A NOTE ON CLASS NUMBERS OF PURE QUARTIC FIELDS

JIANING LI

Abstract. For a prime $p \equiv 15 \bmod 16$, we show that 4 divides the class number of $\mathbb{Q}(\sqrt[4]{p})$ which improves a result of Parry.

1. Introduction

Let p be a prime number. For a number field F, let h_F denote its class number. It is well-known that $h_{\mathbb{Q}(\sqrt{p})}$ is odd by the genus theory of Gauss. For the field $\mathbb{Q}(\sqrt[4]{p})$, Parry [3] showed that the 2-part of the class group of $\mathbb{Q}(\sqrt[4]{p})$ is cyclic. Moreover,

(i) If $p = 2$ or $p \equiv 3, 5 \bmod 8$, then $2 \nmid h_{\mathbb{Q}(\sqrt[4]{p})}$. See [3, Theorem 8 and Corollary on Page 68].
(ii) If $p \equiv 7 \bmod 16$, then $2 \parallel h_{\mathbb{Q}(\sqrt[4]{p})}$. See [3, Theorem 3].
(iii) If $p \equiv 15 \bmod 16$, then $2 \mid h_{\mathbb{Q}(\sqrt[4]{p})}$. See [3, Theorem 3].
(iv) If $p \equiv 1 \bmod 8$, then $2 \mid h_{\mathbb{Q}(\sqrt[4]{p})}$. Moreover, if 2 is not a fourth power modulo p, then $2 \parallel h_{\mathbb{Q}(\sqrt[4]{p})}$. See [3, Theorem 4].
(v) If $p \equiv 9 \bmod 16$, then $2 \parallel h_{\mathbb{Q}(\sqrt[4]{p})}$. See [2].

In this note, we show that

Theorem 1. *If $p \equiv 15 \bmod 16$ is a prime, then the class number of $\mathbb{Q}(\sqrt[4]{p})$ is divisible by 4.*

Remark 2. *These results lead us to study the class numbers of $\mathbb{Q}(\sqrt[4]{p})$ when $p \equiv 15 \bmod 32$. There are 4927 primes p such that $p < 10^6$ and $p \equiv 15 \bmod 32$. Pari-gp shows that there are 2416 primes p such that $4 \parallel h_{\mathbb{Q}(\sqrt[4]{p})}$ and there are 2511 primes p such that $8 \parallel h_{\mathbb{Q}(\sqrt[4]{p})}$. We can not explain this.*

The proof is using Chevalley's ambiguous class number formula. Instead of considering the extension $\mathbb{Q}(\sqrt[4]{p})/\mathbb{Q}(\sqrt{p})$ which Parry used, we use the extensions $\mathbb{Q}(\sqrt{p}, \sqrt{2})/\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt[4]{p}, \sqrt{2})/\mathbb{Q}(\sqrt{p}, \sqrt{2})$ and $\mathbb{Q}(\sqrt[4]{p}, \sqrt{2})/\mathbb{Q}(\sqrt[4]{p})$.

We now state the ambiguous class number formula. Let L/K be a cyclic extension of number fields with Galois group G. Let Cl_K and Cl_L be the class groups of K and L respectively. Then

$$|\mathrm{Cl}_L^G| = |\mathrm{Cl}_K| \frac{\prod_v e_v}{[L:K]} \frac{1}{[\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap N(L^\times)]}. \tag{1.1}$$

Here e_v is the ramification index of v and the product runs over all places (including the infinite places). For our purpose, G will be a ℓ-cyclic group where ℓ is a prime, then $\ell \nmid |\mathrm{Cl}_L^G|$ implies $\ell \nmid |\mathrm{Cl}_L|$ by the following well-known lemma.

Lemma 3. *Let H be a finite cyclic ℓ-group where ℓ is a prime. Let A be a finite abelian group with an action of H. Then $\ell \nmid |A^H|$ implies that $\ell \nmid |A|$.*

Proof. Note that for $a \notin A^H$, the cardinality of the orbit of a is divisible by ℓ. Thus $|A| \equiv |A^H| \bmod \ell$. □

For completeness, we prove the following result of Parry.

Proposition 4. *Let p be an odd prime. Then the 2-part of the class group of $\mathbb{Q}(\sqrt[4]{p})$ is cyclic.*

2010 *Mathematics Subject Classification.* 11R29, 11R26, 11R11.

Proof. Let A be the 2-part of the class group of $\mathbb{Q}(\sqrt[4]{p})$ and $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{p})/\mathbb{Q}(\sqrt{p}) = \{1, \sigma\}$. Since the class number of $\mathbb{Q}(\sqrt{p})$ is odd, we have $a^\sigma a = 1$ for $a \in A$. This implies $A^G = A[2]$ where $A[2] = \{a \in A | a^2 = 1\}$. Note that the 2-part of $\mathrm{Cl}^G_{\mathbb{Q}(\sqrt[4]{p})}$ is A^G. Applying Chevalley's formula on the quadratic extension $\mathbb{Q}(\sqrt[4]{p})/\mathbb{Q}(\sqrt{p})$ gives

$$|A[2]| = |A^G| = \frac{\prod_v e_v}{2} \frac{1}{[\mathcal{O}^\times_{\mathbb{Q}(\sqrt{p})} : \mathcal{O}^\times_{\mathbb{Q}(\sqrt{p})} \cap N(\mathbb{Q}(\sqrt[4]{p})^\times)]}.$$

Note that $-1 \notin N(\mathbb{Q}(\sqrt[4]{p}))$ since there is one infinite place ramified. This implies $[\mathcal{O}^\times_{\mathbb{Q}(\sqrt{p})} : \mathcal{O}^\times_{\mathbb{Q}(\sqrt{p})} \cap N(\mathbb{Q}(\sqrt[4]{p})^\times)] = 2$ or 4. We claim that $\prod_v e_v = 8$ for any odd p. Hence $|A[2]| = 1$ or 2. This implies that A is trivial or cyclic.

Now we prove the claim. Obviously, $(\sqrt{p})$ and ∞ are two ramified places of $\mathbb{Q}(\sqrt{p})$ where ∞ is the real embedding such that $\infty(\sqrt{p}) < 0$. Thus $\prod_{v \nmid 2} e_v = 4$. We compute the ramification index at 2 as follows.

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

If $p \equiv 5 \bmod 8$, then 2 is inert in $\mathbb{Q}(\sqrt{p})$. Locally, note that $(x+1)^2 - \sqrt{p}$ is an Eisenstein polynomial in $\mathbb{Q}_2(\sqrt{p})$, so 2 is ramified in $\mathbb{Q}_2(\sqrt[4]{p})$. Therefore $2\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$ is ramified in $\mathbb{Q}(\sqrt[4]{p})$. Hence $\prod_v e_v = 8$ where v runs over all places of $\mathbb{Q}(\sqrt{p})$.

If $p \equiv 1 \bmod 16$, $x^4 - p$ has solutions in $\mathbb{Q}_2$. Let $\sqrt[4]{p}$ be a solution. Then $\sqrt{p} = (\sqrt[4]{p})^2 \equiv 1 \bmod 8$. 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, $2\mathcal{O}_{\mathbb{Q}(\sqrt[4]{p})} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3^2$. Hence, among the two prime ideals of $\mathbb{Q}(\sqrt{p})$ above 2, one ramifies and the other splits in $\mathbb{Q}(\sqrt[4]{p})$. This implies that $\prod_v e_v = 8$ where v runs over all places of $\mathbb{Q}(\sqrt{p})$.

If $p \equiv 9 \bmod 16$, then $x^4 - p = (x^2 - \sqrt{p})(x^2 + \sqrt{p})$, and $\sqrt{p} \equiv \pm 3 \bmod 8$. We have $x^2 \pm \sqrt{p}$ are irreducible in $\mathbb{Q}_2[x]$ and exactly one of them is ramified. (recall $x^2 - 3$ is ramified and $x^2 - 5$ is unramified over $\mathbb{Q}_2$.) Among the two prime ideals of $\mathbb{Q}(\sqrt{p})$ above 2, one is ramified and the other is inert in $\mathbb{Q}(\sqrt[4]{p})$. Thus $\prod_v e_v = 8$ where v runs over all places of $\mathbb{Q}(\sqrt{p})$. This proves the claim. □

2. Proof

Let $p \equiv 15 \bmod 16$ be a prime in the rest of this note. Let $L = \mathbb{Q}(\sqrt[4]{p})$, $M = \mathbb{Q}(\sqrt[4]{p}, \sqrt{2})$ and $K = \mathbb{Q}(\sqrt{p}, \sqrt{2})$. Let $k_1 = \mathbb{Q}(\sqrt{p}), k_2 = \mathbb{Q}(\sqrt{2p}), k_3 = \mathbb{Q}(\sqrt{2})$ be the quadratic subfields of K.

Proposition 5. *We have $4 \mid h_L$ if and only if $2 \mid h_M$.*

Proof. Note that M/L is unramified outside 2. Since $p \equiv 15 \bmod 16$, $\mathbb{Q}_2(\sqrt[4]{p}) = \mathbb{Q}_2(\sqrt[4]{-1}) = \mathbb{Q}_2(\zeta_8) \supset \mathbb{Q}_2(\sqrt{2})$. Thus M/L is unramified at every prime ideal above 2, hence everywhere unramified.

By Hasse's norm theorem and local class field theory, $[\mathcal{O}_L^\times : \mathcal{O}_L^\times \cap N(M^\times)] = 1$. Applying Chevalley's formula (1.1) to M/L gives

$$|\mathrm{Cl}_M^{\mathrm{Gal}(M/L)}| = \frac{|\mathrm{Cl}_L|}{2}.$$

Therefore 4 divides $|\mathrm{Cl}_L| \iff 2$ divides $|\mathrm{Cl}_M^{\mathrm{Gal}(M/L)}| \iff 2$ divides $|\mathrm{Cl}_M|$. The last equivalence is due to Lemma 3. □

Proposition 6. (1) *The class numbers $h_{k_1}, h_{k_2}, h_{k_3}, h_K$ are all odd.*

(2) *Let $\epsilon_1, \epsilon_2, 1 + \sqrt{2}$ be the fundamental units of k_1, k_2, k_3 respectively. Then $\mathcal{O}_K^\times = \langle \sqrt{\epsilon_1}, \sqrt{\epsilon_2}, 1 + \sqrt{2} \rangle \times \{\pm 1\}$.*

Proof. (1) The oddness of $h_{k_1}, h_{k_2}, h_{k_3}$ is easy to prove by applying Chevalley's formula. We leave it to the readers. Note that the only ramified prime in K/k_1 is the unique prime ideal of k_1 above 2. Let $u \in \mathcal{O}_{k_1}$, 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 $u \in N_{K/k_1}(K^\times)$ by Hasse's norm theorem. Applying Chevalley's formula to K/k_1 and Lemma 3 give $2 \nmid h_K$.

(2) We first show that $\sqrt{\epsilon_i} \in K$ for $i = 1, 2$. Let $\mathfrak{q}_i$ be the unique prime ideal of k_i above 2. Since h_i is odd and $\mathfrak{q}_i^2 = (2)\mathcal{O}_{k_i}$, $\mathfrak{q}_i = (\pi_i)$ is principal. Thus $\frac{\pi_i^2}{2} \in \mathcal{O}_{k_i}^\times$. Since $p \equiv 15 \bmod 16$,

$N_{k_i/\mathbb{Q}}(\pi_i) = 2$. Therefore we may choose the generator π_i such that π_i is totally positive and $\epsilon_i = \frac{\pi_i^2}{2}$. Then $\sqrt{\epsilon_i} = \frac{\pi_i}{\sqrt{2}} \in K$. To prove the proposition, we need to show that $[\mathcal{O}_K^\times : \mathcal{O}_{k_1}^\times \mathcal{O}_{k_2}^\times \mathcal{O}_{k_3}^\times] = 4$.

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

$$[\mathcal{O}_K^\times : \mathcal{O}_{k_1}^\times \mathcal{O}_{k_2}^\times \mathcal{O}_{k_3}^\times] = \frac{4h_K}{h_1 h_2 h_3}.$$

Since $h_K, h_{k_1}, h_{k_2}, h_{k_3}$ are odd, it suffices to show that the index is a power of 2. Suppose not, let r be an odd prime divides this index. Then there exists a unit $\eta \in \mathcal{O}_K^\times$ such that $\eta^r = \pm\epsilon_1^a \epsilon_2^b (1+\sqrt{2})^c$ and $r \nmid \gcd(a,b,c)$. Note that $N_{K/k_1}(\eta^r) = \pm\epsilon_1^{2a}$, this implies $r \mid a$. Similarly, $r \mid b$ and $r \mid c$. This is a contradiction. □

Proposition 7. (1) *The product of ramification indices for M/K is* 16.

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

Proof. (1) Obviously, M/K is unramified outside $2, p, \infty$. In fact, M/K is unramified at 2, since

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

So the ramification places of M/K are $\mathfrak{p}_1, \mathfrak{p}_2, \infty_1, \infty_2$, where $\mathfrak{p}_1, \mathfrak{p}_2$ are the two prime ideals of K 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 $i = 1, 2$.

(2) As in the proof of the Proposition 6, we let $\mathfrak{q}_i$ $(i = 1, 2)$ be the unique prime ideal of k_i above 2. Let π_i be the totally positive generator of $\mathfrak{q}_i$ such that $\frac{\pi_i^2}{2}$ is the fundamental unit of k_i. Thus by Proposition 6,

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

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

Now we go to show that

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

Note that the left side is a subgroup of $\mathcal{O}_K^\times$ with index 4. 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 K 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. □

Lemma 8. (1) *We have $2 \pm \sqrt{2}$ is a square in $\mathbb{Q}_p$.*

(2) *We have π_1 is a square in $\mathbb{Q}_p(\sqrt{p})$.*

(3) *We have π_2 is a square in $\mathbb{Q}_p(\sqrt{2p}) = \mathbb{Q}_p(\sqrt{p})$.*

Proof. (1) Since $p \equiv 15 \bmod 16$, 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 $(\zeta_{16} + \zeta_{16}^{-1})^2 = \zeta_8 + \zeta_8^{-1} + 2 = 2 \pm \sqrt{2}$.

(2) Write $\pi_1 = a + b\sqrt{p}$ 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,

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

Since $a^2 \equiv 2 \bmod b$, i.e. $\left(\frac{2}{b}\right) = 1$, one has $b \equiv \pm 1 \bmod 8$ and then $b^2 \equiv 1 \bmod 16$. Thus $a^2 = 2 + pb^2 \equiv 1 \bmod 16$. Therefore $\left(\frac{2}{a}\right) = 1$. Hence $\pi_1 \bmod \sqrt{p}$ is a square in $\mathbb{Z}_p[\sqrt{p}]/(\sqrt{p})$. By Hensel's lemma, π_1 is a square in $\mathbb{Q}_p(\sqrt{p})$.

(3) Write $\pi_2 = c + d\sqrt{2p}$ with $c \in \mathbb{Z}_{\geq 1}, d \in \mathbb{Z}$. By Hensel's lemma, it is enough to prove that π_2 is a square modulo $\sqrt{2p}$, or equivalently $c \bmod p$ is a square. Write $c = 2^w c'$, where $2 \nmid c'$. From the identity $c^2 - 2pd^2 = 2$, one has

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

□

We are now ready to prove the Theorem.

Proof of the Theorem. The above two propositions and Chevalley's formula (1.1) show that

$$|\mathrm{Cl}_M^{\mathrm{Gal}(M/K)}| = 2.$$

By Proposition 5, we have $4 \mid h_L$. This finishes the proof. □

References

[1] F. Lemmermeyer, Kuroda's class number formula. Acta Arith. 66 (1994)245-260.
[2] P. Monsky. A reuslt of Lemmermeryer on class numbers. `https://arxiv.org/abs/1009.3990`.
[3] C.J. Parry, A genus theory for quartic fields. J. Reine Angew. Math. 314 (1980), 4071.

Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui 230026, China
E-mail address: `lijn@ustc.edu.cn`