




On class numbers of pure quartic fields

Jianing Li¹ · Yue Xu¹ 

Received: 18 December 2019 / Accepted: 17 January 2020 / Published online: 21 July 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract

Let p be a prime. The 2-primary part of the class group of the pure quartic field $\mathbb{Q}(\sqrt[4]{p})$ has been determined by Parry and Lemmermeyer when $p \not\equiv \pm 1 \pmod{16}$. In this paper, we improve the known results in the case $p \equiv \pm 1 \pmod{16}$. In particular, we determine all primes p such that 4 does not divide the class number of $\mathbb{Q}(\sqrt[4]{p})$. We also conjecture a relation between the class numbers of $\mathbb{Q}(\sqrt[4]{p})$ and $\mathbb{Q}(\sqrt{-2p})$. We show that this conjecture implies a distribution result of the 2-class numbers of $\mathbb{Q}(\sqrt[4]{p})$.

Keywords Class group · Pure quartic field

Mathematics Subject Classification 11R29 · 11R16

1 Introduction

Let p be a prime number. Let K be the pure quartic number field $\mathbb{Q}(\sqrt[4]{p})$. The goal of this paper is to study the 2-primary part of the class group Cl_K of K . This question has been studied by Parry [1] and Lemmermeyer [2]. Parry showed that this group is cyclic. So the question becomes to determine the exact divisibility of 2-powers of the class number h_K of K . We list the known results.

- (i) If $p = 2$ or $p \equiv \pm 3 \pmod{8}$, then $2 \nmid h_K$.
- (ii) If $p \equiv \pm 7 \pmod{16}$, then $2 \parallel h_K$. The case $p \equiv -7 \pmod{16}$ is due to Lemmermeyer [2].

Research is partially supported by Anhui Initiative in Quantum Information Technologies (Grant No. AHY-10200), NSFC (Grant No. 11571328) and the Fundamental Research Funds for the Central Universities (No. WK0010000058).

✉ Yue Xu
wasx250@mail.ustc.edu.cn

Jianing Li
lijn@ustc.edu.cn

¹ CAS Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei 230026, Anhui, China

(iii) If $p \equiv \pm 1 \pmod{16}$, then $2 \mid h_K$. In the case $p \equiv 1 \pmod{16}$, $2 \parallel h_K$ if the quartic residue symbol $\left(\frac{2}{p}\right)_4$ equals to -1 .

We remark that in fact one has $2 \nmid h_{\mathbb{Q}(\sqrt[n]{p})}$ if $p \equiv \pm 3 \pmod{8}$ for any $n \geq 1$ and $2 \parallel h_{\mathbb{Q}(\sqrt[n]{p})}$ if $p \equiv 7 \pmod{16}$ for any $n \geq 2$, see [3]. Thus the remaining problems are to determine the 2-divisibilities of h_K when $p \equiv \pm 1 \pmod{16}$. Our first result is the following.

Theorem 1.1 *Let $p \equiv 1 \pmod{16}$ be a prime. Then $2 \parallel h_K$ if and only if the quartic residue symbol $\left(\frac{2}{p}\right)_4 = -1$.*

By Chebotarev's density theorem, the natural density of the set $\{p \text{ primes} : p \equiv 1 \pmod{16} \text{ and } 2 \parallel h_K\}$ among all primes is $\frac{1}{16}$, see Remark 2.2.

We then turn to study the case $p \equiv -1 \pmod{16}$. We prove the following improvement of Parry's and therefore we determine all primes p such that $2 \parallel h_K$.

Theorem 1.2 *Let $p \equiv -1 \pmod{16}$ be a prime. Then the 2-primary part of Cl_K is cyclic and the class number h_K is divisible by 4.*

Suppose $p \equiv -1 \pmod{16}$. By class field theory, K admits a unique unramified cyclic quartic extension which we call it 4-Hilbert class field of K . It is not hard to see that $K(\sqrt{2})$ is an unramified quadratic extension of K . We construct the 4-Hilbert class field in terms of the units of the ring of integer in the quartic field $\mathbb{Q}(\sqrt{2\sqrt{p}})$. It can be shown that there exists a totally positive unit ξ such that the unit group $\mathcal{O}_{\mathbb{Q}(\sqrt{2\sqrt{p}})}^\times$ is generated by $\xi, \bar{\xi}, -1$ and the relative norm $N_{\mathbb{Q}(\sqrt{2\sqrt{p}})/\mathbb{Q}(\sqrt{p})}(\xi) = \xi\bar{\xi}$ of ξ is the fundamental unit of $\mathbb{Q}(\sqrt{p})$ (see Proposition 3.5).

Theorem 1.3 *Let $p \equiv -1 \pmod{16}$ be a prime and ξ as above. Then the 4-Hilbert class field of K is $K(\sqrt{\xi})$.*

We observe that there are some relations between h_K and $h(-2p)$, where $h(-2p)$ is class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-2p})$. Due to Gauss, we know that the 2-primary part of the class group $\text{Cl}_{\mathbb{Q}(\sqrt{-2p})}$ of $\mathbb{Q}(\sqrt{-2p})$ is cyclic and nontrivial. We list the known results on 2-divisibility of $h(-2p)$. For $p \equiv \pm 1 \pmod{8}$, write $p = u^2 - 2v^2$ with $u, v \in \mathbb{N}$ and $u \equiv 1 \pmod{4}$. The following results are due to Rédei [4], Reichardt [5], Hasse [6] and Leonard-Williams [7]. We refer the readers to [7].

- (i) $2 \parallel h(-2p)$ if and only if $p \equiv \pm 3 \pmod{8}$.
- (ii) Suppose $p \equiv 1 \pmod{8}$. We have that $4 \parallel h(-2p)$ if and only if $\left(\frac{2}{p}\right)_4 = -1$ and that $8 \parallel h(-2p)$ if and only if $\left(\frac{u}{p}\right)_4 = -1$.
- (iii) Suppose $p \equiv -1 \pmod{8}$. We have that $4 \parallel h(-2p)$ if and only if $p \equiv 7 \pmod{16}$ and that $8 \parallel h(-2p)$ if and only if $p \equiv -1 \pmod{16}$ and $(-1)^{\frac{p+1}{16}} \left(\frac{2u}{v}\right) = -1$.

The residue symbols $\left(\frac{u}{p}\right)_4$ and $\left(\frac{2u}{v}\right)$ are independent of the choices of u, v (see [7] or Lemma 4.1). By comparing the results on h_K , one finds that if $p \equiv \pm 3 \pmod{8}$ or $p \equiv 7 \pmod{16}$, then $\text{ord}_2(h(-2p)) = \text{ord}_2(h_K) + 1$. Based on numerical evidence, we propose the following conjecture.

- Conjecture** (1) If $p \equiv 15 \pmod{32}$ is a prime, then $4 \parallel h_K \iff 16 \mid h(-2p)$.
 (2) If $p \equiv 31 \pmod{32}$ is a prime, then $4 \parallel h_K \iff 8 \parallel h(-2p)$.

By the above results on $h(-2p)$, this conjecture is equivalent to the following.

Equivalent Form of the Conjecture Let $p \equiv -1 \pmod{16}$ be a prime number. Write $p = u^2 - 2v^2$ with $u, v \in \mathbb{N}$. Let (p) denote the Jacobi symbol $(\frac{2u}{v})$. Then

$$4 \parallel h_K \iff (p) = -1.$$

Based on Cohen–Lenstra heuristic, Milovic [8, Conjecture 1] conjectures that for each $k \geq 1$, the natural density of the set $\{p : p \equiv -1 \pmod{4} \text{ and } 2^k \parallel h(-2p)\}$ is $\frac{1}{2^{k+1}}$. For $k = 1, 2$, this follows from the above results on $h(-2p)$ and the Dirichlet's density theorem on arithmetic progressions. Milovic [8] proves the case $k = 3$ by showing that

$$\lim_{X \rightarrow \infty} \frac{\#\{p \leq X : p \equiv -1 \pmod{16} \text{ and } (-1)^{\frac{p+1}{16}}(p) = -1\}}{\#\{p \leq X : p \equiv -1 \pmod{16}\}} = \frac{1}{2}. \quad (*)$$

Use his method, we show the following.

Theorem 1.4 Let (p) be as in the above conjecture. Then

$$\lim_{X \rightarrow \infty} \frac{\#\{p \leq X, p \equiv -1 \pmod{16} : (p) = -1\}}{\#\{p \leq X, p \equiv -1 \pmod{16}\}} = \frac{1}{2}.$$

Thus we obtain the following result.

Corollary 1.5 Assume the above conjecture holds. Then

$$\lim_{X \rightarrow \infty} \frac{\#\{p \leq X : p \equiv -1 \pmod{16} \text{ and } 4 \parallel h_K\}}{\#\{p \leq X : p \equiv -1 \pmod{16}\}} = \frac{1}{2}.$$

There are 4927 primes p such that $p < 10^6$ and $p \equiv 15 \pmod{32}$. Pari-gp [9] shows that there are 2416 primes p such that $4 \parallel h_K$ and there are 2511 primes p such that $8 \parallel h_K$. Combine with (4.5) and the above corollary, one can see that (under the Conjecture)

$$\begin{aligned} & \lim_{X \rightarrow \infty} \frac{\#\{p \leq X : p \equiv 15 \pmod{32} \text{ and } 4 \parallel h_K\}}{\#\{p \leq X : p \equiv 15 \pmod{32}\}} \\ &= \lim_{X \rightarrow \infty} \frac{\#\{p \leq X : p \equiv 31 \pmod{32} \text{ and } 4 \parallel h_K\}}{\#\{p \leq X : p \equiv 31 \pmod{32}\}} = \frac{1}{2}. \end{aligned}$$

This partially explains the above data.

The rest of this paper is organized as follows. In Sect. 2, we give some preliminaries and prove the result for $p \equiv 1 \pmod{16}$. In Sect. 3, we prove Theorem 1.2 and 1.3. In Sect. 4, we discuss the density results on class numbers.

2 Preliminaries and the case $p \equiv 1 \pmod{16}$

In this section, we state Chevalley's ambiguous class number formula which is the main tool we used. Then we give the proof of the cyclicity of the 2-primary part of Cl_K for any p . After that we prove Theorem 1.1.

Let M/L be a cyclic extension of number fields with Galois group G . Then the ambiguous class number formula states as

$$|\text{Cl}_M^G| = |\text{Cl}_L| \frac{\prod_v e_v}{[M:L]} \frac{1}{[\mathcal{O}_L^\times : \mathcal{O}_L^\times \cap N(M^\times)]}. \quad (2.1)$$

Here e_v is the ramification index of v and the products run over all places of L (including the infinite places). The norm N is from M to L . See [10] for a proof of this result. If G is a cyclic ℓ -group where ℓ is a prime, then $\ell \nmid |\text{Cl}_M^G|$ implies that $\ell \nmid |\text{Cl}_M|$. Because for $a \notin \text{Cl}_M^G$, the cardinality of the orbit of a is divisible by ℓ , $|\text{Cl}_M| \equiv |\text{Cl}_M^G| \pmod{\ell}$.

Proposition 2.1 (Parry) *Let p be a prime. Then the 2-primary part of the class group of K is cyclic.*

Proof It is readily verified that the Proposition holds for $p = 2$. A be the 2-primary part of Cl_K . Put $k = \mathbb{Q}(\sqrt{p})$ and $G = \text{Gal}(K/k) = \{1, \sigma\}$. It is well known that the class number h_k of k is odd. Thus we have $a^\sigma a = 1$ for $a \in A$. This implies $A^G = A[2] := \{a \in A \mid a^2 = 1\}$. Applying Chevalley's formula on the quadratic extension K/k gives

$$|A[2]| = |A^G| = \frac{\prod_v e_v}{2} \frac{1}{[\mathcal{O}_k^\times : \mathcal{O}_k^\times \cap N(K^\times)]}.$$

We have $-1 \notin N(K^\times)$ since one of the infinite places of k is ramified. This implies $[\mathcal{O}_k^\times : \mathcal{O}_k^\times \cap N(K^\times)] = 2$ or 4 . We will show that for any odd prime p one has $\prod_v e_v = 8$ where v runs over all places of k . It follows that $|A[2]| = 1$ or 2 . Hence A is trivial or cyclic.

Obviously, K/k is unramified outside places above 2 , p and ∞ . Here ∞ denotes the real place ∞ such that $\infty(\sqrt{p}) < 0$. Also note that $(\sqrt{p})\mathcal{O}_k$ is ramified. Thus $\prod_{v \nmid 2} e_v = 4$. We compute the ramification index at 2 as follows.

If $p \equiv 3 \pmod{4}$, then $(x+1)^4 - p$ is an Eisenstein polynomial in $\mathbb{Q}_2[x]$. Thus 2 is totally ramified in K/\mathbb{Q} . This implies that $\prod_v e_v = 8$ where v runs over all places of k .

If $p \equiv 5 \pmod{8}$, then 2 is inert in k . Because $(x+1)^2 - \sqrt{p}$ is an Eisenstein polynomial in $\mathbb{Q}_2(\sqrt{p})$, we have $2\mathcal{O}_k$ is ramified in K . Hence $\prod_v e_v = 8$.

If $p \equiv 1 \pmod{16}$, $x^4 - p$ has two solutions $\pm \sqrt[4]{p}$ in \mathbb{Q}_2 . Thus in $\mathbb{Q}_2[x]$, we have $x^4 - p = (x - \sqrt[4]{p})(x + \sqrt[4]{p})(x^2 + \sqrt{p})$. Note that $(x+1)^2 + \sqrt{p}$ is an Eisenstein polynomial. Therefore, there are three primes in K above 2 and exactly one of them ramified. This implies that $\prod_v e_v = 8$.

If $p \equiv 9 \pmod{16}$, then $x^4 - p = (x^2 - \sqrt{p})(x^2 + \sqrt{p})$ with $\sqrt{p} \equiv \pm 3 \pmod{8\mathbb{Z}_2}$. We have $x^2 \pm \sqrt{p}$ are irreducible in $\mathbb{Q}_2[x]$. Note that, $\mathbb{Q}_2(\sqrt{3})/\mathbb{Q}_2$ is ramified and $\mathbb{Q}_2(\sqrt{-3})/\mathbb{Q}_2$ is unramified. Thus $\prod_v e_v = 8$.

The proof of the proposition is complete. \square

Now we give the proof of Theorem 1.1. Much of the proof are as same as Lemmermeyer's proof of that if $p \equiv 9 \pmod{16}$ implies $2 \parallel h_K$. The only difference is that in the case $p \equiv 1 \pmod{16}$, we need to investigate all the units of a quartic field.

Proof of the Theorem 1.1. For $p \equiv 1 \pmod{8}$, the following are proved in [2]. Let F be the unique quartic subfield of the p -th cyclotomic field $\mathbb{Q}(\zeta_p)$. Then $L := FK$ is a quadratic unramified extension of K and F is the field $\mathbb{Q}(\sqrt{\epsilon\sqrt{p}})$ where ϵ is the fundamental unit of $k := \mathbb{Q}(\sqrt{p})$. One has

$$2 \parallel h_K \quad \text{if and only if} \quad 2 \nmid h(L).$$

We present Lemmermeyer's proof of the case of $p \equiv 9 \pmod{16}$ in this paragraph. To prove $2 \mid h(L)$, Lemmermeyer uses Chevalley's formula on $L/k(\sqrt{\epsilon})$. The class number of $k(\sqrt{\epsilon})$ is odd. This can be proved by the fact that $2 \mid h_k$ and ϵ has norm -1 . The primes of $k(\sqrt{\epsilon})$ ramified in L are the two prime ideals above p . In the case $p \equiv 9 \pmod{16}$, $\sqrt{\epsilon}$ is not a norm of L^\times . (In the case $p \equiv 1 \pmod{16}$, -1 and $\sqrt{\epsilon}$ are norms of L^\times .) In particular the unit index

$$[\mathcal{O}_{k(\sqrt{\epsilon})}^\times : \mathcal{O}_{k(\sqrt{\epsilon})}^\times \cap N(L^\times)] \geq 2.$$

So one obtains $2 \nmid h(L)$, hence $2 \parallel h_K$ when $p \equiv 9 \pmod{16}$.

In order to prove our result, we need to show that for $p \equiv 1 \pmod{16}$,

$$[\mathcal{O}_{k(\sqrt{\epsilon})}^\times : \mathcal{O}_{k(\sqrt{\epsilon})}^\times \cap N(L^\times)] = 2 \quad \text{if and only if} \quad \left(\frac{2}{p}\right)_4 = -1. \quad (2.2)$$

Since $p \equiv 1 \pmod{16}$, 2 splits in k , say $(2)\mathcal{O}_k = q\bar{q}$. Then we may assume that q is ramified in K and \bar{q} splits in K . Since q and \bar{q} are both unramified in F , we have q is ramified in $k(\sqrt{\epsilon})$ and \bar{q} is unramified in $k(\sqrt{\epsilon})$. Then $q\mathcal{O}_{k(\sqrt{\epsilon})} = \mathfrak{Q}^2$. Let $\pi \in \mathcal{O}_k$ be the generator of the principal ideal q^{h_k} . Since the class number of $k(\sqrt{\epsilon})$ is odd, we have $\mathfrak{Q}^{h_k} = \alpha\mathcal{O}_{k(\sqrt{\epsilon})}$. Then we produce a unit $\frac{\alpha^2}{\pi}$ of $\mathcal{O}_{k(\sqrt{\epsilon})}$. The unit group $\mathcal{O}_{k(\sqrt{\epsilon})}^\times$ is isomorphic to $\mathbb{Z}^2 \times \mathbb{Z}/2\mathbb{Z}$ by Dirichlet's unit theorem. We claim that the following 3-dimensional \mathbb{F}_2 -vector space

$$\mathcal{O}_{k(\sqrt{\epsilon})}^\times / (\mathcal{O}_{k(\sqrt{\epsilon})}^\times)^2 \text{ is generated by } -1, \sqrt{\epsilon}, \text{ and } \frac{\alpha^2}{\pi}.$$

First we show that $\frac{\alpha^2}{\pi}$ and -1 are linearly independent in this vector space. Otherwise, we have $\frac{\alpha^2}{\pi} = \pm a^2$ for some $a \in k(\sqrt{\epsilon})$. Then $\sqrt{\pm\pi} \in k(\sqrt{\epsilon})$ and $k(\sqrt{\pm\pi}) = k(\sqrt{\epsilon})$. It follows that $\pm\pi = \epsilon c^2$ for some $c \in k$. This contradicts to that $\pi\mathcal{O}_k = q^{h_k}$,

because h_k is odd. It is easy to see that -1 and $\sqrt{\epsilon}$ are linearly independent. Suppose that these three elements are not linearly independent. Then $\frac{\alpha^2}{\pi} = \pm \sqrt{\epsilon}b^2$ for some $b \in k(\sqrt{\epsilon})$. By taking norm from $k(\sqrt{\epsilon})$ to \mathbb{Q} , we obtain $-1 = c^2$ for some $c \in \mathbb{Q}$. Here we use the fact ϵ has norm -1 . This is a contradiction. This proves the claim.

Let $\mathfrak{p}_1, \mathfrak{p}_2$ be the prime ideals above p in $k(\sqrt{\epsilon})$. They are exactly the places of $k(\sqrt{\epsilon})$ ramified in L . Note that $L = k(\sqrt{\epsilon})(\sqrt{\sqrt{p}})$. Then by Hasse's norm theorem, $\frac{\alpha^2}{\pi} \notin N(L^\times)$ if and only if the quadratic Hilbert symbol $(\frac{\alpha^2}{\pi}, \sqrt{p})_{\mathfrak{p}_i} = -1$ for $i = 1, 2$. Write $\pi = m + n\sqrt{p}$. Then $\pi \equiv m \pmod{\sqrt{p}}$ and $m^2 - n^2p = 2$. Then

$$\left(\frac{\alpha^2}{\pi}, \sqrt{p}\right)_{\mathfrak{p}_i} = (\pi, \sqrt{p})_{\mathfrak{p}_i} = (m, \sqrt{p})_{\mathfrak{p}_i} = (m, p)_p = \left(\frac{m}{p}\right) = \left(\frac{2}{p}\right)_4.$$

Hence (2.2) is proved. This finishes the proof of the theorem. \square

Remark 2.2 (1) We remark that for $p \equiv 1 \pmod{16}$, then $\left(\frac{2}{p}\right)_4 = -1 \iff 4 \parallel h(-2p) \iff 4 \parallel h(-p)$, where $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$. See [7].

(2) In order to compute the natural density of the set $\{p : p \equiv 1 \pmod{16} \text{ and } \left(\frac{2}{p}\right)_4 = -1\}$, we consider the Galois extension $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})/\mathbb{Q}$. Note that the degree of this extension is 16. Let τ be the generator of $H := \text{Gal}(\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})/\mathbb{Q}(\zeta_{16}))$. Then the order of the conjugate class of τ is 1 since H is a normal subgroup. A prime $p \equiv 1 \pmod{16}$ and $\left(\frac{2}{p}\right)_4 = -1$ if and only if the Frobenius of p is τ . By Chebotarev's density theorem, the natural density of $\{p : p \equiv 1 \pmod{16} \text{ and } \left(\frac{2}{p}\right)_4 = -1\}$ is $\frac{1}{16}$.

3 Proof of Theorems 1.2 and 1.3

Let $p \equiv -1 \pmod{16}$ be a prime in this section. Put $L = K(\sqrt{2})$ and $F = \mathbb{Q}(\sqrt{p}, \sqrt{2})$. Let $k = \mathbb{Q}(\sqrt{p})$, $k' = \mathbb{Q}(\sqrt{2p})$ and $k_0 = \mathbb{Q}(\sqrt{2})$ be the quadratic subfields of F . In order to prove Theorem 1.2, we consider the extensions F/k , L/F and L/K .

Lemma 3.1 *We have $4 \mid h_K$ if and only if $2 \mid h_L$.*

Proof First note that L/K is unramified outside 2 because $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is unramified outside 2. Since $p \equiv -1 \pmod{16}$, $\mathbb{Q}_2(\sqrt[4]{p}) = \mathbb{Q}_2(\sqrt[4]{-1}) = \mathbb{Q}_2(\zeta_8) \supset \mathbb{Q}_2(\sqrt{2})$. It follows that L/K is unramified at every prime ideal above 2, hence everywhere unramified. By Hasse's norm theorem and local class field theory, we have $[\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap N(L^\times)] = 1$. Applying Chevalley's formula (2.1) to L/K gives

$$|\text{Cl}_L^{\text{Gal}(L/K)}| = \frac{|\text{Cl}_K|}{2}.$$

Therefore 4 divides $|\text{Cl}_K| \iff 2$ divides $|\text{Cl}_L^{\text{Gal}(L/K)}| \iff 2$ divides $|\text{Cl}_L|$. \square

Proposition 3.2 (1) *The class numbers $h_k, h_{k'}, h_{k_0}$ and h_F are all odd.*

- (2) Let $\epsilon, \epsilon', 1 + \sqrt{2}$ be the fundamental units of k, k', k_0 respectively. Then $\mathcal{O}_F^\times = \langle \sqrt{\epsilon}, \sqrt{\epsilon'}, 1 + \sqrt{2} \rangle \times \{\pm 1\}$.

Proof (1) The oddness of $h_k, h_{k'}, h_{k_0}$ is well-known. Alternately, it is easy to prove this by applying Chevalley's formula. We leave it to the readers.

Note that the only ramified prime in F/k is the unique prime ideal of k above 2. Take $u \in \mathcal{O}_k^\times$, by local class field theory u is a local norm except at 2. However by the Artin reciprocity law (or the product formula), u must be a norm at 2. Then $u \in N_{F/k}(K^\times)$ by Hasse's norm theorem. Applying Chevalley's formula (2.1) to F/k shows that $2 \nmid h_F$.

(2) We first show that $\sqrt{\epsilon}$ and $\sqrt{\epsilon'}$ are in F . Let \mathfrak{q} (resp. \mathfrak{q}') be the unique prime ideal of k (resp. k') above 2. Since both h and h' are odd and $2\mathcal{O}_k = \pi^2\mathcal{O}_k$ and $2\mathcal{O}_{k'} = \pi'^2\mathcal{O}_{k'}$. Then $\frac{\pi^2}{2} \in \mathcal{O}_k^\times$ and $\frac{\pi'^2}{2} \in \mathcal{O}_{k'}^\times$. We may choose totally positive generators π and π' such that $\epsilon = \frac{\pi^2}{2}$ and $\epsilon' = \frac{\pi'^2}{2}$. Thus $\sqrt{\epsilon} = \frac{\pi}{\sqrt{2}}, \sqrt{\epsilon'} = \frac{\pi'}{\sqrt{2}} \in \mathcal{O}_F^\times$.

To prove the proposition, it suffices to show that $[\mathcal{O}_K^\times : \mathcal{O}_k^\times \mathcal{O}_{k'}^\times \mathcal{O}_{k_0}^\times] = 4$.

Kuroda's class number formula [11, Theorem 1] gives

$$[\mathcal{O}_F^\times : \mathcal{O}_k^\times \mathcal{O}_{k'}^\times \mathcal{O}_{k_0}^\times] = \frac{4h_F}{h_k h_{k'} h_{k_0}}.$$

Since $h_K, h_k, h_{k'}, h_{k_0}$ are odd, it suffices to show that the units index is a power of 2. Suppose not, let r be an odd prime divides this index. Then there exists a unit $\eta \in \mathcal{O}_F^\times$ such that $\eta^r = \pm \epsilon^a \epsilon'^b (1 + \sqrt{2})^c$ and $r \nmid \gcd(a, b, c)$. Note that $N_{F/k}(\eta^r) = \pm \epsilon^{2a}$, this implies $r \mid a$. Similarly, $r \mid b$ and $r \mid c$. This contradiction shows the index is a power of 2, as desired. This completes the proof. \square

Lemma 3.3 (1) The product of ramification indices of all places of F in L/F is 16.

(2) The index $[\mathcal{O}_F^\times : N(L^\times) \cap \mathcal{O}_F^\times]$ is 4.

Proof (1) Obviously L/F is unramified outside the places above 2, p and the infinite places. In fact L/F is unramified at the prime ideal above 2, because

$$\mathbb{Q}_2(\sqrt[4]{p}, \sqrt{2}) = \mathbb{Q}_2(\sqrt{p}, \sqrt{2}) = \mathbb{Q}_2(\zeta_8).$$

On the other hand, the places $\mathfrak{p}_1, \mathfrak{p}_2, \infty_1$ and ∞_2 are clearly ramified, where $\mathfrak{p}_1, \mathfrak{p}_2$ are the two prime ideals of F above p and ∞_1, ∞_2 are the two real embeddings such that $\infty_i(\sqrt{p}) < 0$ and $\infty_i(\sqrt{2}) = (-1)^i \sqrt{2}$ for $i = 1, 2$. This proves (1).

(2) As in the proof of the above proposition. We let \mathfrak{q} (resp. \mathfrak{q}') be the unique prime ideal of k (resp. k') above 2. Let π (resp. π') be the totally positive generators of \mathfrak{q} (resp. \mathfrak{q}') such that $\frac{\pi^2}{2}$ (resp. $\frac{\pi'^2}{2}$) are the fundamental unit of k (resp. k'). Then by the above proposition,

$$\mathcal{O}_F^\times = \left\langle \frac{\pi_1}{\sqrt{2}}, \frac{\pi_2}{\sqrt{2}}, 1 + \sqrt{2}, -1 \right\rangle.$$

Since $-1, \pm(1 + \sqrt{2})$ are negative at ∞_1 or ∞_2 , they are not norms at ∞_1 or ∞_2 and then not norms of L . This shows the index $[\mathcal{O}_F^\times : N(L^\times) \cap \mathcal{O}_F^\times] \geq 4$.

Now we go to show that

$$\left\langle \frac{\sqrt{2}(1+\sqrt{2})}{\pi_1}, \frac{\sqrt{2}(1+\sqrt{2})}{\pi_2}, (1+\sqrt{2})^2 \right\rangle \subset N(L^\times).$$

Note that the left side is a subgroup of \mathcal{O}_F^\times with index 4, so this would imply the desired results. Because the above units are totally positive, so they are norms at ∞_1 and ∞_2 . For \mathfrak{p}_1 and \mathfrak{p}_2 , note that the localization of F at \mathfrak{p}_i ($i = 1, 2$) is $\mathbb{Q}_p(\sqrt{p})$, thus the proposition follows from the following lemma and Hasse's norm theorem. \square

Lemma 3.4 (1) *The elements $2 \pm \sqrt{2}$ are squares in \mathbb{Q}_p^\times .*

(2) *The elements π and π' are squares in $\mathbb{Q}_p(\sqrt{p})^\times$.*

Proof (1) Note that $(2+\sqrt{2})(2-\sqrt{2}) = 2$ is a square in \mathbb{Q}_p^\times . So $2+\sqrt{2} \in (\mathbb{Q}_p^\times)^2$ if and only if $2-\sqrt{2} \in (\mathbb{Q}_p^\times)^2$. Since $p \equiv -1 \pmod{16}$, p splits completely in $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$. This implies that $\zeta_{16} + \zeta_{16}^{-1} \in \mathbb{Q}_p$. Note that $(\zeta_{16} + \zeta_{16}^{-1})^2 = \zeta_8 + \zeta_8^{-1} + 2 = 2 + \sqrt{2}$ or $2 - \sqrt{2}$.

(2) Write $\pi = a + b\sqrt{p}$ with $a \in \mathbb{Z}_{\geq 1}$, $b \in \mathbb{Z}$. Then $a^2 - pb^2 = 2$ and $2 \nmid ab$. By the quadratic reciprocity law for Jacobi symbols,

$$\left(\frac{a}{p}\right) = \left(\frac{-p}{a}\right) = \left(\frac{2}{a}\right).$$

Note that $a^2 \equiv 2 \pmod{b}$, in particular $\left(\frac{2}{b}\right) = 1$. Hence $b \equiv \pm 1 \pmod{8}$ and then $b^2 \equiv 1 \pmod{16}$. Thus $a^2 = 2 + pb^2 \equiv 1 \pmod{16}$ and $\left(\frac{2}{a}\right) = 1$. This implies that $\left(\frac{a}{p}\right) = 1$. Hence $\pi_1 \pmod{\sqrt{p}}$ is a square in $\mathbb{Z}_p[\sqrt{p}]/(\sqrt{p})$. By Hensel's lemma, π_1 is a square in the local field $\mathbb{Q}_p(\sqrt{p})$.

Note that $\mathbb{Q}_p(\sqrt{p}) = \mathbb{Q}_p(\sqrt{2p})$. Write $\pi' = c + d\sqrt{2p}$ with $c \in \mathbb{Z}_{\geq 1}$, $d \in \mathbb{Z}$. By Hensel's lemma, it is enough to prove that π' is a square modulo $\sqrt{2p}$, or equivalently c is a square modulo p . Write $c = 2^w c'$ with $2 \nmid c'$. From the identity $c^2 - 2pd^2 = 2$, one has

$$\left(\frac{c}{p}\right) = \left(\frac{2^w c'}{p}\right) = \left(\frac{c'}{p}\right) = \left(\frac{-p}{c'}\right) = \left(\frac{1}{c'}\right) = 1.$$

\square

We are now ready to prove Theorem 1.2.

Proof of the Theorem 1.2 Proposition 2.1 proves the cyclic property. The above two propositions and Chevalley's formula (2.1) show that $|\text{Cl}_L^{\text{Gal}(L/K)}| = 2$. In particular, $2 \mid h_L$. By Proposition 3.1, we have $4 \mid h_K$. This completes the proof. \square

Now we go to prove Theorem 1.3. By Lemma 3.1, we see that L is the 2-Hilbert class field of K . To construct the 4-Hilbert class field, we need the following results on the field $K' = \mathbb{Q}(\sqrt{2\sqrt{p}})$.

Proposition 3.5 *The following statements are true:*

- (1) *The unique prime ideal $\pi\mathcal{O}_k$ above 2 in k splits in K'/k .*
- (2) *The class number of K' is odd.*
- (3) *There exists a totally positive unit ξ of $\mathcal{O}_{K'}^\times$, such that $\mathcal{O}_{K'}^\times = \langle \xi, \bar{\xi}, -1 \rangle$ and $N_{K'/k}(\xi) = \xi\bar{\xi} = \epsilon$.*

Proof For (1), note that $\mathbb{Q}_2(\sqrt{p}) = \mathbb{Q}_2(\sqrt{-1})$ and $\sqrt[4]{-p} \in \mathbb{Q}_2$. Then the fact that $\pi\mathcal{O}_k$ splits in K' follows from $x^2 - 2\sqrt{p} = x^2 - (1 + \sqrt{-1})^2\sqrt{-p} = (x - (1 + \sqrt{-1})\sqrt[4]{-p})(x + (1 + \sqrt{-1})\sqrt[4]{-p})$ in $\mathbb{Q}_2(\sqrt{p})[x]$.

For (2), note that the places of k ramified in K' are $\sqrt{p}\mathcal{O}_k$ and the infinite place which sends \sqrt{p} to $-\sqrt{p} \in \mathbb{R}$. Then $-1 \notin N(K'^\times)$. Since $\epsilon = \frac{\pi^2}{2}$ is totally positive, it is a norm at the infinite places. By product formula, ϵ must also be a norm at $\sqrt{p}\mathcal{O}_k$. Then $\epsilon \in N(K'^\times)$. By Chevalley's formula, the class number of K' is odd.

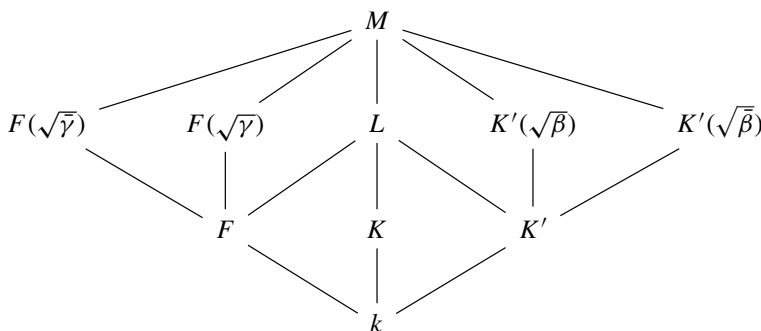
For (3), by [12, Proposition 1.3.4] and (2), we have $\epsilon \in N(\mathcal{O}_{K'}^\times)$. Note that $\mathcal{O}_{K'}^\times/\mathcal{O}_k^\times$ is an abelian group of rank 1. We claim that it is torsion-free. Otherwise, there exists $u \in \mathcal{O}_{K'}^\times \setminus \mathcal{O}_k^\times$ such that $u^j \in \mathcal{O}_k^\times$ for some $j \geq 2$. Then $K' = k(u)$. The conjugate element of u is ζu for some $\zeta \in \langle \zeta_j \rangle \cap K'$ where ζ_j is a j -th primitive root of unity. So $\zeta = \pm 1$ and $N(u) = u\zeta u = \pm u^2 \in \mathcal{O}_k^\times$. This implies that K'/k is unramified at p . This is a contradiction. Hence we prove the claim.

Take $\eta \in \mathcal{O}_{K'}^\times$ such that it is a generator in $\mathcal{O}_{K'}^\times/\mathcal{O}_k^\times$. We then have $\mathcal{O}_{K'}^\times = \langle -1, \eta, \epsilon \rangle$. Since $\epsilon \in N(\mathcal{O}_{K'}^\times)$, the norm of η must be an odd power of ϵ , say $N(\eta) = \epsilon^{2k+1}$. Put $\xi = \text{sgn}(\eta)\eta\epsilon^{-k}$. Then ξ is totally positive and $N(\xi) = \epsilon$. Hence $\mathcal{O}_{K'}^\times = \langle -1, \xi, \epsilon \rangle = \langle -1, \xi, \bar{\xi} \rangle$. \square

Proof of Theorem 1.3 Let M be the 4-Hilbert class field of K . Since K/k is Galois, M/k is also Galois. By class field theory, one has

$$\text{Gal}(M/K) \cong \text{Cl}_K/4\text{Cl}_K \quad \text{as } \text{Gal}(K/k)\text{-modules.}$$

Here $\text{Gal}(K/k) := \{1, \sigma\}$ acts on $\text{Gal}(M/K)$ by lifting inner automorphisms. Let A_K be the 2-primary part of Cl_K . Given an ideal class $a \in A_K$, we have $N_{K/k}(a) = a\sigma(a) = 1$ as h_k is odd. In other words, $\sigma(a) = a^{-1}$. Hence $\text{Gal}(M/k)$ is isomorphic to D_4 , the dihedral group of order 8. We then have a diagram of fields by Galois theory.



Here β is an element of K' and $\bar{\beta}$ is the conjugate element of β respect to the extension K'/k . Similarly, γ is an element of K and $\bar{\gamma}$ is the conjugate element of γ respect to the extension K/k . Note that $L = K'(\sqrt{\beta\bar{\beta}}) = k(\sqrt{2}\sqrt{p}, \sqrt{\beta\bar{\beta}})$ and $k(\sqrt{\beta\bar{\beta}}) = F$ or K .

Since the class number h' of K' is odd, we have $K'(\sqrt{\beta^{h'}}) = K'(\sqrt{\beta})$. Let $\beta\mathcal{O}_{K'} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k}$ be the prime ideals factorization. Then $\beta' := \beta^{h'} = u\varpi_1^{a_1} \cdots \varpi_k^{a_k}$ where $u \in \mathcal{O}_{K'}^\times$ and $\varpi_i \in \mathcal{O}_{K'}$ is a generator of $\mathfrak{p}_i^{h'}$ for each i . We may assume $a_i = 0$ or 1 for each i . Since F/k is unramified outside 2, so are L/K' and M/K' . In particular, $K'(\sqrt{\beta})/K'$ is unramified outside the prime ideals above 2. This implies $\beta'\mathcal{O}_{K'} = (\eta_1), (\eta_2), (\eta_1\eta_2)$ or $\mathcal{O}_{K'}$. Here $\eta_i\mathcal{O}_{K'} = \mathfrak{q}_i^{h'}$ ($i = 1, 2$) and \mathfrak{q}_i is the prime ideal above $\pi\mathcal{O}_k$. (Recall that $\pi\mathcal{O}_k$ is the unique prime above 2 in k .) Note that in each case $k(\sqrt{\beta\bar{\beta}})/k$ is unramified at $\sqrt{p}\mathcal{O}_k$. So one must have $k(\sqrt{\beta\bar{\beta}}) = F$.

We claim that $\beta'\mathcal{O}_{K'} = \mathcal{O}_{K'}$. If $\beta' = u\eta_i$ for some unit u ($i = 1$ or 2), then $\beta'\bar{\beta}' = v\pi^{h'}$. Because $F = k(\sqrt{\beta\bar{\beta}}) = k(\sqrt{2})$, $v\pi^{h'} = 2t^2$ for some $t \in k^\times$ and $v \in \mathcal{O}_k^\times$. This is a contradiction since h' is odd. Hence $\beta' \neq u\eta_i$. If $\beta' = u\eta_1\eta_2$, then both \mathfrak{q}_1 and \mathfrak{q}_2 are ramified in the extensions $K'(\sqrt{\beta'})/K'$, $K'(\sqrt{\bar{\beta}})/K'$ and L/K' respectively. It follows that M/L is ramified at the primes above 2. This is a contradiction since M/L is unramified everywhere. Therefore, we must have β' is a unit in $\mathcal{O}_{K'}$. This proves the claim.

Since $K'(\sqrt{\beta})/K'$ is unramified at the infinite places, we have $K'(\sqrt{\beta}) = K'(\sqrt{\xi}), K'(\sqrt{\bar{\xi}})$ or $K'(\sqrt{\xi\bar{\xi}})$. As $\xi\bar{\xi} = \epsilon \in k$, this case cannot happen. So $K'(\sqrt{\beta}) = K'(\sqrt{\xi})$ or $K'(\sqrt{\bar{\xi}})$. It follows that $M = L(\sqrt{\xi}) = LK'(\sqrt{\xi}) = K(\sqrt{\xi})$. This completes the proof of Theorem 1.3. \square

4 Distribution of the primes with 4 $\parallel h_K$

In Sect. 4.1, we reprove the Theorem of Leonard–Williams [7] on the 16-divisibility of the class number $h(-2p)$ of $\mathbb{Q}(\sqrt{-2p})$. In [7], they give a sketch of this proof by using the language of quadratic forms. Milovic says (see [8, p. 976]) that he was unable to verify the proof in [7] and he gives a technical proof by using 4-Hilbert class field of $\mathbb{Q}(\sqrt{-2p})$, see [8, Proposition 1]. We will follow the ideas in [7] to prove this result in the language of ideals. In Sect. 4.2, we prove Theorem 1.4 and give some corollaries.

4.1 16-Divisibility of $h(-2p)$

Lemma 4.1 *Let $p \equiv -1 \pmod{8}$ be a prime. For any decomposition $p = u^2 - 2v^2$ with $u, v \in \mathbb{N}$, the Jacobi symbol $\left(\frac{2u}{v}\right)$ is independent on the choices of u and v .*

Proof Suppose $p = u'^2 - 2v'^2$ with $u', v' \in \mathbb{N}$. Then $u' + v'\sqrt{2} = (1 + \sqrt{2})^{2k}(u + v\sqrt{2})$ or $(1 + \sqrt{2})^{2k}(u - v\sqrt{2})$ for some $k \in \mathbb{Z}$. It suffices to consider $k = 1$. In the first case, $u' = 3u + 4v$ and $v' = 2u + 3v$. Since $p \equiv -1 \pmod{8}$, we have that u, v are odd and that $v \equiv 2u + 3v \pmod{4}$. Then $\left(\frac{2u'}{v'}\right) = \left(\frac{-v}{2u+3v}\right) = \left(\frac{2u}{v}\right)$ by the quadratic reciprocity law. The second case can be proved similarly. \square

Recall that we denote this Jacobi symbol $\left(\frac{2u}{v}\right)$ by (p) .

Theorem 4.2 *Let $p \equiv -1 \pmod{8}$ be a prime. Then the following statements hold:*

- (1) (Hasse) $4 \parallel h(-2p) \iff p \equiv 7 \pmod{16}$.
- (2) (Leonard–Williams) $8 \parallel h(-2p) \iff p \equiv -1 \pmod{16}$ and $(-1)^{\frac{p+1}{16}}(p) = -1$.

Proof Let J_2 be the prime ideal of $k := \mathbb{Q}(\sqrt{-2p})$ above 2. Then we have that $N(J_2) = |\mathcal{O}_k/J_2| = 2$ and that J_2 has order 2 in the class group Cl_k . One can write $p = u^2 - 2v^2$ such that $u \in \mathbb{N}$ and $u \equiv 1 \pmod{4}$. Hence $(2v + \sqrt{-2p})(2v - \sqrt{-2p}) = 2u^2$. Note that the ideals $(2v + \sqrt{-2p})J_2^{-1}$ and $(2v - \sqrt{-2p})J_2^{-1}$ are coprime. It follows that there exists an ideal J_u such that $(2v + \sqrt{-2p}) = J_u^2 J_2$. Automatically, $N(J_u) = u$ and $\text{cl}(J_u)$ has order 4 in Cl_k .

Since the genus field of k is $k(\sqrt{2})$, the Artin map induces an isomorphism

$$\left[\frac{k(\sqrt{2})/k}{-} \right] : \text{Cl}_k/2\text{Cl}_k \cong \text{Gal}(k(\sqrt{2})/k).$$

Therefore, we have

$$\begin{aligned} 8 \mid h(-2p) &\iff \text{cl}(J_u) \in 2\text{Cl}_k \\ &\iff \left[\frac{k(\sqrt{2})/k}{J_u} \right] = 1 \iff \left[\frac{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}{N(J_u)} \right] = \left(\frac{2}{u} \right) = 1 \\ &\quad \text{(by norm-functoriality of Artin map)} \\ &\iff u^2 \equiv 1 \pmod{16} \iff u \equiv 1 \pmod{8}, \text{ since } u \equiv 1 \pmod{4} \\ &\iff p \equiv -1 \pmod{16} \text{ (since } p = u^2 - 2v^2 \text{ with } u, v \text{ odd)}. \end{aligned}$$

Now let us prove (2). Since $8 \mid h(-2p)$, we choose an integral ideal J_s with norm s such that $\text{cl}(J_s)^2 = \text{cl}(J_u)$. By approximation theorem, we can further assume that $\gcd(s, 2up) = 1$. Hence $\text{cl}(J_s)$ has order 8 in Cl_k and one has that

$$16 \mid h(-2p) \iff \text{cl}(J_s) \in 2\text{Cl}_k \iff \left[\frac{k(\sqrt{2})/k}{J_s} \right] = 1 \iff \left(\frac{2}{s} \right) = 1.$$

Thus it remains to prove that

$$\left(\frac{2}{s} \right) = (-1)^{\frac{p+1}{16}}(p). \quad (**)$$

In the decomposition $p = u^2 - 2v^2$, we have $u \equiv 1 \pmod{8}$ by (1). We may further assume that $u \equiv 1 \pmod{16}$ by replacing $u + \sqrt{2}v$ to $(1 + \sqrt{2})^4(u + v\sqrt{2})$. Let $x + y\sqrt{-2p}$ and $z + w\sqrt{-2p}$ denote the generators of the principal ideals $\overline{J_u}J_s^2$ and $J_2J_uJ_s^2$, respectively. Here $\overline{J_u} = (u)J_u^{-1}$ is the conjugate ideal of J_u and we assume $x > 0$. By taking norm of the equality $\overline{J_u}J_s^2 = (x + y\sqrt{-2p})$, we have

$$us^2 = x^2 + 2py^2. \quad (4.1)$$

From the equalities of ideals

$$(z + w\sqrt{-2p}) = J_2 J_u J_s^2 = J_2 J_u^2 J_u^{-1} J_s^2 = (2v + \sqrt{-2p})u^{-1}(x + y\sqrt{-2p}),$$

we can change the sign of z, w such that

$$uw = x + 2vy. \quad (4.2)$$

From (4.1) and (4.2) and $p = u^2 - 2v^2$, we obtain

$$s^2 = uw^2 - 4vyw + 2uy^2. \quad (4.3)$$

We claim that $s^2 \equiv w^2 \pmod{16}$. Since s is odd, we know that y is even and that x is odd from (4.1). From (4.2), we have w is odd. Then the claim holds by (4.3).

Therefore

$$\left(\frac{2}{s}\right) = \left(\frac{2}{|w|}\right) = \left(\frac{u}{|w|}\right) = \left(\frac{w}{u}\right) = \left(\frac{v}{u}\right)\left(\frac{y}{u}\right) = \left(\frac{v}{u}\right) = \left(\frac{u}{v}\right). \quad (4.4)$$

The first equality is by the above claim. The second and the fourth equalities are by (4.3). The third and the last equalities are by the quadratic reciprocity law and the fact that $u \equiv 1 \pmod{16}$. To see the fifth equality, write $y = 2^t y_0$ with $2 \nmid y_0$. Then by $u \equiv 1 \pmod{16}$, we have $\left(\frac{y}{u}\right) = \left(\frac{2^t y_0}{u}\right) = \left(\frac{y_0}{u}\right) = \left(\frac{u}{|y_0|}\right) = 1$. The last equality follows from (4.1).

From $p = u^2 - 2v^2$, we obtain that $2v^2 \equiv 1 - p \pmod{32}$ as $u \equiv 1 \pmod{16}$. Then

$$\left(\frac{2}{v}\right) = (-1)^{\frac{p+1}{16}}.$$

Thus (4.4) and the above equality imply (**). This proves the proposition. \square

4.2 Proof of Theorem 1.4

The following is the main result in [8, Theorem 2].

$$\sum_{\substack{p \leq X \\ p \equiv -1 \pmod{16}}} (-1)^{\frac{p+1}{16}}(p) \ll_{\epsilon} X^{\frac{149}{150} + \epsilon}. \quad (4.5)$$

Here $f(X) \ll_{\epsilon} g(X)$ means that for each $\epsilon > 0$, there exists some positive constant C_{ϵ} such that $|f(X)| \leq C_{\epsilon} g(X)$. Then by Theorem 4.2, Milovic obtains the density of the set of primes p such that $p \equiv 3 \pmod{4}$ and $16 \mid h(-2p)$.

We will show that Milovic's method can be used to prove the following.

$$A^+(X) - A^-(X) = \sum_{\substack{p \leq X \\ p \equiv -1 \pmod{16}}} (p) \ll_{\epsilon} X^{\frac{149}{150} + \epsilon}. \quad (4.6)$$

Here $A^\pm(X) = \#\{p \leq X, p \equiv -1 \pmod{16}, (p) = \pm 1\}$. On the other hand, by Dirichlet's density theorem,

$$A^+(X) + A^-(X) = \sum_{\substack{p \leq X \\ p \equiv -1 \pmod{16}}} 1 \sim \frac{1}{8} \frac{X}{\log X}.$$

Here $f(X) \sim g(X)$ means the limit of $f(X)/g(X)$ is 1 as $X \rightarrow \infty$. We conclude that

$$A^-(X) \sim \frac{1}{16} \frac{X}{\log X}.$$

Theorem 1.4 then follows. It remains to prove (4.6).

To prove (4.5), Milovic [8, Section 3.2] defines the spin symbol for all totally positive elements of $\mathbb{Z}[\sqrt{2}]$ as follows.

$$[u + v\sqrt{2}] = \begin{cases} \left(\frac{v}{u}\right) & \text{if } u \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

In order to prove our result, we define the twisted spin symbol for all totally positive elements of $\mathbb{Z}[\sqrt{2}]$ as

$$[u + v\sqrt{2}]' = [u + v\sqrt{2}]\lambda(u + v\sqrt{2}),$$

where $\lambda(u + v\sqrt{2}) = (-1)^{\frac{u^2 - 2v^2 + 1}{16}}$ if $u^2 - 2v^2 \equiv -1 \pmod{16}$ and 1 otherwise. One can easily show that the twisted spin symbol satisfies $[(1 + \sqrt{2})^8(u + v\sqrt{2})]' = [u + v\sqrt{2}]'$ which is an analogous property of the spin symbol $[u + v\sqrt{2}]$ as in [8, Proposition 2]. Then one can replace $[u + v\sqrt{2}]$ in [8] by $[u + v\sqrt{2}]'$ to follow Milovic's argument [8, pp. 993–1013]. This gives a proof of (4.6) whence Theorem 1.4.

Using (4.5) and (4.6), we obtain refined results on $h(-2p)$ for $p \equiv -1 \pmod{16}$.

Corollary 4.3 *We have*

$$\begin{aligned} \lim_{X \rightarrow \infty} \frac{\#\{p \leq X : p \equiv 15 \pmod{32} \text{ and } 8 \parallel h(-2p)\}}{\#\{p \leq X : p \equiv 15 \pmod{32}\}} \\ = \lim_{X \rightarrow \infty} \frac{\#\{p \leq X : p \equiv 31 \pmod{32} \text{ and } 8 \parallel h(-2p)\}}{\#\{p \leq X : p \equiv 31 \pmod{32}\}} = \frac{1}{2}. \end{aligned}$$

Proof By (4.5) and (4.6), we have

$$2 \sum_{\substack{p \leq X \\ p \equiv -1 \pmod{32}}} (p) = \sum_{\substack{p \leq X \\ p \equiv -1 \pmod{16}}} (-1)^{\frac{p+1}{16}} (p) + (p) \ll_{\epsilon} X^{\frac{149}{150} + \epsilon}.$$

By Theorem 4.2, for $p \equiv -1 \pmod{32}$ one has $8 \parallel h(-2p)$ if and only if $(p) = -1$. Hence the result follows the Dirichlet's density theorem. The case $p \equiv 15 \pmod{32}$ can be shown similarly. \square

Acknowledgements The authors thank Franz Lemmermeyer for helpful email exchanges.

References

1. Parry, C.J.: A genus theory for quartic fields. *J. Reine Angew. Math.* **314**, 40–71 (1980)
2. Monsky, P.: A Result of Lemmermeyer on Class Numbers. [arXiv:1009.3990](https://arxiv.org/abs/1009.3990) (2010)
3. Li, J., Ouyang, Y., Xu, Y., Zhang, S.: ℓ -Class Groups of Fields in Kummer Towers. [arXiv:1905.04966](https://arxiv.org/abs/1905.04966) (2019)
4. Rédei, L.: Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.* **171**, 55–60 (1934)
5. Reichardt, H.: Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.* **170**, 75–82 (1934)
6. Hasse, H.: Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$. *J. Number Theory* **1**, 231–234 (1969)
7. Leonard, P.A., Williams, K.S.: On the divisibility of the class numbers of $\mathbb{Q}(\sqrt{-p})$ and $\mathbb{Q}(\sqrt{-2p})$ by 16. *Can. Math. Bull.* **25**(2), 200–206 (1982)
8. Milovic, D.: On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-8p})$ for $p \equiv -1 \pmod{4}$. *Geom. Funct. Anal.* **27**, 973–1016 (2017)
9. The PARI Group: Univ. Bordeaux, PARI/GP version 2.7.5. <http://pari.math.u-bordeaux.fr/> (2015)
10. Lemmermeyer, F.: The ambiguous class number formula revisited. *J. Ramanujan Math. Soc.* **28**, 415–421 (2013)
11. Lemmermeyer, F.: Kuroda’s class number formula. *Acta Arith.* **66**, 245–260 (1994)
12. Greenberg, R.: Topics in Iwasawa Theory. <https://sites.math.washington.edu/~greenber/book.pdf> (2001)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.