PACIFIC JOURNAL OF MATHEMATICS
Vol. 185, No. 2, 1998

AN INFINITE FAMILY OF ELLIPTIC CURVES AND GALOIS MODULE STRUCTURE

W. Bley and M. Klebel

Let E be an elliptic curve defined over a number field F with everywhere good reduction. By dividing F-rational torsion points with respect to the group law of E M. Taylor defined certain Kummer orders and studied their Galois module structure. His results led to the conjecture that these Kummer orders are free over an explicitly given Hopf order.

In this paper we prove that the conjecture does not hold for infinitely many elliptic curves which are defined over quadratic imaginary number fields k and endowed with a k-rational 2-torsion point.

1. Introduction.

In [Ta], M. Taylor introduced the notion of a Kummer order with respect to the group law of an abelian variety. In this paper we shall study the Galois module structure of these Kummer orders in the case when the variety is an elliptic curve. In particular, we will give an infinite series of counter-examples to (a variant of) a conjecture of M. Taylor stated in [Ta].

Let E be an elliptic curve defined over a number field F and suppose that all endomorphisms of E are defined over F. Moreover we require that E/F has everywhere good reduction.

For any number field L, we let $\mathcal{O}_L$ denote its ring of algebraic integers, L^c an algebraic closure of L and we set $\Omega_L = \mathrm{Gal}(L^c/L)$.

For a fixed rational prime p and $i \geq 0$ we write G_i for the subgroup of $[p^i]$-torsion points of $E(F^c)$. We denote by $\mathfrak{B}_i(F) = \mathfrak{B}_i$ the $\mathcal{O}_F$-Hopf algebra which represents the $\mathcal{O}_F$-group scheme of $[p^i]$-torsion on E and we write $\mathfrak{A}_i(F) = \mathfrak{A}_i$ for its Cartier dual. We recall from [Ta] that $\mathfrak{B}_i$ is an $\mathcal{O}_F$-order in $B_i = \mathrm{Map}(G_i, F^c)^{\Omega_F}$ and $\mathfrak{A}_i$ an $\mathcal{O}_F$-order in $A_i = (F^c[G_i])^{\Omega_F}$, where Ω_F acts on both G_i and F^c.

For $Q \in E(F)$ we define an Ω_F-stable G_i-set

$$G_Q(i) = \{Q' \in E(F^c) \mid [p^i]Q' = Q\}$$

and a corresponding Kummer algebra

$$F_Q(i) = \mathrm{Map}(G_Q(i), F^c)^{\Omega_F}.$$

Note that $[F_Q(i) : F] = |G_i|$ and that $F_Q(i)$ is an A_i-module, where the A_i action is given by

$$\left(f\left(\sum_{g\in G_i} a_g g\right)\right)(Q') = \sum_{g\in G_i} a_g f(Q'+g) \tag{1}$$

for $f \in F_Q(i)$ and $\sum_{g\in G_i} a_g g \in A_i$.

At the integral level we define $\mathcal{O}_Q(i)$ to be the integral closure of $\mathcal{O}_F$ in the commutative algebra $F_Q(i)$ and we set

$$\tilde{\mathcal{O}}_Q(i) = \{x \in \mathcal{O}_Q(i) \mid x\mathfrak{A}_i \subseteq \mathcal{O}_Q(i)\}. \tag{2}$$

This is the largest $\mathfrak{A}_i$-module contained in $\mathcal{O}_Q(i)$.

We write $cl(\mathfrak{A}_i)$ for the locally free classgroup of $\mathfrak{A}_i$ and for any locally free $\mathfrak{A}_i$-module M we denote by $[M]$ its class in $cl(\mathfrak{A}_i)$.

In [**Ta**] it is shown that the map

$$\begin{aligned} \psi_i : E(F) &\longrightarrow cl(\mathfrak{A}_i), \\ Q &\longmapsto [\tilde{\mathcal{O}}_Q(i)] \end{aligned} \tag{3}$$

is a group homomorphism (see also [**Ag**] for the case when E is not a CM elliptic curve).

Originally this basic theory was set up only for curves admitting complex multiplication by the ring of integers $\mathcal{O}_K$ of a quadratic imaginary number field $K \subseteq F$. In this situation it is possible to replace p^i in the above definitions by any $\alpha \in \mathcal{O}_K$, or even by an integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$ (see [**ST**]). One also obtains a group homomorphism as in (3), which we simply denote by ψ.

In [**Ta**], M. Taylor conjectured that

$$E(F)_{\text{torsion}} \subseteq \ker(\psi).$$

This conjecture was subsequently proved for any non-zero ideal $\mathfrak{a}$ coprime to the number of roots of unity of K ([**ST**, Theorem 1]).

In [**Ag**], A. Agboola proved that for $p > 3$ and any elliptic curve (not necessarily CM) one has $E(F)_{\text{torsion}} \subseteq \ker(\psi_i)$. See also the recent paper [**Pa**] of G. Pappas.

The situation for $p \leq 3$ has been studied by several authors (e.g. [**CS**] or [**Bo**]), always giving an affirmative answer to the conjecture.

In this paper we will focus on the case $p = 2$. Based on a paper of B. Setzer [**Se**] we describe an infinite family of elliptic curves defined over quadratic imaginary number fields k with everywhere good reduction and a k-rational

2-torsion point P such that $P \notin \ker(\psi_i)$ for $p = 2$ and $i \geq 1$. We remark that none of these curves admits complex multiplication.

Henceforth $k = \mathbf{Q}(\sqrt{-m})$ will be a quadratic imaginary number field with a positive, square free integer m.

Theorem 1.1 (Setzer)**.** *There exists an elliptic curve E defined over k with everywhere good reduction and a k-rational 2-torsion point if and only if $m = 65m_1$, where m_1 is a square mod 5 and mod 13 and 65 is a square* $\bmod m_1$.

Let r denote the number of ramified primes in $k/\mathbf{Q}$.

Remark 1.2. Suppose that m satisfies the congruence conditions of Theorem 1.1. If $m \equiv 2, 3 (\bmod 4)$ (resp. $m \equiv 1 (\bmod 4)$), then there are 2^{r-1} (resp. 2^r) isomorphism classes of such curves.

In the case $m \equiv 2, 3 (\bmod 4)$ this number differs from Setzer's result. The remark will be proved in Section 2.

For each of the elliptic curves resulting from Theorem 1.1 we obtain a Weierstrass model

$$E : y^2 = x^3 + Ax^2 + Bx$$

with $A, B \in \mathcal{O}_k$. Obviously $P = (0, 0)$ is a k-rational 2-torsion point. In Section 2 we will show that the coordinates of the other 2-torsion points generate the field $F = k(\sqrt{65})$ over k. For our purposes it is now convenient to consider E as an elliptic curve over F, since then $A_1(F) = F[G_1]$.

Theorem 1.3. *Let $p = 2$. Let E/F be any elliptic curve resulting from Theorem 1.1 and suppose that $m_1 > 1$. Then $P \notin \ker(\psi_i)$ for all $i \geq 1$.*

Remarks 1.4.

1) By [**Ag**, Proposition 1.2] it suffices to prove the theorem for $i = 1$. Let $\mathfrak{M}_{F,G_i}$ be the unique maximal $\mathcal{O}_F$-order in $A_i(F)$. Then extension of scalars and composition with ψ_i induces a group homomorphism

$$\psi_i' : E(F) \longrightarrow cl(\mathfrak{M}_{F,G_i}).$$

We will explicitly compute $\psi_1'(P)$ and then show that it is non-trivial.

2) The case $m_1 = 1$ has been studied numerically applying the methods of [**Bl**]. We obtain 8 non-isomorphic classes of elliptic curves and for 4 of them $\psi_1'(P)$ is trivial. It can be shown that for these curves $\tilde{\mathcal{O}}_P(1)$ is in fact free over $\mathfrak{A}_1$.

3) From [**Ag**, (1.15), (1.19)] it is clear that the result of Theorem 1.3 remains true, if we consider E as an elliptic curve over k.

We conclude this introduction with a brief outline of the structure of the paper. In Section 2 we recall all the necessary results from Setzer's paper [**Se**] and also give the proof of Remark 1.2. We then explicitly compute the orders $\mathfrak{A}_1(F)$ and $\tilde{\mathcal{O}}_P(1)$ in Section 3. Finally, Section 4 contains the proof of Theorem 1.3.

2. Elliptic curves.

In order to provide all the necessery details about the elliptic curves resulting from Theorem 1.1 we give a short outline of Setzer's proof (including a proof of that part of Remark 1.2 which differs from his result). For more details we refer the reader to Setzer's original paper [**Se**].

Suppose that E/k is an elliptic curve with everywhere good reduction and a k-rational 2-torsion point. Then we can find a Weierstrass model

$$E : y^2 = x^3 + Ax^2 + Bx \tag{4}$$

with $A, B \in \mathcal{O}_k$ and discriminant

$$\Delta = -16B^2(A^2 - 4B) = 2^{12}D, \tag{5}$$

where $D \in \mathcal{O}_k$ is prime to 2.

For fixed D the Equation (5) has only finitely many solutions A and B. Moreover Setzer's Theorem 1 implies that only finitely many D (one for each ideal class) have to be tried for a fixed field k.

For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$ we denote by $v_\mathfrak{p}$ the valuation at $\mathfrak{p}$. The proof of Theorem 1.1 will be accomplished by testing good reduction using the following criteria.

Lemma 2.1 (Setzer)**.** *Let E be an elliptic curve with Weierstrass model (4) and discriminant as in (5).*

(a) *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_k$, $(\mathfrak{p}, 2) = 1$. Then E has good reduction at $\mathfrak{p}$ if and only if*

$$v_\mathfrak{p}(\Delta) = 12e, \quad v_\mathfrak{p}(B) = 4e, \quad v_\mathfrak{p}(A) \geq 2e$$

for some $e \in \mathbf{Z}$, $e \geq 0$.

(b) *Let $\mathfrak{q}$ be a ramified prime ideal of $\mathcal{O}_k$ dividing 2 and let $\mathfrak{p} = (2)$. Let $m \equiv 1 (\mathrm{mod}\, 4)$. Then E has good reduction at $\mathfrak{q}$ if and only if A and B satisfy one of the following congruence conditions:*

$$A \equiv 2\alpha^2 (\mathrm{mod}\, \mathfrak{p}^3), \quad B \equiv \alpha^4 (\mathrm{mod}\, \mathfrak{p}^3), \tag{6}$$

$$A \equiv \alpha^2 (\mathrm{mod}\, \mathfrak{p}^2), \quad B \equiv 0 (\mathrm{mod}\, \mathfrak{p}^4), \tag{7}$$

$$\begin{cases} A \equiv 0 (\mathrm{mod}\, \mathfrak{q}^5), & B \equiv \pi^4 + 8\pi (\mathrm{mod}\, \mathfrak{q}^8), \\ \pi^2 A - B \equiv \pi^4 + \pi^6 & \textit{or } 5\pi^4 + 4\pi^5 + \pi^6 (\mathrm{mod}\, \mathfrak{q}^{10}). \end{cases} \tag{8}$$

Here $\alpha \in \mathcal{O}_k$ is relatively prime with $\mathfrak{p}$ and π is a fixed uniformizer for $\mathfrak{q}$.
Let $m \equiv 2(\mathrm{mod}\, 4)$. Then E has good reduction at $\mathfrak{q}$ if and only if (7) or (8) holds.

(c) *Let $\mathfrak{p}$ be an unramified prime ideal of $\mathcal{O}_k$ dividing 2. Then $m \equiv 3(\mathrm{mod}\, 4)$ and E has good reduction at $\mathfrak{p}$ if and only if (7) holds for some $\alpha \in \mathcal{O}_k$, $(\alpha, \mathfrak{p}) = 1$.*

Note that Lemma 2.1 differs from Setzer's Lemma in his Section 3 in (b) and (c). We will give a proof of Lemma 2.1 at the end of this section. Together with Setzer's arguments on pp. 246/247 this will complete the proof of Remark 1.2.

The conditions (6), (7) and (8) leave three possibilities for the 2-part of B:

$$
\begin{aligned}
&\text{(I)} && B = 2^e\beta, \quad e \in \{0,4\}, \quad (\beta, 2) = 1.\\
&\text{(II)} && B = 2^2\beta, \quad (\beta, 2) = 1 \text{ and } 2 \text{ ramifies.}\\
&\text{(III)} && v_{\mathfrak{p}}(B) = 0,\ v_{\mathfrak{p}'}(B) = 4,\ \text{where } 2\mathcal{O}_k = \mathfrak{p}\mathfrak{p}', \mathfrak{p} \neq \mathfrak{p}'.
\end{aligned}
$$

In [**Se**] it is shown that cases (II) and (III) do not lead to any curves. We therefore may assume that (I) holds. In addition it is easy to verify that this occurs if and only if either (6) or (7) is satisfied for $\mathfrak{p} = (2)$. Lemma 2.1 (a) implies that $(\beta) = \mathfrak{b}^4$ for some odd integral ideal $\mathfrak{b}$, $\Delta = \pm 2^{12}\beta^3$ and $A^2 = \alpha\beta$ for some $\alpha \in \mathcal{O}_k$. Substituting this into the discriminant formula (5) one can show that either $A^2 = 65\beta$ and $e = 4$ or $A^2 = 260\beta$ and $e = 0$. We set

$$
\begin{aligned}
A_1 &= A, && \text{if } A^2 = 65\beta,\\
A_1 &= A/2, && \text{if } A^2 = 260\beta
\end{aligned}
$$

and may now assume that

$$
(9) \qquad A_1^2 = 65\beta, \quad (\beta) = \mathfrak{b}^4, \quad \mathfrak{b} \text{ integral and prime to } 2.
$$

If A_1 is a square mod 4 we will show that 1 or 4 non-isomorphic curves result according to $m \equiv 2, 3(\mathrm{mod}\, 4)$ or $m \equiv 1(\mathrm{mod}\, 4)$. Conversely the congruence conditions (6) and (7) imply that A_1 is congruent to a square mod 4.

Consider first the case $m \equiv 2, 3(\mathrm{mod}\, 4)$. Here (7) implies that 2^4 divides B. Consequently we have $B = 2^4\beta$ and $A = \pm A_1$. But if A_1 is a square mod 4, then $-A_1$ does not satisfy (7), since -1 is not a square mod 4. Hence we obtain one curve, namely

$$
A = A_1, \quad B = \frac{16A_1^2}{65}, \quad A_1^2 = 65\beta.
$$

Assume now that $m \equiv 1 (\operatorname{mod} 4)$. Then -1 is a square mod 4 and either (6) or (7) is satisfied. This leads to 4 non-isomorphic curves, namely

$$\begin{aligned} A &= \pm 2A_1, \quad B = \frac{A_1^2}{65}, \qquad A_1^2 = 65\beta \text{ in case (6)}, \\ A &= \pm A_1, \quad\ \ B = \frac{16A_1^2}{65}, \quad A_1^2 = 65\beta \text{ in case (7)}. \end{aligned}$$

Suppose now that an ideal $\mathfrak{b}$ as in (9) has 1 or 4 non-isomorphic classes of curves attached. In [**Se**] it is shown that any other ideal $\mathfrak{b}_1$ in the same ideal class leads to an isomorphic set of curves. Hence it remains to answer the question which ideal classes c of the ideal classgroup cl_k of k do lead to elliptic curves. The precise condition is, firstly that $\mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{b}^2 = (A_1)$ is principal, where $\mathfrak{p}_5$ and $\mathfrak{p}_{13}$ denote the prime ideals of $\mathcal{O}_k$ above 5 and 13 respectively, and secondly that $\pm A_1$ is congruent to a square mod 4. The first condition means that $\mathfrak{p}_5\mathfrak{p}_{13}$ is an element of the principal genus ([**BS**, III, §8, Satz 7]), which in turn is equivalent to the congruence conditions of Theorem 1.1. The effects of the second condition are discussed on pp. 246/247 of Setzer's paper and lead to the corrected number of isomorphism classes of Remark 1.2.

We summarize the preceeding discussion in the following:

Proposition 2.2. *Let E/k be any elliptic curve resulting from Theorem 1.1. Then E has a Weierstrass model (4) with discriminant as in (5). There exists an integral odd ideal $\mathfrak{b}$ such that $\mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{b}^2 = (A_1)$ is principal and A_1 is congruent to a square* mod 4. *If $m \equiv 2, 3 (\operatorname{mod} 4)$, then the coefficients $A, B \in \mathcal{O}_k$ are given by*

$$A = A_1, \quad B = \frac{16A_1^2}{65}$$

and satisfy the congruence condition (7) of Lemma 2.1. If $m \equiv 1 (\operatorname{mod} 4)$, then the coefficients are of the form

$$\begin{aligned} A &= \pm 2A_1, \quad B = \frac{A_1^2}{65} \quad \textit{in case (6)}, \\ A &= \pm A_1, \quad\ \ B = \frac{16A_1^2}{65} \textit{ in case (7)}. \end{aligned}$$

Let now $p = 2$. In the following part of this section we compute the subgroup G_1 of 2-torsion points for the elliptic curves of Theorem 1.1, as well as the G_1-set $G_P(1)$ for the k-rational point $P = (0, 0)$. Since $i = 1$ is fixed we write $G = G_1$ and $G_P = G_P(1)$ in what follows. Finally we also determine the points of G that lie in the kernel of reduction modulo primes above 2.

We fix an embedding $k \hookrightarrow \mathbf{C}$ and let k^c denote the algebraic closure of k in $\mathbf{C}$. For $z \in \mathbf{C} \setminus \mathbf{R}_{\leq 0}$ we always normalize $\sqrt{z}$ such that $\mathrm{Re}(\sqrt{z}) > 0$.

For an elliptic curve with model (4) the subgroup of $E(k^c)$ of 2-torsion points is given by

$$G = \left\{ P_0 = 0_E, P = P_1 = (0,0), P_{2/3} = \left(\frac{1}{2} \left(-A \pm \sqrt{A^2 - 4B} \right), 0 \right) \right\}.$$

Using the explicit formulae for A and B given in Proposition 2.2 it is easy to see that the x-coordinate of P_2 or P_3 generates the field $F = k(\sqrt{65})$ over k.

The duplication formula of the group law of an elliptic curve (see e.g. [**Si**, Ch. III, 2.3(d)]) implies that

$$\begin{aligned} G_P = \Big\{ Q_1 &= \left(\sqrt{B}, \sqrt{B(A + 2\sqrt{B}} \right), \qquad Q_1' = \left(\sqrt{B}, -\sqrt{B(A + 2\sqrt{B}} \right), \\ Q_2 &= \left(-\sqrt{B}, \sqrt{B(A - 2\sqrt{B}} \right), \quad Q_2' = \left(-\sqrt{B}, -\sqrt{B(A - 2\sqrt{B}} \right) \Big\}. \end{aligned}$$

Since $G \subseteq E(F)$ acts transitively on G_P, all of the y-coordinates of points of G_P generate the same field $L = F\left(\sqrt{B(A + 2\sqrt{B})}\right)$. The automorphism σ which sends $\sqrt{B(A + 2\sqrt{B})}$ to $-\sqrt{B(A + 2\sqrt{B})}$ generates $\mathrm{Gal}(L/F)$. We also record the following relations:

$$\begin{aligned} &Q_1 + P_1 = Q_1' \ = \ Q_1^\sigma, \\ &Q_1 + P_2 = Q_2, \quad \text{(maybe after relabelling } Q_2 \text{ and } Q_2'), \\ &Q_1 + P_3 = Q_2^\sigma, \\ &Q_2 + P_1 = Q_2' \ = \ Q_2^\sigma, \\ &Q_2 + P_2 = Q_1, \\ &Q_2 + P_3 = Q_1^\sigma. \end{aligned} \tag{10}$$

As usual we denote by $E_1(F_\mathfrak{P})$ the kernel of reduction mod $\mathfrak{P}$ for a prime ideal $\mathfrak{P}$ of $\mathcal{O}_F$. Next we compute the subgroup $E_1(F_\mathfrak{P}) \cap G$ for prime divisors $\mathfrak{P}$ of 2. Suppose first that (7) holds. Then the transformation

$$x = 2^2 x', \quad y = 2^3 y' + 2^2 \alpha x'$$

gives a minimal Weierstrass model for any prime $\mathfrak{P}$ dividing 2. Expressing the points of G in the new coordinates x', y' we obtain

$$P_1' = (0,0), \quad P_{2/3}' = \left(\frac{x(P_{2/3})}{4}, -\frac{\alpha x(P_{2/3})}{8} \right)$$

with $x(P_{2/3}) = \frac{1}{2}(-A \pm \sqrt{A^2 - 4B})$. Let $\mathfrak{p}_2 = \mathbf{Z}2 + \mathbf{Z}\frac{1+\sqrt{65}}{2}$ and $\mathfrak{p}_2' = \mathbf{Z}2 + \mathbf{Z}\frac{1-\sqrt{65}}{2}$ be the prime ideals of $\mathcal{O}_{\mathbf{Q}(\sqrt{65})}$ above 2. We claim that for any prime $\mathfrak{P}$ of F dividing 2 either $G \cap E_1(F_{\mathfrak{P}}) = \langle P_2 \rangle$ or $\langle P_3 \rangle$. Indeed,

$$2x(P_2) = -A + \sqrt{A^2 - 4B} \equiv \begin{cases} -2A\frac{1-\sqrt{65}}{2}, & \text{if } \operatorname{Re}(A) > 0, \\ -2A\frac{1+\sqrt{65}}{2}, & \text{if } \operatorname{Re}(A) < 0, \end{cases}$$

$$2x(P_3) = -A - \sqrt{A^2 - 4B} \equiv \begin{cases} -2A\frac{1+\sqrt{65}}{2}, & \text{if } \operatorname{Re}(A) > 0, \\ -2A\frac{1-\sqrt{65}}{2}, & \text{if } \operatorname{Re}(A) < 0, \end{cases}$$

where all congruences are mod 16.

Since $(A, 2) = 1$, $\frac{1+\sqrt{65}}{2}\mathcal{O}_{\mathbf{Q}(\sqrt{65})} = \mathfrak{p}_2^4$ and $\frac{1-\sqrt{65}}{2}\mathcal{O}_{\mathbf{Q}(\sqrt{65})} = \mathfrak{p}_2'^4$, the claim follows at once.

Now assume that (6) holds. Then there exists $\varepsilon \in \mathcal{O}_k$ such that $\varepsilon^2 \equiv -1 (\operatorname{mod} 4)$. We choose $\theta \in \mathcal{O}_k$ such that $\theta \equiv A/2 (\operatorname{mod} 8)$ and perform the transformation

$$x = 2^2 x' - \theta, \quad y = 2^3 y' + 2^2 \varepsilon\alpha x'. \tag{11}$$

The new Weierstrass model is integral and minimal with respect to any prime $\mathfrak{P}$ of F dividing 2 and we easily compute

$$P_1' = \left(\frac{\theta}{4}, -\frac{\varepsilon\alpha\theta}{8}\right), \quad P_{2/3}' = \left(\frac{x(P_{2/3}) + \theta}{4}, -\frac{\varepsilon\alpha(x(P_{2/3}) + \theta)}{8}\right).$$

Since $(\varepsilon\alpha\theta, 2) = 1$, P_1 is obviously in the kernel of reduction for any $\mathfrak{P}$ dividing 2. On the other hand, neither P_2 nor P_3 is in $E_1(F_{\mathfrak{P}})$, since

$$x(P_{2/3}) + \theta \equiv \pm\frac{1}{2}\sqrt{A^2 - 4B} \overset{(5)}{=} \pm 2^3 \sqrt{-D/B^2} \equiv 0 (\operatorname{mod} 8).$$

Summing up we have proved the following:

Lemma 2.3. *Let E/k be any elliptic curve resulting from Theorem 1.1. Then $G \subseteq E(F)$ where $F = k(\sqrt{65})$. If (6) holds, then $G \cap E_1(F_{\mathfrak{P}}) = \langle P_1 \rangle$ for any prime $\mathfrak{P}$ of F dividing 2. Assume now that (7) holds. Then*

$$G \cap E_1(F_{\mathfrak{P}}) = \begin{cases} \langle P_2 \rangle, & \textit{if either } \mathfrak{P} \textit{ divides } \mathfrak{p}_2 \textit{ and } \operatorname{Re}(A) > 0 \textit{ or} \\ & \mathfrak{P} \textit{ divides } \mathfrak{p}_2' \textit{ and } \operatorname{Re}(A) < 0, \\ \langle P_3 \rangle, & \textit{if either } \mathfrak{P} \textit{ divides } \mathfrak{p}_2' \textit{ and } \operatorname{Re}(A) > 0 \textit{ or} \\ & \mathfrak{P} \textit{ divides } \mathfrak{p}_2 \textit{ and } \operatorname{Re}(A) < 0. \end{cases}$$

In all cases the $\mathfrak{P}$-valuation of the parameter $z = -x'/y'$ for the non-trivial point of $G \cap E_1(F_{\mathfrak{P}})$ on the formal group afforded by the kernel of reduction mod $\mathfrak{P}$ is given by $v_{\mathfrak{P}}(2)$.

In order to complete our discussion of the elliptic curves of Theorem 1.1 we give a brief proof of that part of Lemma 2.1 that differs from Setzer's Lemma in his Section 3.

Suppose that $\mathfrak{p}$ is an unramified prime of $\mathcal{O}_k$ dividing 2. In [**Se**, pp. 243-244] it is shown that any elliptic curve with model (4) and good reduction at $\mathfrak{p}$ necessarily satisfies one of the conditions (6) or (7). But, contrary to Setzer's claim, curves satisfying (6) do not have good reduction mod $\mathfrak{p}$. (The exact location of Setzer's error is [**Se**, p. 244, lines 16-20].) In order to prove our statement we substitute

$$x = x' - \theta, \quad y = y' + \alpha x'$$

into Equation (4), where $\theta \in \mathcal{O}_k$ is chosen such that $\theta \equiv A/2 (\operatorname{mod} 8)$. The coefficients of the new Weierstrass model are given by

$$\begin{aligned} &a_1 = 2\alpha, \quad a_2 = A - 3\theta - \alpha^2, \quad a_3 = 0, \\ &a_4 = B - 2\theta A + 3\theta^2, \quad a_6 = -\theta B + \theta^2 A - \theta^3. \end{aligned}$$

We quickly verify the following congruences:

$$a_2 \equiv 2\alpha^2 (\operatorname{mod} \mathfrak{p}^2), \ a_4 \equiv 0 (\operatorname{mod} 16), \ a_6 \equiv 0 (\operatorname{mod} 64). \tag{12}$$

Note that (6) implies $A/2 \equiv \alpha^2 \equiv \theta (\operatorname{mod} \mathfrak{p}^2)$. Therefore $a_2 = A - 2\theta - \theta - \alpha^2 \equiv 2\alpha^2 (\operatorname{mod} \mathfrak{p}^2)$. The second congruence follows from

$$\begin{aligned} a_4 &= \theta(2\theta - A) + \theta^2 - A\theta + B \\ &\equiv \theta^2 - A\theta + B = (\theta - A/2)^2 - A^2/4 + B \\ &\equiv -(A^2 - 4B^2)/4 \overset{(5)}{=} 2^6 D/B^2 \equiv 0 (\operatorname{mod} 16). \end{aligned}$$

Finally we have

$$\begin{aligned} a_6 &= -\theta(B - \theta A + \theta^2) = -\theta((\theta - A/2)^2 - (A^2 - 4B/4)) \\ &\equiv \theta(A^2 - 4B)/4 \overset{(5)}{=} 2^6 \theta D/B^2 \equiv 0 (\operatorname{mod} 64). \end{aligned}$$

If E has good reduction at $\mathfrak{p}$, then [**Si**, Ch. VII, Prop. 1.3] together with (12) and [**Si**, Ch. III, Table 1.2] implies that there exist $r, s, t \in \mathcal{O}_{k,\mathfrak{p}}$ such that

$$\begin{aligned} &\text{(I)} && 2\alpha^2 - 2s\alpha + 3r - s^2 && \equiv 0 \ (\operatorname{mod} \mathfrak{p}^2), \\ &\text{(II)} && r\alpha + t && \equiv 0 \ (\operatorname{mod} \mathfrak{p}^2), \\ &\text{(III)} && 2ra_2 - 2\alpha(t + rs) + 3r^2 - 2st && \equiv 0 \ (\operatorname{mod} \mathfrak{p}^4), \\ &\text{(IV)} && ra_4 + r^2 a_2 + r^3 - t^2 - 2rt\alpha && \equiv 0 \ (\operatorname{mod} \mathfrak{p}^6). \end{aligned}$$

From the congruences (II)-(IV) we deduce that $\mathfrak{p}^2$ divides r. Hence by (I) we get $(s+\alpha)^2 \equiv -\alpha^2 (\operatorname{mod} \mathfrak{p}^2)$, which implies that -1 is a square mod $\mathfrak{p}^2$. This is certainly not true for $m \equiv 3 (\operatorname{mod} 4)$. The same argumentation also explains the differences between Lemma 2.1 and Setzer's lemma for ramified prime divisors of 2.

3. The orders $\mathfrak{A}_F(1)$ and $\tilde{\mathcal{O}}_P(1)$.

Let E/k be an elliptic curve as in Theorem 1.1. From now on we always view E as a curve defined over $F = k(\sqrt{65})$. In this section we shall compute the orders $\mathfrak{A}_F(1)$ and $\tilde{\mathcal{O}}_P(1)$ for $P = P_1 = (0,0)$ and $p = 2$. We first recall some necessary results concerning the orders $\mathfrak{A}_i$ and $\mathfrak{B}_i$ from [**Ta**] and [**Ag**]. These orders are determined by their localizations at each prime $\mathfrak{Q}$ of $\mathcal{O}_F$. Let $G_{i,\mathfrak{Q}}$ denote the $\mathcal{O}_{F_\mathfrak{Q}}$-group scheme obtained by localizing the $\mathcal{O}_F$-group scheme afforded by G_i at $\mathfrak{Q}$. As in [**Ag**], we denote by $G^0_{i,\mathfrak{Q}}$ the component of the identity of $G_{i,\mathfrak{Q}}$ and write $G'_{i,\mathfrak{Q}}$ for the maximal étale quotient $G_{i,\mathfrak{Q}}/G^0_{i,\mathfrak{Q}}$. Then the group scheme $G'_{i,\mathfrak{Q}}$ is represented by the algebra $\mathfrak{B}'_{i,\mathfrak{Q}} := \operatorname{Map}(G'_{i,\mathfrak{Q}}(F^c_\mathfrak{Q}), \mathcal{O}_{F^c_\mathfrak{Q}})^{\Omega_{F_\mathfrak{Q}}}$. We let $F(X,Y) \in \mathcal{O}_{F_\mathfrak{Q}}[[X,Y]]$ denote the formal group afforded by the kernel of reduction mod $\mathfrak{Q}$ on $E(F_\mathfrak{Q})$. For each endomorphism b of E we write $[b](X)$ for the power series corresponding to the induced endomorphism of $F(X,Y)$. Then $\mathfrak{B}^0_{i,\mathfrak{Q}} := \mathcal{O}_{F_\mathfrak{Q}}[[X]]/[p^i](X)\mathcal{O}_{F_\mathfrak{Q}}[[X]]$ represents the group scheme $G^0_{i,\mathfrak{Q}}$. Here we view $\mathfrak{B}^0_{i,\mathfrak{Q}}$ as an order in $B^0_{i,\mathfrak{Q}} := \operatorname{Map}(G^0_{i,\mathfrak{Q}}(F^c_\mathfrak{Q}), F^c_\mathfrak{Q})^{\Omega_{F_\mathfrak{Q}}}$ via the rule $[b](X)(g) = [b](z(g))$ for $g \in G^0_{i,\mathfrak{Q}}(F^c_\mathfrak{Q})$, where $z(g)$ denotes the parameter for g on the formal group $F(X,Y)$.

We finally set $\mathfrak{B}_{i,\mathfrak{Q}} = \mathfrak{B}'_{i,\mathfrak{Q}} \otimes_{\mathcal{O}_{F_\mathfrak{Q}}} \mathfrak{B}^0_{i,\mathfrak{Q}}$, so that $\mathfrak{B}_{i,\mathfrak{Q}}$ represents the group scheme $G_{i,\mathfrak{Q}}$. We remark that $\mathfrak{B}_{i,\mathfrak{Q}} = \operatorname{Map}(G_{i,\mathfrak{Q}}(F^c_\mathfrak{Q}), \mathcal{O}_{F^c_\mathfrak{Q}})^{\Omega_{F^c_\mathfrak{Q}}}$ for any prime $\mathfrak{Q}$ such that $(\mathfrak{Q}, 2) = 1$.

The Cartier dual $\mathfrak{A}_i$ of $\mathfrak{B}_i$ is now described explicitly by

$$\mathfrak{A}_i = \left\{ \frac{1}{p^i} \sum_{g \in G_i} f(g)g \mid f \in \mathfrak{B}_i \right\}. \tag{13}$$

This completes our collection of facts from [**Ta**] and [**Ag**].

Since $i = 1$ and $p = 2$ will be fixed for the rest of the section we write $\mathfrak{B} = \mathfrak{B}_i(F)$, $\mathfrak{A} = \mathfrak{A}_1(F)$, $G = G_1$, etc. Recall that $2\mathcal{O}_{\mathbf{Q}(\sqrt{65})} = \mathfrak{p}_2\mathfrak{p}'_2$.

Proposition 3.1. *Let E/k be an elliptic curve resulting from Theorem 1.1. If (6) is satisfied, then*

$$\mathfrak{A} = \mathcal{O}_F P_0 \oplus \mathcal{O}_F \frac{P_0 + P_1}{2} \oplus \mathcal{O}_F P_3 \oplus \mathcal{O}_F \frac{P_2 + P_3}{2}.$$

Suppose now that (7) *holds. Then:*

$$\mathfrak{A}_{\mathfrak{P}} = \begin{cases} \mathcal{O}_{F_{\mathfrak{P}}} P_0 \oplus \mathcal{O}_{F_{\mathfrak{P}}} \frac{P_0+P_2}{2} \oplus \mathcal{O}_{F_{\mathfrak{P}}} P_3 \oplus \mathcal{O}_{F_{\mathfrak{P}}} \frac{P_1+P_3}{2}, & \textit{if } G \cap E_1(F_{\mathfrak{P}}) = \langle P_2 \rangle, \\ \mathcal{O}_{F_{\mathfrak{P}}} P_0 \oplus \mathcal{O}_{F_{\mathfrak{P}}} \frac{P_0+P_3}{2} \oplus \mathcal{O}_{F_{\mathfrak{P}}} P_2 \oplus \mathcal{O}_{F_{\mathfrak{P}}} \frac{P_1+P_2}{2}, & \textit{if } G \cap E_1(F_{\mathfrak{P}}) = \langle P_3 \rangle, \\ \mathcal{O}_{F_{\mathfrak{P}}}[G], & \textit{if } (\mathfrak{P}, 2) = 1. \end{cases}$$

Proof. Suppose first that (6) holds. For any prime ideal $\mathfrak{P}$ of $\mathcal{O}_F$ dividing 2 we have $G \cap E_1(F_{\mathfrak{P}}) = \langle P_1 \rangle$ (see Lemma 2.3). This implies that $G^0_{\mathfrak{P}}(F^c_{\mathfrak{P}}) = \langle P_1 \rangle$ and $G'_{\mathfrak{P}}(F^c_{\mathfrak{P}}) \simeq \langle P_2 \rangle$. Since $G \subseteq E(F)$, the map

$$\begin{aligned} \mathcal{O}_{F_{\mathfrak{P}}} \oplus \mathcal{O}_{F_{\mathfrak{P}}} &\longrightarrow \mathfrak{B}'_{\mathfrak{P}} = \operatorname{Map}(G'_{\mathfrak{P}}(F^c_{\mathfrak{P}}), \mathcal{O}_{F_{\mathfrak{P}}}), \\ (a,b) &\longmapsto (P_0 \mapsto a, P_2 \mapsto b), \end{aligned}$$

is an isomorphism of $\mathcal{O}_{F_{\mathfrak{P}}}$-algebras. We write $z_i = z(P_i), i = 0, 1,$ for the parameter of P_i on the formal group. Viewing $\mathfrak{B}^0_{\mathfrak{P}} \otimes_{\mathcal{O}_{F_{\mathfrak{P}}}} \mathfrak{B}'_{\mathfrak{P}}$ as an $\mathcal{O}_{F_{\mathfrak{P}}}$-order in $B_{\mathfrak{P}} = \operatorname{Map}(G, \mathcal{O}_{F_{\mathfrak{P}}})$, the equality (13) implies that

$$\mathfrak{A}_{\mathfrak{P}} = \Big\{ \frac{1}{2} \left(f(z_0) a P_0 + f(z_1) a P_1 + f(z_0) b P_2 + f(z_1) b P_3 \right) | a, b \in \mathcal{O}_{F_{\mathfrak{P}}}, \\ f(X) \in \mathcal{O}_{F_{\mathfrak{P}}}[[X]] \Big\}.$$

Since $z_0 = 0$ and $v_{\mathfrak{P}}(z_1) = v_{\mathfrak{P}}(2)$ (see Lemma 2.3) it is easily verified that

$$\mathfrak{A}_{\mathfrak{P}} = \mathcal{O}_{F_{\mathfrak{P}}} P_0 \oplus \mathcal{O}_{F_{\mathfrak{P}}} \frac{P_0 + P_1}{2} \oplus \mathcal{O}_{F_{\mathfrak{P}}} P_3 \oplus \mathcal{O}_{F_{\mathfrak{P}}} \frac{P_2 + P_3}{2}.$$

The assertion of Proposition 3.1 for the case (6) follows now immediately, because $\mathfrak{A}_{\mathfrak{Q}} = \mathcal{O}_{F_{\mathfrak{Q}}}[G]$ for any prime $\mathfrak{Q}$ of $\mathcal{O}_F$ prime to 2.

The second part of the proposition is proved in exactly the same way, taking into account the results of Lemma 2.3 for the case (7). □

We now turn to the computation of $\tilde{\mathcal{O}}_P = \tilde{\mathcal{O}}_P(1)$, where $P = P_1 = (0,0)$. Recall from Section 2 that $G_P \subseteq E(L)$, where $L = F\left(\sqrt{B(A + 2\sqrt{B})}\right)$. The map

$$\begin{aligned} \tau : F_P = \operatorname{Map}(G_P, F^c)^{\Omega_F} &\longrightarrow L \oplus L, \\ f &\longmapsto (f(Q_1), f(Q_2)) \end{aligned}$$

is an isomorphism of F-algebras. The natural action of $A = F[G]$ induces via τ the structure of an A-module on $L \oplus L$. By (10) we get for $\alpha, \beta \in L$ and $\langle \sigma \rangle = \operatorname{Gal}(L/F)$:

$$\begin{aligned} (\alpha, \beta) \cdot P_0 &= (\alpha, \beta), \quad & (\alpha, \beta) \cdot P_1 &= (\alpha^\sigma, \beta^\sigma), \\ (\alpha, \beta) \cdot P_2 &= (\beta, \alpha), \quad & (\alpha, \beta) \cdot P_3 &= (\beta^\sigma, \alpha^\sigma). \end{aligned} \tag{14}$$

In the following we always identify F_P and $L \oplus L$ as A-modules via τ, the action of A on $L \oplus L$ induced by (14).

Proposition 3.2. *If (6) is satisfied, then*

$$\tilde{\mathcal{O}}_P = (\mathcal{O}_F + 2\mathcal{O}_L) \oplus (\mathcal{O}_F + 2\mathcal{O}_L).$$

Assume now that (7) holds. Then:

$$\tilde{\mathcal{O}}_P = \begin{cases} \{(\alpha,\beta) \in \mathcal{O}_L \oplus \mathcal{O}_L \mid \alpha+\beta \equiv 0 (\operatorname{mod} \mathfrak{p}_2\mathcal{O}_L) \textit{ and} & \\ \qquad\qquad\qquad\qquad\qquad \alpha + \beta^\sigma \equiv 0 (\operatorname{mod} \mathfrak{p}_2'\mathcal{O}_L)\}, & \textit{if } \operatorname{Re}(A) > 0, \\ \{(\alpha,\beta) \in \mathcal{O}_L \oplus \mathcal{O}_L \mid \alpha+\beta \equiv 0 (\operatorname{mod} \mathfrak{p}_2'\mathcal{O}_L) \textit{ and} & \\ \qquad\qquad\qquad\qquad\qquad \alpha + \beta^\sigma \equiv 0 (\operatorname{mod} \mathfrak{p}_2\mathcal{O}_L)\}, & \textit{if } \operatorname{Re}(A) < 0. \end{cases}$$

Proof. Suppose first that (6) holds. From Proposition 3.1, (2) and (14) we conclude that

$$(\alpha,\beta) \in \tilde{\mathcal{O}}_P \Longleftrightarrow \alpha,\beta \in \mathcal{O}_L \text{ and } Tr_{L/F}(\alpha), Tr_{L/F}(\beta) \in 2\mathcal{O}_F.$$

We claim that

$$\{\gamma \in \mathcal{O}_L \mid Tr_{L/F}(\gamma) \in 2\mathcal{O}_F\} = \mathcal{O}_F + 2\mathcal{O}_L. \tag{15}$$

Indeed, since E/k has everywhere good reduction, the extension L/k is unramified. Hence $\mathcal{O}_L$ is a cohomologically trivial $\operatorname{Gal}(L/F)$-module. Let $\gamma \in \mathcal{O}_L$. Then $\operatorname{Tr}_{L/F}(\gamma) \in 2\mathcal{O}_L \Longleftrightarrow \gamma - \gamma^\sigma \in 2\mathcal{O}_L$. The triviality of the Tate cohomology group $\hat{H}^{-1}(\operatorname{Gal}(L/F), 2\mathcal{O}_L)$ implies that there exists $\delta \in 2\mathcal{O}_L$ such that $\gamma - \gamma^\sigma = \delta - \delta^\sigma$. It follows that $\gamma = (\gamma - \delta) + \delta \in \mathcal{O}_F + 2\mathcal{O}_L$. The converse is obvious, thus proving the claim and the first part of the proposition.

The proof of the second part is achieved by considering the localizations of $\tilde{\mathcal{O}}_L$ at each prime ideal $\mathfrak{P}$ of $\mathcal{O}_F$. Suppose that $\operatorname{Re}(A) > 0$. From Proposition 3.1, Lemma 2.3, (2) and (14) we derive

$$(\alpha,\beta) \in \tilde{\mathcal{O}}_{P,\mathfrak{P}} \Longleftrightarrow \begin{cases} \alpha,\beta \in \mathcal{O}_{L,\mathfrak{P}} \text{ and } \alpha \equiv -\beta (\operatorname{mod} \mathfrak{p}_2\mathcal{O}_L), & \text{if } \mathfrak{P} \text{ divides } \mathfrak{p}_2, \\ \alpha,\beta \in \mathcal{O}_{L,\mathfrak{P}} \text{ and } \alpha \equiv -\beta^\sigma (\operatorname{mod} \mathfrak{p}_2'\mathcal{O}_L), & \text{if } \mathfrak{P} \text{ divides } \mathfrak{p}_2', \\ \alpha,\beta \in \mathcal{O}_{L,\mathfrak{P}}, & \text{if } (\mathfrak{P}, 2) = 1. \end{cases}$$

Since $\tilde{\mathcal{O}}_P$ is uniquely determined by its localizations, this proves the second part of the proposition for $\operatorname{Re}(A) > 0$. Of course, the case $\operatorname{Re}(A) < 0$ is completely analogous. □

4. Proof of Theorem 1.3.

As in the preceeding section we fix $i = 1$ and $p = 2$. Let E/k be an elliptic curve resulting from Theorem 1.1. We omit any occurrence of i in our notation, in particular we write

$$\psi : E(F) \longrightarrow cl(\mathfrak{A})$$

for the group homomorphism in (3). Let $\mathfrak{M}$ be the unique maximal $\mathcal{O}_F$-order in $A = F[G]$. Then extension of scalars and composition with ψ induces a group homomorphism

$$\begin{aligned} \psi' : E(F) &\longrightarrow cl(\mathfrak{M}), \\ P &\longmapsto [\tilde{\mathcal{O}}_P \otimes_{\mathfrak{A}} \mathfrak{M}]. \end{aligned}$$

As usual we identify $\tilde{\mathcal{O}}_P \otimes_{\mathfrak{A}} \mathfrak{M}$ with the submodule $\tilde{\mathcal{O}}_P\mathfrak{M}$ of A generated by $\tilde{\mathcal{O}}_P$ over $\mathfrak{M}$. Let

$$\begin{aligned} e_1 &= \frac{1}{4}(P_0 + P_1 + P_2 + P_3), \quad & e_2 &= \frac{1}{4}(P_0 + P_1 - P_2 - P_3), \\ e_3 &= \frac{1}{4}(P_0 - P_1 + P_2 - P_3), \quad & e_4 &= \frac{1}{4}(P_0 - P_1 - P_2 + P_3) \end{aligned}$$

be the primitive idempotents of A. Then, for any $\mathfrak{M}$-module M, we have a decomposition

$$M = Me_1 \oplus Me_2 \oplus Me_3 \oplus Me_4,$$

according to the splitting

$$\mathfrak{M} = \mathfrak{M}e_1 \oplus \mathfrak{M}e_2 \oplus \mathfrak{M}e_3 \oplus \mathfrak{M}e_4.$$

Since each of the direct summands of $\mathfrak{M}$ is naturally isomorphic to $\mathcal{O}_F$, we obtain a group isomorphism

$$cl(\mathfrak{M}) \longrightarrow \bigoplus_{i=1}^{4} cl_F, \tag{16}$$

induced by $[M] \mapsto (c(Me_i))_{i=1,\dots,4}$, where $c(Me_i)$ denotes the Steinitz class of the $\mathcal{O}_F$-module Me_i. The composition of ψ' and (16) will again be denoted by ψ'.

Recall from Proposition 2.2 that associated to E/k there is an odd integral ideal $\mathfrak{b}$ of $\mathcal{O}_k$ such that $\mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{b}^2 = (A_1)$ is principal. Here $\mathfrak{p}_5$ and $\mathfrak{p}_{13}$ denote the ramified primes of $\mathcal{O}_k$ above 5 and 13 respectively. We also recall the decomposition $2\mathcal{O}_{\mathbf{Q}(\sqrt{65})} = \mathfrak{p}_2\mathfrak{p}_2'$ with $\mathfrak{p}_2 = \mathbf{Z}2 + \mathbf{Z}\frac{1+\sqrt{65}}{2}$.

Proposition 4.1. *$\psi'(P) = (1, 1, [\mathfrak{b}\mathcal{O}_F], [\mathfrak{b}\mathcal{O}_F])$ for $P = P_1 = (0, 0)$.*

Proof. We have to compute the Steinitz invariants of $\tilde{\mathcal{O}}_P e_i$ for $i = 1, \dots, 4$. If (6) holds, then $\tilde{\mathcal{O}}_P = (\mathcal{O}_F + 2\mathcal{O}_L) \oplus (\mathcal{O}_F + 2\mathcal{O}_L)$. For $i = 1, 2$ it is easily seen that $\tilde{\mathcal{O}}_P e_i \simeq \frac{1}{2}\mathcal{O}_F$ as $\mathcal{O}_F$-modules. For $(\alpha, \beta) \in \tilde{\mathcal{O}}_P$ we compute

$$(\alpha, \beta) e_{3/4} = \frac{1}{4}\left((\alpha \pm \beta)^{1-\sigma}, (\beta \pm \alpha)^{1-\sigma}\right). \tag{17}$$

Hence

(18)
$$\tilde{\mathcal{O}}_P e_{3/4} \simeq \frac{1}{4}\{\alpha^{1-\sigma} \mid \alpha \in 2\mathcal{O}_L\} = \frac{1}{2}\mathcal{O}_L^{1-\sigma} = \frac{1}{2}\{\alpha \in \mathcal{O}_L \mid Tr_{L/F}(\alpha) = 0\},$$

where the last equality follows from the cohomological triviality of $\mathcal{O}_L$. Recall that $L = F(\theta)$ with $\theta = \sqrt{B(A + 2\sqrt{B})}$. From (18) we deduce

$$\tilde{\mathcal{O}}_P e_{3/4} \simeq \frac{1}{2}(F\theta \cap \mathcal{O}_L). \tag{19}$$

It therefore remains to determine the ideal factorization of θ. Using Proposition 2.2 we get

$$\theta = \pm 2 \frac{A_1}{\sqrt{65}} \sqrt{\frac{A_1}{\sqrt{65}} \frac{\pm 1 \pm \sqrt{65}}{2}},$$

the signs depending on $A = \pm A_1$ and $\mathrm{Re}(A_1) > 0$ or $\mathrm{Re}(A_1) < 0$. This implies that $\theta\mathcal{O}_L = (2\mathfrak{b}^3\mathfrak{q}^2)\mathcal{O}_L$ with $\mathfrak{q} \in \{\mathfrak{p}_2, \mathfrak{p}_2'\}$ and therefore $F\theta \cap \mathcal{O}_L = (2\mathfrak{b}^3\mathfrak{q}^2\mathcal{O}_F)^{-1}\theta$. We note that $\mathfrak{q}^2 = \left((7 \pm \sqrt{65})/2\right)\mathcal{O}_F$ is principal. Hence we obtain from (19) and [**FT**, Theorem 13] that $c(\tilde{\mathcal{O}}_P e_{2/3}) = [\mathfrak{b}^{-3}\mathcal{O}_F] = [\mathfrak{b}\mathcal{O}_F]$. This completes the proof for case (6).

Suppose now that (7) holds. Proposition 3.2 implies that $\tilde{\mathcal{O}}_P e_i \simeq \frac{1}{2}\mathcal{O}_F$ for $i = 1, 2$. To conclude the proof we claim that for $i = 3, 4$ we also get $\tilde{\mathcal{O}}_P e_{3/4} \simeq \frac{1}{2}\{\alpha \in \mathcal{O}_L \mid Tr_{L/F}(\alpha) = 0\}$ as in case (6). Indeed, from (17) and Proposition 3.1 we will deduce that $\tilde{\mathcal{O}}_P e_{3/4} \simeq \frac{1}{2}\mathcal{O}_L^{1-\sigma}$: The inclusion "$\supseteq$" is obvious. The converse inclusion follows from

$$\begin{aligned}(\alpha \pm \beta)^{1-\sigma} &\in (\mathfrak{p}_2\mathcal{O}_L)^{1-\sigma} \cap (\mathfrak{p}_2'\mathcal{O}_L)^{1-\sigma} \\ &\overset{(*)}{=} \{\nu_1 \in \mathfrak{p}_2\mathcal{O}_L \mid Tr_{L/F}(\nu_1) = 0\} \cap \{\nu_2 \in \mathfrak{p}_2'\mathcal{O}_L \mid Tr_{L/F}(\nu_2) = 0\} \\ &= \{\nu \in 2\mathcal{O}_L \mid Tr_{L/F}(\nu) = 0\},\end{aligned}$$

where (*) holds true since $\mathfrak{p}_2\mathcal{O}_L$ (resp. $\mathfrak{p}_2'\mathcal{O}_L$) is a cohomologically trivial $\mathrm{Gal}(L/F)$-module (see [**Ul**, Corollary 1.4]). Finally the proof follows by computing the ideal factorization of θ using Proposition 2.2 for case (7). □

Proof of Theorem 1.3. It simply remains to show that $\mathfrak{b}\mathcal{O}_F$ is not principal if $m_1 > 1$. Assume it were principal. Then $N_{F/k}(\mathfrak{b}\mathcal{O}_F) = \mathfrak{b}^2$ is also principal.

Since by the construction of E the ideal $\mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{b}^2 = (A_1)$ is principal, too, it follows that $\mathfrak{p}_5\mathfrak{p}_{13}$ is principal. This happens if and only if $m_1 = 1$. □

Note in proof. In the recent manuscript [**CJ**] Ph. Cassou-Noguès and A. Jehanne describe counter-examples to Taylor's conjecture for $p = 2$ and elliptic curves with complex multiplication.

References

[Ag] A. Agboola, *Torsion points on elliptic curves and galois module structure*, Invent. Math., **123** (1996) 105-122.

[Bl] W.Bley, *Computing associated orders and Galois generating elements of unit lattices*, J. Number Theory, **62** (1997), 242-256.

[BS] S.I. Borewics and L.R. Safarevic, *Zahlentheorie*, Birkhäuser, Basel Stuttgart, 1966.

[Bo] K. Bouklou, *Arithmétique d'espaces homogènes principaux associés à une courbe elliptique*, Thèse, Univ. Bordeaux I, 1996.

[CJ] Ph. Cassou-Noguès and A. Jehanne, *Espaces homogènes principaux et points de 2-division de courbes elliptiques*, preprint, 1998.

[CS] Ph. Cassou-Noguès and A. Srivastav, *On Taylor's conjecture for Kummer orders*, Journal de Théorie des nombres de Bordeaux, **2** (1990) 349-363.

[FT] A. Fröhlich and M.J. Taylor, *Algebraic number theory*, Cambridge studies in advanced mathematics, **27**, Cambridge University Press, 1991.

[Pa] G. Pappas, *On torsion line bundles and torsion points on abelian varieties*, preprint, 1996.

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

[Si] J. Silverman, *The arithmetic of elliptic curves*, Springer, Berlin Heidelberg New York, 1986.

[ST] A. Srivastav and M.J. Taylor, *Elliptic curves with complex multiplication and Galois module structure*, Invent. Math., **99** (1990), 165-184.

[Ta] M.J. Taylor, *Mordell-Weil groups and the Galois module structure of rings of integers*, Ill. J. Math., **32** (1988), 428-452.

[Ul] S.V. Ullom, *Normal basis in Galois extensions of number fields*, Nagoya Math. J., **34** (1969), 153-167.

Received February 14, 1997 and revised September 19, 1997.

Institut für Mathematik der Universität Augsburg
Universitätsstr. 8
D-86159 Augsburg
Deutschland
E-mail address: bley@uni-augsburg.de