

(ii') *If $D$ is even, then $-D$ is a rational norm from $k$.*

(iii) *If $D \equiv \pm 3 \pmod 8$, then $m \equiv 5 \pmod 8$*

(iii') *If $D$ is even then $m \equiv 4 + D \pmod{16}$.*

*Further, if these conditions are satisfied by $k$, then there are $2^{s-1}$ curves $E_{A,u}$ (up to isomorphism) over $k$ having good reduction everywhere. Here, $s$ is the number of primes ramifying in $k/Q$.*

The proof of Theorem 2(a) shows that there are infinitely many real fields which support an $E_{A,u}$ with good reduction everywhere, provided $A \in \mathscr{R}$. As to complex quadratic fields, it is evidently necessary that $\varepsilon D > 0$ or $D < 0$ as $D$ is odd or even, respectively. Given this, the proof of Theorem 2(a) shows that infinitely many complex quadratic fields have $E_{A,u}$ with good reduction everywhere. It should be noted that $D$ is even, for $A \in \mathscr{R}$, if and only if $A \equiv 4 \pmod{16}$.

Stroeker shows (loc. cit.) that no elliptic curve over a complex quadratic field can have an integral model with unit discriminant (that is, have good reduction everywhere and a global minimal model). The $E_{A,u}$, however, give examples of such curves over real quadratic fields. If $k$ is real, $\eta$ will denote a fundamental unit of $k$.

THEOREM 3. *Let $A \in \mathscr{R}$, $k = Q[\sqrt{m}]$ satisfy the conditions of Theorem 2(b). Then, for some $u \in k^*$, $E_{A,u}$ has good reduction everywhere and a global minimal model if and only if $k$ is real, $N(\delta) = \varepsilon D$ for some $k$-integer $\delta$, and, if $m \equiv 3 \pmod 4$, $\mathrm{Tr}(\delta) \equiv 2 \pmod 4$ for some such $\delta$. If $A$ and $k$ satisfy these further conditions, the number of such $E_{A,u}$ (up to isomorphism) is*

1 *if $N(\eta) = -1$,*
2 *if $N(\eta) = +1$ and $m \not\equiv 3 \pmod 4$,*
4 *if $m \equiv 3 \pmod 8$,*
2 *if $m \equiv 7 \pmod 8$ and $\mathrm{Tr}(\eta) \equiv 0 \pmod 4$,*
4 *if $m \equiv 7 \pmod 8$ and $\mathrm{Tr}(\eta) \equiv 2 \pmod 4$.*

The curves with $A = 17$ and 257 have 2-division points over their fields of definition. All values of $A$ giving such curves are described in the following result.

THEOREM 4. *An elliptic curve $E$ over a quadratic field $k$ having rational $j$-invariant and good reduction everywhere has a 2-division point over $k$ if and only if the $j$-invariant is one of* $17^3$, $257^3$, $-15^3$, $255^3$, or $20^3$.

The $D$ of Theorem 2(b) is 65, 65, $-7$, 7, 2 respectively. As 65, 65, $-7$, $-7$, $-2$, respectively, must be a rational norm from $k$, only the first two values of $A$ can give curves over complex quadratic fields. This is consistent with [1].

Section 1 gives the proofs of the Theorems and Section 2 gives some examples.

## Section 1

The following lemma collects all the facts needed to determine whether $E_{A,u}$ has good reduction locally. Indeed, part (a) is true for any valuation not dividing 2 or 3 while (b)–(e) are true provided the valuation is locally quadratic. The proof makes heavy use of Tate's exposition of the formulae describing changes of variables and their effect on models of a given curve [3, p. 299]. Throughout, valuations are normalized to be onto the rational integers.

LEMMA. *Let $A$ be a rational integer, $A \neq 0$, 12 and let $k = Q[\sqrt{m}]$ be a quadratic field and $u$ a non-zero element of $k$. If $v$ is a valuation of $k$, then $E_{A,u}$ has good reduction at $v$ if and only if all of the following conditions are satisfied:*

(a) *If* $v(2) = v(3) = 0$ *then* $2v(u) \equiv v(A^3 - 1728) \pmod 4$.

(b) *If $v$ divides 3 and 3 does not divide $A$ then* $v(u) \equiv v(3) \pmod 2$.

(c) *If $v$ divides 3 and 3 divides $A$ then*

$$A \equiv 12 \pmod{27} \quad \text{and} \quad v(3) + v(A - 12) + 2v(u) \equiv 0 \pmod 4.$$

(d) *If $v$ divides 2 and 2 does not divide $A$ then $u = u_1 u_2^2$ where $u_1 \equiv w^2 \pmod{\mathfrak{p}^{v(4)}}$, $u_1$, $u_2$, $w$ are in $k$, $v(w) = 0$ and $\mathfrak{p}$ is the prime at $v$.*

(e) *If $v$ divides 2 and 2 divides $A$ then one of the following is true:*

(i) 16 *divides $A$, $u = 2u_1 u_2^2$ where $u_1 \equiv -w^2 \pmod{\mathfrak{p}^{v(4)}}$, $u_1$, $u_2$, $w$ are in $k$, $v(w) = 0$ and $\mathfrak{p}$ is the prime at $v$.*

(ii) 16 *divides* $A - 4$, $m \equiv 6B \pmod 8$, $u = u_1 u_2^2$ *where* $u_1 = a + b\sqrt{m}$, $v(u_1) = 1$, $a \equiv 3B + 5m/2 \pmod 8$, $B = (A - 12)/8$.

It should be noted that in (e) (ii), $m \equiv 2 \pmod 4$ necessarily since $B$ is odd.

*Proof.* A necessary condition for good reduction at a valuation $v$ is that $v(\Delta) \equiv 0 \pmod{12}$ where $\Delta$ is the discriminant of a model of the curve in question. Applied to $E_{A,u}$, the congruences on $v(u)$ in (a)–(c) are seen to be necessary. Throughout the proof, $\mathfrak{p}$ will be the prime of $v$.

(a) An elliptic curve $E$ has good reduction at a valuation $v$, $v$ not dividing 2 or 3, if and only if for every model of $E$, $v(\Delta) \equiv 0 \pmod{12}$ and $3v(c_4) \geq v(\Delta)$ where $\Delta$ is the discriminant of that model and $c_4$ is as defined in [3]. Applied to $E_{A,u}$ and assuming $2v(u) \equiv v(A^3 - 1728) \pmod 4$, both conditions are seen to be true.

(b) Let $u = 3u_1$. Assuming $v(u) \equiv v(3) \pmod 2$, then $v(u_1) \equiv 0 \pmod 2$. Adjusting $u_1$ by a square, we may assume $v(u_1) = 0$. The transformation $x \mapsto x + r$ where $r \equiv -3A^2u_1 \pmod{\mathfrak{p}^{v(9)}}$ puts $E_{A,u}$ in the form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

The following congruences hold:

$$\begin{aligned} a_2 &= 3r \equiv 0 \pmod{\mathfrak{p}^{v(9)}}, \\ a_4 &\equiv 3(r - 3A^2u_1)(r + 3A^2u_1) \equiv 0 \pmod{\mathfrak{p}^{v(81)}}, \\ a_6 &\equiv (r + 3A^2u_1)^2(r - 6A^2u_1) \equiv 0 \pmod{\mathfrak{p}^{v(729)}}, \end{aligned}$$

and $v(\Delta) = 12v(3)$. Since $v(a_i) \geq iv(\Delta)/12$ for $i = 2, 4, 6$, $E_{A,u}$ has good reduction at $v$.

(c) The cases $A \equiv 0 \pmod 9$, $A \equiv 6 \pmod 9$, $A \equiv 3, 21 \pmod{27}$, $A \equiv 12 \pmod{27}$ are treated in that order.

Suppose first that 9 divides $A$. From $v(\Delta) \equiv 0 \pmod{12}$, $2v(u) \equiv v(3) \pmod 3$. So, $v(3) = 2$ and $v(u) \equiv 1 \pmod 2$. Letting $A = 3A_1$ and changing variables by $x \mapsto 9x$, $y \mapsto 27y$ $E_{A,u}$ becomes

$$y^2 = x^3 - 9A_1(27A_1^3 - 64)u^2x - 2(27A_1^3 - 64)^2u^3 \tag{2}$$

with $\Delta = 2^{12} \cdot 3^3(27A_1^3 - 64)^3u^6$. We may assume $v(u) = 1$. $E_{A,u}$ has good reduction at $v$ only if there is a $v$-integral $r$ such that $x \mapsto x + r$ transforms (2) to (1) with $v(a_i) \geq 2i$, $i = 2, 4, 6$. That is

$$\begin{gathered} 3r \equiv 0 \pmod{\mathfrak{p}^2}, \qquad 3r^2 \equiv 0 \pmod{\mathfrak{p}^4}, \\ 16u^3 + 9A_1u^2r + r^3 \equiv 0 \pmod{\mathfrak{p}^6}. \end{gathered} \tag{3}$$

These congruences imply $v(r) = 1$ and $r^3 \equiv 11u^3 \pmod{\mathfrak{p}^6}$. But, since $v(r) = v(u) = 1$, $r$, $u \equiv \pm\sqrt{m} \pmod{\mathfrak{p}^2}$, so (3) implies $\pm m \equiv 11(\pm m) \pmod{\mathfrak{p}^6}$ or $\pm 1 \equiv 11 \pmod 9$ since 3 divides $m$. This contradiction shows that no such $r$ can be found, so $E_{A,u}$ has bad reduction at $v$.

Next, assume $A \equiv 6 \pmod 9$. From $v(\Delta) \equiv 0 \pmod{12}$, $2v(u) \equiv v(3) \pmod 4$ so $v(3) = 2$, $v(u) \equiv 1 \pmod 2$. Letting $A = 3A_1$ and transforming $E_{A,u}$ as in the previous case,

$$y^2 = x^3 - 3A_1(A_1^3 - 64)u^2x - 2(A_1^3 - 64)^2u^3 \tag{4}$$

with $\Delta = 2^{12} \cdot 3^3 \cdot (A_1^3 - 64)^3u^6$. We may assume $v(u) = 1$. As in the previous case, we must solve these congruences

$$\begin{gathered} 3r^2 - 3A_1(A_1^3 - 64)u^2 \equiv 0 \pmod{\mathfrak{p}^4}, \\ r^3 - 3A_1(A_1^3 - 64)u^2r - 2(A_1^3 - 64)u^3 \equiv 0 \pmod{\mathfrak{p}^6}. \end{gathered} \tag{5}$$

From the first congruence, $v(r) \geq 1$. Using this and $A_1 \equiv 2 \pmod 3$, the second congruence in (5) becomes

$$r^3 + 3ru^2 + u^3 \equiv 0 \pmod{\mathfrak{p}^6} \tag{6}$$

From this, $v(r) = 1$ so $r \equiv \pm u \pmod{\mathfrak{p}^2}$. Using this, (6) implies $5u^3 \equiv 0 \pmod{\mathfrak{p}^6}$ or $3u^3 \equiv 0 \pmod{\mathfrak{p}^6}$ neither of which holds. $E_{A,u}$ has bad reduction at $v$.

Next, assume that $A \equiv 3$ or $21 \pmod{27}$. From $v(\Delta) \equiv 0 \pmod{12}$, $v(3) \equiv 2v(u) \pmod 4$, so $v(3) = 2$ and $v(u) \equiv 1 \pmod 2$. As before, letting $A = 3A_1$ and transforming $E_{A,u}$ and assuming $v(u) = 1$, the following congruences must be solved:

$$\begin{aligned} 3r^2 - 3A_1(A_1^3 - 64)u^2 &\equiv 0 \pmod{\mathfrak{p}^8}, \\ r^3 - 3A_1(A_1^3 - 64)u^2 r - 2(A_1^3 - 64)^2 u^3 &\equiv 0 \pmod{\mathfrak{p}^{12}}. \end{aligned} \tag{7}$$

However, since $v(A_1^3 - 64) = 4$, no value of $v(r)$ is consistent with the second congruence in (7). $E_{A,u}$ has bad reduction at $v$.

Finally, assume $A \equiv 12 \pmod{27}$. As noted before, the congruence condition in the lemma is necessary for good reduction at $v$. Assuming this, we may, indeed, assume $v(u) = \frac{1}{2}(v(3) + v(A - 12))$. Then $v(\Delta) = 18v(3) + 6v(A - 12)$. In the notation of (1), applied to $E_{A,u}$,

$$6v(a_2) \geq v(\Delta), \qquad 3v(a_4) = 18v(3) + 6v(A - 12) \geq v(\Delta)$$

and, since $v(A - 12) \geq 3v(3)$,

$$2v(a_6) = 15v(3) + 7v(A - 12) \geq v(\Delta).$$

So, $E_{A,u}$ has good reduction at $v$.

(d) In this part, and in (c), the following result is used. Let $E$ be an elliptic curve over a number field $k$ and let $v$ be a valuation of $K$ dividing 2. Then $E$ has good reduction at $v$ if and only if for any model (1) of $E$, with $a_2 = 0$, $\Delta = 2^{12}D$, $v(D) = 0$, the following congruences can be solved:

$$\begin{aligned} a_4 &\equiv -3s^4 + 8s\alpha \pmod{\mathfrak{p}^{v(16)}}, \\ a_6 &\equiv s^2 a_4 + s^6 + 16\alpha^2 \pmod{\mathfrak{p}^{v(64)}}. \end{aligned} \tag{8}$$

These are obtained from the transformation formulae (1.14) on page 301 in [3] by letting $4\alpha = t - sr - s^3$. Note that if $s$, $\alpha$ is one solution of (8) and $s_1 \equiv s \pmod{\mathfrak{p}^{v(2)}}$, say $s_1 = s + 2w$, then, with $\alpha_1 \equiv \alpha + s^2 w + sw^2 \pmod{\mathfrak{p}^{v(2)}}$, $s_1$, $\alpha$, is another solution.

Considering the situation in (1), from $v(\Delta) \equiv 0 \pmod{12}$ applied to $E_{A,u}$, $v(u) \equiv 0 \pmod 2$. We may assume $v(u) = 0$. The result above applies and (8) becomes

$$\begin{aligned} -3A^4u^2 &\equiv -3s^4 + 8s\alpha \pmod{\mathfrak{p}^{v(16)}}, \\ -2A^6u^3 &\equiv -3A^4u^2s^2 + s^6 + 16\alpha^2 \pmod{\mathfrak{p}^{v(64)}}. \end{aligned} \tag{9}$$

From the first congruence, $v(s) = 0$. From the second,

$$(s^2 - A^2u)^2(s^2 + 2A^2u) \equiv 0 \pmod{\mathfrak{p}^{v(16)}}$$

so $u \equiv A^2u \equiv s^2 \pmod{\mathfrak{p}^{v(4)}}$, which shows necessity. Conversely, if $u \equiv s^2 \pmod{\mathfrak{p}^{v(4)}}$ with $v(s) = 0$ and $\alpha$ is chosen so that

$$\alpha \equiv (s^4 - A^4u^2)/8s \pmod{\mathfrak{p}^{v(2)}},$$

the congruences (9) are satisfied. So, $E_{A,u}$ does have good reduction at $v$.

(e) The cases $A \equiv 2 \pmod 4$, $A \equiv 8 \pmod{16}$, $A \equiv 0 \pmod{16}$, $A \equiv 12 \pmod{16}$ and $A \equiv 4 \pmod{16}$ are considered, in that order. First, assume $A \equiv 2 \pmod 4$. From $v(\Delta) \equiv 0 \pmod{12}$, $2v(u) \equiv v(2) \pmod 4$. So $v(2) = 2$ and $v(u) \equiv 1 \pmod 2$. We may assume $v(u) = -3$, so (8) applies. Now, $v(a_4) = 2$ (in the notation of (1)) so the first congruence in (8) cannot be satisfied. $E_{A,u}$ has bad reduction at $v$.

Next, assume $A \equiv 8 \pmod{16}$. Then, from $v(\Delta) \equiv 0 \pmod{12}$, $v(u) \equiv v(2) \pmod 2$. We may assume $v(u) = -3v(2)$ so (8) applies. But, $v(a_4) = 3v(2) = 3$ or 6 so the first congruence in (8) cannot be satisfied. $E_{A,u}$ has bad reduction at $v$.

Next assume $A \equiv 0 \pmod{16}$. From $v(\Delta) \equiv 0 \pmod{12}$, $v(u) \equiv v(2) \pmod 2$. We may assume $v(u) = -3v(2)$, so (8) applies. Let $u_3 = 8u$, so $v(u_3) = 0$. In the notation of (1), $v(a_4) \geq 4v(2)$. Also, $a_6 \equiv -16u_3^3 \pmod{64}$. So, (8) is equivalent to $s \equiv 0 \pmod{\mathfrak{p}^{v(2)}}$ and $u_3^3 \equiv -\alpha^2 \pmod{\mathfrak{p}^{v(4)}}$. $E_{A,u}$ has good reduction at $v$ if and only if $u_3 \equiv -w^2 \pmod{\mathfrak{p}^{v(4)}}$ for some $w$ with $v(w) = 0$. This is equivalent to (e) (i).

Next, assume $A \equiv 12 \pmod{16}$. Let $e = v(A - 12)/v(2) \geq 4$. From $v(\Delta) \equiv 0 \pmod{12}$, $v(u) \equiv \frac{1}{2}ev(2) \pmod 2$. We may assume $v(u) = -\frac{1}{2}(e + 4)v(2)$, so (8) applies. In the notation of (1), $v(a_4) = 2v(2)$ and $v(a_6) \geq 5v(2)$. (8) implies

$$\begin{aligned} a_4 &\equiv -3s^4 + 8s\alpha \pmod{\mathfrak{p}^{v(4)}}, \\ 0 &\equiv s^2a_4 + s^6 + 16\alpha^2 \pmod{\mathfrak{p}^{v(32)}}. \end{aligned} \tag{10}$$

From the first congruence, $v(s) = \frac{1}{2}v(2)$, so $v(2) = 2$. Substituting for $a_4$ in the second congruence, and simplifying,

$$s^6 - 4s^3\alpha - 8\alpha^2 \equiv 0 \pmod{\mathfrak{p}^8}.$$

Thus, $v(\alpha) = 0$ and

$$\left(\frac{s^3}{2\alpha}\right)^2 - 2\frac{s^3}{2\alpha} - 2 \equiv 0 \pmod{\mathfrak{p}^4}.$$

Now, $s \equiv s^3/2\alpha \pmod{\mathfrak{p}^2}$ so $s^2 \equiv 2s + 2 \pmod{\mathfrak{p}^4}$. From (10), then

$$a_4 \equiv -4 + 8s \pmod{\mathfrak{p}^8}. \tag{11}$$

But, $a_4 = 4bw_0^2$ or $2bw_1^2$ where $b \in Z$, $v(b) = v(w_0) = 0$, $v(w_1) = 1$. Since $w_0 \equiv 1$ or $1 + s \pmod{\mathfrak{p}^2}$, $w_0^2 \equiv \pm 1 \pmod{\mathfrak{p}^4}$. Similarly, $w_1^2 \equiv 2 + 2s \pmod{\mathfrak{p}^4}$. The

two alternative forms for $a_4$ imply $a_4 \equiv \pm 4$ or $4 + 4s \pmod{\mathfrak{p}^6}$, respectively, both contradict (11), so $E_{A,u}$ has bad reduction at $v$.

Finally, assume $A \equiv 4 \pmod{16}$. From $v(\Delta) \equiv 0 \pmod{12}$, $2v(u) \equiv v(2) \pmod 4$ so $v(2) = 2$ and $v(u) \equiv 1 \pmod 2$. We may assume $v(u) = -7$, so (8) applies. Let $u = 16u_1$, so $v(u) = 1$. In the notation of (1),

$$a_4 = -3A(A^3 - 1728)2^{-8}u_1^2 \equiv 2Bu_1^2 \pmod{\mathfrak{p}^{10}}$$

and

$$a_6 = -2(A^3 - 1728)^2 2^{-12}u_2^3 \equiv -8u_2^3 \pmod{\mathfrak{p}^{12}}$$

where $B = (A - 12)/8$ is an odd integer. The first congruence in (8) implies $v(s) = 1$, so (8) is equivalent to

$$\begin{aligned} 2Bu_2^3 &\equiv -3s^4 + 8s\alpha \pmod{\mathfrak{p}^8}, \\ -8u_2^3 &\equiv 2s^2Bu_2 + s^6 + 16\alpha^2 \pmod{\mathfrak{p}^{12}} \end{aligned} \tag{12}$$

Substituting the first into the second, taken $\pmod{\mathfrak{p}^{10}}$, and simplifying, $s^6 + 4s^3 - 4s^3\alpha - 8\alpha^2 \equiv 0 \pmod{\mathfrak{p}^8}$.

From this, $v(\alpha) = 0$ and $s^6 \equiv 8 \pmod{\mathfrak{p}^8}$. Thus, $s^2 \equiv 2 \pmod{\mathfrak{p}^4}$ and $m$ is even. By the remarks following (8), we may assume $s = \sqrt{m}$ since $s \equiv \sqrt{m} \pmod{\mathfrak{p}^2}$. Also, we may take $\alpha = 1$ or $1 + \sqrt{m}$. Now $u_1 \equiv 2a_1 + b\sqrt{m} \pmod{64}$ where $a_1$ and $b$ are rational, $v$-integral and $v(b) = 0$. Substituting into (12), (12) is equivalent to

$$\begin{aligned} 2a_1 &\equiv 3B + 5m/2 \pmod{\mathfrak{p}^6}, \qquad m \equiv 6B \pmod{\mathfrak{p}^6}, \\ \alpha &\equiv 1 + ((m + 2B)/8 - 1)\sqrt{m} \pmod{\mathfrak{p}^2}. \end{aligned}$$

These are equivalent to the conditions in (e) (ii). ∎

*Proof of Theorem* 1. The curve $E'_{j,u}$ given by

$$y^2 = x^3 - 3j(j - 1728)u^2x - 2j(j - 1728)^2u^3 \tag{13}$$

is an elliptic curve with $j$-invariant $j$ if $j \neq 0, 1728$, and $u \neq 0$. If $E$ is any elliptic curve, over a field $K$, with $j$-invariant $j \in K, j \neq 0, 1728$, then $E$ is isomorphic to $E'_{j,u}$ for some $u \in K^*$. Note also that $E'_{j,u_1}$ and $E'_{j,u_2}$ are isomorphic over $K$ if and only if $u_1 u_2 \in K^{*2}$. If $K$ is a number field, then for $E'_{j,u}$ to have good reduction everywhere over $K$ it is necessary that the ideal generated by the discriminant of $E'_{j,u}$ be a 12th power. Since the discriminant of $E'_{j,u}$ is $2^{12} \cdot 3^6 \cdot (j - 1728)^3 j^2 u^6$, this implies that $j$ generates an ideal which is a cube. If $K$ is quadratic over $Q$ and $j \in Q$, this implies that $j = A^3$ where $A \in Q^*$. It is evident that for an elliptic curve to have good reduction at a valuation of $K$, it is necessary for the $j$-invariant of the curve to be integral at $j$. In the case at hand, this implies that $A \in Z$. Now, letting $j = A^3$ in (13) and replacing $u$ by $A^{-1}u$, $E_{A,u}$ results for $A \neq 0, 12$.

If an elliptic curve over a field $K$ has $j$-invariant 0 or 1728, then it is isomorphic to $E_{0,u}$ or $E_{12,u}$, respectively, with $u \in K^*$. Note that the isomorphism class of $E_{0,u}$ (resp. $E_{12,u}$) determines $u$ up to a sixth power (resp. fourth power). ∎

*Proof of Theorem* 2. (a) If $A \neq 0$, 12 and $A \notin \mathscr{R}$ then the lemma shows that $E_{A,u}$ has bad reduction at some valuation dividing 6 over any quadratic field $k$. (Indeed, $E_{A,u}$ has bad reduction over any number field with a locally quadratic valuation dividing each of 2 and 3.) We see next that $E_{0,u}$ and $E_{12,u}$ must have bad reduction also.

Consider $E_{0,u}$. If $v_3$ is a valuation of $k$ dividing 3 then from $v_3(\Delta) \equiv 0 \pmod{12}$, $3v_3(3) + 2v_3(u) \equiv 0 \pmod{12}$ so $v_3(3) = 2$ and $v_3(u) \equiv 3 \pmod 6$. We may assume $v_3(u) = 3$. For $E_{0,u}$ to have good reduction at $v$ it is necessary that $r$ exist such that

$$-3r \equiv 0 \pmod 3, \qquad -3r^2 \equiv 0 \pmod 9, \qquad -r^3 + u \equiv 0 \pmod{27}$$

since $v_3(\Delta) = 12$. These congruences are equivalent to $v_3(r) = 1$ and $u \equiv r^3 \pmod{27}$. Now, $3 \mid m$ since $v_3$ ramifies, so $r = x + y\sqrt{m}$ where $x$, $y$ are 3-integral rational, 3 divides $x$, and 3 does not divide $y$. Then, $u \equiv \pm m\sqrt{m} \pmod{27}$ so

$$N(u) \equiv \pm 27 \pmod{243} \tag{14}$$

If $v_2$ is a valuation of $k$ dividing 2, from $v_2(\Delta) \equiv 0 \pmod{12}$, $v_2(u) \equiv 4v_2(2) \pmod 6$. We may assume $v_2(u) = 4v_2(2)$. For any valuation $v$ of $k$ not dividing 6, similarly, $v(u) \equiv 0 \pmod 6$. Thus $[u] = [16]\mathfrak{p}_3^3\mathfrak{a}^6$ where $\mathfrak{p}_3^2 = [3]$ and $\mathfrak{a}$ is integral. So,

$$N(u) = \pm 16^2 \cdot 27 \cdot N(\mathfrak{a})^6 \equiv \pm 108 \pmod{243}$$

which contradicts (14). $E_{0,u}$ must have bad reduction at some valuation over $k$.

Next, consider $E_{12,u}$. Let $v_2$ be a valuation of $k$ dividing 2. from $v_2(\Delta) \equiv 0 \pmod{12}$, $v_2(u) \equiv 2v_2(2) \pmod 4$. We may assume $v_2(u) = 2v_2(2)$ for all valuations dividing 2, so (8) applies. Letting $u = 4u_1$, (8) becomes

$$\begin{aligned} 4u_1 &\equiv -3s^4 + 8s\alpha \pmod{16}, \\ 0 &\equiv 4s^2u_1 + s^6 + 16\alpha^2 \pmod{64}. \end{aligned} \tag{15}$$

By methods similar to those used in the lemma, $u_1 \equiv 1 + 2\sqrt{m} \pmod 4$ and $m \equiv 3 \pmod 4$ so $N(u_1) \equiv 5 \pmod 8$. But, for any valuation of $k$ not dividing 2, $v(u) = v(u_1) \equiv 0 \pmod 4$. Thus $[u_1] = \mathfrak{a}^4$ so $N(u_1) \equiv \pm 1 \pmod{16}$, a contradiction. $E_{12,u}$ has bad reduction at some valuation over $k$.

Given $A \in \mathscr{R}$, to show that there is a $k$ and $u \in k^*$ such that $E_{A,u}$ has good reduction everywhere, it is only necessary to show that there is a quadratic field $k$ satisfying the conditions of part (b) of this Theorem. This can be done as follows. Let $m = qD$ where $q$ is $\pm$ an odd prime. $k$ has the required properties, provided $q$ satisfies the following conditions:

(a′) For all primes $p$ dividing $D$, $(-\varepsilon q/p) = 1$.
(b′) $m > 0$ if $\varepsilon D < 0$.
(c′) $q \equiv 5D \pmod 8$ if $D \equiv \pm 3 \pmod 8$ and $q \equiv D + 1 \pmod 8$ if $D$ is even.

Here, $\varepsilon = -1$ if $D$ is even, otherwise as in (ii). The form of $m$ ensures that (i) is true, while (c′) ensures that (iii) and (iii′) are true. By Dirichlet's Theorem, there is such a prime $q$ satisfying all the conditions. These conditions imply that the norm equation $x^2 - my = \varepsilon D$ is everywhere locally solvable. Finally, Hasse's principle implies that $\varepsilon D$ is a rational norm from $k$, which is (ii) and (ii′).

(b) First consider the case that $A$ is odd and in $\mathscr{R}$. We show the necessity of (i), (ii), and (iii) first. According to the lemma, if $p$ is an odd prime dividing $D$ then $v(p) = 2$ for a valuation of $k$ dividing $p$. This implies (i). Let $3^2(A^3 - 1728) = Dd_1^2 d_2^4$ where $d_1$ and $D$ are square-free, rational integers. Parts (a)–(c) of the lemma imply $[u] = \mathscr{d} d_1 \mathfrak{a}^2$ where $\mathscr{d}^2 = [D]$. We may assume that $u$ is integral and relatively prime to 2, so $N(u) = \pm Dc^2$ where $c$ is an odd integer. Part (d) of the lemma implies that $u$ is a square (mod 4). This implies that $N(u) \equiv 1 \pmod 8$ unless $m \equiv 5 \pmod 8$ in which case $N(u) \equiv 5 \pmod 8$ is possible. This, with $N(u) = \pm Dc^2$, implies the necessity of (ii) and (iii).

Now assume that (i), (ii), (iii) are satisfied for a given odd $A \in \mathscr{R}$ and field $k$. (ii) implies that $[w] = \mathscr{d}\mathfrak{a}^2$ for some ideal $\mathfrak{a}$ and $w \in k^*$. Moreover, $w$ and $\mathfrak{a}$ may be chosen so that $N(w) = \varepsilon Dc^2$ where $c$ is an odd rational integer. Then, $u = d_2 w$ satisfies the conditions of the lemma for good reduction at all valuations not dividing 2. If $m \not\equiv 3 \pmod 4$, then $N(u) \equiv 1 \pmod 4$ implies that one of $\pm u$ is a square (mod 4). If $m \equiv 3 \pmod 4$ then $N(u) \equiv 1 \pmod 4$ implies that both $\pm u$ or both $\pm u\rho$ are squares (mod 4). Here, $\rho = \frac{1}{2}(m + 1) + \sqrt{m}$ and $[\rho] = \mathfrak{p}_2^{-2}[1 + \sqrt{m}]^2$ so $u\rho$ is still suitable at valuations not dividing 2. In any case, there is at least one $u \in k^*$ that satisfies all the conditions (a)–(d) of the lemma, so $E_{A,u}$ has good reduction everywhere over $k$.

To count the number of curves, up to isomorphism, for given $A$ and $k$, suppose that both $E_{A,u_0}$ and $E_{A,u_1}$ have good reduction everywhere over $k$ and $u_1$, $u_0$ are both relatively prime to 2. Let $u_0 = \alpha u_1$; then $\alpha \in k^*$, $[\alpha] = \mathfrak{a}^2$, $N(\alpha) > 0$, $\alpha$ is relatively prime to 2, and $\alpha$ is a square (mod 4). Conversely, given such an $\alpha$, and given $u_1$, then $E_{A,\alpha u_1}$ is easily seen to have good reduction everywhere over $k$. The number of such $\alpha$, modulo $k^{*2}$, is the desired number of curves. Now, from $[\alpha] = \mathfrak{a}^2$ and $N(\alpha) > 0$, $[\alpha] = [a\gamma^2]$ where $a$ is a square-free rational integer dividing the discriminant of $k$. Evidently, $\alpha = \pm a\gamma^2$ if $k$ does not have a non-trivial unit. If $\eta$ is a fundamental unit of norm 1, then, for some $x \in k^*$, $\eta = x^{-2}b$ where $b = N(x)$ is a square-free integer which divides the discriminant of $k$. Thus, if $\alpha = \pm\eta a\gamma^2$ then $\alpha = \pm ab(\gamma x^{-1})^2 = \pm a'(\gamma'')^2$. A standard set of $a$'s is built up from the following set. Let $a_1, \ldots, a_t$ be chosen to be distinct, positive, odd rational integers such that each $a_i$ divides $m$, and $a_i a_j \neq |m|$ for all $i, j$. Taking $t$ to be as large as possible, $t = 2^{s-1}$ if $m \not\equiv 3 \pmod 4$, where $s$ is the number of primes ramifying in $k/Q$.

Consider, first, $m \not\equiv 3 \pmod 4$. It is easily seen that all of $a_1, \ldots, a_t, -a_1, \ldots, -a_t$ are distinct mod $k^{*2}$. By the above argument, $\alpha = \pm a_i \gamma^2$ for some $i$. But, 1 is a square (mod 4) and 3 is not, so for exactly half of the $\pm a_i$ is $\alpha$ a square (mod 4). There are, therefore, $t = 2^{s-1}$ choices of $\alpha$, as desired.

Consider next $m \equiv 3 \pmod 4$. All of $a_1, \ldots, -a_1, \ldots, \rho a_1, \ldots, -\rho a_1, \ldots, -\rho a_t$ are distinct mod $k^{*2}$. By the previous argument $\alpha = \pm a_i \gamma^2$ or $\pm 2a_i \gamma^2$ for some $i$. If $\alpha = \pm 2a_i \gamma^2$ then

$$\alpha = \pm a_i \rho \left( \frac{2\gamma}{1 + \sqrt{m}} \right)^2,$$

so any suitable $\alpha$ is equivalent to one of the entries in the above list. Now, both 1 and 3 are squares (mod 4) while $\rho$ is not so there are $2t = 2^{s-1}$ choices of $\alpha$, as desired. This completes the case $A$ odd.

If 16 divides $A$, the argument is similar. The 2-condition is that $-u$ is a square (mod 4), so the counting is exactly the counting of $\alpha$'s as above.

Finally, consider the case $A \equiv 4 \pmod{16}$. As before, (i) is necessary. By the lemma, $u_1$ must be found so that $[u_1] = \mathscr{d} d_1 \mathscr{a}^2$ ($\mathscr{d}$, $d_1$ as before), and $u_1 = a + b\sqrt{m}$ where $a \equiv 3B + (5m/2) \pmod 8$ and $a$, $b$ are rational integers. Now, $B \equiv (3m/2) \pmod 4$ so $a \equiv 2 \pmod 4$. Thus, from

$$N(u_2) \equiv \varepsilon D c^2 \tag{16}$$

we have

$$4 - m \equiv \varepsilon D \pmod{16}. \tag{17}$$

But, $D \equiv (A^3 - 1728)/64 \pmod{16}$ so $D \equiv 6B + 12 \pmod{16}$. So, $\varepsilon = 1$ would imply $m \equiv 0 \pmod 4$. Thus $\varepsilon = -1$, which, with (16), implies (ii′) and, with (17), implies (iii′).

Suppose, conversely, that (i), (ii′) and (iii′) are satisfied for given $A$ and $k$. There is a $u_1 \in k$ such that $[u_1] = [d_1]\mathscr{d}\,\mathscr{a}^2$ and $N(u) = -Dc^2$, $c$ an odd integer. From (iii′), $u_2 = a + b\sqrt{m}$ where $a$, $b$ are rational integers, $a \equiv 2 \pmod 4$, and $b \equiv 1 \pmod 2$. Thus, one of $\pm u_2$ will satisfy all the conditions of the lemma, so one of $E_{A,\pm u}$ will have good reduction everywhere over $k$. The counting reduces to counting those among $a_1, \ldots, a_t, -a_1, \ldots, -a_t$ (defined as before) which are congruent to 1 (mod 4). There are $2^{s-1}$ choices, so there are $2^{s-1}$ curves $E_{A,u}$ over $k$ with good reduction everywhere. ∎

*Proof of Theorem* 3. Preserving the notation of Theorem 2, for $E_{A,u}$ to have good reduction everywhere, it is necessary that $[u] = \mathscr{d}[d_1]\mathscr{a}^2$. Thus, the discriminant of $E_{A,u}$ generates the ideal $[2d_1 d_2]^{12}\mathscr{d}^{12}\mathscr{a}^{12}$. Assuming $E_{A,u}$ has good reduction everywhere over $k$, it has a global minimal model if and only if $\mathscr{d}\mathscr{a}$ is principal (Theorem 1, [1]). Since $\mathscr{d}\mathscr{a}^2$ is principal, this occurs only if both $\mathscr{d}$ and $\mathscr{a}$ are principal. We may assume $\mathscr{a} = [1]$. Then $\delta = u/d_1$ is integral and $N(\delta) = \varepsilon D$. If $m \equiv 3 \pmod 4$, then $A \not\equiv 4 \pmod{16}$, so $u$ is relatively prime to 2

and $u \equiv \pm 1 \pmod 4$ to ensure good reduction at all valuations dividing 2. This implies that Tr $(\delta) \equiv 2 \pmod 4$. Finally, if $k$ were complex, then $\delta = \pm\sqrt{m}$ as $-m$ is the only possibility for $\varepsilon D$. But $u = \pm d_1\sqrt{m}$ cannot satisfy the conditions for (d) or (e) of the lemma. The conditions of Theorem 3 are thus seen to be necessary.

Assume, then, that all the conditions of Theorems 2 and 3 are satisfied for given $A$ and $k$. We have $\delta$ and $\eta$ defined as above. Arguing as above, $[u] = [d_1\delta]$ and this is sufficient to guarantee good reduction at all valuations not dividing 2. If $N(\eta) = -1$, $N(u) = \varepsilon D$ implies that the only choices for $u$ are $\pm d_1$. Exactly one of these will satisfy (d) and (e) of the lemma. So, one curve $E_{A,u}$ results. If $N(\eta) = 1$ and $m \not\equiv 3 \pmod 4$, then the choices of $u$ are among $\pm d_1\delta$ and $\pm\eta d_1\delta$. Just two will be correct for (d) and (e) of the lemma. If $m \equiv 3 \pmod 8$, then $\delta \equiv \pm 1 \pmod 4$ so $\varepsilon D$ is a principal factor in $k/Q$. Thus, $\delta/\bar{\delta}$ must be an odd power of $\eta$ so $\eta \equiv \pm 1 \pmod 4$. The choice for $u$ is among $\pm d_1\delta$ and $\pm\eta d_1\delta$. $A \not\equiv 4 \pmod{16}$ and all four choices satisfy (d) and (e) of the lemma, so four curves result. If $m \equiv 7 \pmod 8$ and Tr $(\eta) \equiv 0 \pmod 4$, then $\delta$ cannot be a principal factor in $k/Q$ (else, as before, $\eta \equiv \pm 1 \pmod 4$). So, $\delta = \pm\eta\sqrt{m}$, say, and $\eta \equiv \pm\sqrt{m} \pmod 4$. The choices for $u$ are $\pm d_1\sqrt{m}$ and $\pm\eta d_1\sqrt{m}$ of which, only the latter pair will satisfy (d) and (e) of the lemma, so two curves result. Finally, if $m \equiv 7 \pmod 8$ and Tr $(\eta) \equiv 2 \pmod 4$, then $\eta \equiv \pm 1 \pmod 4$ and $\delta \equiv \pm 1 \pmod 4$. All four of $\pm\eta d_1\delta$ and $\pm d_1\delta$ are satisfactory choices for $u$ so four curves result. All possibilities for $k$, $\eta$, have covered, so the proof is complete. ∎

*Proof of Theorem* 4. Assuming $A \neq 0, 12$, $E_{A,u}$ has a rational 2-division point if and only if $E_{A,1}$ does. But, a rational cubic has a root in a quadratic field if and only if it has a rational root. That is, $E_{A,1}$ is an elliptic curve with integral $j$-invariant and a rational 2-division point. Thus, $E_{A,1}$ has a model

$$y = x^3 + a_2x^2 + a_4x \tag{18}$$

with $a_2$, $a_4$ rational. Setting $\gamma = (16a_2^2/a_4) - 64$, we have

$$j = (\gamma + 16)^3\gamma^{-1} \quad \text{with } \gamma \in Q.$$

$\gamma \neq 0$ since (18) is nonsingular. For $j$ to be integral, it is necessary that $\gamma = \pm 2^r$ where $0 \leq r \leq 12$. For $j$ to be a cube, $r = 0, 3, 6, 9, 12$. Of the resulting $j$ values, only the five listed in the theorem are in $\mathscr{R}$. That $E_{A,1}$ indeed has a rational 2-division point for the given values may be checked directly or by noting that

$$y^2 = x^3 + (\gamma + 64)x^2 + 16(\gamma + 64)x$$

has $j$-invariant $(\gamma + 16)^3\gamma^{-1}$. ∎

The proof of Theorem 4 also allows the elliptic curves over $Q$ with integral $j$-invariant and a rational 2-division point to be determined.

## Section 2

Several examples are presented in this section. A computer program was run to determine small values of $|D|$ for values of $A$ in $\mathscr{R}$. In a search with $|A| \leq 21760$ the following values of $A$ and $D$ were found with $|D| \leq 100$:

| $A$ | 4 | −15 | 16 | −16 | 17 | 20 | −32 | 39 |
|---|---|---|---|---|---|---|---|---|
| $D$ | −26 | −7 | 37 | −91 | 65 | 2 | −11 | 79 |

| $A$ | −96 | 255 | 257 | −960 | −2876 | 3376 | −5280 |
|---|---|---|---|---|---|---|---|
| $D$ | −19 | 7 | 65 | −43 | −26 | 37 | −67 |

Certain values of $|D|$ can be shown not to occur, for example: 17, 33, 41, 57, 73, 97. Indeed, if any of these did occur as $|D|$, then Theorem 2(b) shows that some $E_{A,u}$ has good reduction everywhere over $k = Q[\sqrt{-|D|}]$. But, by Theorem 4 of [1], these $k$ do not have elliptic curves with good reduction everywhere defined over them.

We consider $A = -15$, $D = -7$ in some detail. Since $\varepsilon D = -7$, $E_{-15,u}$ will have good reduction everywhere over $k$ only if $k$ is real. In fact, some $E_{-15,u}$ will have good reduction over $k$ if and only if $m = 7$ or $m = 7p_1 \ldots p_r$ where $p_i$ are distinct primes congruent to 1, 2, or 4 (mod 7). By the lemma, $u \in k$ must be chosen so that $[u] = \mathfrak{p}_7 \mathfrak{a}^2$ where $\mathfrak{p}_7$ is the ramified prime dividing 7. $\mathfrak{a}$ may be chosen prime to 2. Further, $u$ must be a square (mod 4).

Letting $k = Q[\sqrt{7}]$ we have the following. Only 2 and 7 ramify in $k/Q$ so there are just two curves $E_{-15,u}$ over $k$ having good reduction everywhere. Actually, in the notation of Theorem 3, $\delta$ exists, say $\delta = \sqrt{7(8 + 3\sqrt{7})}$ where $\eta = 8 + 3\sqrt{7}$ is a fundamental unit of $k$. So, both curves have global minimal models. Appropriate choices of $u$ are $u = \pm(21 + 8\sqrt{7})$. Removing 3, 7 and 19 from $E_{-15,u}$ in each case leaves

$$y^2 = x^3 - 5\eta^2 x \pm 2\sqrt{7}\eta^3.$$

The global minimal models are given by

$$y^2 + xy = x^3 - 2\eta x^2 + \eta^2 x$$

(with $\Delta = -\eta^6$) and the conjugate equation.

Letting $k = Q[\sqrt{14}]$, there are two curves $E_{-15,u}$ which have good reduction everywhere, both have global minimal models. Letting $k = Q[\sqrt{154}]$, there are four curves $E_{-15,u}$ with good reduction everywhere, but only two have global minimal models.

For $A = 255$, we have $D = 7$. A similar discussion to that for $A = -15$ applies. Over $k = Q[\sqrt{7}]$ the two curves given by

$$y^2 + xy = x^3 + 4\eta x^2 + \eta x$$

($\Delta = \eta^6$) and its conjugate are obtained.

Considering $A = 16$, we have $D = 37$. Over $k = Q[\sqrt{37}]$, there is just one

$E_{16,u}$ with good reduction everywhere. It has a global minimal model. Evidently, it must be self conjugate. A model is

$$y^2 = x^3 - 4\sqrt{37}\,\eta x^2 + 192\eta^2 x - 80\sqrt{37}\,\eta^3$$

with $\Delta = 2^{12}\eta^6$. Here, $\eta = 6 + \sqrt{37}$ is a fundamental unit.

Finally, $k = Q[\sqrt{6}]$ is the quadratic field of smallest discriminant over which we have found an elliptic curve with good reduction everywhere, namely $E_{A,u}$ with $A = 20$, $u = 21(2 + \sqrt{6})$. This has a global minimal model

$$y^2 + \sqrt{6}\,xy - y = x^3 - (2 + \sqrt{6})x^2$$

with $\Delta = (5 + 2\sqrt{6})^3$. The conjugate curve is the other $E_{20,u}$ having good reduction everywhere over $Q[\sqrt{6}]$.

## References

1. C. B. Setzer, *Elliptic curves over complex quadratic fields*, Pacific J. Math., vol. 74 (1978), pp. 235–250.
2. R. J. Stroeker, *Elliptic curves over imaginary quadratic number fields*, Report 7209, Econometric Institute, Netherlands School of Economics.
3. J. Tate, "Algebraic formulas in arbitrary characteristic, Appendix I" in S. Lange, *Elliptic functions*, Addison-Wesley, Reading, Mass., 1973.

University of Illinois at Chicago Circle
Chicago, Illinois