PACIFIC JOURNAL OF MATHEMATICS
Vol. 108, No. 2, 1983

REDUCTION OF ELLIPTIC CURVES OVER IMAGINARY QUADRATIC NUMBER FIELDS

R. J. STROEKER

It is shown that an elliptic curve defined over a complex quadratic field K, having good reduction at all primes, does not have a global minimal (Weierstrass) model. As a consequence of a theorem of Setzer it then follows that there are no elliptic curves over K having good reduction everywhere in case the class number of K is prime to 6.

1. Introduction. An elliptic curve over a field K is defined to be a non-singular projective algebraic curve of genus 1, furnished with a point defined over K. Any such curve may be given by an equation in the Weierstrass normal form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

with coefficients a_i in K. In the projective plane $\mathbf{P}_K^2$, the point defined over K becomes the unique point at infinity, denoted by $\underline{0}$. Given such a Weierstrass equation for an elliptic curve E, we define, following Néron and Tate ([12], §1; [6], Appendix 1, p. 299):

$$\begin{cases} b_2 = a_1^2 + 4a_2, & c_4 = b_2^2 - 24b_4, \\ b_4 = a_1a_3 + 2a_4, & c_6 = -b_2^3 + 36b_2b_4 - 216b_6, \\ b_6 = a_3^2 + 4a_6, & \\ b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2, & \\ \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, & j = c_4^3/\Delta. \end{cases} \tag{1.2}$$

The discriminant Δ, defined above, is non-zero if and only if the curve E is non-singular. In particular, we have

$$4b_8 = b_2b_6 - b_4^2 \quad \text{and} \quad c_4^3 - c_6^2 = 2^6 3^3 \Delta. \tag{1.3}$$

The various representations of an elliptic curve over K, with the same point at infinity, are related by transformations of the type

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned} \quad \text{with } r, s, t \in K \text{ and } u \in K^*. \tag{1.4}$$

Let E be an elliptic curve defined over a field K. An equation for E of type (1.1) is called minimal with respect to a discrete valuation ν of K iff $\nu(a_i) \geq 0$ for all i and $\nu(\Delta)$ minimal, subject to that condition. For each discrete valuation of K, there exists a minimal equation for E. This equation is unique up to a change of co-ordinates of the form (1.4) with r, s, $t \in R$ and u invertible in R. Here R stands for the valuation ring. An equation for an elliptic curve E defined over K is called a global minimal equation for E over K iff this equation is minimal with respect to all discrete valuations of K simultaneously. We have the following theorem due to Néron and Tate.

(1.5) THEOREM. *Let $\mathcal{O}_K$ be the ring of integers of an algebraic number field K. If $\mathcal{O}_K$ is a principal ideal domain, then every elliptic curve defined over K has a global minimal equation over K.*

It is not true, in general, that an elliptic curve defined over an algebraic number field K has a global minimal equation over K. Following Tate [13], define the minimal discriminant ideal for an elliptic curve E over a number field K by

$$\Delta_E = \prod_{\text{finite } \nu} \mathfrak{p}_\nu^{\nu(\Delta_\nu)},$$

where Δ_ν is the discriminant of a minimal equation for E at ν and $\mathfrak{p}_\nu$ is the prime ideal of $\mathcal{O}_K$ associated with ν. If a global minimal equation for E over $\mathcal{O}_K$ exists, then Δ_E is principal, for it is generated by the discriminant of any global minimal equation.

For a discrete valuation ν of a field K, let R be the valuation ring, P the unique prime ideal of R and $k = R/P$ the residue class field. Assume ν is normalized and let $\pi \in R$ be a prime with $\nu(\pi) = 1$. If E is an elliptic curve over K, let Γ be a minimal equation for E with respect to ν of type (1.1). Reducing the coefficients a_i of Γ modulo $P = \pi R$, one obtains an equation $\tilde{\Gamma}$ for a plane cubic curve $\tilde{E}$ defined over k. This equation is clearly unique up to a transformation of the form (1.4) over k. If $\tilde{\Gamma}$ is non-singular (over $\bar{k}$) then $\tilde{E}$ is an elliptic curve over k and $\tilde{\Gamma}$ is an equation for $\tilde{E}$ over k. In that case $\tilde{\Delta} \neq 0$ or, equivalently, $\nu(\Delta) = 0$. We say that E has good (or non-degenerate) reduction at ν. In case $\tilde{\Delta} = 0$, i.e. $\nu(\Delta) > 0$, then $\tilde{E}$ is a rational curve and E has bad (or degenerate) reduction at ν. In particular, if $\nu(\Delta) > 0$ and $\nu(c_4) = 0$, then $\tilde{E}$ has a node and we say that E has multiplicative reduction at ν; if $\nu(\Delta) > 0$ and $\nu(c_4) \neq 0$, then $\tilde{E}$ has a cusp and the reduction of E at ν is additive.

(1.6) THEOREM (*Tate*). *There is no elliptic curve defined over* **Q** *with good reduction at all discrete valuations of* **Q**.

Proofs of this theorem may be found in [7] and [**10**], p. 32.

In this paper we will prove and discuss a generalization of Tate's result for elliptic curves defined over imaginary quadratic number fields. More precisely, the purpose of this paper is to prove

(1.7) MAIN THEOREM. *Let K be an imaginary quadratic number field and let E be an elliptic curve defined over K. If E has a global minimal equation over K, then E has bad reduction at v for at least one discrete valuation v of K.*

In fact when E has everywhere good reduction over a number field K, then $\Delta_E = (1)$. The condition placed upon E in the Main Theorem (1.7), to the effect that E must have a global minimal equation over K, is not superfluous. This is shown by the following theorem, first formulated by Tate.

(1.8) THEOREM. *Let n be a rational integer prime to 6 and suppose $j^2 - 1728j \pm n^{12} = 0$. Then the elliptic curve with equation*

$$y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}$$

over $\mathbf{Q}(j)$ has good reduction at every discrete valuation of $\mathbf{Q}(j)$.

For a proof we refer to [**11**] or [**10**], p. 31. See also Setzer [**9**], Theorem 4(b).

In this context we have the following theorem, which is a direct consequence of the Main Theorem (1.7) and a theorem of Setzer (cf. [**9**], Theorem 5).

(1.9) THEOREM. *Let K be an imaginary quadratic number field with class number prime to 6. Then there are no elliptic curves over K having good reduction everywhere.*

Indeed, when the class number of a number field K is prime to 6, the condition 'Δ_E is principal' is equivalent to the existence of a global minimal model over K.

In Ishii [4] a similar but less general result is obtained.

Throughout the rest of this paper, K will stand for the imaginary quadratic number field $\mathbf{Q}(\sqrt{-m})$, where m is a squarefree positive integer. The symbol $\mathcal{O}$ will always denote the ring of integers of K with basis $\{1, \omega\}$, i.e. $\mathcal{O} = \mathbf{Z}[\omega]$.

2. Proof of the main theorem in case $m \neq 1$ or 3. Let E_r denote an elliptic curve, defined over K, with an equation of type

$$\Gamma_r\colon x^3 - y^2 = r \qquad (r \in K^*).$$

As usual $E_r(K)$ will stand for the group of K-rational points of E_r; the group operation in $E_r(K)$ will be written additively.

(2.1) LEMMA. *If $r \in \mathbf{Q}$, then $(x, y) + (\bar{x}, \bar{y}) \in E_r(\mathbf{Q})$ for each point $(x, y) \in E_r(K)$.*

Proof. Let $(x, y) \in E_r(K)$ and put $P = (x, y) + (\bar{x}, \bar{y})$. Then $P \in E_r(K)$ because $r \in \mathbf{Q}$. Clearly, $\bar{P} = P$ and since $K \cap \mathbf{R} = \mathbf{Q}$, we conclude $P \in E_r(\mathbf{Q})$. □

Some easy consequences of the group structure on E_r are laid down in the following formulas. A straightforward calculation shows their validity.

If $r \in \mathbf{Q}$, $(x, y) \in E_r(K)$ and $(x, y) + (\bar{x}, \bar{y}) = (p, q) \in E_r(\mathbf{Q})$, then

$$(2.2)\quad \begin{cases} x + \bar{x} + p = \left(\dfrac{y - \bar{y}}{x - \bar{x}}\right)^2 & \text{and } \; p \cdot \dfrac{y - \bar{y}}{x - \bar{x}} + \dfrac{x\bar{y} - \bar{x}y}{x - \bar{x}} + q = 0 \\ & \text{in case } \bar{x} \neq x, \\ 2x + p = (3x^2/2y)^2 & \text{in case } \bar{x} = x, \bar{y} = y \neq 0, \\ (p, q) = \underline{0} & \text{in case } \bar{x} = x, \bar{y} = -y. \end{cases}$$

(2.3) LEMMA. *If $(x, y) \in E_r(K)$ with $r = \pm 2^6 3^3$ such that $x, y \in \mathcal{O}$ and $x\bar{x} \not\equiv 0$ (mod 2), then $x \in \mathbf{Z}$ and $y \notin \mathbf{Z}$.*

Proof. Lemma (2.1) shows $(x, y) + (\bar{x}, \bar{y}) \in E_r(\mathbf{Q})$. Now $E_r(\mathbf{Q}) \cong \mathbf{Z}_2$ (cf. [3]) and thus $E_r(\mathbf{Q}) = \{\underline{0}, (\pm 12, 0)\}$, where the $\pm$ sign corresponds to that of r. Consequently, we have to consider two possibilities; first, if $(x, y) + (\bar{x}, \bar{y}) = \underline{0}$ then $\bar{x} = x$ and $\bar{y} = -y$. If $y = 0$, then x does not satisfy the condition $x\bar{x} \not\equiv 0$ (mod 2). If $(x, y) + (\bar{x}, \bar{y}) = (\pm 12, 0)$, put $x = a + b\omega$ and $y = c + d\omega$ $(a, b, c, d \in \mathbf{Z})$. Then clearly $b \neq 0$. We distinguish between the cases:

(i) $m \equiv 1$ or 2 (mod 4);

(ii) $m \equiv 3 \pmod 4$.

In case (i), $\omega = \sqrt{-m}$. Put $T = d/b$. We obtain from (2.2):

(i)$_1$ $2a \pm 12 = T^2$;

(i)$_2$ $c = -T^3 + 3aT$;

(i)$_3$ $mb^2 = 3a^2 - 2cT$.

Clearly, a and T are even because of (i)$_1$ (note that $T \in \mathbf{Z}$). Hence $mb^2 \equiv 0 \pmod 4$. This follows from (i)$_3$. Thus b is even, which implies $x \equiv 0 \pmod 2$.

In case (ii), $\omega = \frac{1}{2}(1 + \sqrt{-m})$. Again put $T = d/b$ and $a_1 = 2a + b$, $c_1 = 2c + d$. Formulas (2.2) give

(ii)$_1$ $a_1 \pm 12 = T^2$;

(ii)$_2$ $c_1 = -2T^3 + 3a_1T$;

(ii)$_3$ $mb^2 = 3a_1^2 - 4c_1T$.

Again $T \in \mathbf{Z}$ and a_1, b and T have the same parity as can be seen from (ii)$_1$ and (ii)$_3$. Moreover it follows from (ii)$_2$ that a_1 and c_1 have the same parity. If a_1, b, c_1 and T are even, then $a_1 \equiv b \equiv 0 \pmod 4$ as is clear from (ii)$_1$ and (ii)$_3$. Hence $4x\bar{x} = a_1^2 + mb^2 \equiv 0 \pmod 8$. And if a_1, b, c_1 and T are odd, then $m \equiv 7 \pmod 8$, which is a consequence of (ii)$_3$. Again $4x\bar{x} \equiv 0 \pmod 8$. We may conclude $(x, y) + (\bar{x}, \bar{y}) = \underline{0}$ if $x\bar{x} \not\equiv 0 \pmod 2$. □

(2.4) LEMMA. *Let* (1.1) *be a global minimal equation for the elliptic curve E over K with $v(\Delta) = 0$ for every discrete valuation v of K. Further, let $\mathfrak{p}_2$ be a prime ideal divisor of* 2 *in $\mathcal{O}$. Then $\mathfrak{p}_2$ does not divide a_1.*

Proof. Since $v(\Delta) = 0$ for every discrete valuation of K, Δ is a unit in $\mathcal{O}$. Suppose $\mathfrak{p}_2 | a_1$. Then we see from (1.2) that $\mathfrak{p}_2^2 | b_2$ and $\mathfrak{p}_2 | b_4$ and hence $\mathfrak{p}_2^3 | (\Delta + 27b_6^2)$. It is clear that $\mathfrak{p}_2$ does not divide a_3. For $\mathfrak{p}_2 | a_3$ implies $\mathfrak{p}_2 | b_6$ and thus $\mathfrak{p}_2 | \Delta$. However, Δ is a unit. From (1.2) we also obtain $b_6^2 \equiv a_3^4 \pmod 8$. We observe that we may restrict the values of the coefficients a_1, a_2 and a_3 to

$$a_1, a_3 = 0, 1, \omega \text{ or } 1 + \omega \quad \text{and} \quad a_2 = 0, \pm 1, \pm\omega \text{ or } \pm 1 \pm \omega.$$

We consider the following cases separately:

(i) $m \equiv 1, 2 \pmod 4$.

The principal ideal (2) factors as $\mathfrak{p}_2^2$. Further, $b_6^2 \equiv 1 \pmod{\mathfrak{p}_2^5}$ because $a_3 = 1$ or ω in case m is odd and $a_3 = 1$ or $1 + \omega$ if m is even. If $\mathfrak{p}_2^2$ does not divide a_1, then $\Delta - 1 \equiv \Delta + 27b_6^2 \not\equiv 0 \pmod{\mathfrak{p}_2^4}$. But $\Delta - 1 \equiv 0 \pmod{\mathfrak{p}_2^3}$ implies $\Delta = 1$, because Δ is a unit, contradiction. And if $\mathfrak{p}_2^2 | a_1$ then $\Delta + 27b_6^2 \equiv 0 \pmod{\mathfrak{p}_2^6}$. But then $\Delta + 3 \equiv 0 \pmod{\mathfrak{p}_2^5}$ and this is clearly impossible.

(ii) $m \equiv 3 \pmod 8$.

Now $\mathfrak{p}_2 = (2)$. If $a_3 = 1$ then $b_6^2 \equiv 1 \pmod 8$ and hence $\Delta + 3 \equiv 0 \pmod 8$, an impossibility. Further, if $a_3 = \omega,\ 1 + \omega$, then $b_6^2 \equiv \omega,\ 1 + \omega \pmod 2$ and hence $\Delta \equiv \omega, 1 + \omega \pmod 2$. This is contradictory in case $m \neq 3$. However, if $m = 3$, then $b_6^2 \equiv -\omega,\ \omega^2 \pmod 8$ and this implies $\Delta \equiv 3\omega,\ -3\omega^2 \pmod 8$, again a contradiction.

(iii) $m \equiv 7 \pmod 8$.

We now have $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ with $\mathfrak{p}_2 = (2, \omega)$ and $\mathfrak{p}_2' = (2, \bar{\omega})$. If $\mathfrak{p}_2 | a_1$ then $a_3 = 1$ implies $b_6^2 \equiv 1 \pmod 8$ and $a_3 = 1 + \omega$ gives $b_6^2 \equiv 1 \pmod{\mathfrak{p}_2^3}$. Both cases are impossible. An analogous argument may be used in case $\mathfrak{p}_2' | a_1$. □

We are now in a position to prove the main theorem for $K = \mathbf{Q}(\sqrt{-m})$ with $m \neq 1$ and $m \neq 3$.

Suppose that E has good reduction at every discrete valuation of K. Let (1.1) be a global minimal equation for E. Then $\nu(\Delta) = 0$ for every discrete valuation ν of K. Hence Δ is a unit of $\mathcal{O}$, i.e. $|\Delta| = 1$ since $m \neq 1$ and $m \neq 3$. Now from (1.3) we have

$$c_4^3 - c_6^2 = \pm 2^6 3^3$$

and this yields $c_4\bar{c}_4 \not\equiv 0 \pmod 2$ because of (2.4). Lemma (2.3) then shows that $c_4 \in \mathbf{Z}$ and $c_6 \notin \mathbf{Z}$. Thus $c_6 = y\sqrt{-m}$ with $y \neq 0$ and $y \in \mathbf{Z}$, because $c_6^2 \in \mathbf{Z}$. From (1.2) we obtain

$$y\sqrt{-m} \equiv -a_1^6 \pmod 4.$$

Checking the possibilities $a_1 = 1$, ω and $1 + \omega$, we find an impossible congruence in each case. □

The proof of the main theorem as given above ($m \neq 1$ and $m \neq 3$) depends largely on the fact that the only units of $\mathcal{O}$ are $+1$ and -1. However, in $\mathbf{Z}[i]$ and $\mathbf{Z}[\rho]$, where $\rho = \frac{1}{2}(1 + \sqrt{-3})$, we have the additional units $\pm i$ and $\pm\rho$, $\pm\rho^2$, respectively. Consequently, in order to complete the proof of the theorem, it suffices to show that no point $(x, y) \in \mathcal{O} \times \mathcal{O}$ of the curve with equation

$$x^3 - y^2 = \varepsilon 2^6 3^3, \tag{2.5}$$

where $\mathcal{O} = \mathbf{Z}[i]$ and $\varepsilon = \pm i$ in case $K = \mathbf{Q}(i)$, and where $\mathcal{O} = \mathbf{Z}[\rho]$ and $\varepsilon = \pm\rho,\ \pm\rho^2$ in case $K = \mathbf{Q}(\rho)$, comes from an elliptic curve with global minimal equation of the form (1.1) and $(x, y) = (c_4, c_6)$. This will be done in §3.

3. The exceptional cases. First proof. First, we consider $K = \mathbf{Q}(i)$. Let (x, y) be a solution of (2.5) with $\varepsilon = \pm i$ that comes from an elliptic curve over K with global minimal equation (1.1) such that $(x, y) = (c_4, c_6)$. Then (x, y) must satisfy

$$(3.1) \qquad 1 + i \nmid x, \qquad 3 | y \Rightarrow 3^3 | y.$$

This follows immediately from Lemma (2.4) and (1.2). Now $(-x, iy)$ is also a solution of (2.5) satisfying (3.1). So we need only consider solutions (x, y) of

$$(3.2) \qquad x^3 = y^2 - 3i(24)^2.$$

(3.3) LEMMA. *If* $\theta = \frac{1}{2}(1 + i)\sqrt{6}$, *then* $\theta^2 = 3i$ *and the number field* $\mathbf{Q}(\theta)$ *has the following properties*:

(1) *The set* $\{1, \theta, i, i\theta\}$ *is an integer basis for* $\mathbf{Q}(\theta)$.

(2) *The principal ideals* (2) *and* (3) *factor as* $\mathfrak{p}_2^4$ *and* $\mathfrak{p}_3^2$, *respectively.*

(3) *The class number of* $\mathbf{Q}(\theta)$ *equals* 2.

(4) *The unit* $\eta = 1 + i + \theta$ *is fundamental.*

The proof of this lemma is a straightforward exercise (cf. [**2**]).

We turn our attention to (3.2) and write

$$(3.4) \qquad x^3 = (y - 24\theta)(y + 24\theta).$$

The only possible prime divisor that $y + 24\theta$ and $y - 24\theta$ have in common is $\mathfrak{p}_3$, because of (3.1) and (3.3). We deduce that

$$(y + 24\theta) = \mathfrak{p}_3^a \mathfrak{A}^3,$$

where $a = 0$, 1 or 2 and $\mathfrak{A}$ is an integral ideal. Also

$$(y - 24\theta) = \mathfrak{p}_3^a \mathfrak{A}'^3,$$

where $\mathfrak{A}$ and $\mathfrak{A}'$ are conjugate ideals. Multiplication yields

$$(x)^3 = \mathfrak{p}_3^{2a}(\mathfrak{A}\mathfrak{A}')^3,$$

hence $2a \equiv 0 \pmod 3$ and thus $a = 0$. Since the class number of $\mathbf{Q}(\theta)$ equals 2 and $\mathfrak{A}^3$ is a principal ideal, we deduce that $\mathfrak{A}$ is principal. Then

$$y + 24\theta = \varepsilon(a + b\theta)^3,$$

where ε is a unit and $a, b \in \mathbf{Z}[i]$. By Dirichlet's unit theorem ε can be expressed in the form $\zeta\eta^k$ with $k \in \mathbf{Z}$ and root of unity ζ. The only roots of unity in $\mathbf{Q}(\theta)$ are ± 1 and $\pm i$, all of which may be written as a cube.

Furthermore, the conjugation map $\theta \mapsto -\theta$ takes η into η^{-1}. Consequently, we need only consider

$$\pm y + 24\theta = (1 \text{ or } \eta)(a + b\theta)^3$$

with $a, b \in \mathbf{Z}[i]$.

(1) $\pm y + 24\theta = (a + b\theta)^3$.

Equating coefficients of 1 and θ yields:

$$\pm y = a^3 + 9ab^2 i \quad \text{and} \quad 24 = 3a^2 b + 3b^3 i.$$

Then $b|8$ and the solutions (x, y) are easily obtained. However, none of those satisfies (3.1).

(2) $\pm y + 24\theta = (1 + i + \theta)(a + b\theta)^3$.

Equating coefficients of 1 and θ yields:

$$\pm y = (1 + i)a^3 + 9ia^2 b + 9(-1 + i)ab^2 - 9b^3$$

and

$$24 = a^3 + 3(1 + i)a^2 b + 9iab^2 + 3(-1 + i)b^3.$$

Clearly $3|a$ and hence $3|y$. However, $3^3|y$ implies $3^3|24$. Hence a solution (x, y) of (2.5) cannot possibly satisfy (3.1). This completes the case $K = \mathbf{Q}(i)$.

Next we consider $K = \mathbf{Q}(\rho)$; we recall that $\rho = \frac{1}{2}(1 + \sqrt{-3})$. Let (x, y) be a solution of (2.5) with $\varepsilon = \pm\rho, \pm\rho^2$, coming from an elliptic curve over $\mathbf{Q}(\rho)$ with a global minimal equation (1.1) and $(x, y) = (c_4, c_6)$. According to (1.2) and Lemma (2.4), (x, y) must satisfy

$$(3.5) \qquad 2 \nmid x, \qquad (2\rho - 1)|y \Rightarrow (2\rho - 1)^3|y.$$

Clearly, also $(\bar{x}, \bar{y})$ solves (2.5) and satisfies (3.5). Since $\rho = -\bar{\rho}^2$ and $\bar{\rho} = -\rho^2$, we need only consider the equation

$$(3.6) \qquad x^3 - \sigma\rho 2^6 3^3 = y^2,$$

with $\sigma = \pm 1$.

(3.7) LEMMA. *If $\zeta = \zeta_9 = -\exp \pi i/9$, then the cyclotomic field $\mathbf{Q}(\zeta)$ has the following properties*:

(1) *The set $\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$ is an integer basis for $\mathbf{Q}(\zeta)$.*

(2) *The principal ideal (2) is prime and the ideal (3) factors as $\mathfrak{p}_3^6$.*

(3) *The class number of $\mathbf{Q}(\zeta)$ equals 1.*

(4) *The set $\{1 + \zeta, 1 + \zeta^5\}$ is a set of fundamental units.*

The above statements are all well known. For (1) and (2), see [**5**], p. 39; for (3) see [**14**], Ch. 7, and for (4) see [**1**], p. 378.

We return to (3.6) and observe it may be written as

$$y^2 = (x + 12\sigma\zeta)(x + 12\sigma\zeta^4)(x + 12\sigma\zeta^7).$$

Since 2 does not divide x, we deduce that

$$(x + 12\sigma\zeta) = \mathfrak{p}_3^a \mathfrak{A}^2 \tag{3.8}$$

with $a = 0$ or 1 and integral ideal $\mathfrak{A}$. The conjugation maps $\zeta \mapsto \zeta^4$ and $\zeta \mapsto \zeta^7$ take ρ into ρ while $\mathfrak{p}_3$ too remains unchanged. Hence from (3.8) we obtain the conjugate ideal equations

$$(x + 12\sigma\zeta^4) = \mathfrak{p}_3^a(\mathfrak{A}')^2 \quad \text{and} \quad (x + 12\sigma\zeta^7) = \mathfrak{p}_3^a(\mathfrak{A}'')^2.$$

Then $(y)^2 = \mathfrak{p}_3^{3a}(\mathfrak{A}\mathfrak{A}'\mathfrak{A}'')^2$ and, consequently, $3a \equiv 0 \pmod 2$ or $a = 0$. As a result (3.8) becomes

$$(x + 12\sigma\zeta) = (\alpha + \beta\zeta + \gamma\zeta^2)^2 \quad \text{with } \alpha, \beta, \gamma \in \mathbf{Z}[\rho],$$

and this gives in integers of $\mathbf{Q}(\zeta)$:

$$\begin{cases} x + 12\sigma\zeta = \tau\zeta^a(1 + \zeta)^b(1 + \zeta^5)^c(\alpha + \beta\zeta + \gamma\zeta^2)^2, \\ x + 12\sigma\zeta^4 = \tau\zeta^{4a}(1 + \zeta^4)^b(1 + \zeta^2)^c(\alpha + \beta\zeta^4 + \gamma\zeta^8)^2, \\ x + 12\sigma\zeta^7 = \tau\zeta^{7a}(1 + \zeta^7)^b(1 + \zeta^8)^c(\alpha + \beta\zeta^7 + \gamma\zeta^5)^2, \end{cases} \tag{3.9}$$

where $\tau = \pm 1$, $0 \le a, b, c \le 1$ and $a, b, c \in \mathbf{Z}$. All this is a consequence of Dirichlet's unit theorem and the fact that the only roots of unity of $\mathbf{Q}(\zeta)$ are $\pm\zeta^k$, $k \in \mathbf{Z}$. Multiplication of the three equations (3.9) yields

$$y^2 = \tau(-1)^{a+b}\rho^{a+2b+c}(\alpha^3 - \rho\beta^3 + \rho^2\gamma^3 + 3\rho\alpha\beta\gamma)^2. \tag{3.10}$$

We observe that we may assume $a = 0$ in (3.9). For ζ can be written as a square and thus ζ^a, ζ^{4a}, and ζ^{7a}, respectively, may be absorbed in the square on the right-hand side of the equations (3.9).

We investigate the four cases $(b, c) = (0,0)$, $(1,0)$, $(0,1)$ and $(1,1)$ separately.

(1) $b = c = 0$.

Then (3.10) shows that $\tau = 1$. Equating coefficients of 1, ζ, ζ^2 in the first equation of (3.9) gives

$$x = \alpha^2 - 2\beta\gamma\rho, \quad 12\sigma = 2\alpha\beta - \gamma^2\rho \quad \text{and} \quad 0 = \beta^2 + 2\alpha\gamma.$$

It is clear that $2 \nmid \alpha$, $2|\beta$ and $2|\gamma$. Put $\beta = 2\beta_1$ and $\gamma = 2\gamma_1$. A common prime divisor of α and γ_1 divides 3. Thus $\alpha\gamma_1 = -\beta_1^2$ implies

$$\alpha = \varepsilon_1(2\rho - 1)^p s^2 \quad \text{and} \quad \gamma_1 = \varepsilon_2(2\rho - 1)^p t^2,$$

where $p = 0$ or 1 and ε_1, ε_2 are units such that $\varepsilon_1\varepsilon_2 = -\delta^2$. Now, because of (3.5), we have

$$x \equiv \alpha^2 = (-3)^p \varepsilon_1^2 s^4 \pmod 8,$$

which implies $p = 0$. Further $\beta_1 = \delta(2\rho - 1)^p st = \delta st$ and thus

$$3\sigma = \alpha\beta_1 - \gamma_1^2\rho = \varepsilon_1\delta^{-2}t\{(\delta s)^3 + \rho(\varepsilon_2 t)^3\}. \tag{3.11}$$

Apparently $t|3$ and hence we may write $t = \varepsilon(2\rho - 1)^q$ with $q = 0$, 1 or 2. Substitution of these values of t in (3.11) gives a contradiction in all cases.

(2) $b = 1, c = 0$.

Now $\tau = -1$ as can be seen from (3.10), and we arrive at the equations

$$x = -\alpha^2 + 2\alpha\gamma\rho + \beta^2\rho + 2\beta\gamma\rho,$$
$$-12\sigma = \alpha^2 + 2\alpha\beta - 2\beta\gamma\rho - \gamma^2\rho,$$
$$0 = -\beta^2 - 2\alpha\beta - 2\alpha\gamma + \gamma^2\rho.$$

From the last two equations we find that $\alpha \equiv \beta \equiv \gamma\rho^2 \pmod 2$. Elimination of α and β modulo 2, reduces the last equation to $2\gamma^2\rho^2 \equiv 0 \pmod 4$. And thus $2|\gamma$, $2|\alpha$ and $2|\beta$. The first equation then shows that $2|x$.

(3) $b = 0, c = 1$.

Again $\tau = -1$. As before we find

$$x = -\alpha^2 - \gamma^2 - 2\alpha\beta\rho^2 + 2\beta\gamma\rho,$$
$$12\sigma = -2\alpha\beta - \beta^2\rho^2 + \gamma^2\rho - 2\alpha\gamma\rho^2,$$
$$0 = -\alpha^2\rho + \beta^2 + 2\alpha\gamma + 2\beta\gamma\rho^2.$$

From the second and third equation we find that $\beta \equiv \gamma\rho \pmod 2$ and $\beta \equiv \alpha\rho^2 \pmod 2$. Elimination of α and β modulo 2, reduces the last equation to $2\gamma^2 \equiv 0$ and (mod 4). Consequently, $2|\gamma$, $2|\alpha$ and $2|\beta$. The first equation then shows that $2|x$.

(4) $b = c = 1$.

From (3.10) and (3.9) we obtain, respectively, $\tau = 1$ and

$$x = \alpha^2\rho - \beta^2\rho - \gamma^2 + 2\alpha\beta\rho^2 - 2\alpha\gamma\rho - 2\beta\gamma\rho^2,$$
$$12\sigma = \alpha^2 + \beta^2\rho^2 - \gamma^2\rho^2 + 2\alpha\beta\rho + 2\alpha\gamma\rho^2 - 2\beta\gamma\rho,$$
$$0 = \alpha^2\rho - \beta^2\rho + \gamma^2\rho - 2\alpha\beta - 2\alpha\gamma\rho - 2\beta\gamma\rho^2.$$

The second equation shows $\alpha + \beta\rho + \gamma\rho \equiv 0 \pmod 2$, and the third shows $\alpha + \beta + \gamma \equiv 0 \pmod 2$. Hence $2|\alpha$ and $2|(\beta + \gamma)$. The last equation then reduces to $2\beta\gamma \equiv 0 \pmod 4$ and hence $2|\beta$ and $2|\gamma$. Again the first equation shows $2|x$.

This completes the case $K = \mathbf{Q}(\rho)$. □

4. The exceptional cases. Second proof. We will give yet another proof of the Main Theorem (1.7) in the exceptional cases $K = \mathbf{Q}(i)$ and $K = \mathbf{Q}(\rho)$. This proof depends on the appropriate parts of the following theorem.

(4.1) THEOREM. *Let E be an elliptic curve defined over $K = \mathbf{Q}$, $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{-2})$ or $\mathbf{Q}(\rho)$ with non-degenerate reduction at all discrete valuations of K outside 2. Then E has a point of order 2 rational over K.*

Proof. Since the class number of K equals 1, an elliptic curve E over K has a global minimal equation (1.1) which coefficients a_i belonging to the ring of integers $\mathcal{O}$ of K. Let Δ be the discriminant of this equation. A transformation (1.4) with $u = \frac{1}{2}$, $r = 0$, $s = -\frac{1}{2}a_1$ and $t = -\frac{1}{2}a_3$ leads to an equation

$$y'^2 = x'^3 + a_2'x'^2 + a_4'x' + a_6', \tag{4.2}$$

for E with $a_i' \in \mathcal{O}$, which is minimal with respect to all discrete valuations of K outside 2. In fact $\Delta' = 2^{12}\Delta$. Assume the points $(x', 0)$ of order two on (4.2) are not rational over K, i.e. $x' \notin K$. Then the polynomial $f(x) = x^3 + a_2x^2 + a_4x + a_6 \in \mathcal{O}[x]$ is irreducible. If ξ is a root of $f(x) = 0$ and $L = K(\xi)$, then L/K is unramified at all primes not dividing 2. This is because the discriminant of f divides Δ'. Let M be the splitting field of the extension L/K. Then M/K is Galois and $[M : K] = 3$ or 6. Moreover M/K is unramified at all primes not dividing 2 (cf. **[14]**, 4-10-9 and 4-10-10, p. 178). Let N be the subfield of M corresponding to the subgroup of order 3 in the Galois group $G(M/K)$. In case $|G(M/K)| = 6$, the extension N/K is only ramified at the single prime above 2. For N/K is unramified everywhere else and N/K cannot be unramified at all primes by class field theory, since the class number of K equals 1. This knowledge enables us to list all possible fields N for each of the given fields K:

(1) $K = \mathbf{Q}$; $N = \mathbf{Q}$, $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{2})$ or $\mathbf{Q}(\sqrt{-2})$.

(2) $K = \mathbf{Q}(i)$; $N = \mathbf{Q}(i)$, $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\beta)$ or $\mathbf{Q}(\bar{\beta})$, where α and β are roots of $x^4 + 1 = 0$ and $x^4 - 2x^2 + 2 = 0$, respectively.

(3) $K = \mathbf{Q}(\sqrt{-2})$; $N = \mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\gamma)$ or $\mathbf{Q}(\bar{\gamma})$, where α and γ are roots of $x^4 + 1 = 0$ and $x^4 + 2 = 0$, respectively.

(4) $K = \mathbf{Q}(\rho)$; $N = \mathbf{Q}(\rho)$, $\mathbf{Q}(\rho, i)$, $\mathbf{Q}(\rho, \sqrt{2})$ or $\mathbf{Q}(\rho, \sqrt{-2})$.

All possible fields N have class number 1, as is easily established using the Minkowski bound in each case. Consequently, the only prime that ramifies in M/N is the single prime $\mathfrak{p}$ above 2. Now M/N is abelian and $G(M/N) \cong \mathbf{Z}_3$. By class field theory, to be more precise, by Artin's reciprocity theorem (cf. [**5**], 5.7 p. 164), the order of $G(M/N)$ divides the order of the ray class group modulo $\mathfrak{p}^n$ for sufficiently large exponent n (cf. [**5**], p. 109). In its turn, the order of the ray class group is a divisor of

$$h(N)\mathrm{Norm}_{N/\mathbf{Q}}(\mathfrak{p}^{n-1})\{\mathrm{Norm}_{N/\mathbf{Q}}(\mathfrak{p}) - 1\} = 2^{n-1}$$

in case $K \neq \mathbf{Q}(\rho)$ and of

$$h(N)\mathrm{Norm}_{N/\mathbf{Q}}(\mathfrak{p}^{n-1}) = 4^{n-1}$$

in case $K = \mathbf{Q}(\rho)$. Here $h(N)$ stands for the class number of N (cf. [**5**], 1.3 p. 111 and 1.6 p. 112). This contradicts the fact that $|G(M/N)| = 3$. This completes the proof of the theorem.

We remark that Theorem (4.1) was proved by Ogg [**7**] in case $K = \mathbf{Q}$. □

We return to the problem at hand. Suppose $K = \mathbf{Q}(i)$ or $K = \mathbf{Q}(\rho)$, and let E be an elliptic curve defined over K with good reduction everywhere. According to Theorem (4.1) E has a point of order two rational over K. Now E has a Weierstrass equation

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in \mathcal{O}$ and $\Delta = \varepsilon 2^{12}$, where ε is a unit of $\mathcal{O}$. Transforming the point $(c, 0)$ of order two with $c \in \mathcal{O}$ to $(0, 0)$ by means of (1.4), one obtains

$$Y^2 = X^3 + A_2X^2 + A_4X$$

with $A_i \in \mathcal{O}$ for E. Expressing C_4 and C_6 in terms of A_2 and A_4 leads to the equation

$$A_4^2(A_2^2 - 4A_4) = \varepsilon 2^8 \qquad \text{(see (1.3))}. \tag{4.3}$$

The last equation is easy to deal with, because the only possible prime divisor of A_4 is the prime divisor of 2. In fact it follows easily that no solution of (4.3) comes from an elliptic curve E defined over K having good reduction everywhere.

5. Acknowledgements. The author wishes to express his gratitude to F. Oort and H. W. Lenstra, Jr. for their assistance. Also a word of thanks is due to the referee for his constructive remarks.

References

[1] W. E. H. Berwick, *Algebraic number fields with two independent units*, Proc. London Math. Soc., **34** (1932), 360–378.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Pure and Appl. Math. Ser. Vol. 20, Academic Press, New York & London, 1966.

[3] J. W. S. Cassels, *The rational solutions of the Diophantine equation* $y^2 = x^3 - D$, Acta Math. Stockh., **82** (1950), 243–273.

[4] Hidenori Ishii, *The non-existence of elliptic curves with everywhere good reduction over certain imaginary quadratic number fields*, J. Math. Soc. Japan, **31** (2) (1979), 273–279.

[5] G. J. Janusz, *Algebraic Number Fields*, Pure and Appl. Math. Ser. Vol. 55, Academic Press, New York & London, 1973.

[6] S. Lang, *Elliptic Functions*, Addison-Wesley, 1973.

[7] A. P. Ogg, *Abelian curves of 2-power conductor*, Proc. Cambr. Phil. Soc., **62** (1966), 143–148.

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

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

[10] R. J. Stroeker, *Elliptic curves defined over imaginary quadratic number fields*, Doctoral Dissertation, Amsterdam 1975.

[11] J. T. Tate, *Letter to Serre*, dated July 24th, 1971.

[12] _____, *The arithmetic of elliptic curves*, Invent. Math., **23** (1974), 179–206.

[13] _____, *Algorithm for Determining the Type of Singular Fibre in an Elliptic Pencil*, In: Modular Functions of One Variable IV, Lect. Notes Math. nr. 476, Springer-Verlag, 1975, 33–52.

[14] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, 1963.

Received November 4, 1980.

ECONOMETRIC INSTITUTE
ERASMUS UNIVERSITY ROTTERDAM
P.O. BOX 1738
3000 DR ROTTERDAM
THE NETHERLANDS