Bull. Aust. Math. Soc. **85** (2012), 359–370
doi:10.1017/S0004972711003352

ON THE CLASS NUMBER AND THE FUNDAMENTAL UNIT OF THE REAL QUADRATIC FIELD $k = \mathbb{Q}(\sqrt{pq})$

JAE MOON KIM and JADO RYU ✉

(Received 22 May 2011)

Abstract

For a real quadratic field $k = \mathbb{Q}(\sqrt{pq})$, let t_k be the exact power of 2 dividing the class number h_k of k and η_k the fundamental unit of k. The aim of this paper is to study t_k and the value of $N_{k/\mathbb{Q}}(\eta_k)$. Various methods have been successfully applied to obtain results related to this topic. The idea of our work is to select a special circular unit $\mathcal{E}_k$ of k and investigate $C(k) = \langle \pm\mathcal{E}_k \rangle$. We examine the indices $[E(k) : C(k)]$ and $[C(k) : C_S(k)]$, where $E(k)$ is the group of units of k, and $C_S(k)$ is that of circular units of k defined by Sinnott. Then by using the Sinnott's index formula $[E(k) : C_S(k)] = h_k$, we obtain as much information about t_k and $N_{k/\mathbb{Q}}(\eta_k)$ as possible.

2010 *Mathematics subject classification*: primary 11R11; secondary 11R29.
Keywords and phrases: class number, fundamental unit, circular unit, unit index, index formula.

1. Introduction

Let k be a real quadratic field of the form $k = \mathbb{Q}(\sqrt{pq})$. Let $h = h_k$ be the class number of k, and $t = t_k$ the exact power of 2 dividing h, that is, $2^t \mid h$ but $2^{t+1} \nmid h$. The aim of this paper is to study t and $N_{k/Q}(\eta_k)$, where η_k is the fundamental unit of k. Our results are summarised in Table 1. In this table, $(\cdot/p)$ is the Legendre symbol. And when $p \equiv 1 \pmod 4$, $(\cdot/p)_4$ is defined to be

$$\left(\frac{a}{p}\right)_4 = \begin{cases} 1 & \text{if } a^{(p-1)/4} \equiv 1 \pmod p \\ -1 & \text{if } a^{(p-1)/4} \equiv -1 \pmod p. \end{cases}$$

When $p \equiv 1 \pmod 8$,

$$\left(\frac{-1}{p}\right)_8 = (-1)^{(p-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{16} \\ -1 & \text{if } p \equiv 9 \pmod{16}. \end{cases}$$

Both 1 and -1 occur in the blanks.

This work was supported by INHA UNIVERSITY Research Grant.

Table 1. Summary of results in this paper.

<table>
<tr><th colspan="4">p, q</th><th>t</th><th>$N_{k/\mathbb{Q}}(\eta_k)$</th></tr>
<tr><td>$p \equiv 3 \pmod 4$</td><td colspan="3">$q \not\equiv 1 \pmod 4$</td><td>$t = 0$</td><td>1</td></tr>
<tr><td rowspan="10">$p \equiv 1 \pmod 4$</td><td rowspan="4">$q \equiv 1 \pmod 4$</td><td colspan="2">$(q/p) = -1$</td><td>$t = 1$</td><td>-1</td></tr>
<tr><td rowspan="3">$(q/p) = 1$</td><td>$(q/p)_4 \cdot (p/q)_4 = -1$</td><td>$t = 1$</td><td>1</td></tr>
<tr><td>$(q/p)_4 = (p/q)_4 = -1$</td><td>$t = 2$</td><td>-1</td></tr>
<tr><td>$(q/p)_4 = (p/q)_4 = 1$</td><td>$t \geq 2$</td><td></td></tr>
<tr><td rowspan="4">$q = 2$</td><td colspan="2">$(-1/p)_4 = -1$</td><td>$t = 1$</td><td>-1</td></tr>
<tr><td rowspan="3">$(-1/p)_4 = 1$</td><td>$(-1/p)_8 \cdot (2/p)_4 = -1$</td><td>$t = 1$</td><td>1</td></tr>
<tr><td>$(-1/p)_8 = (2/p)_4 = -1$</td><td>$t = 2$</td><td>-1</td></tr>
<tr><td>$(-1/p)_8 = (2/p)_4 = 1$</td><td>$t \geq 2$</td><td></td></tr>
<tr><td rowspan="2">$q \equiv 3 \pmod 4$</td><td colspan="2">$(q/p) = -1$ or $(2/p) = -1$</td><td>$t = 1$</td><td>1</td></tr>
<tr><td colspan="2">$(q/p) = (2/p) = 1$</td><td>$t \geq 2$</td><td>1</td></tr>
</table>

Various results have been published in relation to to this topic. Kučera [7], for instance, proved the case where $p \equiv q \equiv 1 \pmod 4$ by manipulating a certain circular unit. Brown [1] took care of the case where $p \equiv 1 \pmod 4$ with $(-1/p)_4 = 1$ and $q = 2$ by using the theory of quadratic forms, while Conner and Hurrelbrink [2] applied the theory of group cohomology to handle some of the other cases.

In this paper, we use the circular unit mentioned in [6] to obtain Table 1. The index formula discovered by Sinnott [8] plays the most important role in our work. For real quadratic fields, Sinnott's formula simply reads $h_k = [E(k) : C_S(k)]$ [4], where $E(k)$ is the unit group of k, and $C_S(k)$ is the group of circular units of k defined by Sinnott [8]. Let n be the conductor of k. Put $F = \mathbb{Q}(\zeta_n)$, $\delta_F = 1 - \zeta_n$, and $\delta_E = N_{F/E}(\delta_F)$ for a subfield E of F, where $\zeta_n = e^{2\pi i/n}$. Since $C_S(k)$ is of rank one generated by $\{-1, N_{F/k}(1 - \zeta_n^a) \mid (a, n) = 1\}$, $C_S(k) = \langle -1, \delta_k \rangle$. The generator δ_k can be replaced by δ_k', a conjugate of δ_k over $\mathbb{Q}$.

In Section 2, we study the first row of Table 1. In this case, k is a subfield of $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$. Note that K is a CM-field with $K^+ = k$, and the index formula for K says that $[E(K) : C_S(K)] = (1/2)Q_E(K)h_{K^+}$ [3], where $Q_E(K)$ is the unit index of K. That is, $Q_E(K) = [E(K) : W(K)E(K^+)]$, where $W(K)$ is the group of roots of unity in K. From these two formulas, we obtain the desired results.

In the remaining sections, we assume that $p \equiv 1 \pmod 4$. Roughly, to compute t_k and $N_{k/\mathbb{Q}}(\eta_k)$, we shall choose a special unit $\mathcal{E}_k$ in k, and investigate the subgroup $C(k)$ of $E(k)$ generated by $\pm\mathcal{E}_k$ which contains $C_S(k)$. We then analyse $[E(k) : C(k)]$ and $[C(k) : C_S(k)]$ to get the information about $h_k = [E(k) : C_S(k)]$ and $N_{k/\mathbb{Q}}(\eta_k)$. When $q \equiv 3 \pmod 4$, the conductor n of k is $4pq$, which involves three primes and thus causes extra difficulties. So we have to be a little more careful. The final section takes care of this case. And in Section 3, we discuss the other two cases.

https://doi.org/10.1017/S0004972711003352 Published online by Cambridge University Press

2. $\mathbb{Q}(\sqrt{pq})$ with $p \equiv 3 \pmod 4$ and $q \not\equiv 1 \pmod 4$

In this section, we study t_k and $N_{k/\mathbb{Q}}(\eta_k)$ when $k = \mathbb{Q}(\sqrt{pq})$ with $p \equiv 3 \pmod 4$ and $q \not\equiv 1 \pmod 4$. There are three cases to consider: (i) $q \equiv 3 \pmod 4$ and $q \neq 3$, (ii) $q = 3$, and (iii) $q = 2$. In any case, k is a subfield of $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$. The class number formula for K says that $[E(K) : C_S(K)] = (1/2)Q_E(K)h_{K^+}$ [3]. We first examine the unit index $Q_E(K)$.

LEMMA 2.1. *Let $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$ with $p \equiv 3 \pmod 4$ and $q \not\equiv 1 \pmod 4$. Then we have $Q_E(K) = 2$.*

PROOF. We only give a proof for $q = 2$. The other cases can be treated similarly, or the reader may refer to [5], where the unit index is determined when the conductor is odd. Note that the conductor n of $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-2})$ is $8p$. So $F = \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{8p})$. In order to prove $Q_E(K) = 2$, it suffices to show that $\delta_K^J = -\delta_K$, where J is complex conjugation. We compute $N_{K/\mathbb{Q}(\sqrt{-2})}(\delta_K)$ and $N_{K/\mathbb{Q}(\sqrt{-p})}(\delta_K)$.

Let a be an integer satisfying $ap \equiv 1 \pmod 8$. Then $a \equiv p \pmod 8$. So

$$N_{K/\mathbb{Q}(\sqrt{-2})}(\delta_K) = N_{\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{-2})}(N_{F/\mathbb{Q}(\zeta_8)}(\delta_F)) = N_{\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{-2})}\left(\frac{1-\zeta_8}{1-\zeta_8^p}\right).$$

Note that Gal $(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{-2}))$ is generated by the isomorphism sending ζ_8 to ζ_8^3. Thus

$$N_{K/\mathbb{Q}(\sqrt{-2})}(\delta_K) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 8 \\ -1 & \text{if } p \equiv 7 \pmod 8). \end{cases}$$

On the other hand,

$$N_{K/\mathbb{Q}(\sqrt{-p})}(\delta_K) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p})}(N_{F/\mathbb{Q}(\zeta_p)}(\delta_F)) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p})}\left(\frac{1-\zeta_p}{1-\zeta_p^{2^{-1}}}\right),$$

where 2^{-1} is the inverse of $2 \pmod p$. If $(2/p) = 1$, then the automorphism $\sigma_{2^{-1}}$ of $\mathbb{Q}(\zeta_p)$ sending ζ_p to $\zeta_p^{2^{-1}}$ permutes the elements of Gal $(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p}))$. Thus $N_{K/\mathbb{Q}(\sqrt{-p})}(\delta_K) = 1$. Suppose that $(2/p) = -1$. Then $\sigma_{2^{-1}} \notin$ Gal $(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p}))$. Let $\pi = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p})}(1-\zeta_p)$. Then $\pi^{1+\sigma_2^{-1}} = p$ and $\pi^{1-\sigma_2^{-1}} = \pm 1$. If $\pi^{1-\sigma_2^{-1}} = 1$, then $\pi^{1+\sigma_2^{-1}} = \pi^2 = p$. So $\pi \in \mathbb{Q}(\sqrt{p})$, which is impossible. Thus $N_{K/\mathbb{Q}(\sqrt{-p})}(\delta_K) = \pi^{1-\sigma_2^{-1}} = -1$. Therefore

$$N_{K/\mathbb{Q}(\sqrt{-p})}(\delta_K) = \begin{cases} -1 & \text{if } p \equiv 3 \pmod 8 \\ 1 & \text{if } p \equiv 7 \pmod 8). \end{cases}$$

Hence $N_{K/\mathbb{Q}(\sqrt{-p})}(\delta_K) \neq N_{K/\mathbb{Q}(\sqrt{-2})}(\delta_K)$ in any case.

If $\delta_K^J = \delta_K$, then $\delta_K \in k = \mathbb{Q}(\sqrt{2p})$. So $N_{k/\mathbb{Q}}(\delta_K) = N_{K/\mathbb{Q}(\sqrt{-p})}(\delta_K) = N_{K/\mathbb{Q}(\sqrt{-2})}(\delta_K)$, which is a contradiction. Therefore $\delta_K^J = -\delta_K$, and this proves the lemma. □

https://doi.org/10.1017/S0004972711003352 Published online by Cambridge University Press

By the lemma,

$$[E(K):C_S(K)] = h_{K^+} = h_k \quad \text{and} \quad [E(K):W(K)E(k)] = 2.$$

Note that $\mathrm{rank}_{\mathbb{Z}} E(K) = 1$. Let η_K be a generator of $E(K)$ modulo $W(K)$.

THEOREM 2.2. *Let $k = \mathbb{Q}(\sqrt{pq})$ with $p \equiv 3 \pmod 4$ and $q \not\equiv 1 \pmod 4$. Then we have $N_{k/\mathbb{Q}}(\eta_k) = 1$ and $2 \nmid h_k$.*

PROOF. Since $[E(K):W(K)E(k)] = 2$, $\eta_K^2 = \alpha\eta_k$ for some $\alpha \in W(K)$. Thus

$$N_{k/\mathbb{Q}}(\eta_k) = N_{K/\mathbb{Q}(\sqrt{-p})}(\eta_k) = N_{K/\mathbb{Q}(\sqrt{-p})}(\eta_K^2\alpha^{-1}) = 1.$$

To prove $2 \nmid h_k$, we treat three cases separately.

(i) $q \equiv 3 \pmod 4$ and $q \neq 3$. Since $(q/p)(p/q) = -1$, we may take $(q/p) = -1$. Then

$$N_{K/\mathbb{Q}(\sqrt{-p})}(\delta_K) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p})}(N_{F/\mathbb{Q}(\zeta_p)}(\delta_F)) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p})}\left(\frac{1-\zeta_p}{1-\zeta_p^{q^{-1}}}\right) = \pm 1.$$

Since $(q/p) = -1$, $\sigma_{q^{-1}} \notin \mathrm{Gal}\,(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p}))$, where $\sigma_{q^{-1}}$ is the automorphism of $\mathbb{Q}(\zeta_p)$ sending ζ_p to $\zeta_p^{q^{-1}}$. Then as in the proof of Lemma 2.1, $N_{K/\mathbb{Q}(\sqrt{-p})}(\delta_K) = -1$. Suppose that $2 \mid h_k = [E(K):C_S(K)]$. Put $h_k = 2m$. Then $\eta_K^{2m} = \pm\delta_K^j$ for some odd integer j. By taking norms of both sides from K to $\mathbb{Q}(\sqrt{-p})$, we get a contradiction.

(ii) $q = 3$. In this case, $K = \mathbb{Q}(\sqrt{-3}, \sqrt{-p})$ and $E(K) = \langle -\zeta_3, \eta_K \rangle$. Suppose that $2 \mid h_k$. Then $\eta_K^{2m} = \pm\zeta_3^i\delta_K^j$ for some odd integer j.

If $(p/3) = 1$, then $(3/p) = -1$. After a computation similar to that of case (i), we see that

$$N_{K/\mathbb{Q}(\sqrt{-p})}(\delta_K) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p})}\left(\frac{1-\zeta_p}{1-\zeta_p^{3^{-1}}}\right) = -1.$$

By taking norms of both sides of $\eta_K^{2m} = \pm\zeta_3^i\delta_K^j$ from K to $\mathbb{Q}(\sqrt{-p})$, we have $1 = N_{K/\mathbb{Q}(\sqrt{-p})}(\pm\zeta_3^i\delta_K^j) = -1$, which is absurd. So $2 \nmid h_k$.

On the other hand, suppose that $(p/3) = -1$. In this case, we take norms of both sides of the equation $\eta_K^{2m} = \pm\zeta_3^i\delta_K^j$ from K to $\mathbb{Q}(\sqrt{-3})$. Then

$$N_{K/\mathbb{Q}(\sqrt{-3})}(\eta_K^{2m}) = N_{K/\mathbb{Q}(\sqrt{-3})}(\pm\zeta_3^i\delta_K^j).$$

Since $N_{K/\mathbb{Q}(\sqrt{-3})}(\eta_K)$ is a unit in $\mathbb{Q}(\sqrt{-3})$, the left-hand side is of the form ζ_3^α. And since

$$N_{K/\mathbb{Q}(\sqrt{-3})}(\delta_K) = N_{\mathbb{Q}(\zeta_{3p})/\mathbb{Q}(\zeta_3)}(\delta_F) = \frac{1-\zeta_3}{1-\zeta_3^{p^{-1}}} = -\zeta_3,$$

the right-hand side equals $\zeta_3^{2i}(-\zeta_3)^j = -\zeta_3^\beta$ for some β. Thus $\zeta_3^\alpha = -\zeta_3^\beta$, which cannot happen. Hence $2 \nmid h_k$.

(iii) $q = 2$. We saw in the proof of Lemma 2.1 that $N_{K/\mathbb{Q}(\sqrt{-2})}(\delta_K) = -1$ if $p \equiv 7 \pmod 8$ and $N_{K/\mathbb{Q}(\sqrt{-p})}(\delta_K) = -1$ if $p \equiv 3 \pmod 8$. Suppose that $2 \mid h_k$. Then $\eta_K^{2m} = \pm\delta_K^j$ for some odd integer j. But this is impossible since $N_{K/\mathbb{Q}(\sqrt{-2})}(\eta_K^{2m}) = N_{K/\mathbb{Q}(\sqrt{-p})}(\eta_K^{2m}) = 1$. □

https://doi.org/10.1017/S0004972711003352 Published online by Cambridge University Press

REMARK 2.3. Since $N_{k/\mathbb{Q}}(\eta_k) = 1$, -1 is not a norm of a unit in $E(k)$. That is, $-1 \notin N_{k/\mathbb{Q}}E(k)$. We can say a little more. Indeed, by Remark 4.3 at the end of this paper, $\widehat{H}^0(G, E_k) \longrightarrow \widehat{H}^0(G, k^\times)$ is injective, where $G = \mathrm{Gal}\,(k/\mathbb{Q})$. Thus -1 cannot be a norm element from $k^\times$ either.

3. $\mathbb{Q}(\sqrt{pq})$ with $p \equiv 1 \pmod 4$ and $q \not\equiv 3 \pmod 4$

Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. It is clear that $2 \mid h_k$ since K/k is an unramified extension. We investigate the divisibility of h_k by a higher power of 2 by playing around with a suitable unit of k. Fix a generator σ of $\mathrm{Gal}\,(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and τ of $\mathrm{Gal}\,(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ when $q \neq 2$, and extend them to $\mathbb{Q}(\zeta_n)$ naturally, that is, $\zeta_q^\sigma = \zeta_q$ and $\zeta_p^\tau = \zeta_p$. Let J_1 be the complex conjugation of $\mathbb{Q}(\zeta_p)$ or its extension to $\mathbb{Q}(\zeta_n)$, so that $\zeta_p^{J_1} = \zeta_p^{-1}$ and $\zeta_q^{J_1} = \zeta_q$. We similarly define J_2, that is, $\zeta_p^{J_2} = \zeta_p$ and $\zeta_q^{J_2} = \zeta_q^{-1}$. Thus $J = J_1J_2$ is the complex conjugation of $\mathbb{Q}(\zeta_n)$. When $q = 2$, the conductor of k is $8p$. In this case, τ is a generator of $\mathrm{Gal}\,(\mathbb{Q}(\zeta_{16})^+/\mathbb{Q})$ or its natural extension to $\mathbb{Q}(\zeta_{16p})$ so that $\zeta_{4p}^\tau = \zeta_{4p}$, and J_2 is the complex conjugation of $\mathbb{Q}(\zeta_{16})$ or its extension to $\mathbb{Q}(\zeta_{16p})$. For each integer i, put $v_p(i) = ((1 - \zeta_p^{\sigma^i})/(1 - \zeta_p))\zeta_p^{(1-\sigma^i)/2}$. Then $v_p(i) \in \mathbb{Q}(\zeta_p)^+$. We denote $N_{\mathbb{Q}(\zeta_p)^+/\mathbb{Q}(\sqrt{p})}(v_p(i))$ by $\overline{v}_p(i)$. Note that $\overline{v}_p(1)$ is a unit in $\mathbb{Q}(\sqrt{p})$ which differs from ± 1. In fact, $\overline{v}_p(1)^2$ generates the Sinnott group of circular units of $\mathbb{Q}(\sqrt{p})$ modulo $\{\pm 1\}$.

LEMMA 3.1. *The unit $\overline{v}_p(i)$ satisfies:*

(1) $N_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}(\overline{v}_p(i)) = (-1)^i$;

(2) $\overline{v}_p(i) = \begin{cases} (-1)^m & \text{if } i = 2m \\ (-1)^m \overline{v}_p(1) & \text{if } i = 2m + 1. \end{cases}$

PROOF. Put $t = [\mathbb{Q}(\zeta_p)^+ : \mathbb{Q}(\sqrt{p})] = (p-1)/4$. Then for any integers a, b, and c, $v_p(2t) = -1$, $v_p(2t + c) = -v_p(c)$, and $\sigma^a v_p(b) = v_p(a + b)/v_p(a)$. We prove (1) by induction on i, which is clear when $i = 0$. Assuming the result for i, then

$$\begin{aligned} N_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}\overline{v}_p(i+1) &= N_{\mathbb{Q}(\zeta_p)^+/\mathbb{Q}} v_p(i+1) \\ &= \prod_{\alpha=0}^{2t-1} \frac{v_p(i+1+\alpha)}{v_p(\alpha)} \\ &= \frac{\prod_{\alpha=0}^{2t-2} v_p(i+1+\alpha)}{\prod_{\alpha=0}^{2t-1} v_p(\alpha)} v_p(i+2t) \\ &= -\prod_{\beta=0}^{2t-1} \frac{v_p(i+\beta)}{v_p(\beta)} \\ &= -N_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}\overline{v}_p(i). \end{aligned}$$

We omit the proof of (2) since it is similar to that of (1). □

https://doi.org/10.1017/S0004972711003352 Published online by Cambridge University Press

3.1. $p \equiv q \equiv 1 \pmod 4$. Let σ_q be the Frobenius automorphism of $\mathbb{Q}(\zeta_p)$ for q, and l_q an integer such that $\sigma_{q^{-1}} = \sigma^{l_q}$. Then $N_{F/\mathbb{Q}(\zeta_p)}((1-\zeta_n)\zeta_n^{-1/2}) = v_p(l_q)^{-1}$. By interchanging the roles of p and q, we have $N_{F/\mathbb{Q}(\zeta_q)}((1-\zeta_n)\zeta_n^{-1/2}) = v_q(l_p)^{-1}$. Note that $2 \mid l_p$ if and only if $p^{(q-1)/2} \equiv 1 \pmod q$, that is, $(p/q) = 1$. Since $p \equiv q \equiv 1 \pmod 4$, $(p/q) = (q/p)$. Thus $2 \mid l_p$ if and only if $2 \mid l_q$. Similarly $4 \mid l_p$ if and only if $p^{(q-1)/4} \equiv 1 \pmod q$, that is, $(p/q)_4 = 1$.

Let $L = \mathbb{Q}(\zeta_p)^+\mathbb{Q}(\zeta_q)^+$, and $e_L = (1-\zeta_n)(1-\zeta_n^{J_2})\zeta_n^{-(1+J_2)/2}$. It is easy to see that e_L is fixed by J_1 and J_2, so that $e_L \in L$. Note that $N_{F/L}(\delta_F) = e_L^2$ and

$$e_L = N_{F/\mathbb{Q}(\zeta_p)\mathbb{Q}(\zeta_q)^+}(1-\zeta_n)\zeta_n^{-1/2} = -N_{F/\mathbb{Q}(\zeta_p)^+\mathbb{Q}(\zeta_q)}(1-\zeta_n)\zeta_n^{-1/2}.$$

Put

$$e_K = N_{L/K}(e_L),\ e_k = N_{K/k}(e_K) \quad \text{and} \quad \mathcal{E}_k = e_K^{\sigma+\tau}.$$

Since $\mathcal{E}_k^{\sigma\tau} = e_K^{(\sigma+\tau)\sigma\tau} = e_K^{\sigma+\tau} = \mathcal{E}_k$, $\mathcal{E}_k$ is fixed by $\mathrm{Gal}(K/k)$. Thus $\mathcal{E}_k \in k$. In fact, $\mathcal{E}_k = e_k^{\sigma} = e_k^{\tau}$. We express $\mathcal{E}_k$ as

$$\mathcal{E}_k = e_K^{\sigma+\tau} = e_K^{1+\sigma} \cdot e_K^{1+\tau} \cdot e_K^{-2}.$$

Here

$$\begin{aligned} e_K^{1+\sigma} &= N_{K/\mathbb{Q}(\sqrt{q})}(e_K) \\ &= N_{K/\mathbb{Q}(\sqrt{q})}N_{L/K}(e_L) \\ &= N_{K/\mathbb{Q}(\sqrt{q})}N_{L/K}(-N_{F/\mathbb{Q}(\zeta_p)^+\mathbb{Q}(\zeta_q)}((1-\zeta_n)\zeta_n^{-1/2})) \\ &= N_{\mathbb{Q}(\zeta_q)^+/\mathbb{Q}(\sqrt{q})}(v_q(l_p)^{-1}) \\ &= \overline{v}_q(l_p)^{-1}. \end{aligned}$$

Similarly,

$$e_K^{1+\tau} = \overline{v}_p(l_q)^{-1}.$$

Hence

$$\mathcal{E}_k = \overline{v}_q(l_p)^{-1} \cdot \overline{v}_p(l_q)^{-1} \cdot e_K^{-2}.$$

It is possible that $e_K \in k$. Let us examine when this happens. Note that $e_K \in k$ if and only if $e_K^{\sigma\tau} = e_K$. This is equivalent to $e_K^{1+\sigma} = e_K^{1+\tau}$. Hence

$$e_K \in k \text{ if and only if } l_p \equiv l_q \equiv 0 \pmod 2, \text{ and } (-1)^{l_p/2} = (-1)^{l_q/2}.$$

We also have

$$N_{k/\mathbb{Q}}(\mathcal{E}_k) = e_K^{1+\sigma+\tau+\sigma\tau} = e_K^{(1+\sigma)(1+\tau)} = N_{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}(\,\overline{v}_q(l_p)^{-1}) = \begin{cases} 1 & \text{if } 2 \mid l_p \\ -1 & \text{if } 2 \nmid l_p. \end{cases}$$

THEOREM 3.2. *Let $k = \mathbb{Q}(\sqrt{pq})$ with $p \equiv q \equiv 1 \pmod 4$. Then:*

(1) *if $(q/p) = (p/q) = -1$, then $2 \mid h_k$, $4 \nmid h_k$, and $N_{k/\mathbb{Q}}(\eta_k) = -1$;*

(2) *if $(p/q)_4 \cdot (q/p)_4 = -1$, then $2 \mid h_k$, $4 \nmid h_k$, and $N_{k/\mathbb{Q}}(\eta_k) = 1$;*

https://doi.org/10.1017/S0004972711003352 Published online by Cambridge University Press

(3) *if* $(p/q)_4 = (q/p)_4 = -1$, *then* $4 \mid h_k$, $8 \nmid h_k$, *and* $N_{k/\mathbb{Q}}(\eta_k) = -1$;
(4) *if* $(p/q)_4 = (q/p)_4 = 1$, *then* $4 \mid h_k$.

PROOF. Let $C(k) = \langle -1, \mathcal{E}_k \rangle$. Since $N_{F/L}(\delta_F) = e_L^2$, $C_S(k) = \langle -1, e_k^2 \rangle$. Thus $C_S(k) = \langle -1, (e_k^\sigma)^2 \rangle = \langle -1, \mathcal{E}_k^2 \rangle$. Hence $[C(k) : C_S(k)] = 2$. In case (1), l_p (hence l_q as well) is odd. So $N_{k/\mathbb{Q}}(\mathcal{E}_k) = -1$, which implies that $2 \nmid [E(k) : C(k)]$ and $N_{k/\mathbb{Q}}(\eta_k) = -1$. Since

$$h_k = [E(k) : C_S(k)] = [E(k) : C(k)][C(k) : C_S(k)],$$

we get the results as asserted. Next, we suppose that $(p/q)_4 \cdot (p/q)_4 = -1$. We may assume that $(p/q)_4 = -1$ and $(q/p)_4 = 1$. Then $l_q = 4m_1$ and $l_p = 4m_2 + 2$, for some m_1 and m_2. In this case $\mathcal{E}_k = -e_K^{-2}$ and $e_K \notin k$. Hence $2 \nmid [E(k) : C(k)]$, for otherwise $\eta_k^{2m} = \pm\mathcal{E}_k = e_K^{-2}$ would imply that $e_K^{-1} = \pm\eta_k^m \in k$. Since $N_{k/\mathbb{Q}}(\mathcal{E}_k) = 1$, we also have $N_{k/\mathbb{Q}}(\eta_k) = 1$. Therefore $2 \mid h_k$, $4 \nmid h_k$ and $N_{k/\mathbb{Q}}(\eta_k) = 1$. In case (3), l_p and l_q are of the forms $l_p = 4m_1 + 2$ and $l_q = 4m_2 + 2$. Thus $e_K^{1+\sigma} = e_K^{1+\tau} = -1$, $\mathcal{E}_k = e_K^{-2}$, and $e_K \in k$. Put $C' = \langle -1, e_K \rangle$. Then

$$[C' : C_S(k)] = [C' : C(k)][C(k) : C_S(k)] = 4.$$

Moreover, $N_{k/\mathbb{Q}}(e_K) = e_K^{1+\sigma} = -1$. Therefore $2 \nmid [E(k) : C']$ and $N_{k/\mathbb{Q}}(\eta_k) = -1$, and we obtain the desired results. Finally, condition (4) says that both l_1 and l_2 are multiples of 4. So $e_K \in k$ and thus $4 = [C' : C_S(k)] \mid h_k$. This concludes the proof. □

REMARK 3.3. In case (4) of this theorem, both 1 and -1 can be the value of $N_{k/\mathbb{Q}}(\eta_k)$. When $k = \mathbb{Q}(\sqrt{5 \cdot 101})$ or $k = \mathbb{Q}(\sqrt{29 \cdot 181})$, for instance, $N_{k/\mathbb{Q}}(\eta_k) = 1$, while $N_{k/\mathbb{Q}}(\eta_k) = -1$ when $k = \mathbb{Q}(\sqrt{5 \cdot 461})$. If $N_{k/\mathbb{Q}}(\eta_k) = -1$, then $8 \mid h_k$ since $2 \mid [E(k) : C']$. Indeed, the class number of $\mathbb{Q}(\sqrt{5 \cdot 461})$ is 16. And even if $N_{k/\mathbb{Q}}(\eta_k) = 1$, h_k can be a multiple of 8. For example, $\mathbb{Q}(\sqrt{5 \cdot 101})$ has the class number 4, while $\mathbb{Q}(\sqrt{29 \cdot 181})$ has the class number 8.

3.2. $p \equiv 1 \pmod 4$, and $q = 2$. Put $L = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\zeta_p)^+$ and $K = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ as before. Let

$$e_L = (1 - \zeta_{8p})(1 - \zeta_{8p}^{J_2})\zeta_{16p}^{-(1+J_2)}.$$

Since $J_2 \equiv -1 \pmod{16}$, $e_L \in F$. Furthermore, since J_1 and J_2 fix e_L then $e_L \in L$. As in the previous case, put $e_K = N_{L/K}(e_L)$, $e_k = N_{K/k}(e_K)$, and $\mathcal{E}_k = e_K^{\sigma+\tau}$. Then since $N_{F/L}(\delta_F) = e_L^2$, $C_S(k) = \langle -1, e_k^2 \rangle = \langle -1, e_k^{2\sigma} \rangle$. Now we analyse each term of the product

$$\mathcal{E}_k = e_K^{\sigma+\tau} = e_K^{1+\sigma} \cdot e_K^{1+\tau} \cdot e_K^{-2}.$$

First,

$$e_K^{1+\sigma} = N_{L/\mathbb{Q}(\sqrt{2})}(e_L) = N_{\mathbb{Q}(\zeta_{16p})/\mathbb{Q}(\zeta_{16})}((1 - \zeta_{8p})\zeta_{16p}^{-1}) = \frac{1 - \zeta_8}{1 - \zeta_8^{p^{-1}}}\zeta_{16}^{p^{-1}-1},$$

where p^{-1} is the inverse of $p \pmod{16}$. Hence

$$e_K^{1+\sigma} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{16} \\ -1 & \text{if } p \equiv 9 \pmod{16} \\ \pm(\sqrt{2}-1) & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

The second term $e_K^{1+\tau}$ is the same as before. Namely,

$$e_K^{1+\tau} = \bar{v}_p(l_2)^{-1} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{8} \text{ and } \left(\dfrac{2}{p}\right)_4 = 1 \\ -1 & \text{if } p \equiv 1 \pmod{8} \text{ and } \left(\dfrac{2}{p}\right)_4 = -1 \\ \pm\bar{v}_p(1)^{-1} & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

For the last term, $e_K \in k$ if and only if either $p \equiv 1 \pmod{16}$ and $(2/p)_4 = 1$, or $p \equiv 9 \pmod{16}$ and $(2/p)_4 = -1$. Hence $e_K \in k$ if and only if $p \equiv 1 \pmod 8$ and $(-1/p)_8 \cdot (2/p)_4 = 1$. Also note that

$$N_{k/\mathbb{Q}}(\mathcal{E}_k) = N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(e_K^{1+\sigma}) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{8} \\ -1 & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

THEOREM 3.4. *Let $k = \mathbb{Q}(\sqrt{2p})$ with $p \equiv 1 \pmod 4$. Then:*

(1) *if $(-1/p)_4 = -1$, then $2 \mid h_k$, $4 \nmid h_k$, and $N_{k/\mathbb{Q}}(\eta_k) = -1$;*
(2) *if $(-1/p)_8 \cdot (2/p)_4 = -1$, then $2 \mid h_k$, $4 \nmid h_k$, and $N_{k/\mathbb{Q}}(\eta_k) = 1$;*
(3) *if $(-1/p)_8 = (2/p)_4 = -1$, then $4 \mid h_k$, $8 \nmid h_k$, and $N_{k/\mathbb{Q}}(\eta_k) = -1$;*
(4) *if $(-1/p)_8 = (2/p)_4 = 1$, then $4 \mid h_k$.*

PROOF. This can be proved in a similar way to Theorem 3.2. □

REMARK 3.5. As in case (4) of Theorem 3.2, both 1 and -1 occur as the value of $N_{k/\mathbb{Q}}(\eta_k)$ when $(-1/p)_8 = (2/p)_4 = 1$. For example, $N_{k/\mathbb{Q}}(\eta_k) = 1$ when k is $\mathbb{Q}(\sqrt{2 \cdot 257})$ or $\mathbb{Q}(\sqrt{2 \cdot 1217})$. The class numbers are 4 and 8, respectively. And when $k = \mathbb{Q}(\sqrt{2 \cdot 113})$, $N_{k/\mathbb{Q}}(\eta_k) = -1$ and $h_k = 8$, a multiple of 8 as it should be.

4. $\mathbb{Q}(\sqrt{pq})$ with $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$

In this case, the conductor of $k = \mathbb{Q}(\sqrt{pq})$ is $n = 4pq$. Let J_1 and J_2 be such that $\zeta_p^{J_1} = \zeta_p^{-1}$, $\zeta_{8q}^{J_1} = \zeta_{8q}$, and $\zeta_p^{J_2} = \zeta_p$, $\zeta_{8q}^{J_2} = \zeta_{8q}^{-1}$. As in the previous section, σ is a fixed generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, or its natural extension to $\mathbb{Q}(\zeta_{8pq})$ such that $\zeta_{8q}^{\sigma} = \zeta_{8q}$. And τ is a fixed generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ or its extension to $\mathbb{Q}(\zeta_{8pq})$ such that $\zeta_{8p}^{\tau} = \zeta_{8p}$. Then $\tau(\sqrt{-q}) = -\sqrt{-q}$ and $\tau(\sqrt{q}) = -\sqrt{q}$, and thus $\mathrm{Gal}(\mathbb{Q}(\sqrt{q})/\mathbb{Q}) = \{1, \tau\}$. Let $L = \mathbb{Q}(\zeta_{4q})^+\mathbb{Q}(\zeta_p)^+$, and $e_L = (1-\zeta_n)(1-\zeta_n^{J_2})\zeta_{2n}^{-(1+J_2)}$. Since $J_2 \equiv -1 \pmod{8q}$ and since e_L is fixed by J_1 and J_2, $e_L \in L$. Let

$$K = \mathbb{Q}(\sqrt{p}, \sqrt{q}), \; e_K = N_{L/K}(e_L), \; e_k = N_{K/k}(e_K)$$

https://doi.org/10.1017/S0004972711003352 Published online by Cambridge University Press

and $\mathcal{E}_k = e_K^{\sigma+\tau}$ as before. Note that

$$N_{F/L}(1-\zeta_n) = e_L^2, \quad ((1-\zeta_n)\zeta_{2n}^{-1})^{1+J_2} = e_L,$$

and $((1-\zeta_n)\zeta_{2n}^{-1})^{1+J_1} = -e_L$. We analyse each term in the product

$$\mathcal{E}_k = e_K^{\sigma+\tau} = e_K^{1+\sigma} \cdot e_K^{1+\tau} \cdot e_K^{-2}.$$

First,

$$\begin{aligned} e_K^{1+\sigma} &= N_{L/\mathbb{Q}(\sqrt{q})}(e_L) \\ &= N_{L/\mathbb{Q}(\sqrt{q})}(-((1-\zeta_n)\zeta_{2n}^{-1})^{1+J_1}) \\ &= N_{\mathbb{Q}(\zeta_{4q})^+/\mathbb{Q}(\sqrt{q})}((N_{F/\mathbb{Q}(\zeta_{4q})}(1-\zeta_n)) \cdot (N_{\mathbb{Q}(\zeta_{8pq})/\mathbb{Q}(\zeta_{8q})}\zeta_{2n}^{-1})) \\ &= N_{\mathbb{Q}(\zeta_{4q})^+/\mathbb{Q}(\sqrt{q})}\left(\frac{1-\zeta_{4q}}{1-\zeta_{4q}^{p^{-1}}}\zeta_{8q}^{p^{-1}-1}\right) \\ &= N_{\mathbb{Q}(\zeta_{4q})/\mathbb{Q}(\zeta_4,\sqrt{-q})}\left(\frac{1-\zeta_{4q}}{1-\zeta_{4q}^{p^{-1}}}\right) \cdot N_{\mathbb{Q}(\zeta_{8q})/\mathbb{Q}(\zeta_8,\sqrt{-q})}(\zeta_{8q}^{p^{-1}-1}), \end{aligned}$$

where p^{-1} is the inverse of $p \pmod{8q}$. Put $\zeta_{8q} = \zeta_8^x\zeta_q^y$. Then we have

$$N_{\mathbb{Q}(\zeta_{8q})/\mathbb{Q}(\zeta_8,\sqrt{-q})}(\zeta_{8q}^{p^{-1}-1}) = \zeta_8^{x(p^{-1}-1)(q-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \\ -1 & \text{if } p \equiv 5 \pmod 8). \end{cases}$$

Now we look at $u = N_{\mathbb{Q}(\zeta_{4q})/\mathbb{Q}(\zeta_4,\sqrt{-q})}((1-\zeta_{4q})/(1-\zeta_{4q}^{p^{-1}}))$. We have $\zeta_{4q} = \zeta_4^x\zeta_q^{2y}$. If $(p/q) = 1$, then the automorphism sending ζ_q to $\zeta_q^{p^{-1}}$ permutes the elements of Gal $(\mathbb{Q}(\zeta_{4q})/\mathbb{Q}(\zeta_4, \sqrt{-q}))$, which implies that $u = 1$. Suppose that $(p/q) = -1$. We can write u as

$$u = N_{\mathbb{Q}(\zeta_{4q})/\mathbb{Q}(\zeta_4,\sqrt{-q})}\left(\frac{\zeta_4^x(\zeta_4^{-x}-\zeta_q^{2y})}{\zeta_4^x(\zeta_4^{-x}-\zeta_q^{2yp^{-1}})}\right) = \frac{N_{\mathbb{Q}(\zeta_{4q})/\mathbb{Q}(\zeta_4,\sqrt{-q})}(\zeta_4^{-x}-\zeta_q^{2y})}{N_{\mathbb{Q}(\zeta_{4q})/\mathbb{Q}(\zeta_4,\sqrt{-q})}(\zeta_4^{-x}-\zeta_q^{2yp^{-1}})}.$$

Let us denote the numerator by A and the denominator by B. In the equation $(X^q-1)/(X-1) = \prod_{1\le i\le q-1}(X-\zeta_q^i)$, we substitute ζ_4^{-x} for X to obtain $-\zeta_4^{-1} = AB$. Therefore $u = A/B$ cannot be 1 or -1, for otherwise $B = \pm A$ would imply that $A^2 = \pm\zeta_4$, which is impossible since $A \in \mathbb{Q}(\zeta_4, \sqrt{-q})$. Therefore

$$e_K^{1+\sigma} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ and } \left(\dfrac{p}{q}\right) = 1 \\ -1 & \text{if } p \equiv 5 \pmod 8 \text{ and } \left(\dfrac{p}{q}\right) = 1 \\ u & \text{if } p \equiv 1 \pmod 8 \text{ and } \left(\dfrac{p}{q}\right) = -1 \\ -u & \text{if } p \equiv 5 \pmod 8 \text{ and } \left(\dfrac{p}{q}\right) = -1, \end{cases}$$

where $u = -(\zeta_8 A)^2$ is a unit in $\mathbb{Q}(\sqrt{q})$ different from ± 1.

https://doi.org/10.1017/S0004972711003352 Published online by Cambridge University Press

Next, we compute $e_K^{1+\tau}$. Note that $\zeta_{2n}^{1+J_2} \in \mathbb{Q}(\zeta_p)$ since $J_2 \equiv -1 \pmod{8q}$. So

$$\begin{aligned}
e_K^{1+\tau} &= N_{K/\mathbb{Q}(\sqrt{p})}(e_K) \\
&= N_{L/\mathbb{Q}(\sqrt{p})}((1-\zeta_n)\zeta_{2n}^{-1})^{1+J_2} \\
&= N_{\mathbb{Q}(\zeta_p)^+/\mathbb{Q}(\sqrt{p})}((N_{F/\mathbb{Q}(\zeta_p)}(1-\zeta_n)) \cdot (\zeta_{2n}^{-(1+J_2)(q-1)})) \\
&= N_{\mathbb{Q}(\zeta_p)^+/\mathbb{Q}(\sqrt{p})}\left(\frac{((1-\zeta_p^{(2q)^{-1}})/(1-\zeta_p))\zeta_p^{(1-(2q)^{-1})/2}}{(((1-\zeta_p^{2^{-1}})/(1-\zeta_p))\zeta_p^{(1-2^{-1})/2})(((1-\zeta_p^{q^{-1}})/(1-\zeta_p))\zeta_p^{(1-q^{-1})/2})}\right) \\
&= \frac{\overline{v}_p(l_2+l_q)}{\overline{v}_p(l_2)\overline{v}_p(l_q)} \\
&= \begin{cases} -\dfrac{1}{\overline{v}_p(1)^2} & \text{if } l_2 \equiv l_q \equiv 1 \pmod 2 \\ 1 & \text{otherwise.} \end{cases}
\end{aligned}$$

Hence

$$\mathcal{E}_k = e_K^{1+\sigma} \cdot e_K^{1+\tau} \cdot e_K^{-2} = \begin{cases} e_K^{-2} & \text{if } \left(\dfrac{2}{p}\right) = \left(\dfrac{q}{p}\right) = 1 \\ -(\zeta_8 A \cdot e_K^{-1})^2 & \text{if } \left(\dfrac{2}{p}\right) = 1 \text{ and } \left(\dfrac{q}{p}\right) = -1 \\ -e_K^{-2} & \text{if } \left(\dfrac{2}{p}\right) = -1 \text{ and } \left(\dfrac{q}{p}\right) = 1 \\ -(\zeta_8 A \cdot \overline{v}_p(1)^{-1} \cdot e_K^{-1})^2 & \text{if } \left(\dfrac{2}{p}\right) = \left(\dfrac{q}{p}\right) = -1. \end{cases}$$

Note that $e_K \in k$ if and only if $e_K^{1+\sigma} = e_K^{1+\tau}$. And this happens if and only if $(q/p) = (2/p) = 1$.

THEOREM 4.1. *Let $k = \mathbb{Q}(\sqrt{pq})$ with $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. Then $N_{k/\mathbb{Q}}(\eta_k) = 1$, and:*

(1) *if $(2/p) = -1$ or $(q/p) = -1$, then $2 \mid h_k$, $4 \nmid h_k$;*
(2) *if $(2/p) = (q/p) = 1$, then $4 \mid h_k$.*

PROOF. Since $q \equiv 3 \pmod 4$, $x^2 - pqy^2 = -1$ has no integral solution, which implies that $N_{k/\mathbb{Q}}(\eta_k) = 1$. We prove the theorem when $(2/p) = 1$ and $(q/p) = -1$. The other cases are similar to this case or to Theorem 3.2. Put $C(k) = \langle \pm\mathcal{E}_k \rangle$. Then $[C(k) : C_S(k)] = 2$. We have $\mathcal{E}_k = -(\zeta_8 A \cdot e_K^{-1})^2$ in this case. We claim that $\zeta_8 A \cdot e_K^{-1} \notin k$. In fact $\zeta_8 A \cdot e_K^{-1} \notin K$. Suppose, to the contrary, that $\zeta_8 A \cdot e_K^{-1} \in K$. Then $\zeta_8 A \in K$. So $\zeta_8 A$ is fixed by $\mathrm{Gal}(K(\zeta_8)/K)$. Let $\rho \in \mathrm{Gal}(K(\zeta_8)/K)$ be such that $\rho(\zeta_8) = \zeta_8^5$ over K. Then $\rho(\zeta_4) = \zeta_4$ and $\rho(\sqrt{-q}) = \sqrt{-q}$. So $\rho(A) = A$. But $\rho(\zeta_8 A) = \zeta_8^5 A \neq \zeta_8 A$. Hence $\zeta_8 A \cdot e_K^{-1} \notin K$. Therefore $2 \nmid [E(k) : C(k)]$, for otherwise, $\eta_k^{2m} = \pm\mathcal{E}_k$ would give $\eta_k^m = \pm\zeta_8 A \cdot e_K^{-1}$ or $\pm\zeta_4\zeta_8 A \cdot e_K^{-1}$, both of which are impossible. □

https://doi.org/10.1017/S0004972711003352 Published online by Cambridge University Press

Remark 4.2. In case (2) of this theorem, h_k can be a multiple of 8. For example, $h_k = 4$ when $k = \mathbb{Q}(\sqrt{17 \cdot 19})$, while $h_k = 8$ when $k = \mathbb{Q}(\sqrt{17 \cdot 47})$.

Remark 4.3. Let $C_k(2)$ be the Sylow 2-subgroup of the ideal class group C_k of $k = \mathbb{Q}(\sqrt{pq})$. Then $C_k(2)$ is a cyclic group.

Proof. Let $G = \mathrm{Gal}\,(k/\mathbb{Q})$ and $\widehat{H}^i$ be the ith Tate cohomology group. Then we have an exact sequence

$$0 \longrightarrow \widehat{H}^{-1}(G, E(k)) \longrightarrow I_k^G/P_{\mathbb{Q}} \longrightarrow C_k^G \longrightarrow \ker\,(\widehat{H}^0(G, E(k)) \to \widehat{H}^0(G, k^\times)) \longrightarrow 0,$$

where I_k is the ideal group of k, and $P_{\mathbb{Q}}$ is the principal ideal group of $\mathbb{Q}$, which of course equals $I_{\mathbb{Q}}$. Thus $I_k^G/P_{\mathbb{Q}} \simeq (\mathbb{Z}/2\mathbb{Z})^r$, where r is the number of ramified primes of $\mathbb{Q}$ in k. If $N_{k/\mathbb{Q}}(\eta_k) = -1$, then $\widehat{H}^0(G, E(k)) = 0$ and $\widehat{H}^{-1}(G, E(k)) \simeq \mathbb{Z}/2\mathbb{Z}$. Thus the above sequence gives

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow C_k^G \longrightarrow 0.$$

Hence $C_k^G \simeq \mathbb{Z}/2\mathbb{Z}$.

Suppose that $N_{k/\mathbb{Q}}(\eta_k) = 1$. Then $\widehat{H}^0(G, E(k)) \simeq \mathbb{Z}/2\mathbb{Z}$ and $\widehat{H}^{-1}(G, E(k)) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. So

$$0 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^r \longrightarrow C_k^G \longrightarrow \ker\,(\widehat{H}^0(G, E(k)) \to \widehat{H}^0(G, k^\times)) \longrightarrow 0.$$

If $r = 2$, then C_k^G is either trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$. If $r = 3$, then

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow C_k^G \longrightarrow \ker\,(\widehat{H}^0(G, E(k)) \to \widehat{H}^0(G, k^\times)) \longrightarrow 0.$$

Note that if $r = 3$, then we are in the situation $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. In this case, the generator -1 of $\widehat{H}^0(G, E(k))$ cannot be a norm from k to $\mathbb{Q}$ since $x^2 - pqy^2 = -z^2$ does not have an integral solution. Thus $\widehat{H}^0(G, E(k)) \to \widehat{H}^0(G, k^\times)$ is an injection. Hence $C_k^G \simeq \mathbb{Z}/2\mathbb{Z}$.

Note that $C_k^G = \{c \in C_k \mid c^2 = 1\}$ since $N_{k/\mathbb{Q}}(c) = 1$ for every $c \in C_k$. Hence C_k^G consists of elements of order two in $C_k(2)$. Therefore $C_k(2)$ must be a cyclic group since C_k^G is either trivial or $\mathbb{Z}/2\mathbb{Z}$. □

References

[1] E. Brown, 'The class number and fundamental units of $\mathbb{Q}(\sqrt{2q})$, for $p \equiv 1$ (mod) 16 a prime', *J. Number Theory* **16** (1983), 95–99.
[2] P. E. Conner and J. Hurrelbrink, *Class Number Parity*, Series in Pure Mathematics, 8 (World Science, Singapore, 1988).
[3] K. Dohmae, 'On bases of groups of circular units of some imaginary abelian number fields', *J. Number Theory* **61** (1996), 343–364.
[4] K. Dohmae, 'A note on Sinnott's index formula', *Acta Arith.* **82**(1) (1997), 57–67.
[5] M. Hirabayashi and K. Yoshino, 'Remarks on unit indices of imaginary abelian fields', *Manuscripta Math.* **60** (1988), 423–436.

https://doi.org/10.1017/S0004972711003352 Published online by Cambridge University Press

[6] J. Kim and J. Ryu, 'Construction of a certain circular unit and its applications', *J. Number Theory* **131**(4) (2011), 737–744.
[7] R. Kučera, 'On the parity of the class number of a biquadratic field', *J. Number Theory* **52** (1995), 43–52.
[8] W. Sinnott, 'On the Stickelberger ideal and the circular units of an abelian field', *Invent. Math.* **62** (1980), 181–234.

JAE MOON KIM, Department of Mathematics, Inha University,
Incheon 402-751, Korea
e-mail: jmkim@inha.ac.kr

JADO RYU, Department of Mathematics, Inha University, Incheon 402-751, Korea
e-mail: jdryu@inha.ac.kr

https://doi.org/10.1017/S0004972711003352 Published online by Cambridge University Press