ON THE 2-ADIC LOGARITHM OF UNITS OF CERTAIN TOTALLY IMAGINARY QUARTIC FIELDS

JIANING LI

ABSTRACT. In this paper, we prove a result on the 2-adic logarithm of the fundamental unit of the field $\mathbb{Q}(\sqrt[4]{-q})$, where $q \equiv 3 \bmod 4$ is a prime. When $q \equiv 15 \bmod 16$, this result confirms a speculation of Coates-Li and has consequences for certain Iwasawa modules arising in their work.

1. INTRODUCTION

Let q be any prime $\equiv 3 \bmod 4$, and define

$$K = \mathbb{Q}(\sqrt{-q}), \quad F = K(\sqrt[4]{-q}).$$

Then there is a unique prime $\mathfrak{P}$ of F lying above 2 which is ramified in the extension $F/\mathbb{Q}$ (see Lemma 3 below), and we write $\mathrm{ord}_{\mathfrak{P}}$ for the usual order valuation at $\mathfrak{P}$. Moreover, K has odd class number, and it is not difficult to show that F also has odd class number (see Lemma 4 below). The unit group of F has rank 1, and we write η for a fundamental unit of F. We have $\eta \equiv 1 \bmod \mathfrak{P}$ when $q > 3$, so that the usual logarithmic series $\log_{\mathfrak{P}}(\eta)$ will converge in the completion $F_{\mathfrak{P}}$ of F at $\mathfrak{P}$ (see Lemma 4 below, where we also point out how to deal with the slightly exceptional case of $q = 3$). We shall use elementary arguments to prove the following result.

Theorem 1. *Let q be any prime $\equiv 3 \bmod 4$. Let η be a fundamental unit of F, and let $\mathfrak{P}$ be the unique ramified prime of F above 2. Then (1) If $q \equiv 3 \bmod 8$, we have $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) = 0$; (2) If $q \equiv 7 \bmod 16$, we have $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) = 2$; and (3) If $q \equiv 15 \bmod 16$, we have $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) \geq 4$.*

We first remark that assertions (1) and (2) can be viewed as an exact $\mathfrak{P}$-adic form of the Brauer-Siegel theorem as q varies. Secondly, our motivation for proving the above theorem came from a recent paper of J. Coates and Y. Li [1], which uses 2-adic arguments from Iwasawa theory to prove various non-vanishing theorems for the values at $s = 1$ of the complex L-series of certain elliptic curves with complex multiplication. In fact, the results in [1] are concerned with the field $F^* = \mathbb{Q}(\sqrt{-\sqrt{-q}})$, but we note that the fields F and F^* are isomorphic extensions of $\mathbb{Q}$, and so Theorem 1 remains valid with F^* replacing F. Assume first that $q \equiv 7 \bmod 8$, so that 2 splits in K, and let $\mathfrak{p}$ be the unique prime of K lying below $\mathfrak{P}$. By class field theory, there is a unique extension K_∞/K with Galois group $\mathrm{Gal}(K_\infty/K) \xrightarrow{\sim} \mathbb{Z}_2$, which is unramified outside the prime $\mathfrak{p}$. Define $F^*_\infty = F^* K_\infty$, and let $\Gamma = \mathrm{Gal}(F^*_\infty/F)$. Let $M(F^*_\infty)$ (resp. $M(F^*)$) denote the maximal abelian 2-extension of F^*_∞ (resp. F^*) which is unramified outside the primes of F^*_∞ (resp. F^*) lying above $\mathfrak{p}$. Let $X(F^*_\infty) = \mathrm{Gal}(M(F^*_\infty)/F^*_\infty)$. Now $M(F^*_\infty)$ is clearly a Galois extension of F^*, and hence, as always in Iwasawa theory [3], Γ will act on $X(F^*_\infty)$ by lifting inner automorphisms. Writing $X(F^*_\infty)_\Gamma$ for the Γ-coinvariants of $X(F^*_\infty)$, we see immediately that $X(F^*_\infty)_\Gamma = \mathrm{Gal}(M(F^*)/F^*_\infty)$. Moreover we have $X(F^*_\infty) = 0$ if and only if $X(F^*_\infty)_\Gamma = 0$. By global class field theory, the Galois group $\mathrm{Gal}(M(F^*)/F^*_\infty)$ is a finite group, and a classical theorem of Coates and Wiles (see [1, Theorem 8.2]) shows that

$$[M(F^*) : F^*_\infty] = 2^{(\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta))-2)/2}, \tag{1.1}$$

where η now denotes a fundamental unit of the field F^*. Now when $q \equiv 7 \bmod 16$, Coates and Li show in [1] by a simple Iwasawa theoretic argument based on Nakayama's lemma that $X(F^*_\infty) = 0$,

2010 *Mathematics Subject Classification.* 11R29, 11R27, 11R29.
Key words and phrases. 2-adic logarithm, units, class groups, pure quartic fields.

whence it follows from (1.1) that $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) = 2$. Based on numerical computations carried out by Zhibin Liang, they also conjecture in [1] that $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) \geq 4$ when $q \equiv 15 \bmod 16$, but say that they cannot prove this conjecture by the arguments of Iwasawa theory. Thus our theorem above confirms their conjecture, as well as giving a new and simple proof of their result when $q \equiv 7 \bmod 16$. In fact, when combined with the arguments from Iwasawa theory given in [1], our result shows that $X(F_\infty^*)$ is a free finitely generated $\mathbb{Z}_2$-module of strictly positive rank when $q \equiv 15 \bmod 16$. Let B be the abelian variety defined over K, which is the restriction of scalars from the Hilbert class field of K to K of the elliptic curve A, with complex multiplication by the ring of integers of K, which was first defined by Gross (an equation for this elliptic curve is recalled in [1], p. 1). Then in fact, when $q \equiv 15 \bmod 16$, our result shows that either $B(F_\infty^*)$ contains a point of infinite order, or the Tate-Shafarevich group of B/F_∞^* contains a copy of $\mathbb{Q}_2/\mathbb{Z}_2$. When $q \equiv 3 \bmod 8$, none of the above Iwasawa theoretic arguments remain literally valid, because 2 now remains prime in K. Nevertheless, we cannot help speculating whether assertion (1) of Theorem 1 for F^* could somehow be used to attack the non-vanishing Conjecture 1.8 of [1]. However, our theorem has the following consequence for primes $q \equiv 3 \bmod 8$.

Corollary 2. *Suppose $q \equiv 3 \bmod 8$. Let F_∞ be the compositum of all $\mathbb{Z}_2$-extensions of F. Let $M(F)$ denote the maximal abelian 2-extension of F which is unramified outside $\mathfrak{P}$. Then $M(F) = F_\infty$ and $\mathrm{Gal}(M(F)/F) \cong \mathbb{Z}_2^3$.*

We end this Introduction with two unrelated remarks. Firstly, the arguments used to prove Theorem 1 break down completely for primes $q \equiv 1 \bmod 4$, because then both K and F have even class numbers. Secondly, the elementary arguments given in the next section hinge on the following simple observations. Firstly, we use repeatedly the identity

$$\eta^2 \pm 1 = \eta(\eta \pm \eta^{-1}).$$

Secondly, since the prime $\mathfrak{P}$ has ramification index 2, we have $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(w)) = \mathrm{ord}_{\mathfrak{P}}(w-1)$ for any element of w of F with $\mathrm{ord}_{\mathfrak{P}}(w-1) > 2$.

2. Proofs

In this section, we present our elementary proof for Theorem 1. Next we prove Corollary 2 by using a standard result of class field theory. Finally, we give another very simple proof for Theorem 1(3) by the Coates-Wiles formula (1.1).

Lemma 3. *There exists a unique ramified prime ideal $\mathfrak{P}$ of F above 2 which has ramification index 2 in the extension $F/\mathbb{Q}$.*

Proof. A number field is ramified at a rational prime if and only if its Galois closure is ramified at that prime. It follows that $F/\mathbb{Q}$ is ramified at 2 since its Galois closure $F(\sqrt{-1})$ is clearly ramified at 2. If $q \equiv 3 \bmod 8$, then 2 is inert in K. Hence $\mathfrak{p} = 2\mathcal{O}_K$ must be ramified in F/K, with ramification index 2. Assume next that $q \equiv 7 \bmod 8$. Then 2 splits in K, say $2\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. The prime ideal $\mathfrak{p}$ induces an embedding from K to $\mathbb{Q}_2$. We fix the choice of $\sqrt{-q}$ such that $\sqrt{-q} \equiv 3 \bmod 8\mathbb{Z}_2$ when $q \equiv 7 \bmod 16$ and that $\sqrt{-q} \equiv 7 \bmod 8\mathbb{Z}_2$ when $q \equiv 15 \bmod 16$. Then $\mathfrak{p}$ is ramified in F. Note that $\bar{\mathfrak{p}}$ is inert in F when $q \equiv 7 \bmod 16$ and that $\bar{\mathfrak{p}}$ splits in F when $q \equiv 15 \bmod 16$. This proves the lemma. □

Lemma 4. (1)*Assume $q > 3$. Then the norm $N(\eta)$ of η from F to K is 1 and η is congruent to 1 modulo $\mathfrak{P}$.*

(2) *The class number h of F is odd.*

Proof. Note that $N(\eta)$ is a unit of K and hence $N(\eta) = \pm 1$. Since $q \equiv 3 \bmod 4$, the quadratic Hilbert symbol in the local field $\mathbb{Q}_q(\sqrt{-q})$

$$\left(\frac{-1, \sqrt{-q}}{\mathbb{Q}_q(\sqrt{-q})}\right) = \left(\frac{-1, q}{\mathbb{Q}_q}\right) = -1.$$

It follows that $-1 \notin N(F^\times)$. In particular, $N(\eta) = 1$.

If $q \equiv 7 \bmod 8$, then $\mathcal{O}_F/\mathfrak{P} \cong \mathbb{F}_2$ by the above lemma. Hence $\eta \equiv 1 \bmod \mathfrak{P}$ clearly. Suppose next that $q \equiv 3 \bmod 8$. Note that the polynomial $(x+1)^2 - \sqrt{-q}$ is Eisenstein in $K_{\mathfrak{p}}[x]$ where $K_{\mathfrak{p}} = \mathbb{Q}_2(\sqrt{3})$ is the completion of K at $\mathfrak{p} = 2\mathcal{O}_K$. It follows that the ring of integers of F is $\mathcal{O}_K[\sqrt[4]{-q}]$. Write $\eta = a + b\sqrt[4]{-q}$ with $a, b \in \mathcal{O}_K$. By (1), the conjugate of η is η^{-1} and hence $\eta + \eta^{-1} = 2a \equiv 0 \bmod \mathfrak{P}$. Thus $\eta \equiv 1 \bmod \mathfrak{P}$ by the structure of the finite field $\mathcal{O}_F/\mathfrak{P} = \mathbb{F}_4$. This proves (1).

For (2), we first note that K has odd class number by genus theory. The ambiguous class number formula [4, Chapter 13, Lemma 4.1] states that for a cyclic extension F/K of number fields, the order of the $\mathrm{Gal}(F/K)$-invariant subgroup of the ideal class group Cl_F of F is given by:

$$|\mathrm{Cl}_F^{\mathrm{Gal}(F/K)}| = |\mathrm{Cl}_K| \frac{\prod_v e_v}{[F:K][\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap N(F^\times)]}.$$

Here Cl_K is the ideal class group of K, the product runs over all the places of K and e_v is the ramification index of v in F/K. In our case, the ramified places are $\sqrt{-q}\mathcal{O}_K$ and $\mathfrak{p}$. Recall that $\mathfrak{p}$ is the prime of K lying below $\mathfrak{P}$. By (1), we know that $-1 \notin N(F^\times)$. Applying the above formula gives $2 \nmid |\mathrm{Cl}_F^{\mathrm{Gal}(F/K)}|$. Hence $2 \nmid h = |\mathrm{Cl}_F|$ by Nakayama's lemma. □

We remark that for $q = 3$, multiplying η by a third root of unity if needed, we can also assume that $\eta \equiv 1 \bmod \mathfrak{P}$.

Lemma 5. (1) *If* $q \equiv 3 \bmod 8$, *then* $\mathrm{ord}_{\mathfrak{P}}(\eta + \eta^{-1}) = \mathrm{ord}_{\mathfrak{P}}(\eta - \eta^{-1}) = 2$*;*
(2) *If* $q \equiv 7 \bmod 16$, *then* $\mathrm{ord}_{\mathfrak{P}}(\eta + \eta^{-1}) = 4$.
(3) *If* $q \equiv 15 \bmod 16$, *then* $\mathrm{ord}_{\mathfrak{P}}(\eta + \eta^{-1}) \geq 6$.

Proof of Lemma 5. The ideas of the proofs are the same for all cases. We first consider the case $q \equiv 3 \bmod 8$ which is slightly easier to handle. If $q = 3$, then $\eta = \frac{\sqrt{-3}+1}{2} - \sqrt[4]{-3}$, and it is readily verified that (1) holds. Assume now that $q > 3$. We have $\mathfrak{p} = 2\mathcal{O}_K = \mathfrak{P}^2$. Then $\mathfrak{P} = \gamma\mathcal{O}_F$ for some $\gamma \in \mathcal{O}_F$ since the class number h of F is odd. It follows that $\frac{\gamma^2}{2}$ is a unit of $\mathcal{O}_F$. Thus $\frac{\gamma^2}{2} = \pm\eta^k$ for some integer k. We claim that k is odd. Indeed, if k is even, we would have that $(\gamma\eta^{-k/2})^2 = \pm 2$, whence $F = K(\sqrt{\pm 2})$, which is a contradiction. This proves the claim. By replacing γ by $\gamma\eta^{-\frac{k-1}{2}}$, we may assume that $\frac{\gamma^2}{2}$ is the fundamental unit η. In the proof of part (2) of Lemma 4, we have shown that $\mathcal{O}_F = \mathcal{O}_K[\sqrt[4]{-q}]$. Thus we can write $\gamma = a + b\sqrt[4]{-q}$ with $a, b \in \mathcal{O}_K$, whence

$$\eta = \frac{a^2 + b^2\sqrt{-q}}{2} + ab\sqrt[4]{-q} \quad \text{and} \quad N(\gamma) = a^2 - b^2\sqrt{-q} = \pm 2.$$

In fact, one can show that $N(\gamma) = -2$ by computing the Hilbert symbols of -2 and $\sqrt{-q}$, but we will not need this finer result. We need to calculate $a \bmod 2 \in \mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_4$. It is easy to see that $a \not\equiv 0 \bmod 2\mathcal{O}_K$. We claim that $a \not\equiv 1 \bmod 2\mathcal{O}_K$. Note that $\sqrt{-q} \equiv 1 \bmod 2\mathcal{O}_K$. It follows that $a^2 \equiv b^2 \bmod 2\mathcal{O}_K$. Suppose $a \equiv 1 \bmod 2\mathcal{O}_K$. Then $a^2 \equiv b^2 \equiv 1 \bmod 4\mathcal{O}_K$. This contradicts to the equality $N(\gamma) = \pm 2$ and this proves the claim. Since $a \not\equiv 1 \bmod 2\mathcal{O}_K$, we have $a^2 + 1 \not\equiv 0 \bmod 2\mathcal{O}_K$ by the structure of the finite field $\mathbb{F}_4$. Since $N(\eta) = 1$, the conjugate of η is η^{-1}. We then have $\mathrm{ord}_{\mathfrak{P}}(\eta + \eta^{-1}) = \mathrm{ord}_{\mathfrak{P}}(a^2 + b^2\sqrt{-q}) = \mathrm{ord}_{\mathfrak{P}}(2(a^2+1)) = 2$ and $\mathrm{ord}_{\mathfrak{P}}(\eta - \eta^{-1}) = \mathrm{ord}_{\mathfrak{P}}(2ab\sqrt[4]{-q}) = 2$. This completes the proof for $q \equiv 3 \bmod 8$.

Now we assume $q \equiv 7 \bmod 8$ in the rest of the proof. We have $\mathfrak{P}^h = \gamma\mathcal{O}_F$ for some $\gamma \in \mathcal{O}_F$. Put $\pi = N(\gamma) \in \mathcal{O}_K$. The equalities of ideals $\mathfrak{p}^h\mathcal{O}_F = \mathfrak{P}^{2h} = \pi\mathcal{O}_F = \gamma^2\mathcal{O}_F$ gives a unit $\frac{\gamma^2}{\pi}$ of F. We have $\frac{\gamma^2}{\pi} = \pm\eta^k$ for some odd integer k, for the same reason as in the case $q \equiv 3 \bmod 8$. As $\eta \equiv 1 \bmod \mathfrak{P}$, we have $\mathrm{ord}_{\mathfrak{P}}(\pm\eta^k \pm \eta^{-k}) = \mathrm{ord}_{\mathfrak{P}}(\eta + \eta^{-1})$. We may assume that $\frac{\gamma^2}{\pi}$ is the fundamental unit η. Write $\gamma = a + b\sqrt[4]{-q}$ with $a, b \in K$. Then

$$\eta = \frac{a^2 + \sqrt{-q}b^2}{\pi} + \frac{2ab\sqrt[4]{-q}}{\pi} \quad \text{and} \quad a^2 - \sqrt{-q}b^2 = \pi.$$

From now on, we work in $F_{\mathfrak{P}}$, which is a quadratic extension of $K_{\mathfrak{p}} = \mathbb{Q}_2$. Recall that as in the proof of Lemma 3, the embedding induced by $\mathfrak{p}$ is chosen so that $\sqrt{-q} \equiv 3 \bmod 8$ when $q \equiv 7 \bmod 16$ and that $\sqrt{-q} \equiv 7 \bmod 8$ when $q \equiv 15 \bmod 16$. Note that the ring of integers of $F_{\mathfrak{P}}$ is $\mathbb{Z}_2[\sqrt[4]{-q}]$. Since γ is integral in $F_{\mathfrak{P}}$, we have $a, b \in \mathbb{Z}_2$. Since $\mathrm{ord}_{\mathfrak{p}}(\pi) = h$, we can write $\pi = 2^h u$ with $u \in \mathbb{Z}_2^\times$. Note that one must have $\mathrm{ord}_2(a) = \mathrm{ord}_2(b)$. Otherwise, the valuation of $\pi = N_{F_{\mathfrak{P}}/K_{\mathfrak{p}}}(a + b\sqrt[4]{-q})$ at 2 is even which contradicts to the fact that h is odd. Also note that if $c, d \in \mathbb{Z}_2^\times$, then $N_{F_{\mathfrak{P}}/K_{\mathfrak{p}}}(c+d\sqrt[4]{-q}) \equiv 2 \bmod 4\mathbb{Z}_2$. It follows that $\mathrm{ord}_2(a) = \mathrm{ord}_2(b) = (h-1)/2$. Because $\pi = N_{F_{\mathfrak{P}}/K_{\mathfrak{p}}}(\gamma)$ is a norm, we conclude the following values of the Hilbert symbols

$$\Big(\frac{2^h u, \sqrt{-q}}{K_{\mathfrak{p}}}\Big) = \Big(\frac{2u, 3}{\mathbb{Q}_2}\Big) = 1 \text{ if } q \equiv 7 \bmod 16$$

and

$$\Big(\frac{2^h u, \sqrt{-q}}{K_{\mathfrak{p}}}\Big) = \Big(\frac{2u, 7}{\mathbb{Q}_2}\Big) = 1 \text{ if } q \equiv 15 \bmod 16.$$

This implies that $u \equiv 3 \bmod 4$ if $q \equiv 7 \bmod 16$ and that $u \equiv 1 \bmod 4$ if $q \equiv 15 \bmod 16$. Thus

$$\frac{\eta + \eta^{-1}}{2} = \frac{a^2 + \sqrt{-q}b^2}{\pi} = \frac{2a^2 - \pi}{\pi} = (\frac{a}{2^{\frac{h-1}{2}}})^2 u^{-1} - 1 \equiv u^{-1} - 1 \equiv \begin{cases} 2 \bmod 4 & \text{if } q \equiv 7 \bmod 16, \\ 0 \bmod 4 & \text{if } q \equiv 15 \bmod 16. \end{cases}$$

This finishes the proof of Lemma 5 by the fact $\mathrm{ord}_{\mathfrak{P}}(2) = 2$. □

Proof of Theorem 1. As we mentioned in the end of the introduction, the basic fact that $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(x)) = \mathrm{ord}_{\mathfrak{P}}(x-1)$ if $\mathrm{ord}_{\mathfrak{P}}(x-1) > 2$ will be used. For a proof, see [5, Lemma 5.5]. Assume $q \equiv 3 \bmod 8$. Then $\mathrm{ord}_{\mathfrak{P}}(\eta^2+1) = \mathrm{ord}_{\mathfrak{P}}(\eta^2 + \eta\eta^{-1}) = \mathrm{ord}_{\mathfrak{P}}(\eta + \eta^{-1}) = 2$ and $\mathrm{ord}_{\mathfrak{P}}(\eta^2 - 1) = \mathrm{ord}_{\mathfrak{P}}(\eta^2 - \eta\eta^{-1}) = \mathrm{ord}_{\mathfrak{P}}(\eta - \eta^{-1}) = 2$. Hence $\mathrm{ord}_{\mathfrak{P}}(\eta^4 - 1) = 4$. This gives $\mathrm{ord}_{\mathfrak{P}} \log_{\mathfrak{P}}(\eta^4) = 4$. Thus $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) = \mathrm{ord}_{\mathfrak{P}} \log_{\mathfrak{P}}(\eta^4) - \mathrm{ord}_{\mathfrak{P}}(4) = 0$. This proves (1).

Assume $q \equiv 7 \bmod 16$. We have $\mathrm{ord}_{\mathfrak{P}}(\eta^2+1) = \mathrm{ord}_{\mathfrak{P}}(\eta^2 + \eta\eta^{-1}) = \mathrm{ord}_{\mathfrak{P}}(\eta + \eta^{-1}) = 4$. Then $\mathrm{ord}_{\mathfrak{P}}(\eta^2 - 1) = \mathrm{ord}_{\mathfrak{P}}(\eta^2 + 1 - 2) = \mathrm{ord}_{\mathfrak{P}}(2) = 2$. This gives $\mathrm{ord}_{\mathfrak{P}}(\eta^4 - 1) = 6$. Thus $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta^4)) = \mathrm{ord}_{\mathfrak{P}}(\eta^4 - 1) = 6$. Hence $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) = 6 - \mathrm{ord}_{\mathfrak{P}}(4) = 2$. This proves (2).

Assume $q \equiv 15 \bmod 16$. Then $\mathrm{ord}_{\mathfrak{P}}(\eta^4 - 1) = \mathrm{ord}_{\mathfrak{P}}(\eta^2 + 1) + \mathrm{ord}_{\mathfrak{P}}(\eta^2 - 1) \geq 6 + 2 = 8$. Then $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta^4)) = \mathrm{ord}_{\mathfrak{P}}(\eta^4 - 1) \geq 8$. Thus $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) \geq 4$. This completes the proof of Theorem 1. □

Now, we prove Corollary 2, and we begin by recalling a classical result from global class field theory. Let L be any number field, and p be a prime number. For a prime ideal v of L, let $U_{1,v}$ denote the principal units in the completion L_v of L, and put $U_1 = \prod_{v|p} U_{1,v}$. Let ϕ be the canonical embedding $L \hookrightarrow \prod_{v|p} L_v$. Denote by $\mathcal{E}_1$ the group of global units of L whose images lie in U_1, and let $\overline{\phi(\mathcal{E}_1)}$ denote the closure of $\phi(\mathcal{E}_1)$ in U_1 under the p-adic topology. Let H be the p-Hilbert class field of L. Finally let $M(L)$ be the maximal abelian p-extension of L, which is unramified outside the primes of L lying above p. Then the Artin map induces an isomorphism

$$U_1/\overline{\phi(\mathcal{E}_1)} \cong \mathrm{Gal}(M(L)/H).$$

This is a standard consequence of global class field theory (see, for example, [5, Theorem 13.4]). Note that U_1 is a finitely generated $\mathbb{Z}_p$-module of rank $[L : \mathbb{Q}]$. Moreover, the $\mathbb{Z}_p$-module $\overline{\phi(\mathcal{E}_1)}$ has rank $\leq r_1 + r_2 - 1$, and Leopoldt's conjecture asserts that this rank is always equal to $r_1 + r_2 - 1$; here r_1 and r_2 are the number of real and complex places of L, respectively.

Proof of Corollary 2. We apply the above isomorphism to the field F with $q \equiv 3 \bmod 8$ and the prime 2. In this case, $U_1 = 1 + \mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}}$ has $\mathbb{Z}_2$-rank $[F : \mathbb{Q}] = 4$, and $\overline{\phi(\mathcal{E}_1)} = \overline{\langle \eta, -1 \rangle}$ clearly has $\mathbb{Z}_2$-rank 1. Moreover, the 2-Hilbert class field of F is F itself since F has odd class number by Lemma 4. Thus we obtain an isomorphism of $\mathbb{Z}_2$-modules

$$(1 + \mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}})/\overline{\langle \eta, -1 \rangle} \cong \mathrm{Gal}(M(F)/F).$$

In order to prove $M(F) = F_\infty$, it suffices to show that there is no nontrivial torsion element in the group on the left. Consider the commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & \{\pm 1\} \arrow[r] \arrow[d] & \overline{\phi(\mathcal{E}_1)} \arrow[r, "\log_{\mathfrak{P}}"] \arrow[d] & \mathbb{Z}_2 \log_{\mathfrak{P}}(\eta) \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \mu(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}}) \arrow[r] & 1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}} \arrow[r, "\log_{\mathfrak{P}}"] & \log_{\mathfrak{P}}(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}}) \arrow[r] & 0. \end{tikzcd}$$

Here $\mu(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}})$ is the group of roots of unity in $1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}}$ which equals $\{\pm 1\}$ as one can check that $\sqrt{-1} \notin F_{\mathfrak{P}}$. Thus the logarithm induces an isomorphism

$$(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}})/\overline{\langle \eta, -1\rangle} \cong \log_{\mathfrak{P}}(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}})/\mathbb{Z}_2 \log_{\mathfrak{P}}(\eta).$$

Since $\mathrm{ord}_{\mathfrak{P}}(2) = 2$, it is clear from the logarithmic series that $\log_{\mathfrak{P}}(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}}) \subset \mathcal{O}_{F_{\mathfrak{P}}}$. We claim that the $\mathbb{Z}_2$-module $\log_{\mathfrak{P}}(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}})/\mathbb{Z}_2 \log_{\mathfrak{P}}(\eta)$ is free. Suppose not. Then there exists an element a in $\log_{\mathfrak{P}}(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}}) \subset \mathcal{O}_{F_{\mathfrak{P}}}$ but not in $\mathbb{Z}_2 \log_{\mathfrak{P}}(\eta)$ such that $2a \in \mathbb{Z}_2 \log_{\mathfrak{P}}(\eta)$. Write $2a = r \log_{\mathfrak{P}}(\eta)$ with $r \in \mathbb{Z}_2$. Note that r must be in $\mathbb{Z}_2^\times$. This would give $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) = \mathrm{ord}_{\mathfrak{P}}(2a) > 0$ which contradicts to Theorem 1. Thus we have that $\mathrm{Gal}(M(F)/F) \cong \log_{\mathfrak{P}}(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}})/\mathbb{Z}_2 \log_{\mathfrak{P}}(\eta)$ is a free $\mathbb{Z}_2$-module of rank 3 and hence $M(F) = F_\infty$. This completes the proof. □

We end this paper by noting a second and very simple proof of Theorem 1(3). Suppose $q \equiv 7 \bmod 8$, so that 2 splits in K, and recall that $\mathfrak{p}$ is the restriction of $\mathfrak{P}$ to K. As before, let $M(F)$ be the maximal abelian 2-extension which is unramified outside $\mathfrak{P}$. By class field theory and the fact that F has odd class number [2, Theorem 11], we have

$$(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}})/\overline{\langle \eta, -1\rangle} \cong \mathrm{Gal}(M(F)/F).$$

Suppose now $q \equiv 15 \bmod 16$. The embedding $K \hookrightarrow K_{\mathfrak{p}} = \mathbb{Q}_2$ induced by $\mathfrak{p}$ makes that $\sqrt{-q} \equiv -1 \bmod 8$ whence $F_{\mathfrak{P}} = \mathbb{Q}_2(\sqrt{-1})$. Clearly $\sqrt{-1}$ is in $1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}}$ but not in $\overline{\langle \eta, -1\rangle}$. Thus $\mathrm{Gal}(M(F)/F)$ has an element of order 2. Now let $F_\infty = FK_\infty$, where K_∞ is the unique $\mathbb{Z}_2$-extension of K unramified outside $\mathfrak{p}$. Since $\mathrm{Gal}(F_\infty/F)$ is a free $\mathbb{Z}_2$-module of rank 1, it follows that $\mathrm{Gal}(M(F)/F_\infty)$ must contain the element of order 2, and so $\mathrm{Gal}(M(F)/F_\infty) \neq 0$. By the formula (1.1) of Coates-Wiles, it follows that we must have $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) \geq 4$, as required.

Acknowledgments

The author thanks Professor John Coates and Yongxiong Li for their carefully reading of this paper and helpful suggestions. The author is supported by the Fundamental Research Funds for the Central Universities (No. WK0010000058), NSFC (Grant No. 11571328) and by the Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200).

References

[1] J. Coates and Y. Li. *Non-vanishing theorems for central L-values of some elliptic curves with complex multiplication,* arXiv:1811.07595v3(2020).

[2] J. Coates, A. Wiles. *Kummer's criterion for Hurwitz numbers,* Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), Japan Soc. Promotion Sci. Tokyo, (1977), 9-23.

[3] K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2) 98 (1973), 246-326.

[4] S. Lang, *Cyclotomic fields I and II*, Graduate Texts in Mathematics **121**, Springer, 1990.

[5] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics **83**, Springer, 1997.

CAS Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, China

E-mail address: lijn@ustc.edu.cn