PHILIPPE CASSOU-NOGUÈS
ANUPAM SRIVASTAV

On Taylor’s conjecture for Kummer orders

Journal de Théorie des Nombres de Bordeaux, tome 2, n° 2 (1990), p. 349-363

<http://www.numdam.org/item?id=JTNB_1990__2_2_349_0>
On Taylor’s conjecture for Kummer orders.*

by PHILIPPE CASSOU-NOGUÈS AND ANUPAM SRIVASTAV

1. Introduction

Let \( \overline{\mathbb{Q}} \) denote the algebraic closure of \( \mathbb{Q} \) in \( \mathbb{C} \) and let \( \overline{\mathcal{O}} \) be the ring of algebraic integers of \( \overline{\mathbb{Q}} \). For a number field \( F \subseteq \overline{\mathbb{Q}} \) we denote by \( \mathcal{O}_F \) its ring of algebraic integers and we set \( \Omega_F = \text{Gal}(\overline{\mathbb{Q}}/F) \).

Let \( K \) be a quadratic imaginary number field, \( L \) a finite extension of \( K \) and \( (E/L) \) be an elliptic curve, defined over \( L \), with everywhere good reduction and admitting complex multiplication by \( \mathcal{O}_K \).

Let \( \mathfrak{A} = (a) \) denote a non-zero integral \( \mathcal{O}_K \)-ideal. Let us write \( \mathcal{G} = \mathcal{G}(\mathfrak{A}) \) for the subgroup of points in \( E(\overline{\mathbb{Q}}) \) that are killed by all elements of \( \mathfrak{A} \). For \( P \in E(L) \), we set

\[
G_P = G_P(\mathfrak{A}) = \{ R \in E(\overline{\mathbb{Q}}) : [a]R = P \}
\]

the corresponding \( \mathcal{G} \)-space of points on \( E \). We define the corresponding Kummer algebra by

\[
L_P = L_P(\mathfrak{A}) = \text{Map}(G_P, \overline{\mathbb{Q}})^{\Omega_L}
\]

where the addition and multiplication are given value-wise on \( \Omega_L \) maps from \( G_P \) to \( \overline{\mathbb{Q}} \). In [T] M.-J. Taylor considered the \( \mathcal{O}_L \)-algebra \( \mathcal{B} \) which represents the \( \mathcal{O}_L \)-group scheme of \( \mathfrak{A} \) points of \( E \). In fact \( \mathcal{B} \) is an \( \mathcal{O}_L \)-Hopf order in the \( L \)-algebra \( L_\Omega = \text{Map}(G, \overline{\mathbb{Q}})^{\Omega_L} \), where \( O \) is the origin of \( E \). The \( \mathcal{O}_L \)-Cartier dual of \( \mathcal{B} \) is an \( \mathcal{O}_L \)-order in the dual algebra \( \mathcal{A} = (\overline{\mathbb{Q}}[G])^{\Omega_L} \) that we denote by \( \Lambda \). Taylor [T] defined the Kummer order \( \overline{\mathcal{O}}_P \) as the largest \( \Lambda \)-module contained in \( \mathcal{O}_P \) the integral closure of \( \mathcal{O}_L \) in \( L_P \). He showed that \( \overline{\mathcal{O}}_P \) is a locally free \( \Lambda \)-module. We write \( (\overline{\mathcal{O}}_P) \) for its class in \( \text{Cl}(\Lambda) \), the class group of locally free \( \Lambda \)-modules.

*This work was done while the second named author was visiting lecturer at Bordeaux University. He wishes to express his gratitude to the University for their hospitality.

Manuscrit reçu le 7 mai 1990
In [T] the map \( \psi : E(L) \to C\ell(\Lambda) \), given by \( \psi(P) = (\bar{\rho} P) \) is shown to be a group homomorphism. Moreover it follows from the definition of \( \bar{\rho} \) that \([a]E(L) \subset \text{Ker} \psi \). Taylor conjectured in [T] :

(1-3) **Conjecture.** For any non-zero principal \( O_K \)-ideal,

\[
E(L)_{\text{torsion}} \subset \text{Ker} \psi.
\]

We remark that in [S-T] the above framework was generalised to include the case of non principal \( O_K \)-ideals.

Let \( w_K \) denote the number of roots of unity of \( K \). The above conjecture was proved in [S-T] under the hypothesis that the ideal \( \mathfrak{A} \) be coprime to \( w_K \). In this article we consider the conjecture for the case where \( |G| = 2 \).

We now assume that there is a principal prime ideal \( \mathfrak{p} = (\pi) \) dividing \( 2 \). Moreover we assume that \( \mathfrak{p} \) is either ramified or split in \( (K/Q) \) and that \( K \neq Q(\sqrt{-1}) \). We set \( \mathfrak{A} = \mathfrak{p} \), so that \( G = E[\pi] \) and \( |G| = 2 \). By the theory of complex multiplication we can also deduce that \( G \subset E[2] \subset E(L) \).

Therefore \( \mathcal{A} = L[G] \) and \( \mathfrak{B} = Map(G, L) \). From [T], Proposition 1, we conclude that the order \( \Lambda \), in the present case, is given by

\[
(1-4) \quad \Lambda = 1_G \cdot O_L + (\pi^{-1} \sigma_G) O_L.
\]

where \( \sigma_G = \sum_{g \in G} g \).

Let \( \mathfrak{M} \) denote the unique maximal \( O_L \)-order of \( L[G] \). As usual, we denote by \( D(\Lambda) \) the kernel of the extension map \( e : C\ell(\Lambda) \to C\ell(\mathfrak{M}) \). We define the homomorphism \( \psi' : E(L) \to C\ell(\mathfrak{M}) \) to be the composite map \( e \circ \psi \).

For \( P \in E(L) \), it is shown in [T] that \( |G| \) annihilates \( \psi(P) \). Thus, in the present case, \( \psi(P)^2 = 1 \) in \( C\ell(\Lambda) \) and \( \psi'(P)^2 = 1 \) in \( C\ell(\mathfrak{M}) \). In the second section we shall prove :

**Theorem 1.** Let \( \mathfrak{p} = (\pi) \) be a ramified or split principal prime ideal dividing \( 2O_K \). Moreover, assume that \( E[4] \subset E(L) \). Then for \( G = E[\pi] \),

\[
E(L)_{\text{torsion}} \subset \text{Ker} (\psi').
\]

Let \( \Phi \) denote the quotient map \( O_L \to O_L/\pi O_L \), where \( \pi \) is the complex conjugate of \( \pi \). We denote the image of \( O_L^* \) under \( \Phi \) by \( \text{Im} O_L^* \). In section 2 we also calculate \( D(\Lambda) \).

**Theorem 2.** The group kernel is given by

\[
D(\Lambda) = (O_L/\pi O_L)^*/\text{Im} O_L^*.
\]
The main aim of section 3 is to treat cases where $E[4]$ is not contained in $E(L)$.

We first assume that 2 is split in $(K/Q)$; we denote by $p = (\pi)$ a prime ideal of $K$ above 2. We now fix a fractional ideal $\Omega$ of $K$, viewed as a $\mathbb{C}$ lattice, and a 4-division point $\nu$ of $\mathbb{C}/\Omega$ such that $2\nu$ has annihilator $2\mathcal{O}_K$. Corresponding to the pair $(\Omega, \nu)$ we define the “minimal Fueter model” as the elliptic curve $E$ given by:

\[
y^2 + \sqrt{t} xy = x^3 + x
\]

where $t = t_{\Omega, \nu} = 12\rho_\Omega(2\nu)/(\rho_\Omega(\nu) - \rho_\Omega(2\nu))$. We let $L = K(\sqrt{t})$. Our model is then defined over $L$. From $[CN - T_2], IX, (5 - 4)$, we know that $K(t) = K(4)$, the ray class field mod $4\mathcal{O}_K$. Moreover, since 2 is split in $(K/Q)$, we know that $t^2 - 2^6$ is a unit, $[CN - T_2], IX, (5 - 10)$. Therefore $E$ has good reduction everywhere. One can check, using classfield theory, that $E[\pi] \subset E(L)$. We let $Q$ be the primitive $\pi$-division point of $E$. We now assume that $E[2] \subset E(L)$. We consider the map $h : G_Q \to \bar{O}$ defined by $h(\mathcal{O}) = y(\mathcal{O})$, for $\mathcal{O} \in G_Q$. It will be proved that $h$ lies in $\bar{O}_Q$.

Next we consider the Swan module $(\sqrt{t}, \pi^{-1}\sigma_G)\Lambda$. Since $t^2 - 2^6$ is a unit, $\sqrt{t}$ is relatively prime to $|G| = 2$. Then this module is a locally free ideal of $\Lambda$ (cf. [U],[S]).

**Theorem 3.** Let $Q$ be the primitive $\pi$-division point of the minimal Fueter curve $E$. Then

\[
\sqrt{t}\bar{O}_Q = h(\sqrt{t}, \pi^{-1}\sigma_G)\Lambda.
\]

One can observe that the Swan module is the obstruction to the $\Lambda$-freeness of $\bar{O}_Q$. As a consequence of Theorem 2 and Theorem 3 we obtain:

**Corollary 1.** Under the hypothesis of Theorem 3, $E(L)_{\text{torsion}} \subset \text{Ker}\psi$ if and only if there exists a unit $u$ of $L$ such that $\sqrt{t} \equiv u \mod \mathfrak{p}\mathcal{O}_L$.

**Proof.** Since $E[\pi^2] \not\subset E(L)$ the inclusion $E(L)_{\text{torsion}} \subset \text{Ker}\psi$ is equivalent with $\psi(Q) = 1$, (see section 2). By Theorem 3 we know that $\psi(Q) = 1$ if and only if $(\sqrt{t}, \pi^{-1}\sigma_G)\Lambda$ is a free $\Lambda$-module. Since we know that the element of $\mathcal{C}(\Lambda)$ defined by $(\sqrt{t}, \pi^{-1}\sigma_G)\Lambda$ belongs to $D(\Lambda)$ and is represented by $\sqrt{t}$, the conclusion follows Theorem 2. \qed
It will be obviously very interesting to know whether the condition of the corollary is always satisfied. In section 4 we checked that the condition is fulfilled when $K = \mathbb{Q}(\sqrt{-7})$.

Acknowledgement: The authors wish to thank J. Martinet for providing useful computer calculations of certain units for section 4.

2. Proof of Theorems 1 and 2.

We keep the notations of section 1. Let $m$ be the largest positive integer such that $E[\pi^m] \subset E(L)$. We know that $[\pi]E(L) \subset \text{Ker}\psi \subset \text{Ker}\psi'$. Therefore, in order to prove Theorem 1, it suffices to show that

$$E[\pi^m] - E[\pi^{m-1}] \subset \text{Ker}\psi'.$$

Let us now fix $Q \in E(L)$ such that $G_Q \notin E(L)$. In this case $L_Q$ can be identified with $L(Q)$, the field generated over $L$ by the coordinates of all points of $G_Q$. Of course, now $[L(Q) : L] = 2$. Let $R \in E(Q)$ be such that

$$\pi R = Q.$$

Then the map:

$$\text{Gal}(L(Q)/L) \to G$$

$$\omega \to R^\omega - R$$

induces a group isomorphism which is independent of the particular choice of $R$. We may identify these two groups. Let $\gamma$ be the non trivial element of $G$.

Proof of Theorem 1.

The proof splits in two steps.

(I) Preliminary step

Let $\hat{G}$ denote the group of characters of $G$. We have an isomorphism

$$\theta : \text{Cl}(M) \cong \prod_{\chi \in \hat{G}} \text{Cl}(O_L).$$

For $y \in \text{Cl}(M)$ we write $\theta_\chi(y)$ to denote its projection on the $\chi$-component $\text{Cl}(O_L)$. Now $G$ acts as automorphisms on $L(Q)$. We write this action exponentially. For $\chi \in \hat{G}$ and $b \in \text{Map}(G_Q, \mathbb{Q})$, the Lagrange resolvent of $b$ is defined by

$$(b|\chi) = \sum_{g \in G} b^g \chi(g^{-1})$$
PROPOSITION 1. Let $\chi \in \hat{G}$ and $y \in L(Q)$ be such that $y^2 = y \chi(g)$, \( \forall g \in G \). Then there exists a fractional ideal $I(\chi)$ of $L$ whose class in $Cl(O_L)$ is independent of the choice of $y$, such that $y^2 O_L = I(\chi)^2$. Moreover, $\theta_\chi(\psi'(Q)) = [I(\chi)]^{-1}$.

Proof. Clearly the class of $I(\chi)$ does not depend on the choice of $y$. We may, therefore, take $y = \pi^{-1}(d|\chi)$ where $d$ generates a normal basis of $L(Q)$ over $L$. From [T], Proposition 6 and Theorem 3, we deduce that there exists a fractional ideal $I(\chi)$ of $L$ such that $\theta_\chi(\psi'(Q)) = [I(\chi)]^{-1}$ and $I(\chi)O_{L}(Q) = \pi^{-1}(d|\chi)O_{L}(Q)$.

\[\square\]

COROLLARY 2. The following statements are equivalent

i) $\psi'(Q) = 1$
ii) There exists $y \in L(Q) \setminus L$ such that $y^2 \in L$ and $y^2 O_L$ is a square of a principal $O_L$-ideal.
iii) There exists a unit $u \in L$ such that $L(Q) = L(\sqrt{u})$.

(II) Construction of a unit.

Let us now assume that $E[4] \subseteq E(L)$ and fix $Q \in E[\pi^m]$. Therefore, in this case $m > 1$. We consider a general Weierstrass model of $E$ defined over $L$. Let us fix $R \in G_Q$. Let $S$ be the primitive $\pi$-division point and $V$ a primitive 4-division point of $E(L)$. As $G_Q \not\subseteq E(L)$, the points $[2]R$ and $[2](R + V)$ are both distinct from $S$. Thus $x(R)^7 = x(R + S) \neq x(R)$ and $x(R + V)^7 = x(R + V + S) \neq x(R + V)$.

We then have

\[L(Q) = L(x(R)) = L(x(R + V)).\]

Thus, by the theorem of Fueter-Hasse, [CN-T 2, IX]

\[L(Q) = \begin{cases} L.K(p^{m+1}) & \text{if 2 is ramified in } (K/Q) \\ L.K(4p^{m-1}) & \text{if 2 is split in } (K/Q) \end{cases}\]

where $K(f)$ denotes the $K$-ray class field mod $f$ for any $O_K$-ideal $f$.

Next we fix an analytic parametrisation

\[C/\Omega \rightarrow E(C)\]

for a certain lattice $\Omega$ of $C$. 

On Taylor’s conjecture

353
We now set:

\[
A_Q = \begin{cases} 
\frac{h_Q(R)-h_Q(R+S)}{h_Q(Q)-h_Q(Q+S)}, & \text{if } 2 \text{ is ramified in } (K/Q) \\
\frac{h_Q(R+V)-h_Q(R+V+S)}{h_Q(Q+V)-h_Q(Q+V+S)}, & \text{if } 2 \text{ is split in } (K/Q) 
\end{cases}
\]

where \(h_Q\) is the first Weber's function. Once again from the theory of complex multiplication we know that \(A_Q \in K(p^{m+1})\) (resp. \(K(4p^{m-1})\)) if 2 is ramified (resp. split) in \((K/Q)\). Moreover we obtain that

\[
\begin{align*}
K(p^{m+1}) &= K(p^m)(A_Q), & \text{if } 2 \text{ is ramified in } (K/Q) \\
K(4p^{m-1}) &= K(4p^{m-2})(A_Q), & \text{if } 2 \text{ is split in } (K/Q)
\end{align*}
\]

From (2.3) we then deduce that

\[
L(Q) = L(A_Q) \text{ and } A_Q^2 \in L.
\]

Let \(\rho_Q\) be the Weierstrass \(\rho\) function for \(\Omega\). From the definition of \(h_Q\) we deduce that

\[
A_Q = \begin{cases} 
\frac{\rho_Q(R)-\rho_Q(R+S)}{\rho_Q(Q)-\rho_Q(Q+S)}, & \text{if } 2 \text{ is ramified in } (K/Q) \\
\frac{\rho_Q(R+V)-\rho_Q(R+V+S)}{\rho_Q(Q+V)-\rho_Q(Q+V+S)}, & \text{if } 2 \text{ is split in } (K/Q) 
\end{cases}
\]

Let \(\mathcal{H}\) denote the upper half plane. Let \(\tau \in \mathcal{H}\) be such that \(\Omega = \lambda(\mathbb{Z}\tau + \mathbb{Z})\) for some \(\lambda \in \mathbb{C}^\ast\). For \(z \in \mathcal{H}\) we write \(\Omega_z = \mathbb{Z}z + \mathbb{Z}\). For \(a \in (\mathbb{Q}/\mathbb{Z})^2\) we choose the unique representative \((a_1, a_2) \in \mathbb{Q}^2\) with \(a_1, a_2 \in [0, 1]\). We write \(az = a_1z + a_2\). We define \(r(\text{resp. } s, \text{resp. } v, \text{resp. } q)\) in \((\mathbb{Q}/\mathbb{Z})^3\) such that \(\lambda(r\tau)(\text{resp. } \lambda(s\tau), \text{resp. } \lambda(v\tau), \text{resp. } \lambda(q\tau))\) represents \(R(\text{resp. } S, \text{resp. } V, \text{resp. } Q)\) in \(\mathbb{C} \mod \Omega\). We now consider functions \(F(r, q, s)\) and \(G(r, q, s, v)\) defined by

\[
F(r, q, s)(z) = \frac{\rho_{\Omega_z}(rz) - \rho_{\Omega_z}(rz + sz)}{\rho_{\Omega_z}(qz) - \rho_{\Omega_z}(qz + sz)}
\]

and

\[
G(r, q, s, v)(z) = \frac{\rho_{\Omega_z}(rz + vz) - \rho_{\Omega_z}(rz + vz + sz)}{\rho_{\Omega_z}(qz + vz) - \rho_{\Omega_z}(qz + vz + sz)}
\]

\[
A_Q = \begin{cases} 
F(r, q, s)(\tau) & \text{if } 2 \text{ ramified}, \\
G(r, q, s, v)(\tau) & \text{if } 2 \text{ splits.}
\end{cases}
\]
Functions $F$ and $G$ are modular Weierstrass units of a level which is an appropriate power of 2.

When $f$ and $g$ are functions defined on $\mathcal{H}$ we write

$$f \approx g$$

if there exist integers $n$ and $m$ such that $f^n/g^m$ is a modular function, which is a unit over $\mathbb{Z}$.

For $a \in (\mathbb{Q}/\mathbb{Z})^2$ we introduced in $[CN-T_1]$, (2-7), a function $\tilde{\Psi}(a)$ defined on $\mathcal{H}$. In fact an appropriate power of $\tilde{\Psi}(a)$ is a ratio of Deuring modular units. From $[CN-T_1]$, Proposition 2-8, we obtain

**Lemma 1.** There are equivalences

$$F(r, q, s) \approx \frac{\tilde{\Psi}(q)\tilde{\Psi}(q + s)\tilde{\Psi}(2r + s)}{\tilde{\Psi}(r)\tilde{\Psi}(r + s)\tilde{\Psi}(2q + s)}$$

and

$$G(r, q, s, v) \approx \frac{\tilde{\Psi}(q + v)\tilde{\Psi}(q + s + v)\tilde{\Psi}(2r + 2v + s)}{\tilde{\Psi}(r + v)\tilde{\Psi}(r + v + s)\tilde{\Psi}(2q + 2v + s)}$$

We now show:

**Lemma 2.** (i) If 2 is ramified in $(K/\mathbb{Q})$, then $F(r, q, s)(\tau)$ is a unit.

(ii) If 2 is split in $(K/\mathbb{Q})$ and $m > 2$, then $G(r, q, s, v)(\tau)$ is a unit.

Proof (i) Let 2 be ramified in $(K/\mathbb{Q})$ and suppose $m = 2t$, $t > 1$ (if $m$ is odd the proof is similar). Then, $q\tau$ (resp. $(q + s)\tau$, $\tau$, resp. $(2q + s)\tau$, resp. $(r + s)\tau$, resp. $(2r + s)\tau$) defines a primitive $p^{2t}$ (resp. $p^{2t}$, $p^{2t+1}$, $p^{2t+1}$, $p^{2t-1}$)-division point of $C/\Omega_\tau$.

For two algebraic numbers $a, b$ we write $a \sim b$ if $ab^{-1}$ is a unit. From $[CN-T_1]$, Proposition 3-5, we deduce that

$$\begin{cases}
\tilde{\Psi}(q)(\tau) \sim \tilde{\Psi}(q + s)(\tau) \sim 2^{(2^{2t})} \\
\tilde{\Psi}(r)(\tau) \sim \tilde{\Psi}(r + s)(\tau) \sim 2^{(2^{2t-1})} \\
\tilde{\Psi}(2q + s)(\tau) \sim 2^{(2^{2t-1})} \\
\tilde{\Psi}(2r + s)(\tau) \sim 2^{(2^{1-2t})}.
\end{cases}$$

(2-10)
Thus from Lemma 1 and (2-10) we conclude that $F(q, r, s)(\tau)$ is a unit.

(ii) Now suppose that 2 is split in $(K/\mathcal{Q})$ and $m > 2$. Then $(q + v)\tau$ and $(q + v + s)\tau$ are primitive $\mathfrak{p}^m\mathfrak{p}^2$ division points; $(r + v)\tau$ and $(r + v + s)\tau$ are primitive $\mathfrak{p}^{m+1}\mathfrak{p}^2$-division points. Moreover $(2r + 2v + s)\tau$ (resp. $(2q + 2v + s)\tau$) is a primitive $\mathfrak{p}^m\mathfrak{p}$ (resp. $\mathfrak{p}^{m+1}\mathfrak{p}$)-division point. Since these points are primitive of composite order, it follows from $[CN - T_1]$, Proposition 3-5, that each factor in the right hand side of the equivalence in Lemma 1 gives a unit when evaluated at $\tau$. From (2-9) and Lemma 2 we now conclude that $A_Q$ is a unit. Therefore Theorem 1 is proved, via Corollary 2, except in the case where 2 is split in $(K/\mathcal{Q})$ and $m = 2$. We can, nevertheless, treat this case in a similar fashion by replacing $A_Q$ by $A_Q'$ given by

$$A_Q' = \pi^{-1}(P_\Omega(R + V) - P_\Omega(R + V + S))$$

where $P_\Omega$ is the function considered by Schertz [Sh]. We know that

$$A_Q' = \kappa(h_\Omega(R + V) - h_\Omega(R + V + S))$$

where $\kappa \in K(1)$. We thus have $A_Q' \in L_Q \setminus L$ and $(A_Q')^2 \in L$. We now deduce from [Sch], (12) and Satz 3, that $A_Q'$ is a unit. This now completes the proof of Theorem 1.

\[\square\]

Proof of Theorem 2. We recall that the order $\Lambda$ is explicitly given by (1-4). Let us consider the fiber product of orders

$$\Lambda \xrightarrow{\epsilon} O_L, \quad \eta \downarrow \quad \phi \downarrow \quad \Lambda/(\pi^{-1}\sigma_G) \xrightarrow{\tilde{\epsilon}} O_L/\bar{\pi}O_L,$$

where $\eta$ and $\phi$ are the quotient maps, $\epsilon$ is the augmentation map and $\tilde{\epsilon}$ is induced by $\epsilon$. Using the Mayer-Vietoris sequence of Reiner-Ullom, [S], [U], we obtain an exact sequence of groups and homomorphisms.

$$O_L^* \times (\Lambda/(\pi^{-1}\sigma_G))^* \xrightarrow{\phi^{-1}} (O_L/\bar{\pi}O_L)^* \xrightarrow{\delta} D(\Lambda) \to \{1\}$$

where $\delta$ is the connecting homomorphism.
We also need to observe that
\[ D(O_L) = D(\Lambda/(\pi^{-1}\sigma_G)) = \{1\}. \]
Moreover, for \( s \) coprime with \( v \), \( \delta(s \mod \pi O_L) \) is given by the class of the corresponding Swan module \( (s, \pi^{-1}\sigma_G)\Lambda \). Since \( O_L \) and \( \Lambda/(\pi^{-1}\sigma_G) \) can be naturally identified as rings, we conclude that
\[ D(\Lambda) = (O_L/\pi O_L)^* / Im \ O_L^*. \]

3. Minimal Fueter model

We recall in this section that \( p = (\pi) \) is a principal, prime ideal of \( K \), above 2, which is split in \((K/Q)\). Moreover we suppose that \( E[\pi] \subset E(L) \) and \( E[\pi^2] \notin E(L) \). We let \( \Omega \) be a fractional ideal of \( K \) and \( \nu \) a primitive 4\( O_K \)-division point of \( C/\Omega \).

In [CN – T2] a Fueter elliptic curve was considered, corresponding to the pair \((\Omega, \nu)\), given by

\[ (3.1) \quad y^2 = 4x^3 + tx^2 + 4x \]

with
\[ t = 12\rho_\Omega((2\nu))/((\rho_\Omega(\nu) - \rho_\Omega(2\nu))). \]
In fact one defines a complex analytic isomorphism between \( C/\Omega \) and the complex points of this curve by considering

\[ (3.2) \quad z \rightarrow \begin{cases} (T(z), T_1(z), 1) & \text{if } z \neq 2\nu \\ (0, 1, 0) & \text{if } z = 2\nu \end{cases} \]

where \( T \) and \( T_1 \) are Fueter’s elliptic functions, [CN – T2], IV. The minimal Fueter model \( E \) is obtained from (3.1) by the change of coordinates

\[ (3.3) \quad (x, y) \rightarrow (x, \sqrt{t}x + 2y). \]

From (3.2) and (3.3) we deduce an isomorphism between \( C/\Omega \) and the \( C \)-points of \( E \) given by

\[ (3.4) \quad z \rightarrow \begin{cases} (T(z), U(z), 1) & \text{if } z \neq 2\nu \\ (0, 1, 0) & \text{if } z = 2\nu \end{cases} \]

where \( U(z) = (1/2)(T_1(z) - \sqrt{t} T(z)) \).
We remark that $0 = (0, 0, 1)$ is taken to be the identity of the group law. It is also worth remarking that $i \in K(t)$. We set $A = (i, 0, 1)$. It is worth to notice that, using the theory of complex multiplication, one can show that $A \in E(L)$ and has infinite order. Let $\alpha$ be the parameter of $A$ in $C/\Omega$ under the isomorphism (3-4).

The divisor of $T$ is given by

\[(3-5) \quad (T) = 2(0) - 2(2\nu).\]

From $[CN - T_2], IV$ we know that

\[(3-6.a) \quad T(z).T(z + 2\nu) = 1.\]

\[(3-6.b) \quad T_1(z + 2\nu) = \frac{-T_1(z)}{T^2(z)}.\]

Therefore, since $T$ is an even function and $T_1$ is an odd function, we deduce that

\[(3-7) \quad U(2\nu - z) = U(z)/T^2(z).\]

Moreover, the elliptic function $U$ has divisor

\[(3-8) \quad (U) = (0) + (\alpha) + (2\nu - \alpha) - 3(2\nu).\]

We denote by $N$ the point of $E(Q)_{\text{torsion}}$ defined by $\nu$. Let $Q$ be the primitive $\pi$-division point of $E$. We fix a point $R \in G_Q$ and denote by $\rho$ its parameter in $C/\Omega$.

Now $R + Q = -R$, therefore $G_Q = \{R, -R\}$.

Thus, $x(R) = x(R + Q) = x(-R) = x(R)$. Then $L(Q) = L(y(R)) = L(T_1(\rho)) = L(D(\rho))$ where $D(\rho) = T_1(\rho)/T(\rho)$.

From $[CN - T_2]$, IX, (6-7) we know that $D^4(\rho) = t^2 - 2^6$, which is a unit. Since $D^2(\rho) \in L$ we conclude from Corollary 2 that $\psi'(Q) = 1$.

Until the end of this section the $x$ and $y$ coordinates are those of model (1-5).

We now want to study $\psi(Q)$. First, we have

**Lemma 3.** Let $\mathfrak{P}$ be a prime ideal of $O_K$. Let $P \in E(Q)_{\text{torsion}}$ be such that $\{P, [2]N - P\} \cap E[\mathfrak{P}^n] = \phi$. Then $x(P)$ is a $\mathfrak{P}$-unit (i.e. unit at all primes dividing $\mathfrak{P}$).

Proof. We first observe that for any $P \in E(Q)$, $P \neq [2]N$, $x(P)$ is a $\mathfrak{P}$-integer if and only if $y(P)$ is a $\mathfrak{P}$-integer. Under the given hypothesis both
\( x(P) \) and \( y(P) \) are well defined and are non zero. Since \( x(P).x([2]N - P) = 1 \), it suffices to show that \( x(P) \) is a \( \mathfrak{P} \)-integer.

Let \( M \) be a finite extension of \( L \) such that \( \{ P, [2]N - P \} \subset E(M) \). Suppose \( x(P) \) is not a \( \mathfrak{P} \)-integer. Then there exists \( \mathfrak{P}_M \), a maximal \( \mathcal{O}_M \)-ideal, with \( \mathfrak{P}_M \cap \mathcal{O}_K = \mathfrak{P} \) and \( v(x(P)) < 0 \) where \( v \) denote the standard valuation on the completion of \( M \) at \( \mathfrak{P}_M \). From the equation of the minimal Fueter model \( E \) we see that \( 2v(y(P)) = 3v(x(P)) \). Thus, under the reduction mod \( \mathfrak{P}_M \), \( P \) is mapped onto \((0,1,0)\). This means that \([2]N - P\) is in the kernel of reduction mod \( \mathfrak{P}_M \) which is impossible since the set of torsion points in the kernel of reduction is precisely \( \bigcup_{n > 0} E[\mathfrak{P}^n] \).

\[ \square \]

**Lemma 4.** \( x(R) \sim \pi \)

Proof. Since \( R \) is a primitive \( \pi^2 \)-division point of \( E \), \([2]N - R \) is a torsion point of composite order. From Lemma 3 we conclude that \( x(R) \) is a unit outside the prime divisors of \( p = (\pi) \). For a prime \( \mathfrak{P} \) of \( L(\mathbb{Q}) \) that divides \( p \), using that \( R \) is a primitive \( \pi^2 \)-division point in the kernel of reduction mod \( \mathfrak{P}_{L(\mathbb{Q})} \) and that \( x(R)/y(R) \) is the parameter of \( R \) in the associated formal group we can find the valuation \( v_{\mathfrak{P}_{L(\mathbb{Q})}}(x(R)) \).

\[ \square \]

**Remark :** Lemma 3 and 4 can both be proved using the technique of modular functions as developed in section 2, Lemma 1 and 2.

It follows from the equation of \( E \) that \( y(R)^2/\pi \) is an algebraic integer and a \( p \)-unit.

We now consider the map

\[
\begin{align*}
h : G_Q &\to \hat{\mathcal{O}}_Q \\
M &\to y(M).
\end{align*}
\]

\[ (3-9) \]

**Proposition 2.**

i) The map \( h \) lies in \( \hat{\mathcal{O}}_Q \)

ii) Let \( \chi \in \hat{G} \) and \( M \in G_Q \), then

\[
(h|\chi)(M) \sim \begin{cases} 
\sqrt[2]{x(M)}, & \text{if } \chi \text{ is trivial} \\
x(M), & \text{otherwise}.
\end{cases}
\]

Proof. We first prove (ii). Since \( x \) is an even function and \( T_1 \) an odd function, we obtain from the definition of \( h \) and (3-4)
(h|\chi)(M) = \begin{cases} -\sqrt{t}x(m), & \text{if } \chi \text{ is the identity character} \\ T_1(m) & \text{otherwise} \end{cases}

where \( m \) is the parameter of \( M \) in \( \mathbb{C}/\mathbb{Q} \). Since \( m = \pm \rho \) we have \( T_1(m) = \pm D(\rho)x(M) \) and then, since \( D(\rho) \) is a unit, \( T_1(m) \sim x(M) \). We now prove i). By lemma 4 it is evident that \( h \in \mathcal{O}_Q \). Since

\[ \Lambda = 1_GO_L + (\pi^{-1}\sigma_G)O_L, \]

we need only check that \( h(\pi^{-1}\sigma_G) \in \mathcal{O}_Q \). For \( M \in G_Q \) we obtain

\[ h(\pi^{-1}\sigma_G)(M) = \pi^{-1}(h|\epsilon)(M) = -\pi^{-1}\sqrt{t} \cdot x(M) \]

where \( \epsilon \) is the identity character. Using Lemma 4 we conclude that \( h(\pi^{-1}\sigma_G)(M) \in \mathcal{O}_Q \). Hence \( h \) lies in \( \mathcal{O}_Q \).

\[ \square \]

Proof of Theorem 3. The proof is similar to that of Theorem 5 in [S-T]. We must show the equality locally. For each prime \( \mathfrak{p} \) of \( L \) we write

\[ \mathcal{O}_{Q,\mathfrak{p}} = \theta_{\mathfrak{p}}\Lambda_{\mathfrak{p}} \]

\[ (\sqrt{t}, \pi^{-1}\sigma_G)\Lambda_{\mathfrak{p}} = a_{\mathfrak{p}}\Lambda_{\mathfrak{p}} \]

where \( \theta_{\mathfrak{p}}(\text{resp.} a_{\mathfrak{p}}) \) belongs to \( \mathcal{O}_{Q,\mathfrak{p}}(\text{resp.} \Lambda_{\mathfrak{p}}) \). From Theorem 3 of [T] we know that for \( M \in G_Q \) and \( \chi \in G \) we have

\[ (\theta_{\mathfrak{p}}|\chi)(M) \sim \pi. \]

We let \( \chi \) act on \( L_{\mathfrak{p}}[G] \) by \( L_{\mathfrak{p}} \)-linearity. We first observe that \( \chi(\Lambda_{\mathfrak{p}}) = O_{L,\mathfrak{p}} \).

Then, by looking at \( \chi(\Lambda_{\mathfrak{p}}) \), we obtain

\[ \chi(a_{\mathfrak{p}}) \sim \begin{cases} 1, & \text{if } \chi \text{ is the identity character} \\ \sqrt{t}, & \text{otherwise.} \end{cases} \]

We now can write

\[ \theta_{\mathfrak{p}}(\sqrt{t}b_{\mathfrak{p}}) = ha_{\mathfrak{p}} \]

with \( b_{\mathfrak{p}} \in L_{\mathfrak{p}}[G] \). In order to prove the theorem we must show that \( b_{\mathfrak{p}} \in \Lambda_{\mathfrak{p}} \). Since \( h \in \mathcal{O}_{Q,\mathfrak{p}} \), \( \sqrt{t} \) and \( h(\pi^{-1}\sigma_G) \) lie in \( \mathcal{O}_{Q,\mathfrak{p}} \). We conclude from (3-10) that \( ha_{\mathfrak{p}} \in \mathcal{O}_{Q,\mathfrak{p}} \) and, from (3-13), that \( \sqrt{t}b_{\mathfrak{p}} \in \Lambda_{\mathfrak{p}} \).
For $\chi \in \hat{G}$ we consider the Lagrange resolvent of both sides of (3-13). We obtain

\begin{equation}
\sqrt{t}(\theta_{\mathfrak{P}}|\chi)\chi(b_{\mathfrak{P}}) = (h|\chi)\chi(a_{\mathfrak{P}}).
\end{equation}

Using Lemma 4, Proposition 2, (3-11) and (3-12), we deduce from (3-14) that $\chi(b_{\mathfrak{P}}) \sim 1$.

We now consider two cases.

Case 1. $\mathfrak{P} \nmid \sqrt{t}$. In this case $\sqrt{t}b_{\mathfrak{P}} \in \Lambda_{\mathfrak{P}}$ implies that $b_{\mathfrak{P}} \in \Lambda_{\mathfrak{P}}$; so $b_{\mathfrak{P}} \in \Lambda_{\mathfrak{P}}^*$, since $\chi(b_{\mathfrak{P}})$ is a unit for all $\chi \in \hat{G}$.

Case 2. $\mathfrak{P} | \sqrt{t}$. Since $\sqrt{t}$ is coprime with 2, $\mathfrak{P} \nmid 2$. Then $\Lambda_{\mathfrak{P}}$ is the unique maximal order and $b_{\mathfrak{P}} \in \Lambda_{\mathfrak{P}}^*$ since $\chi(b_{\mathfrak{P}})$ is a unit for all $\chi \in \hat{G}$.

Remark: If 2 splits in $(K/\mathbb{Q}), (2) = (\pi)(\overline{\pi})$ and $E$ denotes the Fueter minimal model

\[ y^2 + \sqrt{t}xy = x^3 + x, \]

then for any number field $L \supset K(\sqrt{t})$ and $G = E[\pi]$ we have that $E(L)_{\text{torsion}} \subset \text{Ker} \psi'$.

One can easily check that if $E[\pi^2] \subset E(L)$ then $E[4] \subset E(L)$ and we can use the results of section 2.

4. Examples

In this section we consider the set up of section 3 for the particular case of $K = \mathbb{Q}(\sqrt{-7})$.

We set $\pi = (1 + \sqrt{-7})/2$ and $2 = \pi \overline{\pi}$, where $\overline{\pi}$ is the complex conjugate of $\pi$. We note that the class number of $K$ is 1, $K(2) = K$ and $[K(4) : K] = 2$. Since $i \in K(t) = K(4)$ we must have $K(t) = K(i)$. Moreover, since $t^2 - 2^6$ is a unit in $K(2)$, we know that $t^2 - 2^6 = \pm 1$. The possibility $t^2 - 2^6 = 1$ contradicts the fact that $K(t) = K(i)$. Hence $t^2 = 63$ and $L = K(\sqrt{63})$; therefore $L$ is the splitting field of $X^4 - 63$.

We first determine the group kernel $D(\Lambda)$ considered in Theorem 2.

**Proposition 3.** $D(\Lambda) = \{1\}$.

**Proof.** By Theorem 2 we know that

\[ D(\Lambda) = (O_{L}/\overline{\pi}O_{L})^*/\text{Im} \ O_{L}^*. \]
It is easily checked that the ramification index of (2) in \( L \) is 4. Hence the group \((O_L/\pi O_L)^*\) is of order 8. We have to show that \( \text{Im}(O_L)^* \) also has order 8. Let \( \alpha = \sqrt[6]{3} \) and \( \beta = (1+i)\alpha \). We set \( u = (1-i)(1+\pi)+\alpha \), \( v = 1-3\alpha+\alpha^3/3 \) and \( w = 5-2\beta-12\pi-2\pi\beta \). We verify that

\[
\begin{align*}
u^2 &= iw, \quad u(5+2\beta-12\pi+2\pi\beta) = 1 \\
v(127+45\alpha+12\alpha^2+17\alpha^3/3) &= 1
\end{align*}
\]

Therefore \( u, v \) and \( w \) are all units of \( L \). We also have

\[
\begin{align*}
u^2 &\equiv i \mod \pi O_L, \quad v^2 \equiv 1 \mod \pi O_L \\
i^2 &\equiv 1 \mod \pi O_L
\end{align*}
\]

and

\[
\begin{align*}
i &\not\equiv 1 \mod \pi O_L, \quad v \not\equiv 1 \mod \pi O_L, \\
v &\not\equiv i \mod \pi O_L
\end{align*}
\]

Let \( \Phi \) be the quotient map

\[
\Phi : O_L \to (O_L/\pi O_L)
\]

It follows from (4-2) and (4-3) that \( \Phi(u) \) is of order 4 and that \( \Phi(v) \) doesn’t lie in the subgroup generated by \( \Phi(u) \). Hence we must have that the order of \( \text{Im}(O_L^*) \) is 8.

\[
\square
\]

We know from section 3 that

\[
L(E[\pi^2]) = L((t^2-2^6)^{1/4}) = L(\sqrt{i}).
\]

Therefore:

\[
E(L)_{\text{torsion}} \subset \text{Ker}\psi'.
\]

Hence, from Proposition 3, we conclude

**Corollary 3.**

\[
E(L)_{\text{torsion}} \subset \text{Ker}\psi.
\]

**REFERENCES**


Centre de Recherche en Mathématiques de Bordeaux
Université Bordeaux I
C.N.R.S. U.A. 226
U.F.R. de Mathématiques
351, cours de la Libération
33405 Talence Cedex, FRANCE

and

SPIC Science Fondation
East Coast Chambers
92 GN Chetty road
600017 Madras INDIA.