

On the equation $X^2 - \varepsilon_2 \varepsilon_{p_1 p_2} \varepsilon_{2 p_1 p_2} = 0$ for some fundamental units ε_i

A. AZIZI, M. TAOUS and A. ZEKHNINI

MSC 2010 Classifications: Primary 11R16; 11R29; 11R11; Secondary 11R80.

Keywords and phrases: Quadratic number fields, biquadratic number fields, Units group, Class group, class number.

Abstract Let $p_1 \equiv p_2 \equiv 5 \pmod{8}$ be prime numbers satisfying the condition $\left(\frac{p_1}{p_2}\right) = -1$ and let $\mathbb{L} = \mathbb{Q}(\sqrt{2}, \sqrt{p_1 p_2})$. The aim of this paper is to characterize, using biquadratic symbols, the existence of solutions to the equation $X^2 - \varepsilon_2 \varepsilon_{p_1 p_2} \varepsilon_{2 p_1 p_2} = 0$ in $\mathbb{L}$, where the ε_j are the fundamental units of the real quadratic subfields of $\mathbb{L}$.

1 Introduction

Let d_1, d_2 be two square-free distinct positive integers; put $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Denote by ε_1 (resp. $\varepsilon_2, \varepsilon_3$) the fundamental unit of $k_1 = \mathbb{Q}(\sqrt{d_1})$ (resp. $k_2 = \mathbb{Q}(\sqrt{d_2})$, $k_3 = \mathbb{Q}(\sqrt{d_1 d_2})$); assume that $\varepsilon_1, \varepsilon_2$, and ε_3 have norms equal to -1 . Many mathematicians have studied the units of the field K and have provided the Fundamental System of Units (FSU) of K in terms of the three units $\varepsilon_1, \varepsilon_2$, and ε_3 . The problem was to determine when the product $\varepsilon_1 \varepsilon_2 \varepsilon_3$ is a square in K . Consider the following numbers:

$$\begin{aligned}\alpha_1 &= \varepsilon_1 \varepsilon_2 \varepsilon_3 + \varepsilon_1 + \varepsilon_2 - \varepsilon_3, \\ \alpha_2 &= \varepsilon_1 \varepsilon_2 \varepsilon_3 + \varepsilon_1 - \varepsilon_2 + \varepsilon_3, \\ \alpha_3 &= \varepsilon_1 \varepsilon_2 \varepsilon_3 - \varepsilon_1 + \varepsilon_2 + \varepsilon_3, \\ \alpha_4 &= \varepsilon_1 \varepsilon_2 \varepsilon_3 - \varepsilon_1 - \varepsilon_2 - \varepsilon_3, \\ c_j &= \text{trace}_{K/\mathbb{Q}}(\alpha_j), \text{ where } j \in J = \{1, 2, 3, 4\},\end{aligned}$$

where $\text{trace}_{K/\mathbb{Q}}(\alpha_j)$ is the trace of α_j in the biquadratic number field extension $K/\mathbb{Q}$, which is defined as the sum of all the conjugates of α_j in K .

Using these numbers, T. Kubota in [7] proved that $c_j = \frac{\alpha_j^2}{\varepsilon_1 \varepsilon_2 \varepsilon_3}$ for all $j \in J$. Thus, $\varepsilon_1 \varepsilon_2 \varepsilon_3$ is a square in K if and only if there exists $j \in J$ such that c_j is a square in K . Based on this last result, A. Azizi in [1], concluded that $\varepsilon_1 \varepsilon_2 \varepsilon_3$ is a square in K if and only if there exist $(i, j) \in \{0, 1\}^2$ such that $d_1^i d_2^j \text{trace}_{K/\mathbb{Q}}(\alpha_1)$ is a square in $\mathbb{N}$. The same conclusion was found by M. Hirabayashi and K. Yoshino in [4], who stated that $\varepsilon_1 \varepsilon_2 \varepsilon_3$ is a square in K if and only if $\text{trace}_{K/\mathbb{Q}}(\alpha_3)$ is a square in K . Similarly, H. Wada used $\text{trace}_{K/\mathbb{Q}}(\alpha_j)$ in [9] to determine when $\varepsilon_1 \varepsilon_2 \varepsilon_3$ is a square in K .

In this note, we answer this question using biquadratic rational symbols in the case where $d_1 = 2$ and $d_2 = p_1 p_2$, with p_1 and p_2 are positive prime integers.

Let p_1 and p_2 be two positive prime integers satisfying $p_1 \equiv p_2 \equiv 5 \pmod{8}$ and $\left(\frac{p_1}{p_2}\right) = -1$. Define $\mathbb{L} = \mathbb{Q}(\sqrt{2}, \sqrt{p_1 p_2})$, and let ε_2 (resp. $\varepsilon_{p_1 p_2}, \varepsilon_{2 p_1 p_2}$) be the fundamental unit of $k_1 = \mathbb{Q}(\sqrt{2})$ (resp. $k_2 = \mathbb{Q}(\sqrt{p_1 p_2})$, $k_3 = \mathbb{Q}(\sqrt{2 p_1 p_2})$). Then, all these units have negative norms (see Lemma 2.2 below). According to S. Kuroda [8], a Fundamental System of Units (FSU) of $\mathbb{L} = \mathbb{Q}(\sqrt{2}, \sqrt{p_1 p_2})$ is either $\{\varepsilon_2, \varepsilon_{p_1 p_2}, \sqrt{\varepsilon_2 \varepsilon_{p_1 p_2} \varepsilon_{2 p_1 p_2}}\}$ or $\{\varepsilon_2, \varepsilon_{p_1 p_2}, \varepsilon_{2 p_1 p_2}\}$, depending on whether the equation $X^2 - \varepsilon_2 \varepsilon_{p_1 p_2} \varepsilon_{2 p_1 p_2} = 0$ has or not a solution in $\mathbb{L}$. In the main result Theorem 2.4, we use biquadratic symbols to determine under which conditions the unit $\varepsilon_2 \varepsilon_{p_1 p_2} \varepsilon_{2 p_1 p_2}$ is a

square in $\mathbb{L}$, and we establish a relation between this answer and $h_2(-p_1p_2)$, the 2-class number of the field $\mathbb{Q}(\sqrt{-p_1p_2})$.

2 The Result

We begin by stating some preliminary results that will be useful later. Let a be a square-free natural integer, and Q be the Hasse's unit index of the field $\mathbb{Q}(\sqrt{a}, i)$. Then, we have:

Lemma 2.1. *If one of the following conditions holds, then $Q = 1$.*

1. $a \equiv 1 \pmod{4}$.
2. *There exists an odd integer a' dividing a such that $a' \equiv 5 \pmod{8}$.*

Proof. See Corollary 3.2 in [2].

Since the biquadratic symbol $\left(\frac{a}{b}\right)_4$, and the quadratic residue symbol $\left(\frac{a}{b}\right)$ play a fundamental role in our main result, Theorem 2.4, we emphasize their importance in determining when the unit $\varepsilon_2 \varepsilon_{p_1 p_2} \varepsilon_{2 p_1 p_2}$ is a square in $\mathbb{L}$. In particular, the second symbol appears in conditions related to the norm of fundamental units in some quadratic subfields of $\mathbb{L}$, as stated in the following lemma.

Lemma 2.2. *If $d = 2p_1p_2$ with p_1 and p_2 being prime integers such that $p_1 \equiv p_2 \equiv 1 \pmod{4}$ and at least two of the elements $\left\{\left(\frac{p_1}{p_2}\right), \left(\frac{2}{p_1}\right), \left(\frac{2}{p_2}\right)\right\}$ are equal to -1 , then the norm of the fundamental unit of $\mathbb{Q}(\sqrt{2p_1p_2})$ is -1 .*

Proof. See Corollary 3.6 in [2].

The next result establishes an explicit relation between biquadratic symbols and quadratic residue symbols, which will be crucial for proving the main result Theorem 2.4.

Proposition 2.3. *Let p_1 and p_2 be two prime integers such that $p_1 \equiv p_2 \equiv 1 \pmod{4}$ and $\left(\frac{2}{p_1}\right) = \left(\frac{2}{p_2}\right) = \left(\frac{p_1}{p_2}\right)$. We factorize p_1 and p_2 in $\mathbb{Z}[i]$ as follows: $p_1 = \pi_1\pi_2 = (a_1 + 2ib_1)(a_1 - 2ib_1)$ and $p_2 = \pi_3\pi_4 = (a_2 + 2ib_2)(a_2 - 2ib_2)$. Then,*

$$\left(\frac{p_1p_2}{2}\right)_4 \left(\frac{2p_1}{p_2}\right)_4 \left(\frac{2p_2}{p_1}\right)_4 = \left(\frac{\pi_3}{\pi_1}\right) \left(\frac{2}{a_1 + 2b_1}\right) \left(\frac{2}{a_2 + 2b_2}\right).$$

Proof. As $p_1 = \pi_1\pi_2 = (a_1 + 2ib_1)(a_1 - 2ib_1)$ and $p_2 = \pi_3\pi_4 = (a_2 + 2ib_2)(a_2 - 2ib_2)$, then, by the biquadratic reciprocity law, we obtain:

$$\begin{aligned} \left(\frac{2p_1}{p_2}\right)_4 \left(\frac{2p_2}{p_1}\right)_4 &= \left(\frac{2p_1}{\pi_3}\right)_4 \left(\frac{2p_2}{\pi_1}\right)_4 \\ &= \left(\frac{2}{\pi_1\pi_3}\right)_4 \left(\frac{p_1}{\pi_3}\right)_4 \left(\frac{p_2}{\pi_1}\right)_4 \\ &= \left(\frac{2}{\pi_1\pi_3}\right)_4 \left(\frac{\pi_3}{\pi_1}\right). \end{aligned}$$

Since $2 = i^3(1+i)^2$, we have:

$$\begin{aligned} \left(\frac{2}{\pi_1}\right)_4 \left(\frac{2}{\pi_3}\right)_4 &= \left(\frac{i^3(1+i)^2}{\pi_1}\right)_4 \left(\frac{i^3(1+i)^2}{\pi_3}\right)_4 \\ &= \left(\frac{i}{\pi_1}\right)_4 \left(\frac{1+i}{\pi_1}\right) \left(\frac{i}{\pi_3}\right)_4 \left(\frac{1+i}{\pi_3}\right) \\ &= i^{\frac{p_1+p_2-2}{4}} \left(\frac{1+i}{\pi_1}\right) \left(\frac{1+i}{\pi_3}\right) \\ &= i^{\frac{p_1+p_2-2}{4}} \left(\frac{2}{a_1 + 2b_1}\right) \left(\frac{2}{a_2 + 2b_2}\right). \end{aligned}$$

Furthermore, since $\frac{p_1-1}{8} + \frac{p_2-1}{8} \equiv \frac{p_1p_2-1}{8} \pmod{2}$, we obtain:

$$\left(\frac{p_1p_2}{2}\right)_4 = (-1)^{\frac{p_1p_2-1}{8}} = (-1)^{\frac{p_1+p_2-2}{8}} = i^{\frac{p_1+p_2-2}{4}}.$$

Thus,

$$\left(\frac{2}{\pi_1}\right)_4 \left(\frac{2}{\pi_3}\right)_4 = \left(\frac{p_1p_2}{2}\right)_4 \left(\frac{2}{a_1+2b_1}\right)_4 \left(\frac{2}{a_2+2b_2}\right)_4.$$

This proves the result. $\square$

Before stating our main theorem, recall that the unit index of the field $\mathbb{L}$, $q(\mathbb{L}/\mathbb{Q})$, is defined by: $q(\mathbb{L}/\mathbb{Q}) = [E_{\mathbb{L}} : E_{k_1}E_{k_2}E_{k_3}]$, where $E_{\mathbb{L}}$ is the unit group of $\mathbb{L}$, and $E_{k_1}, E_{k_2}, E_{k_3}$ are the unit groups of its three quadratic subfields k_1, k_2, k_3 .

Theorem 2.4. *Let p_1 and p_2 be two prime integers such that $p_1 \equiv p_2 \equiv 5 \pmod{8}$ and $\left(\frac{p_1}{p_2}\right) = -1$, and let $\mathfrak{k} = \mathbb{Q}(\sqrt{2}, \sqrt{p_1p_2})$. Then, the following statements are equivalent:*

1. $\varepsilon_{2\varepsilon_{p_1p_2}}\varepsilon_{2p_1p_2}$ is a square in $\mathbb{L}$.
2. $\left(\frac{p_1p_2}{2}\right)_4 \left(\frac{2p_1}{p_2}\right)_4 \left(\frac{2p_2}{p_1}\right)_4 = -1$.

Proof. Since $p_1p_2 \equiv 1 \pmod{8}$, there exist an even integer x and an odd integer y such that $\varepsilon_{p_1p_2} = x + y\sqrt{p_1p_2}$, hence $x^2 + 1 = y^2p_1p_2$. According to [6], we obtain:

$$\begin{cases} x \mp i = iy_1^2\pi_1\pi_3 \\ x \pm i = -iy_2^2\pi_2\pi_4 \end{cases} \quad (2.11) \text{ or } \begin{cases} x \mp i = iy_1^2\pi_1\pi_4 \\ x \pm i = -iy_2^2\pi_2\pi_3 \end{cases} \quad (2.12) \quad (2.1)$$

from which we deduce:

$$\left. \begin{aligned} \sqrt{\varepsilon_{p_1p_2}} &= z_1\sqrt{\pi_1\pi_3} + z_2\sqrt{\pi_2\pi_4} \quad (2.21) \\ \text{or} \\ \sqrt{\varepsilon_{p_1p_2}} &= z_1\sqrt{\pi_1\pi_4} + z_2\sqrt{\pi_2\pi_3} \quad (2.22) \end{aligned} \right\} \quad (2.2)$$

where z_2 is the conjugate of z_1 in $\frac{1}{2}\mathbb{Z}[i]$.

Similarly, there exist a and b in $\mathbb{N}$ such that $\varepsilon_{2p_1p_2} = a + b\sqrt{2p_1p_2}$, hence:

$$\left\{ \begin{aligned} a \mp i &= (1+i)b_1^2\pi_1\pi_3 \\ x \pm i &= (1-i)b_2^2\pi_2\pi_4 \end{aligned} \right. \quad (2.31) \text{ or } \left\{ \begin{aligned} x \mp i &= (1+i)b_1^2\pi_1\pi_4 \\ x \pm i &= (1-i)b_2^2\pi_2\pi_3 \end{aligned} \right. \quad (2.32) \text{ or } \left\{ \begin{aligned} a \mp i &= i(1+i)b_1^2\pi_1\pi_3 \\ x \pm i &= -i(1-i)b_2^2\pi_2\pi_4 \end{aligned} \right. \quad (2.33) \text{ or } \left\{ \begin{aligned} x \mp i &= i(1+i)b_1^2\pi_1\pi_4 \\ x \pm i &= -i(1-i)b_2^2\pi_2\pi_3 \end{aligned} \right. \quad (2.34) \quad (2.3)$$

from which it follows that:

$$\left. \begin{aligned} \sqrt{2\varepsilon_{2p_1p_2}} &= u_1\sqrt{(1+i)\pi_1\pi_3} + u_2\sqrt{(1-i)\pi_2\pi_4} \quad (2.41) \text{ or } \\ \sqrt{2\varepsilon_{2p_1p_2}} &= u_1\sqrt{(1+i)\pi_1\pi_4} + u_2\sqrt{(1-i)\pi_2\pi_3} \quad (2.42) \text{ or } \\ \sqrt{\varepsilon_{2p_1p_2}} &= u_1\sqrt{(1+i)\pi_1\pi_3} + u_2\sqrt{(1-i)\pi_2\pi_4} \quad (2.43) \text{ or } \\ \sqrt{\varepsilon_{2p_1p_2}} &= u_1\sqrt{(1+i)\pi_1\pi_4} + u_2\sqrt{(1-i)\pi_2\pi_3} \quad (2.44) \end{aligned} \right\} \quad (2.4)$$

where u_2 and u_1 are conjugates in $\mathbb{Z}[i]$ or $\frac{1}{2}\mathbb{Z}[i]$.

Finally, we have:

$$\sqrt{2\varepsilon_2} = \sqrt{1+i} + \sqrt{1-i}. \quad (2.5)$$

Multiplying the equalities (2.21), (2.41), and (2.5); (2.21), (2.43), and (2.5); (2.22), (2.42), and (2.5); (2.22), (2.44), and (2.5), we find that $\varepsilon_{2\varepsilon_{p_1p_2}}\varepsilon_{2p_1p_2}$ is a square in $\mathbb{L}$.

Thus, $\varepsilon_{2\varepsilon_{p_1p_2}}\varepsilon_{2p_1p_2}$ is a square in $\mathbb{L}$ if and only if x and a take one of the following forms: (2.11) and (2.31) or (2.11) and (2.33) or (2.12) and (2.32) or (2.12) and (2.34).

Applying the quadratic residue symbol to these four cases, we find:

$$\left(\frac{\pi_3}{\pi_1}\right) \left(\frac{2}{a_1 + 2b_1}\right) \left(\frac{2}{a_2 + 2b_2}\right) = \left(\frac{\pi_3}{\pi_1}\right) \left(\frac{1+i}{\pi_1}\right) \left(\frac{1+i}{\pi_3}\right) = -1.$$

And Proposition 2.3 gives:

$$\left(\frac{p_1 p_2}{2}\right)_4 \left(\frac{2p_1}{p_2}\right)_4 \left(\frac{2p_2}{p_1}\right)_4 = -1.$$

On the other hand, the other forms give:

$$\left(\frac{p_1 p_2}{2}\right)_4 \left(\frac{2p_1}{p_2}\right)_4 \left(\frac{2p_2}{p_1}\right)_4 = \left(\frac{\pi_3}{\pi_1}\right) \left(\frac{1+i}{\pi_1}\right) \left(\frac{1+i}{\pi_3}\right) = 1.$$

This establishes the equivalence needed. $\square$

The two assertions of Theorem 2.4 are in reality equivalent to other results.

Corollary 2.5. *Let p_1 and p_2 be two prime integers such that $p_1 \equiv p_2 \equiv 5 \pmod{8}$ and $\left(\frac{p_1}{p_2}\right) = -1$, and let $\mathfrak{k} = \mathbb{Q}(\sqrt{2}, \sqrt{p_1 p_2})$. Then, the following statements are equivalent:*

1. $\varepsilon_{2\varepsilon_{p_1 p_2} \varepsilon_{2p_1 p_2}}$ is a square in $\mathbb{L}$.
2. $\left(\frac{p_1 p_2}{2}\right)_4 \left(\frac{2p_1}{p_2}\right)_4 \left(\frac{2p_2}{p_1}\right)_4 = -1$.
3. The unit index of the field $\mathbb{L}$ is $q(\mathfrak{k}/\mathbb{Q}) = 2$.
4. The 2-class group $C_2(\mathbb{Q}(\sqrt{-p_1 p_2}))$ of $\mathbb{Q}(\sqrt{-p_1 p_2})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
5. The 2-class number of $\mathbb{Q}(\sqrt{-p_1 p_2})$ is $h_2(-p_1 p_2) = 8$.
6. The number of ideal classes of $\mathbb{Q}(\sqrt{2p_1 p_2})$ that become principal in $\mathbb{Q}(\sqrt{2}, \sqrt{p_1 p_2})$ is exactly 2.

Proof. For the equivalence between (1) and (2) see Theorem 2.4. The equivalence between (1) and (3) is a well-known result. For the equivalences (2) $\Leftrightarrow$ (4) and (2) $\Leftrightarrow$ (5), see [5]. For the equivalence between (1) and (6), see [3]. $\square$

Acknowledgment

We would like to sincerely thank the referee for his/her several helpful and constructive suggestions, comments and corrections that helped us to considerably improve our paper.

References

- [1] A. Azizi, *Sur les unités de certains corps de nombres de degré 8 sur $\mathbb{Q}$* , Ann. Sci. Math. Québec **29** (2005), no. 2, 111-129.
- [2] A. Azizi et M. Taous, *Détermination des corps $\mathbf{k} = \mathbb{Q}(\sqrt{d}, i)$ dont le 2-groupe de classes est de type $(2, 4)$ ou $(2, 2, 2)$* , Rend. Istit. Mat. Univ. Trieste **40** (2008), 93-116.
- [3] E. Benjamin, F. Sanborn, and C. Snyder, *Capitulation in unramified quadratic extensions of real quadratic number fields*, Glasgow J. Math. **36** (1994), 385-392.
- [4] M. Hirabayashi and K. Yoshino, *Unit Indices of Imaginary Abelian Number Fields of Type $(2, 2, 2)$* , J. Number Theory **34** (1990), no. 3, 346-361.
- [5] P. Kaplan, *Sur le 2-groupe de classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. **283/284** (1976), 313-363.
- [6] K. S. Williams, *On the evaluation of $(\varepsilon_{q_1 q_2}/p)$* , Rocky Mountain J. Math. **10** (1980), no. 3, 559-573.
- [7] T. Kubota, *Über den bzyklischen biquadratischen Zahlkörper*, Nagoya Math. J. **10** (1956), 65-85.
- [8] S. Kuroda, *Über den Dirichletschen Körper*, J. Fac. Sci. Imp. Univ. Tokyo, Sect. I, **14** (1943), 383-406.

- [9] H. Wada, *On the class number and the unit group of certain algebraic number fields*, J. Fac. Sci. Univ. Tokyo, Sect. I, **13** (1966), 201-209.

Author information

A. AZIZI, SupMTI Oujda, Morocco.

E-mail: abdelmalekazizi@yahoo.fr

M. TAOUS, Department of Mathematics, Sciences Faculty, Mohammed Premier University, Oujda, Morocco.

E-mail: taousm@hotmail.com

A. ZEKHNINI, Department of Mathematics, Sciences Faculty, Mohammed Premier University, Oujda, Morocco.

E-mail: zekha1@yahoo.fr