A Fast Algorithm to Test the Principality of Ideals

Soufiane Mezroui, Abdelmalek Azizi and M’hammed Ziane

ACSA Laboratory
Department of Mathematics and Informatics
Mohammed First University
Oujda 60000, Morocco

Abstract

Using the LLL algorithm we develop a method by which one can test the principality of ideals in some bicyclic biquadratic fields. Moreover, we will show that this algorithm run, at most, in polynomial running time.

Keywords: biquadratic extension, LLL algorithm, principality

1 Introduction

In this paper we present an algorithm which can be used to test the principality of ideals in the ring of integers of some biquadratic number fields. The new algorithm can also be used to test the equivalence between two of these ideals.

Buchmann [2] developed an algorithm for testing the principality of ideals which can be used to compute a system of fundamental units and the class number of algebraic number fields. Nevertheless, it runs in subexponential running time.

In this paper, using the LLL algorithm we develop a method by which one can test the principality of ideals in some bicyclic biquadratic fields. Moreover, we will show that this algorithm run, at most, in polynomial running time.
2 A polynomial algorithm for testing principality of ideals

Throughout this section, we would to work over particular cases of bicyclic biquadratic fields described in [1]. Hence, we fix $\mathbb{L} = \mathbb{Q}(i, \sqrt{n})$ where $n$ is a positive square free integer such that $n \equiv 1 \pmod{4}$, and further $O_L$ is a ring of integers of $\mathbb{L}$. We do the other cases of [1] in the same way. Now, consider the map $\varphi$,

$$\varphi : O_L \rightarrow \mathbb{R}^4 \quad \alpha \mapsto (\text{Re}(\alpha), \text{Im}(\alpha), \text{Re}(\sigma(\alpha)), \text{Im}(\sigma(\alpha)))$$

where $\sigma$ is the automorphism of $\mathbb{L}$ satisfying $\sigma(\sqrt{n}) = -\sqrt{n}$ and $\sigma(i) = i$. We need the following definition (see [4]).

**Definition 2.1.** Let $v = (v_1, v_2, v_3, v_4)$ be a vector of real numbers. The $v$-norm $|| \alpha ||_v$ of $\alpha$ is defined by:

$$|| \alpha ||_v^2 = 2e^{v_1}(\text{Re}(\alpha)^2 + \text{Im}(\alpha)^2) + 2e^{v_2}(\text{Re}(\sigma(\alpha))^2 + \text{Im}(\sigma(\alpha))^2).$$

A $\mathbb{Z}$-basis $\alpha_1, \alpha_2, \alpha_3$, and $\alpha_4$, of $I$ is LLL-reduced in the direction of $v$ if it is LLL-reduced for the quadratic form $|| \alpha ||_v^2$.

We give at first the following theorem.

**Theorem 2.2.** Given any $\alpha \in O_L$, $\varphi(\alpha)$ is one of the shortest vectors of the lattice $\varphi((\alpha))$ according to the $v$-norm $|| \cdot ||_v$, where

$$v = \left(\ln \left(\frac{N_L}{q(\sqrt{n})}(\sigma(\alpha))\right), \ln \left(\frac{N_L}{q(\sqrt{n})}(\sigma(\alpha))\right), \ln \left(\frac{N_L}{q(\sqrt{n})}(\alpha)\right), \ln \left(\frac{N_L}{q(\sqrt{n})}(\alpha)\right)\right).$$

**Proof.** The ideal $(\alpha) = O_L \times \alpha$ is the set of the elements

$$A\alpha + B\alpha i + C\alpha \frac{1 + \sqrt{n}}{2} + D\alpha i \frac{1 + \sqrt{n}}{2}$$

where $A, B, C$, and $D$, run through $\mathbb{Z}$. We obtain, following direct computation,

$$\varphi \left( A\alpha + B\alpha i + C\alpha \frac{1 + \sqrt{n}}{2} + D\alpha i \frac{1 + \sqrt{n}}{2} \right) =$$

$$\begin{pmatrix}
(A + C \frac{1 + \sqrt{n}}{2})\text{Re}(\alpha) - (B + D \frac{1 + \sqrt{n}}{2})\text{Im}(\alpha) \\
(B + D \frac{1 + \sqrt{n}}{2})\text{Re}(\alpha) + (A + C \frac{1 + \sqrt{n}}{2})\text{Im}(\alpha) \\
(A + C \frac{1 - \sqrt{n}}{2})\sigma(\text{Re}(\alpha)) - (B + D \frac{1 - \sqrt{n}}{2})\sigma(\text{Im}(\alpha)) \\
(B + D \frac{1 - \sqrt{n}}{2})\sigma(\text{Re}(\alpha)) + (A + C \frac{1 - \sqrt{n}}{2})\sigma(\text{Im}(\alpha))
\end{pmatrix}.$$  (1)
This yields

\[
\frac{1}{2} \left\| \varphi \left( A\alpha + B\alpha i + C\alpha \frac{1 + \sqrt{n}}{2} + D\alpha i \frac{1 + \sqrt{n}}{2} \right) \right\|_v^2 = \\
\left( A + C\frac{1 + \sqrt{n}}{2} \right)^2 + \left( B + D\frac{1 + \sqrt{n}}{2} \right)^2 \mathbb{N}_{\mathbb{L}/\mathbb{Q}(\sqrt{n})}(\alpha \sigma(\alpha)) + \\
\left( A + C\frac{1 - \sqrt{n}}{2} \right)^2 + \left( B + D\frac{1 - \sqrt{n}}{2} \right)^2 \mathbb{N}_{\mathbb{L}/\mathbb{Q}(\sqrt{n})}(\alpha \sigma(\alpha)) = \\
\left( 2A^2 + 2AC + \frac{n+1}{2} C^2 + 2B^2 + 2BD + \frac{n+1}{2} D^2 \right) \mathbb{N}_{\mathbb{L}/\mathbb{Q}(\sigma(\alpha))}, \quad (2)
\]

where

\[
v = \left( \ln \left( \mathbb{N}_{\mathbb{L}/\mathbb{Q}(\sqrt{n})}(\sigma(\alpha)) \right), \ln \left( \mathbb{N}_{\mathbb{L}/\mathbb{Q}(\sqrt{n})}(\sigma(\alpha)) \right), \ln \left( \mathbb{N}_{\mathbb{L}/\mathbb{Q}(\sqrt{n})}(\sigma(\alpha)) \right), \ln \left( \mathbb{N}_{\mathbb{L}/\mathbb{Q}(\sqrt{n})}(\sigma(\alpha)) \right) \right). \quad (3)
\]

We recall that \( A, B, C, \) and \( D \) cannot be all equal to 0. Hence, the minimum of \( 2A^2 + 2AC + \frac{n+1}{2} C^2 + 2B^2 + 2BD + \frac{n+1}{2} D^2 \) is 2, where \( A = 1 \) and \( B = C = D = 0 \). Therefore, \( \varphi(\alpha) \) is a short vector of \( \varphi(I) \) according to the \( v \)-norm \( \left\| . \right\|_v \).

\[\square\]

From Propositions 2.6.2 of [3], we know that every ideal of \( \mathbb{O_L} \) is of the following form

\[
I = c \times \left( \mathbb{Z}a + \mathbb{Z}a + \mathbb{Z} b + \sqrt{n} \mathbb{Z}i + \mathbb{Z} b + \sqrt{n} \mathbb{Z}i \right)
\]

where \( a, b \) and \( c \) are in \( \mathbb{Z}[i] \) and further \( 4a \mid b^2 - n \). It suffices to test the principality of \( \frac{1}{c}I \) and we can put \( c = 1 \). To test the principality of the ideal \( I \), one can use the general algorithm of Buchmann (see [2]), which has a subexponential running time. However, we wish to describe an algorithm for testing the principality which is specific for our case and further, it has a polynomial running time. In view of this, we have

\[
\varphi(I) = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \mathbb{Z}v_3 + \mathbb{Z}v_4 \quad (4)
\]

where
\[ v_1 = \begin{pmatrix} \text{Re}(a) \\ \text{Im}(a) \\ \text{Re}(a) \\ \text{Im}(a) \end{pmatrix}, \quad v_2 = \begin{pmatrix} \text{Re}(ai) \\ \text{Im}(ai) \\ \text{Re}(ai) \\ \text{Im}(ai) \end{pmatrix}, \quad v_3 = \begin{pmatrix} \text{Re}(b + \sqrt{n}i) \\ \text{Im}(b + \sqrt{n}i) \\ \text{Re}(b - \sqrt{n}i) \\ \text{Im}(b - \sqrt{n}i) \end{pmatrix}, \]
\[ v_4 = \begin{pmatrix} \text{Re}(\frac{b + \sqrt{n}}{2}i), \text{Im}(\frac{b + \sqrt{n}}{2}i), \text{Re}(\frac{b - \sqrt{n}}{2}i), \text{Im}(\frac{b - \sqrt{n}}{2}i) \end{pmatrix}. \]

In fact, \( \varphi(I) \) is a lattice of rank 4.

We apply the LLL algorithm to the lattice \( \varphi(I) \), and we find in polynomial time the shortest vectors \( \{u_1, \ldots, u_i\} \) of the lattice \( \varphi(I) \) according to the \( v \)-norm \( ||.||_v \), where \( i \in \mathbb{N} \).

By comparing \( (N_{L/Q(i)}(\varphi^{-1}(u_j))) \) and \( N_{L/Q(i)}(I) = (a) \) we can check if one of the elements \( \varphi^{-1}(u_j) \) gives us \( I = (\varphi^{-1}(u_j)) \). In fact, if
\[ (N_{L/Q(i)}(\varphi^{-1}(u_j))) = (a), \]
then \( I = (\varphi^{-1}(u_j)) \). Otherwise, we deduce that \( I \) is not principal. This yields us an algorithm which tests if \( I \) is principal or not. It is easy to see that it runs in polynomial time since the LLL algorithm requires a polynomial time for a fixed rank.

Acknowledgements. This work was supported by Académie Hassan 2 under the project

“Mathématiques et Applications: cryptographie” and URAC6-CNRST.

References


Received: August 5, 2014