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

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

Then there is a unique prime $\mathfrak{P}$ of F lying above 2 which is ramified in the extension $F/\mathbb{Q}$ 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 2.2 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 2.2 below, where we also point out how to deal with the slightly exceptional case of $q = 3$). In this paper, we shall prove the following result.

Theorem 1.1. *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 $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) \geq 6$.*

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 1.1 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 [5], 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, class field theory.

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 1.1 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 1.2. *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 $\mathrm{Gal}(M(F)/F) \cong \mathbb{Z}_2^3$.*

The proof of (1) and (2) of Theorem 1.1 is elementary and will be present in §2. In [4, Remark 3.2], Gras also presents some numerical data for our theorem, and he remarks that one can prove the statements (1) and (2) of the Theorem 1.1 by using his fixed points formula. Our elementary argument also works when $q \equiv 15 \bmod 16$. However, in this case that argument only gives $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) \geq 4$. In §3, we use a more complicated method to prove Theorem 1.1(3) which studies various surrounding extensions of F and K.

2. Preliminaries and proofs of Theorem 1.1(1) and (2)

In this section, we present our elementary proof for Theorem 1.1. Although the results are about units, the class groups will play important roles in the whole arguments. We first review Chevalley's ambiguous class number formula which will be used later, mostly in the next section. For a number field L, let Cl_L denote its class group. Suppose S is a finite set of prime ideals of L, the S-class group is defined as

$$\mathrm{Cl}_{L,S} := \mathrm{Cl}_L/\langle \text{ideal classes generated by primes of } S\rangle.$$

Alternatively, $\mathrm{Cl}_{L,S}$ is isomorphic to the class group of the ring $\mathcal{O}_{L,S}$ of S-integers of L. Suppose M/L is a cyclic extension of number fields with Galois group G. The S-class group $\mathrm{Cl}_{M,S}$ of M is Cl_{M,S_M} where S_M is the set of primes of M lying above those of S. Chevalley's ambiguous class number states that the order of the G-invariant subgroup of $\mathrm{Cl}_{M,S}$ is given by

$$|\mathrm{Cl}_{M,S}^G| = |\mathrm{Cl}_{L,S}| \frac{\prod_{v\in S} e_v f_v \prod_{v\notin S} e_v}{[M:L][\mathcal{O}_{L,S}^\times : \mathcal{O}_{L,S}^\times \cap N_{M/L}(M^\times)]}. \tag{2.1}$$

Here the second product runs over the places of L which are not in S, e_v and f_v are the ramification index and the residue degree of v respectively, $\mathcal{O}_{L,S}^\times$ is the group of S-units of L, and $N_{M/L}$ is the norm map. For a proof of this formula, see [6] for example. For our applications, the degree $[M:L] = \ell^n$ is always a prime power, where ℓ is a prime. We will frequently use the simple fact that

$$\ell \nmid |\mathrm{Cl}_{M,S}| \text{ if and only if } \ell \nmid |\mathrm{Cl}_{M,S}^G|.$$

This can be proved easily by counting the orbits of the G-action or by Nakayama's lemma. The unit index in (2.1) can be computed by Hilbert symbols provided that M/L is a Kummer extension. More precisely, we have:

Proposition 2.1. *Let* $\mathrm{Ram}(M/L)$ *be the set of places of* L *which are ramified in* M/L*. Let* $d = [M : L]$*. Assume* $\mu_d \subset L$ *so that* $M = L(\sqrt[d]{a})$ *for some* $a \in L$*. Define*

$$\rho : \mathcal{O}_{L,S}^\times/(\mathcal{O}_{L,S}^\times)^d \longrightarrow \prod_{v \in S \cup \mathrm{Ram}} \mu_d$$
$$x \longmapsto \left(\left(\frac{x, a}{v}\right)\right)_{v \in S \cup \mathrm{Ram}}.$$

Then

(1) $\mathrm{Ker}(\rho) = \mathcal{O}_{L,S}^\times \cap N_{M/L}(M^\times)/(\mathcal{O}_{L,S}^\times)^d$ *and hence* $|\mathrm{Im}(\rho)| = [\mathcal{O}_{L,S}^\times : \mathcal{O}_{L,S}^\times \cap N_{M/L}(M^\times)]$*;*

(2) $\mathrm{Im}(\rho) \subset (\prod_{v \in S \cup \mathrm{Ram}} \mu_d)^{\Pi=1}$ *where the latter is the kernel of the product map; in particular,* $|\mathrm{Im}(\rho)| \leq d^t$ *where* $t = |S \cup \mathrm{Ram}|$*.*

Proof. This result is a standard direct consequence of local class field theory, Hasse's norm theorem, and the product formula for Hilbert symbols. □

Next, we present our elementary proof of Theorem 1.1(1) and (2). We recall that $q \equiv 3 \bmod 4$ is a prime, $K = \mathbb{Q}(\sqrt{-q})$ and $F = \mathbb{Q}(\sqrt[4]{-q})$. The elementary argument crucially relies on the fact that F has odd class number so that one can produce the fundamental unit of F from the ramified primes. The argument also hinges 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 $\mathrm{ord}_{\mathfrak{P}}(w-1) > 2$.

Lemma 2.2. (1) *There exists a unique ramified prime ideal* $\mathfrak{P}$ *of* F *above* 2 *which has ramification index* 2 *in the extension* $F/\mathbb{Q}$*.*

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

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

Proof. (1). 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 $F(i)$ 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 (1).

(2). 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 $q \equiv 3 \bmod 8$. 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 (2).

(3). We first note that K has odd class number by genus theory. Then applying Chevalley's formula (2.1) 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 2.3. (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 2.3. 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 2.2, 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 2.2(1), 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:

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

and

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

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

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

This finishes the proof of Lemma 2.3 by the fact $\mathrm{ord}_{\mathfrak{P}}(2) = 2$. We record an additional result here on Hilbert symbols in the case of $q \equiv 15 \bmod 16$ which will be used in the next section. Note that when $q \equiv 15 \bmod 16$, we proved that $2u \equiv 2 \bmod 8$. It follows that we have

$$\left(\frac{\pi, 3}{\mathfrak{p}}\right) = \left(\frac{2u, 3}{\mathbb{Q}_2}\right) = \left(\frac{2, 3}{\mathbb{Q}_2}\right) = -1. \tag{2.2}$$

□

Proof of Theorem 1.1(1) and (2). As we mentioned, the 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 of this basic fact, see [7, 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 $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) = \mathrm{ord}_{\mathfrak{P}} \log_{\mathfrak{P}}(\eta^4) - \mathrm{ord}_{\mathfrak{P}}(4) = 0$.

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 (1) and (2) and completes our main task in this section.

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 $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) \geq 4$. □

Note that the above elementary method only shows that $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) \geq 4$ when $q \equiv 15 \bmod 16$ and we will use various technique to show that one indeed has $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) \geq 6$ in the next section. Now, we prove Corollary 1.2, 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, [7, 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 1.2. 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

$$(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}})/\overline{\langle \eta, -1\rangle} \cong \mathrm{Gal}(M(F)/F). \tag{2.3}$$

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 $i \notin F_{\mathfrak{P}}$. 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 1.1. 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. □

3. Proof of Theorem 1.1(3)

Let $q \equiv 15 \bmod 16$. In this section, we prove Theorem 1.1(3). We keep the notation of the last section. We also recall some facts and define some new notation:

- Recall that 2 splits in K: $2\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ and that $\mathfrak{p}$ is ramified in F: $\mathfrak{p}\mathcal{O}_F = \mathfrak{P}^2$ and $\bar{\mathfrak{p}}$ splits in F: $\bar{\mathfrak{p}}\mathcal{O}_F = \bar{\mathfrak{P}}_1\bar{\mathfrak{P}}_2$.
- Let S denote the singleton set $\{\mathfrak{p}\}$ in this section.
- For any finite extension M of K, let S_M be the set of primes lying above $S = \{\mathfrak{p}\}$. We let $\mathrm{Cl}_{M,S} := \mathrm{Cl}_{M,S_M}$, $\mathcal{O}_{M,S} = \mathcal{O}_{M,S_M}$ for ease of the notation.
- Recall that h is the class number of F, γ is a generator of $\mathfrak{P}^h$ and $\pi = N_{F/K}(\gamma)$ is a generator of $\mathfrak{p}$. We proved that the fundamental η coincides with γ^2/π up to an element of $(\mathcal{O}_F^\times)^2$.
- Let $E = F(\sqrt[8]{-q})$, $K' = K(i)$, $F' = F(i)$ and $E' = E(i)$.
- If v is a place of a number field M, we denote by ι_v the induced embedding from M to its completion M_v.
- $M(F)$ is the maximal abelian 2-extension of F which is unramified outside $\mathfrak{P}$.
- $F_\infty = FK_\infty$, where K_∞ is the unique $\mathbb{Z}_2$-extension of K unramified outside $\mathfrak{p}$.

We divide the proof into two subsections. In the first one, we reduce the Theorem to certain results on $\mathrm{Cl}_{E,S}$. In the second subsection, we prove the desired results on $\mathrm{Cl}_{E,S}$ by studying the quadratic extension E'/E and the cyclic quartic extension E'/K'.

3.1. The relation between $\log_{\mathfrak{P}}(\eta)$ and $\mathrm{Cl}_{E,S}$.

The main result of this subsection is Proposition 3.2. We first compute the 2-rank of the Galois group $\mathrm{Gal}(M(F)/F)$. Let $\hat{F}_2$ be the subfield of $M(F)$ which is fixed by $2\mathrm{Gal}(M(F)/F)$. Note that $\hat{F}_2$ is the maximal abelian extension of F of exponent 2, which is unramified outside $\mathfrak{P}$.

Proposition 3.1. (1) *$\hat{F}_2 = F(\sqrt{\eta}, \sqrt{\gamma})$ for some suitable choice of the sign of η and γ. Moreover, we have $\sqrt{\eta} \in F_\infty$ and $\sqrt{\gamma} \notin F_\infty$;*

(2) *$\mathrm{Gal}(M(F)/F)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}/2^t\mathbb{Z}$ and $\mathrm{Gal}(M(F)/F_\infty)$ is isomorphic to $\mathbb{Z}/2^t\mathbb{Z}$ for some $t \geq 1$.*

Proof. Our elementary argument in §2 shows $\mathrm{ord}_{\mathfrak{P}}(\log_{\mathfrak{P}}(\eta)) \geq 4$ and hence $[M(F) : F_\infty] \geq 2$ by the Coates-Wiles formula (1.1). This shows that

$$\mathrm{Gal}(\hat{F}_2/F) \cong (\mathbb{Z}/2\mathbb{Z})^k \text{ for some } k \geq 2. \tag{3.1}$$

Let $I_{F,S}$ denote the group of fraction ideals of F which are coprime to $\mathfrak{P}$. Let $\mathrm{Sel}_S(F) = \{a \in F | (a)\mathcal{O}_{F,S} = I^2$ for some ideal $I \in I_{F,S}\}$. By Kummer theory, $\hat{F}_2$ is contained in $F(\sqrt{\mathrm{Sel}_S(F)})$. There is a well known exact sequence

$$0 \to \mathcal{O}_{F,S}^\times/(\mathcal{O}_{F,S}^\times)^2 \to \mathrm{Sel}_S(F) \to \mathrm{Cl}_{F,S}[2] \to 0.$$

Since the class number of F is odd, we have $\mathrm{Cl}_{F,S}[2] = 0$ in particular. On the other hand, $\mathcal{O}_{F,S}^\times/(\mathcal{O}_{F,S}^\times)^2$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$ and is clearly generated by $\{-1, \eta, \gamma\}$. Thus $\hat{F}_2 \subset F(i, \sqrt{\eta}, \sqrt{\gamma})$. However, $F(i)/F$ is ramified at $\bar{\mathfrak{P}}_1$ and $\bar{\mathfrak{P}}_2$, since the local field extension at $\bar{\mathfrak{P}}_i$ is $\mathbb{Q}_2(i)/\mathbb{Q}_2$ for $i = 1, 2$. Therefore, $\hat{F}_2 \subset F(\sqrt{\eta^*}, \sqrt{\gamma^*})$ where $\eta^* = \eta$ or $-\eta$ and $\gamma^* = \gamma$ or $-\gamma$. This implies that

$$\mathrm{Gal}(\hat{F}_2/F) \cong (\mathbb{Z}/2\mathbb{Z})^k \text{ for some } k \leq 2. \tag{3.2}$$

By (3.1), the above inequality is in fact an equality. We may assume that the signs of γ and η are chosen suitably so that

$$\hat{F}_2 = F(\sqrt{\eta}, \sqrt{\gamma}).$$

To prove $\sqrt{\eta} \in F_\infty$, consider the isomorphism from class field theory as in (2.3):

$$1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}/\{\pm 1\} \cong \mathrm{Gal}(M(K)/K).$$

Here $M(K)$ is the maximal abelian 2-extension of K which is unramified outside $S = \{\mathfrak{p}\}$. The isomorphism uses the fact that the class number of K is odd. Note that $1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}/\{\pm 1\} \cong \mathbb{Z}_2$ whence

$M(K) = K_\infty$. Since $\eta = \gamma^2/\pi$ up to a square, we have $K(\sqrt{\eta}) = K(\sqrt{\pi})$ is a quadratic extension of K. Clearly $K(\sqrt{\eta})$ is unramified outside $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. In fact the extension $K(\sqrt{\eta})/K$ is also unramified outside $\bar{\mathfrak{p}}$ since $F(\sqrt{\eta})/K$ is. This shows that $\sqrt{\eta} \in K_\infty \subset F_\infty$ and this finishes the proof of (1).

(2). Since F has odd class number, as before, the Artin map induces an isomorphism

$$\phi : (1 + \mathfrak{P}\mathcal{O}_{F_\mathfrak{P}})/\overline{\langle -1, \eta\rangle} \cong \mathrm{Gal}(M(F)/F). \tag{3.3}$$

Here $\overline{\langle -1, \eta\rangle}$ is the closure of $\langle -1, \eta\rangle$ and clearly has $\mathbb{Z}_2$-rank 1. Note that $1 + \mathfrak{P}\mathcal{O}_{F_\mathfrak{P}}$ has $\mathbb{Z}_2$-rank 2 whence $\mathrm{Gal}(M(F)/F)$ is a finite generated $\mathbb{Z}_2$-module of rank 1. By (3.1) and (3.2), the 2-rank of $\mathrm{Gal}(M(F)/F)$ is 2. This shows that there exists a positive integer t such that

$$\mathrm{Gal}(M(F)/F) \cong \mathbb{Z}_2 \times \mathbb{Z}/2^t\mathbb{Z}.$$

Hence its torsion subgroup $\mathrm{Gal}(M(F)/F_\infty) \cong \mathbb{Z}/2^t\mathbb{Z}$. This completes the proof. □

Proposition 3.2. *The following statements are equivalent:*

(1) *Theorem 1.1(3) holds;*

(2) *The Galois group* $\mathrm{Gal}(M(F)/F_\infty)$ *is isomorphic to* $\mathbb{Z}/2^k\mathbb{Z}$ *for some* $k \geq 2$*;*

(3) *The quadratic Hilbert symbol* $\left(\dfrac{i, \gamma}{\mathfrak{P}}\right)$ *is trivial;*

(4) *The* 2*-primary part of* $\mathrm{Cl}_{E,S}$ *is zero if* $q \equiv 15 \bmod 32$ *and nonzero if* $q \equiv 31 \bmod 32$*.*

Proof. (1)⇔(2). This is done by the Coates-Wiles formula (1.1) and by Proposition 3.1(2).

(2)⇔(3). Note that $\mathcal{O}_{F_\mathfrak{P}} = \mathbb{Z}_2[i]$ and i is clearly an element of order 2 in the left hand side of the isomorphism (3.3). It follows that $\phi(i)$ is an element of order 2 in $\mathrm{Gal}(M(F)/F_\infty) \subset \mathrm{Gal}(M(F)/F)$. We remark that this observation gives a second proof of $[M(F) : F_\infty] > 1$, or equivalently, $\mathrm{ord}_\mathfrak{P}(\log_\mathfrak{P}(\eta)) \geq 4$. Since $\mathrm{Gal}(M(F)/F_\infty)$ is cyclic, we have $|\mathrm{Gal}(M(F)/F_\infty)|$ is divisible by 4 if and only if $\phi(i) \in 2\mathrm{Gal}(M(F)/F_\infty) \subset 2\mathrm{Gal}(M(F)/F)$; or equivalently, $\phi(i)|_{\hat{F}_2} = 1$ as $\hat{F}_2$ is the fixed field of $2\mathrm{Gal}(M(F)/F)$. By Proposition 3.1(1), we have $\hat{F}_2 = F(\sqrt{\eta}, \sqrt{\gamma})$ and $\sqrt{\eta} \in F_\infty$. It follows from $\phi(i) \in \mathrm{Gal}(M(F)/F_\infty)$ that

$$\phi(i)|_{F(\sqrt{\eta})} = \left(\frac{i, \eta}{\mathfrak{P}}\right) = 1. \tag{3.4}$$

Therefore, $\phi(i)|_{\hat{F}_2} = 1$ if and only if $\phi(i)|_{F(\sqrt{\gamma})} = 1$ which in turn is equivalent to the following value of the quadratic Hilbert symbol:

$$\left(\frac{i, \gamma}{\mathfrak{P}}\right) = 1.$$

This proves (2)⇔(3). We remark that although the construction of $\hat{F}_2$ depends on a suitable sign of γ, the Hilbert symbol does not as -1 is a square in $F_\mathfrak{P}^\times$.

(3)⇔(4). The proof is applying Chevalley's formula (2.1) on $(E/F, \mathrm{Cl}_{E,S})$. Without loss of generality, we may assume that the embedding induced by the prime ideals are chosen as follows:

i) If $q \equiv 15 \bmod 32$, we have $\iota_\mathfrak{P}(\sqrt{-q}) \equiv -9 \bmod 16\mathbb{Z}_2$ whence $\iota_\mathfrak{P}(\sqrt[4]{-q}) \equiv 3i \bmod 8\mathbb{Z}_2[i]$. We also have $\iota_{\bar{\mathfrak{P}}_1}(\sqrt[4]{-q}) \equiv 3 \bmod 8\mathbb{Z}_2$, and $\iota_{\bar{\mathfrak{P}}_2}(\sqrt[4]{-q}) \equiv -3 \bmod 8\mathbb{Z}_2$.

ii) If $q \equiv 31 \bmod 32$, we have $\iota_\mathfrak{P}(\sqrt{-q}) \equiv -1 \bmod 16\mathbb{Z}_2$ whence $\iota_\mathfrak{P}(\sqrt[4]{-q}) \equiv i \bmod 8\mathbb{Z}_2[i]$. We also have $\iota_{\bar{\mathfrak{P}}_1}(\sqrt[4]{-q}) \equiv -1 \bmod 8\mathbb{Z}_2$, $\iota_{\bar{\mathfrak{P}}_2}(\sqrt[4]{-q}) \equiv 1 \bmod 8\mathbb{Z}_2$.

By considering the extensions of local fields at those primes, we conclude that the ramified primes of F in E are exactly $\mathfrak{P}, \bar{\mathfrak{P}}_1, \sqrt[4]{-q}\mathcal{O}_F$.

Since every element in $1 + 8\mathbb{Z}_2[i]$ is a square, by (2.2) we have the following values of quadratic Hilbert symbols:

$$\left(\frac{i, \gamma}{\mathfrak{P}}\right) = \begin{cases} \left(\dfrac{3\sqrt[4]{-q}, \gamma}{\mathfrak{P}}\right) = \left(\dfrac{3, N(\gamma)}{\mathfrak{p}}\right)\left(\dfrac{\sqrt[4]{-q}, \gamma}{\mathfrak{P}}\right) = -\left(\dfrac{\sqrt[4]{-q}, \gamma}{\mathfrak{P}}\right) & \text{if } q \equiv 15 \bmod 32; \\ \left(\dfrac{\sqrt[4]{-q}, \gamma}{\mathfrak{P}}\right) & \text{if } q \equiv 31 \bmod 32. \end{cases} \tag{3.5}$$

For the S-units, it is clearly that $\mathcal{O}_{F,S}^{\times}/(\mathcal{O}_{F,S}^{\times})^2$ is generated by $\eta, -1, \gamma$. Now applying Chevalley's formula (2.1) to E/F gives

$$|\mathrm{Cl}_{E,S}^{\mathrm{Gal}(E/F)}| = \frac{2^2}{[\mathcal{O}_{F,S}^{\times} \cap \mathcal{O}_{F,S}^{\times} \cap N_{E/F}(E^{\times})]}.$$

Here we use the fact that F has odd class number. It follows from the lemma below that

$$2 \nmid |\mathrm{Cl}_{E,S}^{\mathrm{Gal}(E/F)}| \text{ if and only if } \Big(\frac{\gamma, \sqrt[4]{-q}}{\mathfrak{P}}\Big) = -1.$$

Since $2 \nmid |\mathrm{Cl}_{E,S}^{\mathrm{Gal}(E/F)}|$ if and only if $2 \nmid |\mathrm{Cl}_{E,S}|$, combining with (3.5) completes the proof. □

Lemma 3.3. *Let ρ be the map as in Proposition 2.1:*

$$\begin{aligned}\rho : \mathcal{O}_{F,S}^{\times}/(\mathcal{O}_{F,S}^{\times})^2 &\longrightarrow \{\pm 1\}^3 \\ x &\longmapsto \Big(\Big(\frac{x, \sqrt[4]{-q}}{\mathfrak{P}}\Big), \Big(\frac{x, \sqrt[4]{-q}}{\bar{\mathfrak{P}}_1}\Big), \Big(\frac{x, \sqrt[4]{-q}}{\sqrt[4]{-q}\mathcal{O}_F}\Big) \Big).\end{aligned}$$

Then

(1) $\rho(-1) = (1, -1, -1)$, $\rho(\eta) = (1, 1, 1)$ *or* $(1, -1, -1)$.

(2) *The unit index* $[\mathcal{O}_{F,S}^{\times} \cap \mathcal{O}_{F,S}^{\times} \cap N_{E/F}(E^{\times})]$ *is equal to* 4 *if* $\Big(\frac{\gamma, \sqrt[4]{-q}}{\mathfrak{P}}\Big) = -1$ *and is equal to* 2 *if* $\Big(\frac{\gamma, \sqrt[4]{-q}}{\mathfrak{P}}\Big) = 1$.

Proof. We have $[\mathcal{O}_{F,S}^{\times} \cap \mathcal{O}_{F,S}^{\times} \cap N_{E/F}(E^{\times})] = |\mathrm{Im}(\rho)|$ and $|\mathrm{Im}(\rho)| \leq 4$ by Proposition 2.1. Note that -1 is not a square in $\mathcal{O}_F/(\sqrt[4]{-q}) = \mathbb{F}_q$, since $q \equiv 3 \bmod 4$. It follows that

$$\Big(\frac{-1, \sqrt[4]{-q}}{\sqrt[4]{-q}\mathcal{O}_F}\Big) = -1.$$

Since $F_{\bar{\mathfrak{P}}_1} = \mathbb{Q}_2$ and $\iota_{\bar{\mathfrak{P}}_1}(\sqrt[4]{-q}) \equiv -1 \bmod 8$, we have

$$\Big(\frac{-1, \sqrt[4]{-q}}{\bar{\mathfrak{P}}_1}\Big) = \Big(\frac{-1, -1}{\mathbb{Q}_2}\Big) = -1.$$

It follows from the product formula that we must have $\rho(-1) = (1, -1, -1)$ whence $2 \leq |\mathrm{Im}(\rho)|$. The inequality $|\mathrm{Im}(\rho)| \leq 4$ follows from the product formula of Hilbert symbols also.

In Lemma 2.2, we proved that $N_{F/K}(\eta) = 1$. In particular, $N_{F_{\mathfrak{P}}/K_{\mathfrak{p}}(\eta)} = 1$. We have

$$\Big(\frac{\eta, \sqrt[4]{-q}}{\mathfrak{P}}\Big) = \begin{cases} \Big(\frac{\eta, 3i}{\mathfrak{P}}\Big) = \Big(\frac{N_{F_{\mathfrak{P}}/K_{\mathfrak{p}}}(\eta), 3}{\mathfrak{p}}\Big)\Big(\frac{\eta, i}{\mathfrak{P}}\Big) = \Big(\frac{\eta, i}{\mathfrak{P}}\Big)\Big(\frac{1, 3}{\mathbb{Q}_2}\Big) = 1 & \text{if } q \equiv 15 \bmod 32 \\ \Big(\frac{\eta, i}{\mathfrak{P}}\Big) = 1 & \text{if } q \equiv 31 \bmod 32 \end{cases}$$

The last equalities in both cases are by (3.4). This proves (1).

(2) is a consequence of (1). □

3.2. **S-Class group of E.** In this subsection, we prove the following desired results on $\mathrm{Cl}_{E,S}$. This would finish the proof of Theorem 1.1(3) by Proposition 3.2.

Proposition 3.4. *The following statements hold:*

(1)*if* $q \equiv 15 \bmod 32$, *then* 2 *does not divide* $|\mathrm{Cl}_{E,S}|$*;*

(2)*if* $q \equiv 31 \bmod 32$, *then* 2 *divides* $|\mathrm{Cl}_{E,S}|$.

The proof is to explore the extensions E'/K' and E'/E. We first prepare some basic results on the biquadratic field K'. The first important fact is that the class number of K' is odd, see the lemma below. The primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are both ramified in K'. Write $\mathfrak{p}\mathcal{O}_{K'} = \mathfrak{p}'^2$. We have $\pi\mathcal{O}_F = \mathfrak{p}^h\mathcal{O}_F = \mathfrak{p}'^{2h}$ where h is the class number of F as before. It turns out that $\mathfrak{p}'^h = \pi'\mathcal{O}_{K'}$ for some $\pi' \in \mathcal{O}_{K'}$, since K' has odd class number. This produces a unit π'^2/π of K'. Note that the unique prime ideal of the real quadratic subfield $\mathbb{Q}(\sqrt{q})$ lying above 2 is ramified in $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$ and this prime must be principal as the class number of $\mathbb{Q}(\sqrt{q})$ is odd by classical genus theory. We denote this prime ideal by $\varpi\mathcal{O}_{\mathbb{Z}[\sqrt{q}]}$. We then obtain another unit $(1+i)/\varpi$ of K'.

Lemma 3.5. *With notation as above, we have*

(1) *the class number of K' is odd;*

(2) *$\mathcal{O}_{K'}^\times/(\mathcal{O}_{K'}^\times)^4$ is generated by $\langle(1+i)/\varpi, i\rangle$ and also by $\langle {\pi'}^2/\pi, i\rangle$.*

(3) *$\mathcal{O}_{K',S}^\times/(\mathcal{O}_{K',S}^\times)^4$ is generated by $(1+i)/\varpi, i, \pi'$.*

Proof. (1) can be proved easily by applying Chevalley's formula on K'/K or $K'/\mathbb{Q}(i)$. We leave the details to the reader.

For (2), note that $\mathbb{Z}[\sqrt{q}]^\times/(\mathbb{Z}[\sqrt{q}]^\times)^2$ is generated by -1 and $\varpi^2/2$. By a theorem of Dirichlet on units of biquadratic field, see [3, Theorem 42], we have

$$[\mathcal{O}_{K'}^\times : \langle\frac{\varpi^2}{2}, i\rangle] = 1 \text{ or } 2 \text{ up to a 2-adic unit.}$$

It follows that $\mathcal{O}_{K'}^\times/E_{K'}^2$ is generated by $(1+i)/\varpi, i$. By Nakayama's lemma, $\mathcal{O}_{K'}^\times/(\mathcal{O}_{K'}^\times)^4$ is also generated by $(1+i)/\varpi, i$. Write ${\pi'}^2/\pi = ((1+i)/\varpi)^a i^b$ with $a, b \in \mathbb{Z}$. To prove (2), it suffices to show that a is odd. Suppose not. Applying the norm map $N_{K'/\mathbb{Q}(\sqrt{p})}$ gives

$$\frac{N_{K'/\mathbb{Q}(\sqrt{p})}(\pi')^2}{2^h} = \frac{2^a}{\varpi^{2a}}.$$

Since h is odd, this equality would imply that 2 is a square in $\mathbb{Q}(\sqrt{q})$. This contradiction completes the proof of (2).

The statement (3) clearly follows from (2). □

Lemma 3.6. (1) *The primes of K' ramified in E'/K' are exactly $\sqrt{-q}\mathcal{O}_{K'}$ and $\mathfrak{p}'$. Moreover, we have the following ramification indexes: $e(\sqrt{-q}\mathcal{O}_{K'}) = 4$ and $e(\mathfrak{p}') = 2$.*

(2) *If $q \equiv 15 \bmod 32$, then $[\mathcal{O}_{K',S}^\times : \mathcal{O}_{K',S}^\times \cap N_{E'/K'}(E')] = 2$.*

(3) *If $q \equiv 31 \bmod 32$, then $[\mathcal{O}_{K',S}^\times : \mathcal{O}_{K',S}^\times \cap N_{E'/K'}(E')] = 1$.*

Proof. (1). The prime $\sqrt{-q}\mathcal{O}_{K'}$ is clearly totally ramified in E'. Note that the local field $K'_{\mathfrak{p}'} \cong K'_{\bar{\mathfrak{p}'}} \cong \mathbb{Q}_2(i)$ and $\iota_{\mathfrak{p}'}(\sqrt{-q}) \equiv -1 \bmod 8$ and $\iota_{\bar{\mathfrak{p}'}}(\sqrt{-q}) \equiv 1 \bmod 8$. Here $\bar{\mathfrak{p}'}$ is the unique prime of K' above $\mathfrak{p}'$. Then it is readily verified that $\bar{\mathfrak{p}'}$ is unramified in E'/K' by considering the corresponding extensions of local fields. We also have that $\mathfrak{p}'$ splits in F'/K' and ramifies in E'/F'. This proves (1).

(2)Note that E'/K' is a quartic cyclic Kummer extension. As in Proposition 2.1, we define the map

$$\begin{aligned} \rho : \mathcal{O}_{K',S}^\times/E_{F,S}^4 &\longrightarrow \mu_4^2 \\ x &\longmapsto \Big(\Big(\frac{x, \sqrt{-q}}{\mathfrak{p}'}\Big)_4, \Big(\frac{x, \sqrt{-q}}{\sqrt{-q}\mathcal{O}_{K'}}\Big)_4\Big). \end{aligned}$$

And we have $[\mathcal{O}_{K',S}^\times : \mathcal{O}_{K',S}^\times \cap N_{E'/K'}(E')] = |\mathrm{Im}(\rho)|$. Note that the residue field of $\sqrt{-q}\mathcal{O}_{K'}$ is $\mathbb{F}_{q^2}$. It follows that the quartic Hilbert symbol

$$\Big(\frac{i, \sqrt{-q}}{\sqrt{-q}\mathcal{O}_{K'}}\Big)_4 = i^{\frac{q^2-1}{4}} = 1.$$

Thus $\rho(i) = (1,1)$ by the product formula. We also have the symbol

$$\Big(\frac{1+i, \sqrt{-q}}{\sqrt{-q}\mathcal{O}_{K'}}\Big)_4 \equiv (1+i)^{\frac{q^2-1}{4}} \equiv (-4)^{\frac{q^2-1}{16}} \equiv 1 \bmod \sqrt{-q}\mathcal{O}_{K'}.$$

It follows from $\varpi^{q-1} \equiv 1 \bmod \sqrt{q}\mathbb{Z}[\sqrt{q}]$ that

$$\Big(\frac{\varpi, \sqrt{-q}}{\sqrt{-q}\mathcal{O}_{K'}}\Big)_4 \equiv \varpi^{\frac{q^2-1}{4}} \equiv 1 \bmod \sqrt{-q}\mathcal{O}_{K'}.$$

Hence we have $\rho((1+i)/\varpi) = (1,1)$ by the product formula. Note that this in fact proves that for any $q \equiv 15 \bmod 16$,

$$[\mathcal{O}_{K'}^{\times} : \mathcal{O}_{K'}^{\times} \cap N_{E'/K'}(E')] = 1.$$

We do not need this result, but it can be used to compute the 2-primary part of the class group $\mathrm{Cl}_{E'}$ of E', see Remark 3.8. It remains to compute $\rho(\pi')$. By the above lemma, we have $\pi'^2 = \pi(\frac{1+i}{\varpi})^a i^b$ with $a, b \in \mathbb{Z}$ and a is odd. Note that $i^{\frac{q^2-1}{8}} \equiv \pi^{\frac{q^2-1}{8}} \equiv \varpi^{\frac{q^2-1}{8}} \equiv 1 \bmod \sqrt{-q}\mathcal{O}_{K'}$, since $q \equiv 15 \bmod 16$. Thus the symbol

$$\Big(\frac{\pi', \sqrt{-q}}{\sqrt{-q}\mathcal{O}_{K'}}\Big)_4 \equiv \pi'^{\frac{q^2-1}{4}} \equiv (1+i)^{\frac{q^2-1}{8}a} \equiv (-4)^{\frac{q^2-1}{32}a} \equiv (-1)^{\frac{q^2-1}{32}} \bmod \sqrt{-q}\mathcal{O}_{K'}.$$

The last step uses that a is odd. Hence $\rho(\pi') = ((-1)^{\frac{q^2-1}{32}}, (-1)^{\frac{q^2-1}{32}})$. In other words,

$$\rho(\pi') = \begin{cases} (-1,-1) & \text{if } q \equiv 15 \bmod 32, \\ (1,1) & \text{if } q \equiv 31 \bmod 32. \end{cases}$$

This completes the proof. □

Proposition 3.7. *Let $q \equiv 15 \bmod 16$ be a prime. We have the following:*
(1)*if $q \equiv 15 \bmod 32$, then 2 does not divide $|\mathrm{Cl}_{E',S}|$;*
(2)*if $q \equiv 31 \bmod 32$, then 2 divides $|\mathrm{Cl}_{E',S}|$;*

Proof. Applying Chevalley's formula (2.1) on E'/K' gives

$$|\mathrm{Cl}_{E',S}^{\mathrm{Gal}(E'/K')}| = \begin{cases} 1 & \text{if } q \equiv 15 \bmod 32, \\ 2 & \text{if } q \equiv 31 \bmod 32. \end{cases}$$

Thus the results. □

Remark 3.8. One can further prove that the 2-primary part of $\mathrm{Cl}_{E'}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ if $q \equiv 15 \bmod 32$. We do not need this result but we sketch the proof. Suppose $q \equiv 15 \bmod 32$. Then $2 \nmid |\mathrm{Cl}_{E',S}|$ implies that the 2-primary part of the class group $\mathrm{Cl}_{E'}$ is generated by the 2-primary part of the ideal classes of the primes above S. In particular, it is equal to the 2-primary of $\mathrm{Cl}_{E',S}^{\mathrm{Gal}(E'/K')}$ which has order 2 by applying Chevalley's formula on the class group Cl_E.

Proof of Proposition 3.4. (1). Suppose $q \equiv 15 \bmod 32$. From the argument of the proof of Proposition 3.2 (3) $\Leftrightarrow$ (4), we have that $\bar{\mathfrak{P}}_2$ is inert in E/F. And the local field $E_{\bar{\mathfrak{P}}_2\mathcal{O}_E} = \mathbb{Q}_2(\sqrt{-3})$. We conclude that $\bar{\mathfrak{P}}_2\mathcal{O}_E$ is ramified in E'/E, since the local extension $\mathbb{Q}_2(\sqrt{-3})(i)/\mathbb{Q}_2(\sqrt{-3})$ is ramified. By class field theory, the norm map from $\mathrm{Cl}_{E'}$ to Cl_E is surjective. Since we have proved that the 2-primary part of $\mathrm{Cl}_{E'}$ is generated by the primes of E' lying above $S = \{\mathfrak{p}\}$, we conclude that the 2-primary part of Cl_E is generated by primes of E lying above $\mathfrak{p}$. In other words, $2 \nmid |\mathrm{Cl}_{E,S}|$. This proves (1).

(2). Suppose $q \equiv 31 \bmod 32$. We again use the convention on embeddings in the proof of Proposition 3.2 (3) $\Leftrightarrow$ (4). Then $\bar{\mathfrak{P}}_1$ is ramified in E/F and $\bar{\mathfrak{P}}_2$ splits in E/F, say $\bar{\mathfrak{P}}_2\mathcal{O}_E = v_1v_2$. And we have $E_{v_1} \cong E_{v_2} \cong \mathbb{Q}_2$. By looking at the extensions of local fields, we conclude that the ramified primes of E in E' are exactly v_1 and v_2. Applying Chevalley's formula (2.1) on E'/E gives

$$|\mathrm{Cl}_{E',S}^{\mathrm{Gal}(E'/E)}| = |\mathrm{Cl}_{E,S}| \frac{2}{[\mathcal{O}_{E,S}^{\times} : \mathcal{O}_{E,S}^{\times} \cap N_{E'/E}(E'^{\times})]}.$$

Note that -1 is not a norm of E', since the quadratic Hilbert symbol of -1 and -1 at $E_{v_1} = \mathbb{Q}_2$ is nontrivial. This shows that the unit index in the formula is at least 2. On the other hand, we have proved that $|\mathrm{Cl}_{E',S}|$ is divisible by 2 and hence so is $|\mathrm{Cl}_{E',S}^{\mathrm{Gal}(E'/E)}|$. It follows that 2 must divide $|\mathrm{Cl}_{E,S}|$. This completes the proof. □

Proof of Theorem 1.1(3). This directly follows from Proposition 3.2 and Proposition 3.4. □

Acknowledgments

The author thanks Professor John Coates and Yongxiong Li for their carefully reading of this paper and helpful suggestions. The author also thanks Professor Georges Gras for informing the paper [4] to him. 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.

[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] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, vol.27. Cambridge University Press, 1993.

[4] G. Gras, *Practice of the Incomplete p-ramification over a number Field – History of abelian p-ramification*, Communications in Advanced Mathematical Sciences. **2** (2019), 251-280.

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

[6] J. Li and C. Yu. *The Chevalley-Gras formula over global fields*, arXiv:2001.11413v2.

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

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

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