PACIFIC JOURNAL OF MATHEMATICS
Vol. 74, No. 1, 1978

ELLIPTIC CURVES OVER COMPLEX QUADRATIC FIELDS

BENNETT SETZER

This paper concerns elliptic curves defined over complex quadratic fields and having good reduction at all primes. Those fields are characterized which support such curves having a 2-division point defined over the field. The number of isomorphism classes, over the ground field, of these curves is also determined. For curves without a 2-divison point defined over the field, the possible Galois groups of the 2-division field over the rationals are determined. Using class field theory, it is shown that certain complex quadratic fields support no elliptic curves with good reduction everywhere.

1. Weil's conjecture concerning elliptic curves defined over the rational field, Q, has inspired much work concerned with determining such curves with bad reduction only at specified primes. For example, Ogg [7] and Coghlan [2] determined all elliptic curves over $\boldsymbol{Q}$ with bad reduction only at 2 and 3. In [8], a certain class of curves is treated having bad reduction only at one prime. In this article, we take up the analogous problem over complex quadratic fields. Throughout, we will let $k = \boldsymbol{Q}[\sqrt{-m}]$ where m is a positive, square-free integer. The specific question we are concerned with is whether there is an elliptic curve defined over k having good reduction everywhere. Tate has given some examples of fields k for which there is such an elliptic curve (unpublished). Stroeker [9], has shown that there are no such curves over the nine fields with class number 1. In the last section, we compare our results with Stroeker's.

The program followed in this paper is to consider separately the case in which the desired curve does or does not have a 2-division point rational over k. We have completely determined those fields k over which there are such curves with a rational 2-division point (Theorem 3). Also, we can specify how many isomorphism classes (over k) of such curves there are. In particular, there are infinitely many suitable fields k. It is of interest that these curves have j-invariant 17^3 or 257^3.

For curves without a 2-division point rational over k, we have determined the possible Galois structures of the normal closure over $\boldsymbol{Q}$ of the 2-division field (Theorem 2). Theorems 2 and 3 together make it possible to determine all the elliptic curve with good reduction everywhere over certain fields k (Theorem 4). In particular, over $\boldsymbol{Q}[\sqrt{-65}]$, there are precisely 8 such curves, up to isomorphism.

For general results on elliptic curves, in particular the isomorphism formulae, see Appendix I in [5]. For a discussion of reduction types and integral models, see Tate's article in [10].

We would like to thank the referee for his comments, particularly concerning the revisions of proof of Theorem 2.

2. The form of the discriminant.

We assume that E is an elliptic curve defined over a number field K. Let $\mathfrak{A}$ be the greatest common divisor of the discriminants of all integral models of K. Any integral model of E then has discriminant $\mathfrak{A}\mathfrak{B}^{12}$ for some integral ideal $\mathfrak{B}$. More precisely:

THEOREM 1. *Let E and $\mathfrak{A}$ be as described. Then, there is an ideal class $\mathfrak{C}$ such that for every integral ideal $\mathfrak{B} \in \mathfrak{C}$ there is an integral model of E with discriminant $\mathfrak{A}\mathfrak{B}^{12}$. Conversely, any integral model of E has discriminant $\mathfrak{A}\mathfrak{B}^{12}$ for some $\mathfrak{B} \in \mathfrak{C}$.*

Proof. The final statement of the theorem reflects that the discriminant is homogeneous of weight 12. Now, suppose E has a model with discriminant $\mathfrak{A}\mathfrak{B}^{12}$ and that $\mathfrak{B}'$ is an integral ideal equivalent to $\mathfrak{B}$, say $\mathfrak{B} = u\mathfrak{B}'$, $u \in K$, $u \neq 0$. We will show the existence of integers r, s, t (determined up to congruences) such that transforming the given model by

$$(1) \qquad x = u^2x' + r \qquad y = u^3y' + u^2sx' + t$$

yields an integral model with discriminant $\mathfrak{A}(\mathfrak{B}')^{12}$. Since r, s, t will be integral, inspection of the transformation equations shows that it will be sufficient to insure the integrality of the new coefficients locally for each prime dividing u to a positive power.

Suppose, then, that $\mathfrak{P}$ is a prime such that $\mathfrak{P}^e$ exactly divides u where $e > 0$. Since $\mathfrak{B}'$ is integral, $\mathfrak{P}^e$ divides $\mathfrak{B}$ and so $\mathfrak{P}^{12e}$ divides the discriminant. Now, by the definition of $\mathfrak{A}$, there are $u_1, r_1, s_1, t_1 \in K$, $u_1 \neq 0$ such that the transformation

$$x = u_1^2x' + r_1 \qquad y = u_1^3y' + s_1u_1^2x' + r_1$$

yields an integral model of E with discriminant $\mathfrak{A}(\mathfrak{B}'')^{12}$ where $\mathfrak{P}$ does not divide $\mathfrak{B}''$. So $\mathfrak{P}^d$ divides u_1 where $d \geqq e$. Now, examining the transformation equations for the coefficients of these models discloses that r_1, s_1, t_1 are $\mathfrak{P}$-integral and may be varied mod $\mathfrak{P}^{6d}$ arbitrarily without disturbing the integrality of the new model at $\mathfrak{P}$. This implies that restricting r, s, t to certain residue classes mod $\mathfrak{P}^{6e}$ will insure integrality at $\mathfrak{P}$ after the transformation (1).

Arguing similarly for each prime dividing u to a positive power and finally applying the Chinese Remainder Theorem proves the theorem.

In our particular case of interest, we have the

COROLLARY. *Let E be an elliptic curve, defined over a number field K, having good reduction everywhere. Then there is an ideal class $\mathfrak{C}$ of K such that the set discriminants of integral models of E is precisely the set of ideals $\mathfrak{B}^{12}$ where $\mathfrak{B}$ is an integral ideal in $\mathfrak{C}$.*

We mention in passing that since $\mathfrak{B}^{12}$ must be principal, we have the further

COROLLARY. *E, K as in the previous corollary. If the class number of K is prime to 6 then E has a global minimal model.*

Indeed, $\mathfrak{B}$ must be principal so the unit ideal is a discriminant of E.

3. In this section, we investigate the normal closure, over the rational field $\boldsymbol{Q}$, of the 2-division field of an elliptic curve. The curves discussed are defined over the field $k = \boldsymbol{Q}[\sqrt{-m}]$ where m is a positive, square-free integer.

THEOREM 2. *Let E be an elliptic curve defined over k having good reduction everywhere, and having no 2-division point defined over k. Let K be the normal closure, over $\boldsymbol{Q}$, of the 2-division field of E. Let $G = \mathrm{Gal}(K/\boldsymbol{Q})$. Then*

(a) *If L is any cubic extension of $\boldsymbol{Q}$, contained in K, then L is not Galois over $\boldsymbol{Q}$. The only primes which can ramify in $L/\boldsymbol{Q}$ are those dividing $2m$. The only prime which can triply ramify in $L/\boldsymbol{Q}$ is 2.*

(b) *G is isomorphic to one of these three groups:* (i) S_3; (ii) $S_3 \times \boldsymbol{Z}/2\boldsymbol{Z}$; (iii) $S_3 \times S_3$.

(c) *In case* (ii), *there is a unique subfield of $\boldsymbol{Q}$ with Galois group S_3 over $\boldsymbol{Q}$. This field is totally real. In case* (iii), *there are exactly two S_3 extensions of $\boldsymbol{Q}$ contained in K. One of these is totally real, the other, totally complex.*

REMARK. Any S_3 extension of $\boldsymbol{Q}$ contains a unique quadratic extension of $\boldsymbol{Q}$. This quadratic field will be called the discriminant quadratic. In the proof of Theorem 2, it will be seen that, given a field K with Galois group G isomorphic to one of those given in (b), the field k may be recovered as follows. If $G \xrightarrow{\sim} S_3$, then k is the discriminant quadratic of K. If $G \xrightarrow{\sim} S_3 \times \boldsymbol{Z}/2\boldsymbol{Z}$, then k is fixed by the S_3 factor of G. If $G \xrightarrow{\sim} S_3 \times S_2$, then k is the third quadratic subfield contained in the composite of the two discriminant quadratics of the two S_3 extensions of $\boldsymbol{Q}$ contained in K.

Proof of Theorem 2. We first introduce some notation: g will denote an element of G which is the restriction to K of some complex conjugation in Gal $(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$. g may depend on the choice of conjugation.

$$B_0 = \text{2-division field of } E \text{ over } k\,.$$
$$B_1 = \text{conjugate of } B_0 \text{ by } g\,.$$
$$H_1 = \mathrm{Gal}\,(K/B_1) \qquad H_0 = \mathrm{Gal}\,(K/B_0) \qquad H = \mathrm{Gal}\,(K/K)\,.$$

H is a normal subgroup of G of index 2. g is not in H, so G is generated by H and g. Since $B_0B_1 = K$, the subgroups H_0 and H_1 have trivial intersection. We also have $H_1 = gH_0g^{-1}$. The following diagram of fields and groups will be useful:

$$\begin{tikzcd}
 & & & B_0 \arrow[dr, dash, "H_0", "f"'] & \\
\boldsymbol{Q} \arrow[r, dash, "2"'] & k \arrow[r, dash, "H/H_0H_1", "e"'] & B_0 \cap B_1 \arrow[ur, dash, "f"'] \arrow[dr, dash, "f"] & & K \\
 & & & B_1 \arrow[ur, dash, "H_1"', "f"] &
\end{tikzcd}$$

Here, e and f denote the field extension degrees.

B_0 is generated over k by the roots of a cubic $x^3 + a_2x^2 + a_4x + a_6$ where $y^2 = x^3 + a_2x^2 + a_4x + a_6$ is a model of E with $a_i \in k$. The 2-division points are, in this model, the points $(x, 0)$ on the curve. Since we assume no 2-division point is defined over k, the cubic $x^3 + a_2x^2 + a_4x + a_6$ is irreducible over k. Thus, B_0 is Galois over k and has Galois group H/H_0 isomorphic to S_3 or $Z/3Z$. Considering the operation of g on H, we see that H_1 is also normal in H and that $H/H_1 \times H/H_0$. This implies that H_0H_1 is a normal subgroup of H.

To determine the structure of the group G, it is helpful to consider the action of G on $X = E(\bar{\boldsymbol{Q}}) \times E(\bar{\boldsymbol{Q}})^g$, where $E(\bar{\boldsymbol{Q}})$ is the set of algebraic points on E. (We take g here to mean complex conjugation on the field of algebraic numbers $\bar{\boldsymbol{Q}}$). X has the structure of an abelian variety defined over $\boldsymbol{Q}$, so Gal $(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ acts naturally on X as a group of homomorphisms. Consider the restriction of this action to X_2, the group of 2-division points of X. X_2 is fixed by Gal $(\bar{\boldsymbol{Q}}/K)$ since K contains the co-ordinates of these points. Thus, there results an action of G on X_2 The action of G may be described as follows. If $h \in H$, then there is a natural action on each factor $E_2(\bar{\boldsymbol{Q}})$ and $E_2(\bar{\boldsymbol{Q}})^g$ since E and E^g are defined over k. Complex conjugation acts by $(P_1, P_2^g)^g = (P_2, P_1^g)$ where $P_1, P_2 \in E_2(\bar{\boldsymbol{Q}})$. X_2 has the structure of a vector space of dimension 4 over $\boldsymbol{F}_2$, the field with two elements. For convenience, we will denote the subspaces $E_2(\bar{\boldsymbol{Q}})$ and $E_2(\bar{\boldsymbol{Q}})^g$ by U_0 and U_1 respectively. G acts as a group of nonsingular linear transformations on X_2. H leaves each subspace U_0 and U_1-invariant. We will choose a basis of X_2 by taking the union of bases for U_0 aud U_1. G then maps homomorphically onto a subgroup of $\mathrm{Gl}\,(4, \boldsymbol{F}_2)$ the group of 4×4 nonsingular matrices with entries in $\boldsymbol{F}_2$. The image of each element of H is of the form

$$M(R, W) = \begin{pmatrix} R & 0 \\ 0 & W \end{pmatrix}$$

where $R, W \in \mathrm{Gl}\,(2, \boldsymbol{F}_2)$. By appropriate choice of basis, we may assume that g has the image

$$\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

where I is the 2×2 identity matrix.

Now, H acts faithfully on X_2 since K is generated over k by the co-ordinates of these points. But, the image of H is a proper subgroup of the image of G since $g \notin \mathrm{Im}\,(H)$. Thus, G also acts faithful on X_2. We will henceforth identify G with its matrix representation. Since B_0 is generated over k by the co-ordinates of points in U_0, H_0 is the subgroup of elements of H of the form $M(I, W)$. Similarly, H_1 is the subgroup of elements of the form $M(R, I)$.

We turn to the proof of (a). The only primes which may ramify in B_0/k, and so also in B_1/k, are those dividing 2. This follows immediately from the fact that the n-division field of an elliptic curve is ramified at most at primes which divide n or the conductor (see [6] p. 673). This implies that for any odd rational prime, the ramification index in $K/\boldsymbol{Q}$ equals the ramification index in $k/\boldsymbol{Q}$ and so is 1 or 2. So, any prime ramifying in $K/\boldsymbol{Q}$ must divide $2m$. Let $L/\boldsymbol{Q}$ be a cubic extension contained in K. The preceeding argument establishes all the assertion of part (a) except that $L/\boldsymbol{Q}$ is not Galois. But, if $L/\boldsymbol{Q}$ where Galois, any prime ramified in $L/\boldsymbol{Q}$ would have ramification index 3. By our previous remarks, no odd prime could ramify in $L/\boldsymbol{Q}$, else 3 would divide the ramification index in $K/\boldsymbol{Q}$ which must be 1 or 2. Thus, the only prime ramifying in $L/\boldsymbol{Q}$ is 2, if $L/\boldsymbol{Q}$ is Galois. There are no such extensions of $\boldsymbol{Q}$. For example, such an extension would have to be contained in a 2-power cyclotomic field. But, the degree of a 2-power cyclotomic field over $\boldsymbol{Q}$ is a power of 2. Now a normal subgroup G of index 3 would correspond to a cubic cyclic extension of $\boldsymbol{Q}$ contained in K. We thus see that G cannot contain a normal subgroup of index 3. We have also proved part (a).

Next, we note that the order of G cannot be greater than 36. In the notation of the subgroup diagram, since H/H_0 is isomorphic to S_3 or $\boldsymbol{Z}/3\boldsymbol{Z}$, we must have $ef = 3$ or 6. Now, the order of G is twice the order of H which is ef^2. The order of G is greater than 36 only if $f = 6$ and $e = 1$, and so $H_0H_1 = H$. But, this implies that $B_0 \cap B_1 = k$ and B_0/k and B_1/k are S_3 extensions. Thus, each field B_i contains a quadratic extension of k, say F_i. Now, $F_0 = k(\zeta)$ and $F_1 = k(\zeta^g)$ where $\zeta^2 = \Delta \in k$ and Δ is the discriminant of a model of E. But, by Theorem 1, Δ generates an ideal which is a 12th power. So, $\Delta\Delta^g = N_{k/Q}(\Delta) = n^{12}$ for some $n \in \boldsymbol{Z}$. Thus $\zeta\zeta^g = n^6 \in k$ so $F_0 = F_1$ and so $k = B_0 \cap B_1 \supset F_0$. This contradiction establishes the second observation.

The proof of part (b) will be completed by determining the subgroups H of $\mathrm{Gl}(4, \boldsymbol{F}_2)$ satisfying the following properties: H consists of matrices of the form $M(R, W)$; H is invariant under conjugation by g; H acts as S_3 or $\boldsymbol{Z}/3\boldsymbol{Z}$ on U_0; the group G generated by g and H is of order less than or equal to 36 and has no normal subgroup of index 3. In the following discussion, we use the notation

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

which are elements of $\mathrm{Gl}(2, \boldsymbol{F}_2)$ and generate that group.

Consider first the case that $H/H_0 \simeq \boldsymbol{Z}/3\boldsymbol{Z}$. In the notation of the subgroup diagram, $ef = 3$, so $f = 1$ or 3. If $f = 3$, then H_0 must contain $M(I, T)$ and H_1 must contain $M(T, I)$ and these matrices generate the respective subgroups. Since $e = 1$, we have $H = H_0H_1$ which is thus generated by both $M(I, T)$ and $M(T, I)$. Finally, G is of order 18 generated by g and $M(I, T)$. However, $M(T, T^2)$ and g generate a normal subgroup of G of order 6, so of index 3. This contradicts the first observation. If $f = 1$, then H is 3 and must be generated either by $M(T, T)$ or $M(T, T^2)$ since $gHg = H$. In the former case, G is abelian of order 6, so has a normal subgroup of index 3. In the latter case, G is isomorphic to S_3 and generated by g and $M(T, T^2)$. This is case (i). The claim made in the remark about this case is evident.

Suppose now that $H/H_0 \simeq S_3$. Since H_0H_1 is a normal subgroup of H, then H_0H_1/H_0 is a normal subgroup of H/H_0, so of order 1, 3 or 6. That is, $f = 1, 3$ or 6. If $f = 6$, then H has order 36, so G has order 72, which contradicts the above observation.

If $f = 3$, then H has order 18. Further, H_0 must be generated by $M(I, T)$ and H_1 by $M(T, I)$. But, since $H/H_0 \simeq S_3$, some matrix

$M(S, W)$ must be in H. If $W = I, T$ or T^2, then $M(S, I) \in H$ and H_1 would actually be of order 6. This implies that $W = S, TS$ or T^2S so $M(S, S) \in H$. The matrices $M(I, T)$, $M(T, I)$ and $M(S, S)$ generate a group of order 18, which must be H. Thus, G is order 36 and generated by $M(I, T)$, $M(S, S)$ and g. Consider the subgroup H_2 of G generated by $M(T, T)$ and $gM(S, S)$ and also the subgroup H_3 generated by $M(T, T^2)$ and g. These are normal subgroups of G with trivial intersection which commute with each other. Each subgroup is isomorphic to S_3, so $G \simeq S_3 \times S_3$. This is case (iii). It is easily checked that H_2 and H_3 are the only normal subgroups of G of index 6. Thus, the fields fixed by H_2 and H_3 are the only S_3 extensions of Q contained in K. k is not the discriminant quadratic of either of these fields since H_2 and H_3 are not contained in H. However, the discriminant quadratics are fixed by the subgroup generated by $M(T, T)$, $gM(S, S)$ and $M(T, T^2)$ and by the subgroup generated by $M(T, T)$, g and $M(T, T^2)$. The composite of the discriminant quadratics is fixed by the subgroup generated by $M(T, T^2)$ and $M(T, T)$. This is a subgroup of H, so k is the third quadratic contained in the composite of the two discriminant quadratics. Finally, since $g \in H_3$, the fixed field is totally real. Conversely, since $g \notin H_2$, the fixed field is totally complex. This is the assertion of part (c) concerning (iii).

The last case to consider is $f = 1$. Since H_0 has order 1, any $M(R, W)$ in H must have R and W the same order. Of the nine such matrices, H must contain at least one of order 2 and one of order 3. If $M(S, TS) \in H$ then $M(T^2, T) = M(S, TS)M(S, TS) \in H$ already. Similarly, if $M(S, T^2S) \in H$ then $M(T^2, T) \in H$. But, if $M(T^2, T) \in H$, then $M(T, T) \notin H$ else, $M(T, I) \in H$ and H_1 would not be order 1. By multiplying a matrix in H of order 2 by one of order 3, we see that H must always contain a matrix $M(S, W)$. It is now evident that H must contain one of these pairs of matrices: $\{M(T, T)^2, M(S, S)\}$, $\{M(T, T^2), M(S, TS)\}$, $\{M(T, T^2), M(S, T^2S)\}$ or $\{M(T, T), M(S, S)\}$. Each pair generates a group of order 6, which must be H. G then has order 12. These four possibilities for G are actually all conjugate to each other by matrices of the form $M(R, W)$. This corresponds to a different choice of basis in U_0 and U_1 and, perhaps, a new choice of the field automorphism with matrix g. We need, then, examine only the case in which G is generated by $M(T, T)$, $M(S, S)$ and g. H evidently commutes with g and $H \simeq S_3$, so $G \simeq S_3 \times Z/2Z$. This is case (ii). Now, g generates the unique normal subgroup of G of index 6, so there is only one S_3 extension of Q contained in K. Since g fixes this field, it must be totally real. This is the assertion of part (c). The decomposition of G into the product $S_3 \times Z/2Z$ is unique, so the subgroup H is determined by G, which is asserted in the remark.

This completes the proof of Theorem 2.

3. Throughout this section, $k = \boldsymbol{Q}[\sqrt{-m}]$ will be an imaginary quadratic field, m a positive integer, square free. Also, an elliptic curve over k having good reduction everywhere and having a 2-division point rational over k will be called admissible.

THEOREM 3. *There is an admissible elliptic curve E if and only if $m = 65m_1$ where m_1 is a square* mod 5 *and* mod 13 *and* 65 *is a square* mod m_1. *If this is the case, then the number of isomorphism classes of such curves is 2^r, where r is the number of primes which ramify in the extension $k/\boldsymbol{Q}$.*

Proof. An admissible curve E has an integral model with odd discriminant. Completing the square and translating a 2-division point to the origin, we obtain a model

$$y^2 = x^3 + Ax^2 + Bx \tag{1}$$

where A and B are integral. The discriminant is then

$$\Delta = -16B^2(A^2 - 4B) = 2^{12}D \tag{2}$$

where D is integral and prime to 2. This equation, for fixed D, has only finitely many solutions A and B. But, Theorem 1 implies that only finitely many D need be tried for a given field k. Using the criteria for good reduction given below, it is routine to check out the theorem for any given field k.

Before proceeding, we give the criteria we will use for testing good reduction.

LEMMA. (a) *Let $\mathfrak{P}$ be a prime not dividing* 2. *Then an elliptic curve E with model* (1) *has good reduction at $\mathfrak{P}$ if and only if for some $e \in \boldsymbol{Z}$, $e \geqq 0$, $\mathfrak{P}^{12e}$ exactly divides Δ, $\mathfrak{P}^{4e}$ exactly divides B and $\mathfrak{P}^{2e}$ divides A.*

(b) *Let $\mathfrak{P}$ be an unramified prime dividing* 2. *Then an elliptic curve with model* (1) *and discriminant as in* (2) *has good reduction at $\mathfrak{P}$ if and only if A and B satisfy either of these sets of congruences*:

$$A \equiv 2\alpha^2 \pmod{\mathfrak{P}^3} \qquad B \equiv \alpha^4 \pmod{\mathfrak{P}^3} \tag{3}$$

$$A \equiv \alpha^2 \pmod{\mathfrak{P}^2} \qquad B \equiv 0 \pmod{\mathfrak{P}^4} \tag{4}$$

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

(c) *Let $\mathfrak{Q}$ be a ramified prime dividing* 2. *Then an elliptic curve with model* (1) *and discriminant* (2) *has good reduction at $\mathfrak{Q}$*

if and only if A and B satisfy either the congruences (3) *or* (4) *with $\mathfrak{P} = 2$ or they satisfy*

$$(5)\qquad \begin{aligned} &A \equiv 0 \pmod{\mathfrak{Q}^5} \qquad B \equiv \pi^4 + 8\pi \pmod{\mathfrak{Q}^8} \\ &\pi^2 A - B \equiv \pi^4 + \pi^6 \quad \textit{or} \quad 5\pi^4 + 4\pi^5 + \pi^6 \pmod{\mathfrak{Q}^{10}} \end{aligned}$$

where π is a fixed uniformizing element.

Proof. (a) Supposing E has good reduction at $\mathfrak{P}$, then E has a model (1) with discriminant not divisible by $\mathfrak{P}$. Note that the conditions of the lemma are satisfied with $e = 0$. Any other model (1) of E is obtained either by a dilation $x' = u^2x$, $y' = u^3y$ or by translating a different 2-division point to the origin. The translation will not change the discriminant and so the condition remains true. The dilation produces $A' = u^2A$, $B' = u^4B$ and $\Delta' = u^{12}\Delta$ as parameters of the new model. Let $v(x)$ be the valuation at $\mathfrak{P}$. Now $v(u) = e \in Z$ and $e \geqq 0$ since Δ' is integral and $v(\Delta) = 0$. But A', B', Δ' satisfy the conditions with e as given.

If a model (1) is given satisfying the conditions, determine u so that $v(u) = -e$ but u is integral at all other primes. Then a dilation with parameter u results in an integral model with $v(\Delta') = 0$.

(b) Supposing E has good reduction at $\mathfrak{P}$, then E has a model

$$(6)\qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with discriminant not divisible by $\mathfrak{P}$. Completing the square yields

$$(7)\qquad y^2 = x^3 + b_2x^2 + 8b_4x + 16b_6$$

where

$$(8)\qquad b_2 = a_1^2 + 4a_2 \qquad b_4 = a_1a_3 + 2a_4 \qquad b_6 = a_3^2 + 4a_6 \,.$$

If $\mathfrak{P}$ were to divide a_1, then $\mathfrak{P}$ could not divide a_3 else (6) would have bad reduction at $\mathfrak{P}$. Then one would deduce that the Newton polygon of the cubic in x would be a single line of slope $-(4/3)$. But, the cubic is assumed to have a root in k, hence, $\mathfrak{P}$ does not divide a_1.

In the remainder of this argument, we will only assume coefficients to be $\mathfrak{P}$-integral. Strong approximation then guarantees the truth of these results for strictly integral models. With this in mind, (6) may be transformed so that $a_3 = 0$. Let $a_1 = \alpha$. Then

$$(9)\qquad b_2^2 \equiv \alpha^2 \pmod{\mathfrak{P}^2} \qquad b_4 \equiv 0 \pmod{\mathfrak{P}} \qquad b_6 \equiv 0 \pmod{\mathfrak{P}^2} \,.$$

Conversely, if (7) satisfies these conditions, we can "uncomplete" the square and eliminate $\mathfrak{P}^{12}$ from the discriminant.

Now, the cubic in (7) has a root which has $\mathfrak{P}$-valuation $\geqq 3$ or $=0$. Translating by one root, say θ, we obtain (1) where

$$\begin{aligned} A &= 3\theta + b_2 & B &= 3\theta^2 + 2b_2\theta + 8b_4 \\ b_2 &= -3\theta + A & 8b_4 &= 3\theta^2 - 2A\theta + B \end{aligned} \tag{10}$$
$$16b_6 = -\theta^3 + A\theta^2 - B\theta\ .$$

If the $\mathfrak{P}$-value of θ is 0, (3) is verified. If the $\mathfrak{P}$-value of θ is $\geqq 3$, then (4) holds. Allowable transformations are dilations by $u \in k^*$ prime to $\mathfrak{P}$, which will not change the congruences, and translating a new point to the origin, which is simply making a new choice of θ. So (3) or (4) are necessarily satisfied.

Suppose, on the other hand, that E has a model (1), discriminant (2) and statisfies either (3) or (4). If (4) is satisfied, by the remarks following (8), we may immediately uncomplete the square and so remove $\mathfrak{P}$ entirely from the discriminant. If (3) is satisfied, then apply $y = y$, $x = x - \theta$ where $\theta \equiv A/2(\text{mod}\ \mathfrak{P}^3)$ to obtain a model (7). Then using (10), the congruences (9) on b_2, b_4 are easily seen to be satisfied. For b_6, note that $\theta^2 - A\theta + B = (\theta - A/2)^2 - 1/4(A^2 - 4B)$. Both terms are divisible by $\mathfrak{P}^6$ so all congruences (9) are satisfied. Again, $\mathfrak{P}$ can be completely removed from the discriminant and (b) is established.

(c) The argument of part (b) applies in this case with $\mathfrak{P} = 2$ except that a_1 may be divisible by $\mathfrak{P}$. We complete part (c) by considering this latter alternative. The valuation of a_1 must be 1, if not 0. This possibility gives rise to the conditions (5) as follows.

Assume we are given a curve E with model (6) and discriminant prime to $\mathfrak{Q}$. We may take $a_1 = \pi$ a uniformizing element for $\mathfrak{Q}$. Further, since a_3 must be prime to $\mathfrak{Q}$, we may take $a_3 = 1$. Then upon completing the square, the b's satisfy these congruences:

$$b_2 \equiv \pi^2\ (\text{mod}\ \mathfrak{Q}^4) \qquad b_4 \equiv \pi\ (\text{mod}\ \mathfrak{Q}^2) \qquad b_6 \equiv 1\ (\text{mod}\ \mathfrak{Q}^4)\ . \tag{11}$$

The cubic in x has roots possibly of valuation 3 or 2. A congruence argument shows that valuation 3 is actually impossible. So asssume θ is a root of value 2. There can be only one such root. It is possible to show that $\theta \equiv \pi^2(\text{mod}\ \mathfrak{Q}^4)$. Translating to a model (1), the equations (10) may be used to demonstrate the first two congruences of (5). The final condition is obtained from the fact that $-Z^3 + AZ^2 - BZ \equiv 16(\text{mod}\ \mathfrak{Q}^{12})$ has a solution with $Z \equiv \pi^2(\text{mod}\ \mathfrak{Q}^4)$. It is easily checked that these conditions on A and B imply the existence of a θ which will translate (1) back to a model (7) satisfying conditions (11). Assuming the discriminant of (1) is given by (2), this insures that uncompleting the square will remove $\mathfrak{Q}$ entirely from the discriminant.

All that remains is to check that the conditions (5) are invariant under permissible transformations of (1). Since there is only one 2-division point, only dilations are allowed. It is easily checked that the conditions will indeed remain unchanged. Finally, we note that the choice of π is arbitrary, so the conditions must remain true even if π is changed.

This completes the lemma.

We turn now to solving the discriminant equation (2). In what follows, we assume $m \neq 1, 3$. These two fields are indeed found to have no admissible curves E. As remarked before, only finitely many possible curves result from (2) and these are easily checked not to have good reduction at some prime.

Examining the conditions (3), (4), (5), there are three possibilities for the 2 part of B:

(I) $B = 2^e\beta$ where $e = 0$ or 4

(II) $B = 2^2\beta$ and 2 ramifies

(III) $v_1(B) = 0$, $v_2(B) = 4$ where 2 splits in k and v_1, v_2 are the two valuations.

β is in each case an algebraic integer prime to 2.

Case (I). According to the lemma, β must generate an ideal which is a fourth power. But also, $\Delta = f2^{12}\beta^3$ where $f = +1$ is a unit. By the lemma, $A^2 = \alpha\beta$ where α is integral. Substituting into (2) we obtain

$$\alpha = 2^{2+e} - f2^{8-2e}$$

so $\alpha = -252, 260, 63$ or 65. Let $A_1 = A/6, A/2, A/3, A$ respectively. Then $A_1^2 = 7\beta$ or 65β. This immediately implies that either 7 or 65 ramifies in $k/\boldsymbol{Q}$. However, $A_1^2 = 7\beta$ is inconsistant with the congruences (3) and (4). Indeed, these latter imply A_1 or $-A_1$ is a square mod 4. But $N(A_1) = 7b^2$ where b is a rational odd integer. (N is the norm $k/\boldsymbol{Q}$.) Congruences will now yield a contradiction.

So now assume $A_1^2 = 65\beta$ and β generates a fourth power ideal. If A_1 is a square mod 4 we show that 2 or 4 nonisomorphic curves with good reduction everywhere result according as $m \not\equiv 1$ or $m \equiv 1 \pmod 4$.

Assume $m \not\equiv 1 \pmod 4$. If β is given then there are two choices of B according to choice of e and then four choices of A namely A_1, $-2A_1$, $-A_1$, $2A_1$. But if A_1 is a square mod 4 then only A_1, $2A_1$ will satisfy the congruences (3) or (4). The other conditions of good reduction are satisfied by construction. To summarize we have

$$A = -2A_1 \qquad B = 16\cdot 65^{-1}A_1^2 \qquad A_1^2 = 65\beta$$

$$A = A_1 \qquad B = 16\cdot 65^{-1}A_1^2 \qquad A_1^2 = 65\beta\ .$$

We compute C_4, C_6 and j for these curves

$$(\mathrm{E}_1)\quad C_4 = 2^4\cdot 65^{-1}\cdot 257\cdot A_1^2 \quad C_6 = 2^6\cdot 65^{-1}\cdot 511\cdot A_1^3 \qquad j = 257^3$$

$$(\mathrm{E}_2)\quad C_4 = 2^4\cdot 17\cdot 65^{-1}\cdot A_1^2 \quad C_6 = 2^6\cdot 65^{-1}\cdot 7\cdot A_1^3 \qquad j = 17^3\,.$$

Comparing j-invariants, these curves are indeed nonisomorphic.

Assume $m \equiv 1 \pmod 4$. The only change is that now $-A_1$, $-2A_1$ both satisfy the congruences (3) or (4). So we get two more curves:

$$A = 2A_1 \qquad B = 65^{-1}A_1^2 \qquad A_1^2 = 65\beta$$

$$A = -A_1 \qquad B = 16_x 65^{-1}A_1^2 \qquad A_1^2 = 65\beta\,.$$

For these curves we have

$$(\mathrm{E}_3)\quad C_2 = 2^4\cdot 65^{-1}\cdot 257\cdot A_1^2 \qquad C_6 = -2^6\cdot 65^{-1}\cdot 511\cdot A_1^3 \qquad j = 257^3$$

$$(\mathrm{E}_4)\quad C_4 = 2^4\cdot 17^{-1}\cdot 65^{-1}\cdot A_1^2 \qquad C_6 = -2^6\cdot 65^{-1}\cdot 7\cdot A_1^3 \qquad j = 17^3\,.$$

Comparing j-invariants and C_6 for all four curves, they are seen to be nonisomorphic. (-1 is not a sixth power since $m \neq 1$.)

We turn now to investigating when possible β exist and how many do. Suppose first that there are curves attached to β and also to β_1. Now β generates an ideal $\mathfrak{B}^4$, β_1 an ideal $\mathfrak{B}_1^4$. We claim that the sets of curves are isomorphic if and only if $\mathfrak{B}$ and $\mathfrak{B}_1$ are equivalent ideals. Indeed the discriminant of any curve attached to β in the above manner generates the ideal $2^{12}\mathfrak{B}^{12}$. If $\mathfrak{B}$ and $\mathfrak{B}_1$ were not equivalent then there could be no u such that $\Delta = u^{12}\Delta_1$ and the curves could not be isomorphic (over k). If, on the other hand, $\mathfrak{B} = u\mathfrak{B}_1$, then the dilation $x = u^2x_1$, $y = u^3y_1$ will carry each curve attached to β_1 to one attached to $\pm\beta$. Indeed, B and A_1 are determined up to sign and powers of 2 by the ideal $\mathfrak{B}$. But $-\beta$ cannot have curves attached since -1 is not a square in k. Thus, the curves obtained by dilation are attached to β.

Thus each ideal class will have 0, 2 or 4 curves attached and different classes have nonisomorphic curves. Let $\mathfrak{P}_5$, $\mathfrak{P}_{13}$ be the ramified primes dividing 5 and 13 respectively. An ideal $\mathfrak{B}$ will give curves precisely when $\mathfrak{P}_5\mathfrak{P}_{13}\mathfrak{B}^2 = [A_1]$ is principal and A_1 is $\pm$ a square mod 4. That $\mathfrak{P}_5\mathfrak{P}_{13}\mathfrak{B}^2$ is principal is just to say that $\mathfrak{P}_5\mathfrak{P}_{13}$ is in the principal genus, which is equivalent to the congruence conditions of the theorem. (See [1] p. 245.) Assume first that $m \not\equiv 1 \pmod 4$. Given any odd integral ideal $\mathfrak{B}$ such that $\mathfrak{P}_5\mathfrak{P}_{13}\mathfrak{B}^2 = [A_1]$ is principal, then A_1 must be $\pm$ a square mod 4 and so two curves will result. Given one such ideal $\mathfrak{B}$, any other is obtained as $\mathfrak{A}\mathfrak{B}$ where $\mathfrak{A}^2$ is principal and prime to 2. There are then 2^{r-1} classes from which $\mathfrak{B}$ may be chosen where r is the number of primes ramifying in k/Q (see [1] p. 247). Thus there are 2^r curves for this field.

Assume $m \equiv 1 \pmod 4$ and $\mathfrak{B}$, A_1 as above. Let $\rho^2 = -m$. Then $A_1 \equiv 1$ or $\rho \pmod 2$. In the former case A_1 is a square mod 4, so no curves result. Now all possible choices of $\mathfrak{B}$ are given as $\mathfrak{A}\mathfrak{B}$ where $\mathfrak{A}^2$ is principal. The ideal class of $\mathfrak{A}$ contains two abmiguous ideals, that is, integral ideal composed entirely of ramified primes. Both ideals are even or both odd. If both of these ideals are odd then $\mathfrak{A}$ may be taken as either one. But this will simply change A_1 by multiplying by an odd rational integer, the norm of $\mathfrak{A}$, which will not change whether A_1 is a square mod 4. On the other hand, let $\mathfrak{A} = \mathfrak{P}_2^{-1}(1 + \rho)$ which is an odd integral ideal. $\mathfrak{A}^2 = [(m - 1)/2 - \rho]$ is principal. Multiplying $\mathfrak{B}$ by $\mathfrak{A}$ will change whether A_1 is a square mod 4. Thus, for general $\mathfrak{A}$, if both ambiguous ideals in the class of are even, then multiplying by $\mathfrak{A}$ will change whether A_1 is a square mod 4. It is now evident that there are 2^{r-2} admissible choices of $\mathfrak{B}$. Since four curves result for each, there are 2^r curves in all.

The remainder of the proof will be to show that cases (II) and (III) do not result in any curves.

Case (II). This results if A, B are to satisfy the congruences (5). Again, since $B = 4\beta$, $D = f\beta^3$ where $f = \pm 1$ and $A^2 = \alpha\beta$. Substituting into (2) we have $\alpha = 0$ or 32.

Assume $\alpha = 0$. Then $A = 0$. The congruences on B then imply that $m = 1 \pmod 4$. If $m = 1 \pmod 8$ then $\beta \equiv 1 + 2\rho$ or $1 + 6\rho \pmod 8$ where $\rho^2 = -m$. But then $N(\beta) \equiv 5 \pmod{16}$ which is not a fourth power. But β generates a fourth power ideal, so this cannot occur. If $m \equiv 5 \pmod 8$ then $\beta \equiv 5$ or $5 + 4\rho \pmod 8$ so $N(\beta) \equiv 9 \pmod{16}$, again not a fourth power. Thus if $\alpha = 0$ no curves result with good reduction everywhere.

Assume $\alpha = 32$, then $A^2 = 32\beta$ and so $A \equiv 4\pi \pmod{\mathfrak{Q}^6}$. Now $N(\beta) = b^4$ where b is an odd rational integer, so $N(A) = 32b^2$. The congruences (5) then imply $m \equiv 2$ or $-2 \pmod{16}$.

If $m \equiv 2 \pmod{16}$ then from $N(\beta) \equiv 1 \pmod{16}$ and $2\beta = (1/16)A^2$ being a square we deduce $\beta \equiv 7 \pmod 4$. But then $B \equiv 12 \pmod{16}$ which contradicts (5). If $m \equiv -2 \pmod{16}$ then $\beta \equiv 1 \pmod 4$ so $B \equiv 4 \pmod{16}$. This again contradicts (5).

This completes case (B). No curves are found for this case.

Case (III). This results when different ones of the congruences (3), (4) hold for the two primes dividing 2. B generates the ideal $\mathfrak{P}_2^4\mathfrak{B}^4$ where $\mathfrak{B}$ is odd and integral. But D generates $\mathfrak{B}^{12}$, assuming good reduction at odd primes. Thus $\mathfrak{P}_2^{12} = [g]$ say. The discriminant equation (2) becomes

$$A^2 = g^{-1} \cdot 4B \cdot (g + 2^6)$$

if g is chosen so that $D = -g^{-1}B^3$. Then $N(g + 2^6)$ is a square. Let $g = 1/2(x + \rho y)$ where x, y are odd integers. Then $N(g + 2^6) = 2^6(128 + x) = 2^6 \cdot t^2$ and t is an odd integer. Let $S = y/t$. Now $(1/2(t + s\rho))^2 = g$. Let $h = 1/2(t + s\rho)$ then $A^2 = h^{-1} \cdot 4B(h + h^*)$, where * denotes complex conjugation. So $h + h^* = t$ which must have even valuation at all primes. Since t is not dividible by any ramified primes, this means t is ± a rational square. Combined with the fact that $t^2 + ms^2 = 256$, this leaves only two possibilities for m: 7 and 255. If $m = 255$ then $[A] = \mathfrak{P}_1\mathfrak{B}^2$. But $\mathfrak{P}_1$ is not a square ideal class so there will be no curves admissible resulting. If $m = 7$, the finitely many solutions are found not to satisfy (3) or (4), so no admissible curves result.

This completes Case (III) and the theorem.

5. In this section, we discuss some numerical examples. These examples result from the fact that for certain complex quadratic fields k, there can be no field K, galois over $\boldsymbol{Q}$, enjoying all the properties described in Theorem 2. If this is the case, then any elliptic curve over k having good reduction everywhere must have a rational 2-division point over k. These curves have been completely determined in Theorem 3.

Determining whether or not suitable fields K exist for a given complex quadratic field k can be reduced to searching a table of cubic extensions of $\boldsymbol{Q}$. To see this, consider the three possibilities for G given in Theorem 2. If K has Galois group S_3, let F be one of the cubic fields contained in K. We claim that the discriminant of F is either $-m$ or $-4m$. Indeed, any prime ramified in $F/\boldsymbol{Q}$ but not dividing 2 cannot be triply ramified, so must appear in the discriminant of F to the first power. Since the discriminant of F is a square times $-m$, such a prime must also divide m. For 2, the highest power that can divide the discriminant of F is 8. These assertions concerning the p-part of the discriminant of F are taken from the table on page 568 in [4]. We now see that the discriminant of F must divide $8m$. Conversely, m must divide the discriminant, since any prime ramifying in $k/\boldsymbol{Q}$ also ramifies in $F/\boldsymbol{Q}$. Finally, $-m$ differs from the discriminant of F by a square factor, so disc $(F) = -m$ or $-4m$ as claimed.

If K has Galois group $S_3 \times \boldsymbol{Z}/2\boldsymbol{Z}$ then, as noted in Theorem 2(b), K must contain a totally real S_3 extension of $\boldsymbol{Q}$. Let F be a cubic field contained inside this S_3 extension. The previous argument applies to show that the discriminant of F must divide $8m$. Also, the discriminant of F must be positive. For the final possibility for G, the argument proceeds as before to show that there are two cubic extensions of $\boldsymbol{Q}$ contained in K having discriminants dividing $8m$ with one positive, one negative. Putting this together, we have the first part of this proposition:

PROPOSITION. *Let $k = \boldsymbol{Q}[\sqrt{-m}]$ be a complex quadratic field, where m is a square-free positive integer. There exists a field B_0 which is an extension of k with Galois group either S_3 or $\boldsymbol{Z}/3\boldsymbol{Z}$ and such that B_0/k is unramified outside of 2 if and only if there is a nongalois cubic extension $F/\boldsymbol{Q}$ with one of these properties:*

(a) $\mathrm{Disc}(F) = -m$ *or* $-4m$

(b) $\mathrm{Disc}(F) > 0$ *and* $\mathrm{disc}(F)$ *divides* $8m$.

To prove the converse, note that in case (a), we may let B_0 be the S_3 extension of $\boldsymbol{Q}$ containing F. In case (b), B_0 is the composite of k and the S_3 field containing F. These fall into cases (i) and (ii) of Theorem 2.

The tables in [3] suffice to check for values of up to $m = 161$. The positive discriminants are listed up to 1296, the negative discriminants, up to 1000 (pp. 159-160). Of the values of m for which it can be shown that no field B_0 exists and which fall in this range, only one satisfies the conditions of Theorem 3. We have then

THEOREM 4. (a) *There are no elliptic curves over $\boldsymbol{Q}[\sqrt{-m}]$ having good reduction everywhere if* $m = 1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 21, 22, 30, 33, 34, 39, 41, 42, 46, 47, 55, 57, 58, 62, 66, 69, 70, 73, 77, 78, 82, 85, 86, 93, 94, 95, 97, 102, 103, 105, 113, 114, 119, 122, 130, 133, 134, 137, 138, 143, 145, 146, 149, 151, 154, 159,$ or 161.

(b) *There are 8 elliptic curves, up to isomorphism, defined over $\boldsymbol{Q}[\sqrt{-65}]$ having good reduction everywhere. Each such curve has a 2-division point defined over $\boldsymbol{Q}[\sqrt{-65}]$.*

Stroeker's main result in [9] is that any elliptic curve defineed over a complex quadratic field k and having good reduction everywhere does not have a global minimal model, that is, the curve does not have an integral model with a unit discriminant. Stroeker deduces from this that for $m = 1, 2, 3, 7, 11, 19, 43, 67, 163$, there are no elliptic curves over $\boldsymbol{Q}[\sqrt{-m}]$ having good reduction everywhere. These are, of course, just the fields of class number 1. By using the second corollary to Theorem 1, this may be extended to:

THEOREM 5. *If the class number of $k = \boldsymbol{Q}[\sqrt{-m}]$ is prime to 6, then there are no elliptic curves defined over k having good reduction everywhere.*

References

1. Z. I. Borevich and I. R. Saferevich, *Number Theory*, Academic Press, New York, N.Y., 1966.

2. F. B. Coghlan, *Elliptic Curves with Conductor* $N = 2^m3^n$, PhD. Thesis. Manchester University, 1967.

3. B. N. Delone and K. K. Fadeev, *The theory of irrationalities of the third degree*, Amer. Math. Soc. Providence, R. I., 1964.

4. H. Hasse, *Arithmetische Theorie der kubischen Zahlkoerper auf Klassen Koerpertheoretischer Grundlage*, Math. Zeit., **31** (1930), 565–582.

5. S. Lang, *Elliptic Functions*, Addison-Wesley Publishing Company, Inc. Reading, Mass., 1973.

6. S. Lang and J. Tate, *Principal homogeneous spaces over Abelian varieties*, Amer. J. Math., **80** (1958), 659–684.

7. A. P. Ogg, *Abelian curves of small conductors*. J. Reine Andgew. Math., **226** (1967), 206–215.

8. C. B. Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc., (2), **10** (1975), 367–378.

9. R. J. Stroeker, *Elliptic Curves Over Imaginary Quadratic Number Fields*, Report 7209, Econometric Institute, Netherlands School of Economics.

10. J. Tate, *Algorithm for Determining the Type of a Singular Fiber in an Elliptic Pencil*, Modular Functions Of One Variable IV. Lecture Notes in Mathematics 476. Springer-Verlag, Berlin, 1975.

Received September 22, 1976 and in revised form June 22, 1977.

University of Illinois at Chicago Circle
Chicago, IL 60680