Ideal Class Group Algorithms
in the Ring of Integral Quaternions

Anton S. Mosunov
St. Petersburg National Research University
of Information Technologies, Mechanics and Optics
49 Kronverkskiy Prospect (St. Petersburg, Russia)
E-mail: antonmosunov@gmail.com

Abstract

An ideal is a classical object of study in the field of algebraic
number theory. In maximal quadratic orders of number fields, ide-
als usually represented by the \( \mathbb{Z} \)-basis. This form of representation
is used in most of the algorithms for ideal manipulation. However,
this is not the only option, as an ideal can also be represented by
its generating set. Moreover, in certain quadratic orders of the ring
of integral quaternions, every ideal can be represented by a single
quaternion, called a \textit{pseudo generator}.

In this paper, we develop algorithms which allow us to manipu-
late ideals using solely their pseudo generators. We also demonstrate
the connection between the three squares problem and factorization.
This result comes as an extension of a number factoring technique
discovered by Fermat, which allows the factoring of an integer if a
pair of its two squares representations is known. In addition to this,
we present a number of identities, which ideals must satisfy; some
computational data on the number of ambiguous classes, generated
by the equation \( \rho \mu = -\mu \rho \); and a new approach to the problem of
finding a non-trivial divisor of a class number.

1 Introduction

In the field of algebraic number theory, an integral two-sided ideal is well
known, and has been thoroughly studied over the past two centuries. In
maximal quadratic orders $\mathcal{O}$ of number fields, $\mathbb{Q}(\sqrt{N})$, where $N$ is a non-zero squarefree integer, there are many things known about ideals. Namely, we know that equivalence classes of ideals in $\mathcal{O}$ form a group, known as the ideal class group. If we consider this group, we know how to manipulate its elements. But there are still many more things that we don’t know about ideals. For example, even though we know that the size of the ideal class group is finite, we do not have any effective algorithm for its computation. There are also various heuristics known, such as the Cohen-Lenstra heuristics [CL83, CL84], which give certain predictions regarding the structure of an odd part of the ideal class group. However, we still don’t have an efficient algorithm to compute its structure.

In this paper, we suggest studying an ideal class group from a different perspective. When $N < 0$, instead of $\mathbb{Q}(\sqrt{N})$, we consider it in the ring of integral quaternions $\mathcal{H}$. The reason is that $\mathcal{H}$ has many beautiful properties that $\mathbb{Q}(\sqrt{N})$ may not have. For example, $\mathcal{H}$ is a principal ideal domain, which means that each ideal of $\mathcal{H}$ can be represented by a single generator. Because of this fundamental property, even though $\mathcal{O}(\mu)$, a quadratic order of $\mathcal{H}$, isomorphic to $\mathcal{O}$, is not a principal ideal domain, we can still represent each ideal in $\mathcal{O}(\mu)$ with a unique (up to a multiplication by a unit) integral quaternion, which we call a pseudo generator. Knowing this, we asked the following question: is it possible to take advantage of this fact, and come up with algorithms, that manipulate ideals using only their pseudo generators? Eventually it was discovered that it is possible, and we introduce these algorithms in the section 4.

Another interesting property of the ring of integral quaternions is that, unlike $\mathcal{O}$ in $\mathbb{Q}(\sqrt{N})$, there are many quadratic orders in $\mathcal{H}$, which are isomorphic to $\mathcal{O}$. The total number of quadratic orders of a fixed discriminant $\Delta$ is related to the number of representations of an integer $|\Delta|$ as a sum of three squares. In the first half of the 20th century, mathematicians Hurwitz and Venkov explored the connections, that arise between various quadratic orders in $\mathcal{H}$. In continuation of this thread, in the section 5 we demonstrate how a pair of quadratic orders can generate a non-trivial factor of $N$. In the same section, we demonstrate that the Fermat number factoring technique is a special case of the theory, introduced in this paper.

In addition to the two sections mentioned above, the paper is structured as follows: section 2 describes the previous work in the field. Section 3 gives background information on the theory of integral quaternions and quadratic orders in $\mathcal{H}$, which was developed by Hurwitz and Venkov. Section
6 describes three identities that ideals must satisfy. Section 7 presents some computational data regarding the number of ambiguous classes within an ideal class group, which were generated by the equation $\rho \mu = -\mu \rho$. Section 8 introduces a novel approach to the problem of finding a divisor of a class number. Finally, section 9 concludes the paper.

2 Previous Work

The theory of integral quaternions was first introduced by Hurwitz [Hur19]. After Hurwitz, it was the soviet mathematician Boris Venkov, who expanded the theory by studying ideals in $\mathcal{H}$ [Ven1, Ven2, Ven3, Ven4]. The monographs of Voight [Voi10] and Vigneras [Vig80] give a thorough explanation on how ideals arise in the context of quaternion algebras.

In terms of algorithms, there is a Sage code written by D. R. Kohel in 2005 [Koh05], and maintained by J. Bobber and W. Stein [BS09], which has a broad functionality on quaternion algebras, including the operations on ideals. However, this code utilizes a different and more generalized approach to ideal manipulation. In this paper, we restrict our attention to the Hamilton algebra, and we tend to operate ideals using only their pseudo generators, without ever mentioning a $\mathbb{Z}$-basis. Among our algorithms, we also describe an algorithm on ideal reduction, which, to our best knowledge, is not present in any literature available.

As for other algorithms, we would like to mention a paper by Kirschmer and Voight [KV10]. Though not related to our research, it demonstrates another application of ideals in quaternion algebras (namely algebras defined over number fields). This paper describes algorithms, which count and enumerate representatives of the ideal classes of an Eichler order in a quaternion algebra defined over a number field.

3 Background

In this paper, we assume that our reader is familiar with some fundamental notions of algebraic number theory, such as an imaginary number field $\mathbb{Q}(\sqrt{-m})$ (for $m$ positive and squarefree), a maximal quadratic order $\mathcal{O}$, and a (two-sided) $\mathcal{O}$-ideal. We encourage our reader to refer to the monographs [JW09, Chap. 4] and [Mol11, Sec. 1.6] for more details.

In this section, we shall primarily focus on the Hurwitz theory and the connection that exists between quadratic orders in number fields and
quadratic orders in the ring of integral quaternions.

Consider the Hamilton algebra, where the trio of imaginary units $i, j, k$ produces the following multiplication table:

$$
\begin{array}{ccc}
  i & j & k \\
  i & -1 & k & -j \\
  j & -k & -1 & i \\
  k & j & -i & -1 \\
\end{array}
$$

The elements of Hamilton algebra are called *quaternions*, and have the form $q = t + xi + yj + zk$, where $t, x, y, z$ are real numbers. We shall use the standard denotations of Venkov [Ven1]

$$
\Re(q) = t; \quad N(q) = t^2 + x^2 + y^2 + z^2;
$$

$$
\bar{q} = t - xi - yj - zk; \quad q^{-1} = \bar{q}/N(q).
$$

to refer to the real part, norm, conjugate and the inverse of a quaternion. We shall also write $\vec{q} = xi + yj + zk$ to denote the vector part of a quaternion $q$.

**Definition 3.1.** An integral quaternion is a quaternion of the form

$$
a + bi + cj + dk
$$

where $a, b, c, d$ are integers that satisfy the congruence $a \equiv b \equiv c \equiv d \pmod{2}$. We shall denote the set of integral quaternions by $\mathcal{H}$.

**Definition 3.2.** An integral quaternion is primitive, if there is no positive integer other than 1, which divides all of its coefficients $a, b, c, d$.

Hurwitz demonstrated that $\mathcal{H}$ is a maximal non-commutative ring with identity [Hur19]. In this ring, there exist 24 units, namely

$$
\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}.
$$

Furthermore, $\mathcal{H}$ is a euclidean domain [Ven1 §4, a), c)], and therefore for any pair of integral quaternions $q, r$ there exists a unique (up to a multiplication by a unit from the left (or right)) integral quaternion, which we shall denote as $\gcd_r(q, r)$ (or $\gcd_l(q, r)$), of the largest norm, which divides both $q$ and $r$ from the right (or left).

In his 2nd letter [Ven2], Venkov formulates the connection between quadratic orders in the ring of integral quaternions and quadratic orders of imaginary
number fields. Following his reasoning, we first notice that each \( q \in \mathcal{H} \) satisfies the relation

\[ q^2 - 2\Re(q)q + N(q) = 0, \]

whence any integral quaternion \( \mu \) of norm \( m \) with a zero real part satisfies the equation \( \mu^2 = -m \). Next, recall that quaternion \( \mu \) commutes with any other quaternion of the form \( X + Y\mu \), where \( X, Y \in \mathbb{Z} \) \[\text{Ven2} \ \S 2, \ a\]. Therefore, the quadratic order \( \mathcal{O}(\mu) = [1, \omega] \), where

\[ \omega = \frac{r - 1 + \mu}{r}, \quad r = \begin{cases} 1, & m \not\equiv 3 \pmod{4}, \\ 2, & m \equiv 3 \pmod{4}, \end{cases} \]

is isomorphic to the maximal quadratic order \( \mathcal{O} \) of \( \mathbb{Q}(\sqrt{-m}) \) \[\text{Ven3} \ \S 2\]. It is important to emphasize that this relation between \( \mathcal{O} \) and \( \mathcal{O}(\mu) \) exists if and only if \( m \) is not representable in the form \( 4^k(8n + 7) \) for some non-negative integers \( k, n \), since there are no three squares representations for integers of this form \[\text{Gro85} \ \text{Chap. 4, \S 1}\]. In the remaining parts of this paper, we shall consider only squarefree values of \( m = N(\mu) \), so \( m \) must satisfy the congruence \( m \not\equiv 7 \pmod{8} \).

After the formation of a quadratic order \( \mathcal{O}(\mu) \), which is isomorphic to \( \mathcal{O} \), it is now possible to study various ideals that belong to \( \mathcal{O}(\mu) \). A natural question arises: if \( \mathcal{O} \) and \( \mathcal{O}(\mu) \) are isomorphic, why do we need to study \( \mathcal{O}(\mu) \)? After all, it is much easier to manipulate algebraic integers than quaternions. There are two main reasonings that led to the study of quadratic orders and ideals in \( \mathcal{H} \):

a) The ring \( \mathcal{H} \) is a Euclidean domain, and therefore it is a principal ideal domain \[\text{Ven1} \ \S 4, \ b\]. As we are about to demonstrate, this property allows us to represent an ideal with a single right (left) pseudo generator (to be defined), which is an integral quaternion, and is unique up to a multiplication by a unit from the left (right);

b) A maximal quadratic order \( \mathcal{O} \) in \( \mathbb{Q}(\sqrt{-m}) \) is unique, which is not true for \( \mathcal{H} \). Unless \( m \equiv 7 \pmod{8} \), there exist several solutions to the equation \( \mu^2 = -m \), hence several quadratic orders, isomorphic to \( \mathcal{O} \). There exist a number of interesting relations between various quadratic orders, which were studied by Venkov (e.g. in \[\text{Ven4} \ \S 19\]), and which we will demonstrate in this paper.

\[\text{Note that all ideals in } \mathcal{O}(\mu) \text{ are two-sided, since all elements of the quadratic order commute to each other } \text{Ven2} \ \S 1, \ a\].
There are other interesting properties of ideals and quadratic orders, which arise in \( \mathcal{H} \) [Ven3, §5, 6]. Consider a primitive ideal \( \mathfrak{a} \) of some fixed quadratic order \( \mathcal{O}(\mu) \), and let the \( \mathbb{Z} \)-basis of \( \mathfrak{a} \) be equal to \([a, b + \omega]\) for some integers \( a, b \). In this case, the norm of \( \mathfrak{a} \) is equal to \( N(\mathfrak{a}) = a \) [JW09, Def. 4.33, Prop. 4.23]. Since \( \mathcal{H} \) is a Euclidean domain, there exist integral quaternions \( \rho = \text{gcd}_x(a, b + \omega) \), and \( \rho' = \text{gcd}_y(a, b + \omega) \). Because \( \mathfrak{a} \) is primitive, \( \rho \) and \( \rho' \) must be primitive as well.

Following the proof of Venkov [Ven2, §14], we can demonstrate that \( N(\mathfrak{a}) = N(\rho) = N(\rho') \). Since \( \mathfrak{a} \) is divisible by \( \rho \) from the right and \( \rho \) is primitive, we have \( \mathfrak{a} = a_0 N(\rho) \) for some positive integer \( a_0 \). We also have \( b + \omega = \xi \rho \) for some integral quaternion \( \xi \), and because \( \rho \) is the greatest common divisor, quaternions \( \xi \) and \( a_0 \rho \) have no common divisors from the right. Since \( N(b + \omega) = N(\xi) N(\rho) \) is divisible by \( a = a_0 N(\rho) \), \( N(\xi) \) is divisible by \( a_0 \) [JW09, Thm. 4.24], and therefore \( a_0 = 1 \), \( N(\rho) = a = N(\mathfrak{a}) \).

Analogously, we can show that \( N(\rho') = N(\mathfrak{a}) \).

Now, let us demonstrate that \( \rho \) unambiguously determines an ideal \( \mathfrak{a} \) of \( \mathcal{O}(\mu) \). Define a set \( \langle \rho \rangle_R \) as follows:

\[
\langle \rho \rangle_R = \{ \xi \rho \mid \xi \in \mathcal{H} \text{ and } \xi \rho \in \mathcal{O}(\mu) \}.
\]

We call \( \rho \) a pseudo generator of \( \langle \rho \rangle_R \), and use the letter \( R \) to indicate that every element of this set is divisible by \( \rho \) from the right. From the definition of \( \langle \rho \rangle_R \), it follows that

\[
\langle \rho \rangle_R = (\rho)_L \cap \mathcal{O}(\mu),
\]

where \( (\rho)_L = \{ \xi \rho \mid \xi \in \mathcal{H} \} \) is a left ideal, generated by \( \rho \). Now, let us demonstrate that \( \mathfrak{a} = \langle \rho \rangle_R \). First of all, notice that all the elements of \( \mathfrak{a} = [a, b + \omega] \) are divisible by \( \rho \) from the right, so \( \mathfrak{a} \subseteq \langle \rho \rangle_R \). To show that the converse statement holds, once again, we follow the proof of Venkov [Ven2, §14]. Pick \( q \in \langle \rho \rangle_R \). Since \( q \in \mathcal{O}(\mu) \), we have \( q = X + \omega Y \) for some integers \( X \) and \( Y \). Since \( X + Y \omega = Y(b + \omega) = X - bY \) is divisible by \( \rho \) from the right, we can put \( X = bY + ca \) for some positive integer \( c \), which means that

\[
X + Y \omega = ca + Y(b + \omega).
\]

We conclude that \( \mathfrak{a} = \langle \rho \rangle_R \). Analogously, we can define

\[
\langle \rho' \rangle_L = \{ \rho' \xi \mid \xi \in \mathcal{H} \text{ and } \rho' \xi \in \mathcal{O}(\mu) \},
\]
and demonstrate that $\mathfrak{a} = \langle \rho' \rangle_L$. In the remaining parts of this paper, we call $\rho$ and $\rho'$ the right and left pseudo generators of $\mathfrak{a} = \langle \rho \rangle_R = \langle \rho' \rangle_L$, respectively. For obvious reasons, if $\mathfrak{a}$ is non-primitive, i.e. representable in the form $c[a, b + \omega]$ for some integer $c > 1$, then both $\rho$ and $\rho'$ will be non-primitive integral quaternions, and their greatest integral divisor will be exactly $c$.

The proof above allows us to make the following observation: even though an ideal $\mathfrak{a}$ in $\mathcal{O}(\mu)$ may have multiple generators, it still has a unique right (left) pseudo generator. Note that the right (left) pseudo generator is unique up to a multiplication by a unit of $\mathcal{H}$ from the left (right), because $\langle \varepsilon \rho \rangle_R = \langle \rho \rangle_R$ for any unit $\varepsilon$ (analogous statement holds for $\langle \rho' \rangle_L$). Hereinafter, all our results will be demonstrated for right pseudo generators, but by analogy we can demonstrate that they hold for left pseudo generators as well.

We now move our attention to the next important topic. Let $\mathfrak{a} = [\omega_1, \omega_2]$ be an arbitrary ideal in $\mathcal{O}(\mu)$. Since $\mathfrak{a} = \langle \rho \rangle_R$ for some integral quaternion $\rho$, there exist a pair of integral quaternions $\zeta_1$ and $\zeta_2$ s.t.

$$\omega_1 = \zeta_1 \rho, \quad \omega_2 = \zeta_2 \rho.$$ 

Since $N(\mathfrak{a}) = N(\rho)$, we conclude that $\zeta_1$, $\zeta_2$ do not have a common divisor from the right, and therefore $\gcd_r(\omega_1 \mu, \omega_2 \mu) = \rho \mu$. On the other hand, since $\omega_1, \omega_2$ both belong to $\mathcal{O}(\mu)$, they commute with $\mu$, whence the greatest common divisor of $\omega_1 \mu = \mu \omega_1$ and $\omega_2 \mu = \mu \omega_2$ is divisible by $\rho$ from the right. This allows us to conclude, that there exists an integral quaternion $\mu'$, which satisfies the relation

$$\rho \mu = \mu' \rho. \quad (3.3)$$

If we multiply the previous equation by $\mu$ from the right, it is not hard to notice that $\mu'^2 = -m$, so $\mu'$ forms another quadratic order $\mathcal{O}(\mu')$ in $\mathcal{H}$. A similar reasoning can be applied towards the left pseudo generator of an ideal. Thus, if $\mathfrak{a} = \langle \rho \rangle_R = \langle \rho' \rangle_L$ belongs to the quadratic order $\mathcal{O}(\mu)$, then the relations

$$\mu' = \rho \mu \rho^{-1}, \quad \mu'' = \rho' \mu \rho'^{-1}$$

generate the right and left orders $\mathcal{O}(\mu')$ and $\mathcal{O}(\mu'')$, respectively. The relation (3.3) describes a very important property of a pseudo generator $\rho$:
while \([a, b+\omega] = \langle \rho \rangle_R\) belongs to the quadratic order \(\mathcal{O}(\mu)\), \([a, b+\omega'] = \langle \rho' \rangle_L\) belongs to the quadratic order \(\mathcal{O}(\mu')\), where \(\omega' = (r - 1 + \mu')/r\).

Let us now answer the following question: if we know the pseudo generators of an ideal \(a = \langle \rho' \rangle_L = \langle \rho \rangle_R\) in \(\mathcal{O}(\mu)\), then how do pseudo generators of \(\overline{a}\) (the conjugate of \(a\)) look like?

**Proposition 3.3.** Let \(a = \langle \rho' \rangle_L = \langle \rho \rangle_R\) belong to the quadratic order \(\mathcal{O}(\mu)\). Then \(\overline{a} = \langle \rho \rangle_L = \langle \rho' \rangle_R\).

**Proof.** Let \(a = [a, b + \omega]\). Then the right and left pseudo generators of an ideal can be found from the following relations:

\[
\rho = \gcd_r(a, b + \omega), \quad \rho' = \gcd_l(a, b + \omega).
\]

Let \(b + \omega = \xi \rho\) for some integral quaternion \(\xi\). Then \(b + \omega = \xi \rho = \overline{\rho} \cdot \xi\). Since \(a = N(\rho)\), the left generator of \(\overline{a} = [a, b + \omega]\) is equal to

\[
\gcd_l(N(\rho), b + \omega) = \gcd_l(\overline{\rho} \cdot \rho, \overline{\rho} \cdot \xi) = \overline{\rho}.
\]

Analogously, we can find the right pseudo generator \(\overline{\rho'}\) of \(\overline{a}\) by noticing that \(a = N(\rho')\).

As a special case of this proposition, we notice that an ambiguous ideal \(a = \langle \rho \rangle_R\), i.e. the ideal with a property \(a = \overline{a}\), has \(\overline{\rho}\) as its left pseudo generator. We also emphasize another important property of ambiguous ideals in the following theorem.

**Theorem 3.4.** If \(a = \langle \rho \rangle_R\) is ambiguous in the quadratic order \(\mathcal{O}(\mu)\), then \(\rho\) divides \((2/r)\mu\) from the right, where \(r\) is defined as in relation \((3.2)\).

**Proof.** Since \(a = \overline{a}\), an ideal \(a = [a, b + \omega]\) contains both \(b + \omega\) and \(\overline{b + \omega}\). Let \(b + \omega = \xi \rho, \overline{b + \omega} = \xi' \rho\) for some \(\xi, \xi' \in \mathcal{H}\). Then

\[
b + \omega - \overline{b + \omega} = b + \frac{r - 1 + \mu}{r} - \left(b + \frac{r - 1 - \mu}{r}\right) = (2/r)\mu = \xi \rho - \xi' \rho;
\]

Hence, \(\xi - \xi' = (2/r)\mu \rho^{-1}\), i.e. the quaternion \((2/r)\mu \rho^{-1}\) is integral, which means that \(\rho\) divides \((2/r)\mu\) from the right.

We are aware that in a maximal quadratic order \(\mathcal{O}\) of \(\mathbb{Q}(\sqrt{-m})\), if \(a\) is ambiguous, then \(N(a)\) divides \((2/r)^2 m\) [JW09, Thm. 7.11]. The theorem above demonstrates that an analogous statement holds for \(\mathcal{O}(\mu)\) as well, where \(N(\mu) = m\). Moreover, we can notice that our theorem implies this
result, for if \( \rho \) divides \((2/r)\mu\) from the right, then \(N(\rho) = N(a)\) divides \(N((2/r)\mu) = (2/r)^2 m\).

So far, we have seen many interesting properties that ideals and their pseudo generators have. Now that we know how ideals get represented in the ring of integral quaternions, it would be interesting to study how to operate them. A common approach to manipulate ideals is to use their \(\mathbb{Z}\)-basis representation \([a, b + c\omega]\), where integers \(a, b\) satisfy inequalities \(a > 0\) and \(0 \leq b < a\), and \(c\) divides both \(a\) and \(b\). This approach is used in ideal reduction \([\text{JW}09\text{, Sec. 5.1}]\) and multiplication \([\text{JW}09\text{, Sec. 5.4}]\) algorithms. In the next section, we introduce a number of algorithms, which allow us to manipulate ideals in the ring of integral quaternions using solely their pseudo generators. While developing these algorithms, our primary goal was to avoid any mentioning of the \(\mathbb{Z}\)-basis. As a result, besides the reduction and multiplication algorithms, we introduce two additional ones: an algorithm to restore the \(\mathbb{Z}\)-basis of an ideal by its pseudo generator, and an algorithm to compute the right pseudo generator of an ideal using its left pseudo generator.

4 Algorithms

We begin our explorations with the series of definitions, where we consider two integral quaternions \(q\) and \(r\) of the form

\[
q = t_0 + x_0i + y_0j + z_0k, \\
r = t_1 + x_1i + y_1j + z_1k.
\]

**Definition 4.1.** A **scalar product** of quaternions \(q\) and \(r\) is the value \((q, r) = x_0x_1 + y_0y_1 + z_0z_1\);

**Definition 4.2.** A **full scalar product** of quaternions \(q\) and \(r\) is the value \((q, r) = t_0t_1 + x_0x_1 + y_0y_1 + z_0z_1 = \Re(q)\Re(r) + (q, r)\).

**Definition 4.3.** A **vector product** of quaternions \(q\) and \(r\) is the value \([q, r] = (y_0z_1 - y_1z_0)i + (x_1z_0 - x_0z_1)j + (x_0y_1 - x_1y_0)k\).

It is not hard to verify that, in case if \(\Re(q) = \Re(r) = 0\), \(q\) and \(r\) satisfy the relation

\[
(4.1) \quad qr = -(q, r) + [q, r].
\]

Finally, we shall introduce one more interesting relation, which holds for any integral quaternions \(q\) and \(r\):
This equality can be easily demonstrated using the properties of quaternion arithmetic. Both of the relations above will be used in the proofs that will be introduced in the following subsections.

The following algorithms allow us to manipulate ideals in the ring of integral quaternions. Note that, in order to migrate from an imaginary number field $\mathbb{Q}(\sqrt{-m})$ to the ring of integral quaternions, we need to generate one initial representation of an integer $m$ as a sum of three squares, i.e. $m = x^2 + y^2 + z^2$. Fortunately, there exists a fast algorithm, which computes integers $x, y, z$ with high probability in random polynomial time [RS86, p. S254].

4.1 Restoring the $\mathbb{Z}$-basis

Consider the following problem: given a primitive ideal $\langle \rho \rangle_R$ and the quadratic order $O(\mu)$ which it belongs to, find the $\mathbb{Z}$-basis of $\langle \rho \rangle_R$. In other words, we need to find integers $a, b$ s.t. $[a, b + \omega] = \langle \rho \rangle_R$.

In the section 3, we have demonstrated that $a = N(a) = N(\rho)$. Now it is left only to find $b$. One possible way to solve this problem is to find the square root of $-m$ mod $r^2a$, where $r$ is defined as in (3.2), for if $[a, b + \omega]$ is a valid ideal, then $b$ has to satisfy the congruence

$$(rb + r - 1)^2 \equiv -m \pmod{r^2a}.$$ 

There exists an effective algorithm [CP05, Alg. 2.3.8] with the worst case complexity $O(\ln^4 a)$, which computes a square root mod $a$ if $a$ is an odd prime. However, we would like to solve this problem for all the possible values of $a$.

Before we introduce another algorithm, which solves the problem for any $a$, let us first prove a couple of important propositions, which shall be quite useful in our future explorations.

Proposition 4.4. If real parts of quaternions $\mu$ and $\mu'$ are equal, then the equality $\rho \mu = \mu' \rho$ implies $(\mu, \rho) = (\mu', \rho)$.

Proof. Let us write $\rho, \mu$ as the sum of their real and vector parts:

$$(\Re(\rho) + \vec{\rho})(\Re(\mu) + \vec{\mu}) = (\Re(\mu') + \vec{\mu'})(\Re(\rho) + \vec{\rho});$$
\[ \Re(\rho)\Re(\mu) + \Re(\rho)\bar{\mu} + \Re(\mu)\bar{\rho} + \bar{\rho}\bar{\mu} = \Re(\mu')\Re(\rho) + \Re(\rho)\bar{\mu'} + \Re(\mu')\bar{\rho} + \bar{\mu'}\bar{\rho}. \]

Since \( \Re(\mu) = \Re(\mu') \),

\[ \Re(\rho)\bar{\mu} + \bar{\rho}\bar{\mu} = \Re(\rho)\bar{\mu'} + \bar{\mu'}\bar{\rho}. \]

If we now apply the relation (4.1), we shall get

\[ -(\rho, \mu) + [\rho, \mu] + \Re(\rho)\bar{\mu} = -(\mu', \rho) + [\mu', \rho] + \Re(\rho)\bar{\mu'}. \]

By taking the real part on both sides of the equality above, we obtain the desirable result: \( (\mu, \rho) = (\mu', \rho) \).

**Proposition 4.5.** If a primitive ideal \([a, b + \omega] = \langle \rho \rangle_R \) belongs to the quadratic order \( \mathcal{O}(\mu) \), then

\[ (\omega, \rho) + \Re(\rho) \left( b + \frac{r - 1}{r} \right) = \Re(\xi)N(\rho). \]

where \( \xi \) is an integral quaternion, which satisfies the relation \( b + \omega = \xi\rho \), and an integer \( r \) is defined as in (3.2).

**Proof.** Since \( b + \omega \) belongs to \( \langle \rho \rangle_R \), there exists an integral quaternion \( \xi \) s.t. \( b + \omega = \xi\rho \). Because \( \langle \rho \rangle_R \) belongs to \( \mathcal{O}(\mu) \), the relation (3.3) must hold for some \( \mu' \) of the same norm as \( \mu \). If we now multiply \( b + \omega = \xi\rho \) by \( \rho \) from the left and from the right, we shall get \( b + \omega' = \rho\xi \), where \( \omega' = (r - 1 + \mu')/r \). Therefore, \( 2b + \omega + \omega' = \rho\xi + \xi\rho \), and from the relation (4.2) we obtain the following system of equations:

\[ \begin{cases} b = \Re(\rho)\Re(\xi) - (\rho, \xi) - \frac{r - 1}{r}; \\ \frac{\omega + \omega'}{2} = \Re(\xi)\bar{\rho} + \Re(\rho)\bar{\xi} + \frac{r - 1}{r}. \end{cases} \]

From the proposition (4.4) it follows that \( (\omega, \rho) = (\omega', \rho) \), and therefore \( \left( \frac{\omega + \omega'}{2}, \rho \right) = (\omega, \rho) \). If we now combine this statement with the second equality of the system (4.4), we shall obtain

\[ (\omega, \rho) = \left( \frac{\omega + \omega'}{2}, \rho \right) = \left( \Re(\rho)\bar{\xi} + \Re(\xi)\bar{\rho} + \frac{r - 1}{r}, \rho \right) = \]

\[ = \Re(\rho)(\rho, \xi) + \Re(\xi)(\rho, \rho) = \Re(\rho)(\rho, \xi) + \Re(\xi)\left( N(\rho) - \Re(\rho)^2 \right). \]
From the first equality of the system (4.4), we know that $(\rho, \xi) = \Re(\rho)\Re(\xi) - b - (r - 1)/r$. Now, a simple substitution of $(\rho, \xi)$ in the equation above will give us the relation (4.3):

$$(\omega, \rho) = \Re(\rho) \left( \Re(\rho)\Re(\xi) - b - \frac{r - 1}{r} \right) + \Re(\xi) \left( N(\rho) - \Re(\rho)^2 \right) = \Re(\rho) \left( b + \frac{r - 1}{r} \right) + \Re(\xi) N(\rho).$$

This proposition allows us to formulate the following algorithm, which computes the \(\mathbb{Z}\)-basis of an ideal \(<\rho>_R\) in the quadratic order \(\mathcal{O}(\mu)\).

**Algorithm 4.6.** *Restoring the \(\mathbb{Z}\)-basis of an ideal by its pseudo generator.*

**Input:** a quadratic order \(\mathcal{O}(\mu)\) and a primitive ideal \(<\rho>_R\), which belongs to this order;
**Output:** Integers \(a\) and \(b\) s.t. \(<\rho>_R = [a, b + \omega]\).

1. Find a unit \(\varepsilon\) s.t. \(\Re(\varepsilon \rho)\) is an odd integer. Put \(\rho := \varepsilon \rho\);
2. If \(N(\rho)\) is even and \(N(\mu), (\mu, \rho)\) have different parity, set \(t := 2\). Otherwise set \(t := 1\);
3. Find \(d = \gcd (\Re(\rho), N(\rho)/t)\);
4. Using the extended Euclidean algorithm, compute the smallest non-negative \(b\), s.t. \(N(\rho) \leq N(b + \omega)\), and

$$rb + r - 1 \equiv -\frac{\mu, \rho}{d} \left( \frac{\Re(\rho)}{d} \right)^{-1} \left( \mod \frac{N(\rho)}{td} \right);$$
5. Return \(a = N(\rho)\) and \(b\).

**Proof of correctness.** The work of this algorithm is based on the relation (4.3). Obviously, if \(\Re(\rho) = 0\), then the summand which contains \(b\), vanishes. This is why we redefine \(\rho\) so that its real part would not be equal to zero. In this case, we pick \(\varepsilon\) to be equal to either \(i\), \(j\), or \(k\), depending on which coefficient of \(\rho\) is odd.

We would also like to avoid the case when \(\rho\) has half-integer coefficients. Fortunately, there will always exist exactly *eight* units of the form \((\pm 1 \pm i \pm j \pm k)/2\), which will make \(\varepsilon \rho\) have integral coefficients. In particular, if \(\rho\)
has even (odd) number of coefficients congruent to 1 mod 4, then all units of the type mentioned above, which have an odd (even) number of 1's, will work.

Finally, we argue that a pseudo generator ρ with integral coefficients will always have at least one odd coefficient, for if this is not the case, then all coefficients of ρ are even, which makes ρ non-primitive.

Now that our ρ has an odd real part, we want to make sure that all the other parts of the relation (4.3) are not half-integers. If we multiply this equality by r, and keep in mind that r(ω, ρ) = (μ, ρ), we get

\[(μ, ρ) + ℝ(ρ)(rb + r - 1) = rℝ(ξ)N(ρ).\]

If r = 2, then all the numbers above are integers, including rℝ(ξ). However, if r = 1, then we have to check whether ℝ(ξ) is a half-integer. This can happen only if N(ρ) is even, because the value on the left side can never be a half-integer.

Suppose that N(ρ) is even. Let us demonstrate that N(ρ) ≡ 2 (mod 4). Recall that N(ρ) divides N(b + ω) = b² + m, where m = N(μ). If m is odd, then b must be odd as well, since 2 divides b² + m. Because m ≡ 1 (mod 4) and b² ≡ 1 (mod 4), we have b² + m ≡ 2 (mod 4), so N(ρ) cannot be divisible by 4. On the other hand, if m is even, then m ≡ 2 (mod 4), because m is squarefree. For the reason that m and b have to be of the same parity, the congruence b² ≡ 0 (mod 4) holds, and therefore b² + m ≡ 2 (mod 4). Once again, this gives us the desirable result.

Now we know: if N(ρ) is even and ξ has half-integer coefficients, then the value on the right side of the previous equation has to be odd. Therefore, the value on the left side must be odd as well. When m (and therefore b) is odd, this can happen only if (μ, ρ) is odd, because ℝ(ρ)b will always be odd. On the other hand, if m (and therefore b) is even, this happens only when (μ, ρ) is odd. Summarizing, when N(ρ) is even and ℝ(ρ) is odd, then we can say that ξ has half-integer coefficients if and only if m and (μ, ρ) have different parity.

If we now set t as it is described at the step 2, then the following equation has no half-integers involved, independently of the input to the algorithm:

\[(μ, ρ) + ℝ(ρ)(rb + r - 1) = trℝ(ξ)\frac{N(ρ)}{t} ≤ \text{integer}.\]

Define d = gcd (ℝ(ρ), N(ρ)/t). Because d divides both ℝ(ρ) and N(ρ)/t, it has to divide (μ, ρ) as well. If we now divide both sides of the equation
above by \( d \), then \( \Re(\rho)/d \) and \( N(\rho)/(td) \) have no common divisor greater than 1, and therefore we can apply the extended Euclidean algorithm to find the value of \( rb + r - 1 \), using the formula introduced in step 4 of the algorithm. Finally, when computing \( b \), we would also like to make sure that \( N(\rho) \leq N(b + \omega) \), just in case if \( N(\rho) > m \).

**Remark 4.7.** Analogous algorithm exists for the ring of polynomials [Sch96, Alg. IDEAL].

**Remark 4.8.** Algorithm 4.6 resides on the Euclidean algorithm, so its time complexity (in the worst case) is estimated by \( O(\log^2 \Re(\rho)) \), where the right pseudo generator \( \rho \) is chosen so that \( \Re(\rho) \) is positive and odd.

### 4.2 Computing the right pseudo generator of an ideal using its left pseudo generator

The next problem of a great interest is the following: given an ideal \( \langle \rho \rangle_L \) in the quadratic order \( \mathcal{O}(\mu) \), find an integral quaternion \( \rho' \) s.t. \( \langle \rho \rangle_L = \langle \rho' \rangle_R \).

Consider the \( \mathbb{Z} \)-basis of an ideal: \( \langle \rho \rangle_L = \langle \rho' \rangle_R = [a, b + \omega] \). Recall that \( \rho' = \gcd_r(a, b + \omega) \), so the most straightforward way to compute \( \rho' \) is to restore the \( \mathbb{Z} \)-basis using the algorithm 4.6 and then apply the Euclidean algorithm to \( a \) and \( b + \omega \). However, as was mentioned earlier, in this paper we try to avoid the usage of the \( \mathbb{Z} \)-basis in our computations. In this section, we present another approach to find \( \rho' \), without obtaining \( b \) in the first place.

Recall that for any integers \( X \) and \( Y \), a quaternion \( aX + (b + \omega)Y \) belongs to the ideal, and therefore has to be divisible by \( \rho' \) from the right. Since the relation (4.3) holds for the left pseudo generator as well, if we now set \( X = -\Re(\xi) \) and \( Y = \Re(\rho)r \), we shall obtain

\[
aX + (b + \omega)Y = (aX + bY) + \omega Y =
\]

\[
= (-\Re(\xi)N(\rho)r + \Re(\rho)br) + r\Re(\rho)\omega = -r(\omega, \rho) - \Re(\rho)(r - 1) + r\Re(\rho)\omega.
\]

Recall that \( a = N(\rho) \) and \( \xi \) satisfies the relation \( b + \omega = \rho\xi \). Since \( r(\omega, \rho) = (\mu, \rho) \) and \( -\Re(\rho)(r - 1) + r\Re(\rho)\omega = \Re(\rho)\mu \), we conclude that

\[
aX + (b + \omega)Y = -r(\omega, \rho) - \Re(\rho)(r - 1) + r\Re(\rho)\omega = -(\mu, \rho) + \Re(\rho)\mu.
\]

Now an application of the Euclidean algorithm will help us to derive \( \rho' \):
\(\rho' = \gcd_r \left( -\langle \mu, \rho \rangle + \Re(\rho)\mu, N(\rho) \right)\).

Consider another approach to the same problem. Since \(\rho\) is the left pseudo generator of an ideal which belongs to \(\mathcal{O}(\mu)\), then there exists an integral quaternion \(\mu'\) of the same norm as \(\mu\), s.t. \(\rho \mu' = \mu \rho\). If we now add \(\rho \mu\) on both sides of this equation, and then apply the relation (4.2), we shall get the following result:

\[
\rho \mu + \rho \mu' = \rho \mu + \mu \rho;
\]
\[
\rho \frac{\mu + \mu'}{2} = \frac{\mu \rho + \rho \mu}{2} = -\langle \mu, \rho \rangle + \Re(\rho)\mu.
\]

So, the following formula can also be used to compute \(\rho'\):

\(\rho' = \gcd_r \left( \rho \frac{\mu + \mu'}{2}, N(\rho) \right)\).

**Remark 4.9.** Analogously, we can solve the problem of finding the left pseudo generator of an ideal given its right pseudo generator. In that case, the formula (4.5) does not change, except for \(\gcd_r\), which gets replaced by \(\gcd_l\). In turn, the formula (4.6) takes the form

\[
\rho' = \gcd_l \left( \frac{\mu + \mu'}{2}, \rho, N(\rho) \right).
\]

### 4.3 Ideal multiplication

Let us now turn our attention to the problem of ideal multiplication. Consider a quadratic order \(\mathcal{O}(\mu)\) and two ideals, \(\langle \rho \rangle_R\) and \(\langle \rho' \rangle_R\), which belong to this quadratic order. The following algorithm multiplies these ideals using solely their pseudo generators.

**Algorithm 4.10. Ideal multiplication.**

**Input:** a quadratic order \(\mathcal{O}(\mu)\), and two primitive ideals, \(\langle \rho \rangle_R\) and \(\langle \rho' \rangle_R\), which belong to this quadratic order;

**Output:** (non-reduced) ideal \(\langle \rho \rangle_R \cdot \langle \rho' \rangle_R\).

1. Compute \(\mu' = \rho' \mu \rho'^{-1}\);
2. Compute \(\rho'' = \gcd_r \left( -\langle \mu, \rho \rangle + \Re(\rho)\mu', N(\rho) \right)\);
3. Return \(\langle \rho'' \rho' \rangle_R\).
Proof of correctness. The problem of ideal multiplication was studied by Venkov in his 4th letter [Ven4, §18]. Let \( a = \langle \rho \rangle_R \) and \( b = \langle \rho' \rangle_R \). Venkov demonstrated that if an ideal \( a = [a, b + \ast] \) (where \( \ast \) can be replaced by \( \omega, \omega', \ldots \) to move an ideal between various quadratic orders) has a right pseudo generator \( \rho'' \) in a quadratic order \( \mathcal{O}(\mu') \), where \( \mu' = \rho' \mu \rho' - 1 \), then \( \rho'' \rho' \) is a right pseudo generator of an ideal \( ab \) in \( \mathcal{O} (\mu) \). The question is, how do we find \( \rho'' \)?

We can compute \( \rho'' \) using an approach similar to the one described in the previous subsection. Let \( \langle \rho \rangle_R = [a, b + \omega] \). Then \( [a, b + \omega'] \), where \( \omega' = \rho' \omega \rho' - 1 \), belongs to the quadratic order \( \mathcal{O}(\mu') \). For any integers \( X \) and \( Y \), the quaternion \( aX + (b + \omega')Y \) belongs to this ideal, and therefore has to be divisible by \( \rho'' \) from the right. Since the relation (4.3) holds for the ideal \( [a, b + \omega] \) in the quadratic order \( \mathcal{O}(\mu) \), then we can set \( X = -\Re(\xi) \) and \( Y = \Re(\rho)r \), which will give us

\[
-r(\omega, \rho) - \Re(\rho)(r - 1) + r\Re(\rho)\omega' = -(\mu, \rho) + \Re(\rho)\mu'.
\]

This integral quaternion belongs to \( [a, b + \omega'] \). Now \( \rho'' \) can be obtained using the Euclidean algorithm, as it is described in the step 2.

Now that we went over the steps of the algorithm, let us prove that \( \rho'' \rho' \) is really a pseudo generator of the product. Consider the product of \( \langle \rho \rangle_R = [a, b + \omega] \) and \( \langle \rho' \rangle_R = [a', b' + \omega] \):

\[
[a, b + \omega] \cdot [a', b' + \omega] = [aa', a(b' + \omega), a'(b + \omega), (b' + \omega)(b + \omega)].
\]

Let \( b' + \omega = \xi' \rho' \) and \( b + \omega' = \xi'' \rho'' \). Then

\[
aa' = \overline{\rho'} \rho'' \rho' \rho';
\]

\[
a(b' + \omega) = a\xi' \rho' = \xi' a\rho' = \xi' \rho'' \rho';
\]

\[
a'(b + \omega) = \overline{\rho'} \rho'(b + \omega) \rho'^{-1} \rho' = \rho'' \xi'' \rho';
\]
\[(b' + \omega)(b + \omega) = \xi' \rho'(b + \omega)\rho'^{-1} \rho' = \xi'\xi'' \rho'.\]

Since \(b + \omega' = \xi'' \rho''\) is primitive, quaternions \(\xi''\) and \(\overline{\rho''}\) do not have a common divisor from the right, and therefore \(\rho'' \rho'\) is the greatest common divisor of \(aa', a(b' + \omega), a'(b + \omega)\) and \((b' + \omega)(b + \omega)\). Since these four quaternions form a \(\mathbb{Z}\)-basis of a resulting ideal, \(\rho'' \rho'\) has to be the right pseudo generator of this ideal. \(\square\)

**Remark 4.11.** Our proof is similar to the proof for the multiplication of ideals in the ring of adèles [KM90].

### 4.4 Ideal reduction

Before we turn our attention to the process of ideal reduction, let us first state some important theorems.

**Theorem 4.12.** Let \(\mathcal{O}(\mu)\) be a quadratic order, \(m = N(\mu)\). If a primitive integral quaternion \(\rho\) satisfies the relation (3.3) for some \(\mu'\), and \(N(\rho)\) is odd when \(m \equiv 3 \pmod{8}\), then it is a right (left) pseudo generator of some ideal in the quadratic order \(\mathcal{O}(\mu)\) (\(\mathcal{O}(\mu')\)). Conversely, if \(\langle \rho \rangle_R\) is an ideal in the quadratic order \(\mathcal{O}(\mu)\), then \(\rho\) satisfies (3.3) for some \(\mu'\), and \(N(\rho)\) is odd when \(m \equiv 3 \pmod{8}\). Moreover, \(\langle \rho \rangle_L\) is an ideal in \(\mathcal{O}(\mu')\).

**Proof.** Let us first argue why it is necessary for \(N(\rho)\) to be odd when \(m \equiv 3 \pmod{8}\). If we consider a primitive ideal \([N(\rho), b + \omega]\), then \(N(\rho) \mid N(b + \omega) = \frac{(2b + 1)^2 + m}{4}\), so \(-m\) has to be a quadratic residue of \(4N(\rho)\). Since any odd integer \(x\) satisfies the congruence \(x^2 \equiv 1 \pmod{8}\), we have \((2b + 1)^2 + m \equiv 4 \pmod{8}\), and therefore \(N(\rho)\) has to be odd. In his 2nd letter, Venkov proved that for any \(\rho\) and \(\mu\), which satisfy the relation (3.3) for some \(\mu'\), \(-m\) has to be a quadratic residue of \(N(\rho)\) [Ven2 §10]. However, when \(m \equiv 3 \pmod{8}\), this does not imply that \(-m\) is a quadratic residue \(\mod 4N(\rho)\). In fact, the implication takes place only if \(N(\rho)\) is odd. In that case, it is easy to see that if \(x^2 \equiv -m \pmod{N(\rho)}\) for some \(x\), then \(4N(\rho)\) divides \(x^2 + m\) if \(x\) is odd, and \((x + N(\rho))^2 + m\) if \(x\) is even. Note that if \(N(\rho)\) is even while \(m \equiv 3 \pmod{8}\), then an ideal \(\langle \rho \rangle_R\) would belong to \([1, \mu]\), which is not isomorphic to the maximal quadratic order \(\mathcal{O} = [1, (1 + \sqrt{-m})/2] \in \mathbb{Q}(\sqrt{-m})\).

\((\Rightarrow)\) Let \(\rho\) satisfy the equation \(\rho \mu = \mu' \rho\) for some \(\mu'\), and \(N(\rho)\) be odd when \(m \equiv 3 \pmod{8}\). Then \(-m\) is a quadratic residue of \(r^2 N(\rho)\), where \(r\) is defined as in (3.2). Define \(b\) as a square root of \(-m \pmod{r^2 N(\rho)}\). Then
\([N(\rho), b + \omega]\) is an ideal in \(\mathcal{O}(\mu)\). Let \(b + \omega = \xi \rho\) for some \(\xi\). Since \(b + \omega\) is primitive, quaternions \(\xi\) and \(\rho\) have no common divisor from the right, which makes \(\rho\) a greatest common divisor of \(N(\rho)\) and \(b + \omega\) from the right, and therefore a right pseudo generator of \([N(\rho), b + \omega]\). Since \(N(\mu) = N(\mu')\), a similar argument can be applied towards the ideal \([N(\rho), b + \omega']\), where \(b + \omega' = \rho(b + \omega)\rho^{-1} = \rho \xi\).

\((\Leftarrow)\) The proof of the converse statement was demonstrated in the section \(\square\)

Next, we must point out that some quadratic orders are equivalent to each other. Note that for any unit \(\varepsilon\) we have \(\langle \varepsilon \rho \rangle_R = \langle \rho \rangle_R\). Hence, if \(\rho\) satisfies the relation \(\rho \mu = \mu' \rho\), then \(\varepsilon \rho\) satisfies

\[\varepsilon \rho \cdot \mu = \varepsilon \mu' \varepsilon \cdot \varepsilon \rho.\]

It means that our \(\mu'\) in the relation (3.3) may vary, depending on the pseudo generator we choose. As a result, we can define the following equivalence relation on the set of all quadratic orders in \(\mathcal{H}\) of a certain discriminant.

**Definition 4.13.** We say that two quadratic orders \(\mathcal{O}(\mu)\) and \(\mathcal{O}(\mu')\) are **equivalent**, if \(\mu\) and \(\mu'\) satisfy the relation \(\mu' = \varepsilon \mu \varepsilon\) for some unit \(\varepsilon\).

It is well known that ideals, which are equivalent to each other, form an **equivalence class**. The following theorem describes how we can fully characterize this set.

**Theorem 4.14.** [Ven3, §9] Consider a quadratic order \(\mathcal{O}(\mu)\), which contains two equivalent ideals \(\langle \rho \rangle_R\) and \(\langle \rho' \rangle_R\). If \(\rho \mu = \mu' \rho\) and \(\rho' \mu = \mu'' \rho'\), then \(\mathcal{O}(\mu')\) and \(\mathcal{O}(\mu'')\) are equivalent.

The theorem above demonstrates a rather interesting fact that all solutions to the equation \(\rho \mu = \mu' \rho\) for given \(\mu\) and \(\mu'\) are pseudo generators of ideals, which are equivalent to each other.

In his 3rd letter, Venkov described the full set of solutions to the equation (3.3). We summarize his results in the following theorem.

**Theorem 4.15.** [Ven3, Ven4] Let \(\mu\) and \(\mu'\) be two primitive integral quaternions with the zero real part, s.t. \(N(\mu) = N(\mu')\). Then the set of all solutions to the equation \(\rho \mu = \mu' \rho\) takes the form of a \(\mathbb{Z}\)-module \([v, v_1]\) for some particular integral quaternions \(v, v_1\).
Proof. In this proof, we will simply describe the form of quaternions $v, v_1$. For more details, we ask our reader to refer to the original works of Venkov. Let

$$
\mu = xi + yj + zk,
$$
$$
\mu' = x'i + y'j + z'k.
$$

If $\mu' \neq -\mu$, then the set of all $\rho$ with integral coefficients is of the form $\rho = vX + \Upsilon Y$, where $X, Y$ are integers, and $v, \Upsilon$ are two integral quaternions, defined by the following system of equations:

$$
\begin{align*}
\begin{aligned}
v &= \frac{x'+x}{d}i + \frac{y'+y}{d}j + \frac{z'+z}{d}k = \frac{\mu' + \mu}{d}, \\
\Upsilon &= \frac{-x}{e}i + \frac{y}{e}j + \frac{z}{e}k.
\end{aligned}
\end{align*}
$$

In this system, $d$ and $e$ are defined as follows:

$$
d = \gcd (x' + x, y' + y, z' + z),
$$
$$
e = \gcd (x' + x, y' + y, z' + z, x' - x, y' - y, z' - z).
$$

Integers $a, b$ and $c$ are defined using the extended Euclidean algorithm:

$$
a(x' + x) + b(y' + y) + c(z' + z) = d.
$$

Integers $p, q$ and $r$ are defined through $a, b, c$:

$$
p = c(y' - y) - b(z' - z), \quad q = a(z' - z) - c(x' - x), \quad r = b(x' - x) - a(y' - y).
$$

The full set of solutions (including those $\rho$ with half-integer coefficients) has the form $\rho = vX + v_1Y$, where $v$ is defined as in system (4.7), and $v_1$ is defined as in one of the following four cases:
(a) If $m \equiv 1, 2 \pmod{4}$, and one of the sums $x' + x, y' + y, z' + z$, for example $x' + x$, is even, then

$$v_1 = \frac{1}{2}(\Upsilon + (a + 1)v);$$

(b) If $m \equiv 3 \pmod{8}$ and one of the sums, for example $x' + x \equiv 2 \pmod{4}$, and others are $\equiv 0 \pmod{4}$, then

$$v_1 = \frac{1}{2}(\Upsilon + (b + c + 1)v),$$

(c) If $m \equiv 3 \pmod{8}$ and all of the sums are $\equiv 2 \pmod{4}$, then

$$v_1 = \frac{1}{2}(\Upsilon + v);$$

(d) Otherwise $v_1 = \Upsilon$.

In case if $\mu' = -\mu$, define $d = \gcd(y, z)$. If $e, f$ are solutions to the equation

$$ey + fz = d,$$

then the set of all $\rho$ satisfying the equation $\rho\mu = -\mu\rho$ is of the form (4.8), where

$$v = \frac{zj - yk}{d}, \quad v_1 = -di + x(ej + fk).$$

While the theorem 4.14 tells us that the relation (3.3) fully characterizes some particular equivalence class, the theorem 4.15 tells us that all pseudo generators of ideals in this equivalence class have to be of the form $\rho = vX + v_1Y$ for some integers $X, Y$ and some fixed integral quaternions $v, v_1$.

Now we have all the results we need to turn our attention to the problem of ideal reduction.
Definition 4.16. An ideal \( \langle r \rangle_R \) in the quadratic order \( \mathcal{O}(\mu) \) is said to be reduced, if in the set of solutions to the equation (3.3), where \( \mu' = r\mu r^{-1} \), it has the smallest positive norm.

By the theorem 4.15, the set of all solutions to the equation (3.3) is equal to the \( \mathbb{Z} \)-module \([v, v_1]\). In turn, the theorem 4.14 tells us that any ideal \( \langle vX + v_1Y \rangle_R \) is equivalent to \( \langle r \rangle_R \). Therefore, our goal is to find an integral quaternion of the smallest positive norm, which belongs to \([v, v_1]\).

It is quite straightforward to find the norm of the reduced ideal. Consider the norm of \( \rho = vX + v_1Y \):

\[
N(\rho)(X, Y) = N(v)X^2 + 2(v, v_1)XY + N(v_1)Y^2.
\]

Since \( N(\rho)(X, Y) \) is a quadratic form, then the problem of finding the smallest norm is equivalent to the problem of finding the smallest integer, representable by the form \((N(v), 2(v, v_1), N(v_1))\). Using the reduction algorithm for quadratic forms [CP05, Alg. 5.6.2], we can find the reduced form \((a, b, c)\), equivalent to the given one. The form \((a, b, c)\) has a property that \(a\) is the smallest integer representable by this form, and therefore it is also the smallest integer representable by the original form [Buc07, Sec. 5.10].

As we have seen, given an ideal \( \langle \rho \rangle_R \) in the quadratic order \( \mathcal{O}(\mu) \), it is possible to find the norm of the reduced ideal \( \langle r \rangle_R \), but not the ideal itself. The following algorithm allows us to compute a pseudo generator of the reduced ideal. Note that \( \lfloor x \rfloor = \lfloor x + 1/2 \rfloor \) defines an integer, which is closest to \( x \).

Algorithm 4.17. Ideal reduction.

Input: a quadratic order \( \mathcal{O}(\mu) \) and a primitive ideal \( \langle \rho \rangle_R \), which belongs to this order;

Output: a reduced ideal, which is equivalent to \( \langle \rho \rangle_R \).

1. Compute \( \mu' := \rho\mu\rho^{-1} \);

2. Compute the \( \mathbb{Z} \)-basis of the module \([v, v_1]\), \( N(v) > N(v_1) \), which characterizes the set of solutions to the equation \( \rho\mu = \mu'\rho \);

3. Switch \( v \) and \( v_1 \);

4. Compute \( X := [(v, v_1)_X/N(v)] \);

5. Put \( \omega_1 := \omega_1 - \omega X \);
6. If $N(v) > N(v_1)$, go to step 3;

7. If $N(v) = N(v_1)$ and $2|(v, v_1)_x| \geq N(v)$, return $\langle v_1 - v \rangle_R$. Otherwise return $\langle v \rangle_R$.

Proof of correctness. Let $N(v_1) \geq N(v)$. Consider the norm of a quaternion $v_1 - vX$:

$$N(v_1 - vX) = N(v)X^2 - 2(v, v_1)_x X + N(v_1).$$

This quadratic function of one variable reaches its minimum at the point $X_0 = (v, v_1)_x/N(v)$. However, we are interested in integral (or half-integral) $X$, s.t. $N(v_1 - vX)$ takes its smallest positive value, and $v_1 - vX$ is an integral quaternion. Note that $X$ can be a half-integer only in one of the following two cases:

(a) When coefficients of $v_1$ are integers, and coefficients of $v$ are integral and odd;

(b) When coefficients of $v_1$ are half-integers, and coefficients of $v$ are integral and even.

Let us demonstrate that during the work of algorithm 4.17 quaternions $v_1$ and $v_1$ cannot satisfy neither (a), nor (b). Note that if any of the above conditions hold, then $v$ is divisible by 2, and therefore it is non-primitive. We aim to show that $v$ and $v_1$ will always be primitive.

The first time we reach the step 3 of our algorithm, $v$ and $v_1$ are primitive and linearly independent, because of the way they were defined in the theorem 4.15. On the step 5, we define $v_1 := v_1 - vX$, so now our new $v_1$ may not be primitive. However, we can demonstrate that this is not the case.

Suppose that in the $\mathbb{Z}$-module $[v, v_1]$ we have $v_1 = \Delta q$ for some integer $\Delta > 1$ and a primitive quaternion $q$. Since $v_1$ is a solution to the equation (3.3), then $q$ is a solution as well. It means that $q = vX + q\Delta Y$ for some integers $X$ and $Y$, because $[v, v_1]$ completely characterizes the set of solutions of the equation (3.3). Therefore, both of the following equalities

$$v = \frac{1 - \Delta Y}{X} q, \quad q = \frac{X}{1 - \Delta Y} v$$

must hold at the same time. Note that $X \neq 0$, since $\Delta > 1$. Now, because $q$ is primitive, $X$ must divide $1 - \Delta Y$, and since $v$ is primitive, $1 - \Delta Y$ must
divide $X$, whence $X = 1 - \Delta Y$. It implies that $v$ is equal to $q$, which contradicts the fact that $v$ and $v_1$ are linearly independent. Therefore, $v$ and $v_1$ are both primitive, which means that $X$ cannot be a half-integer.

Let us now return back to our algorithm. As it was mentioned before, the function (4.10) reaches its minimum at the point $X_0 = (v, v_1)\times/N(v)$. Therefore, an integer $X = [X_0]$ corresponds to an integral quaternion $v_1 - vX$, which has the smallest norm. Now we can replace the $\mathbb{Z}$-module $[v, v_1]$ with the equivalent $\mathbb{Z}$-module $[v, v_1 - vX]$. However, if $N(v_1) > N(v)$, where $v_1 := v_1 - vX$, there is no need to go back to step 3. For if we would perform the norm reduction in the same way one more time (without swapping $v$ and $v_1$, because $N(v_1)$ is already greater than $N(v)$), we would get $X = 0$. As we shall see later, $X = 0$ actually indicates that $\langle v \rangle_R$ is reduced. In case if $N(v) = N(v_1)$, we also don’t need to go back to step 3. If we consider the quadratic form (4.9), which characterizes the norm of $\rho = vX + v_1Y$, the Cauchy-Schwarz inequality holds:

$$|(v, v_1)\times| \leq \sqrt{N(v) \cdot N(v_1)} = N(v).$$

It means that $X$ is either 0 (i.e. $\langle v \rangle_R$ is reduced), or $\pm 1$, depending on the sign of $(v, v_1)\times$. In the second case, we replace a $\mathbb{Z}$-module $[v, v_1]$ with $[v_1 - v, v]$. Note that $N(v_1 - v) \leq N(v)$ because $2|(v, v_1)\times| \geq N(v)$ (i.e. $|X| = 1$). Now, compute

$$X = \left[ \frac{(v_1 - v, v)\times}{N(v_1 - v)} \right] = \left[ \frac{(v, v_1)\times - N(v)}{N(v_1) - 2(v, v_1)\times + N(v)} \right] = \left[ -\frac{1}{2} \right] = 0.$$

Because $X = 0$, we conclude that $\langle v_1 - v \rangle_R$ is reduced.

Summing up, we have to replace $[v, v_1]$ with $[v, v_1 - vX]$ only if $N(v) > N(v_1)$. When this is done, at the step 3 we swap the basis quaternions, in order to ensure that at the step 4 we have $N(v_1) > N(v)$. Note that on each iteration we ensure that the norm of one of the basis quaternions gets lessened. Since norms are bounded below by zero, and we return the result whenever $N(v_1) \geq N(v)$, our algorithm will definitely terminate.

Now, let us prove that if $X = 0$, then the norm of $v$ is the smallest positive integer, which can be represented by a quadratic form $(N(v), 2(v, v_1)\times, N(v_1))$. First of all, recall that the condition $X = [(v, v_1)\times/N(v)] = 0$ means

$$(4.11) \quad -\frac{N(v)}{2} \leq (v, v_1)\times < \frac{N(v)}{2}.$$
Second, suppose that there exists a quaternion \( r \) s.t. \( N(r) \leq N(v) \). Then there exist two integers \( X \) and \( Y \) s.t. \( r = vX + v_1Y \), i.e.

\[
N(r) = N(v)X^2 + 2(v, v_1)XY + N(v_1)Y^2 \leq N(v).
\]

Since \((v, v_1)\) satisfies the relation \((4.11)\), we have

\[
N(v) \geq N(r) \geq N(v)X^2 - N(v)|XY| + N(v_1)Y^2.
\]

On the 3rd step, we ensure that \( v_1 \) has a greater norm than \( v \), so the following inequality holds:

\[
N(v) \geq N(r) \geq N(v)X^2 - N(v)|XY| + N(v)Y^2 \geq 0.
\]

If we now divide all the parts of the inequality above by \( N(v) \neq 0 \), we get

\[
1 \geq \frac{N(r)}{N(v)} \geq X^2 - |XY| + Y^2 \geq 0.
\]

Since \( X^2 - |XY| + Y^2 \) takes only integral values, it has to be equal to either 0 or 1. If it is equal to zero, then \( X = 0 \) and \( Y = 0 \), because \( X^2 - |XY| + Y^2 \) is a positive definite quadratic form \([Buc07, Prop. 1.2.10]\). This implies \( N(r) = 0 \). On the other hand, if \( X^2 - |XY| + Y^2 = 1 \), then \( N(r) = N(v) \). Therefore, \( v \) has the smallest positive norm. \( \Box \)

The following theorem describes an upper bound to the number of iterations that algorithm \((4.17)\) performs in order to compute the reduced ideal.

**Theorem 4.18.** Let \([\alpha_0, \beta_0] \) be a \( \mathbb{Z} \)-module, where \( \alpha_0 \) and \( \beta_0 \) are two arbitrary linearly independent integral quaternions with \( A = N(\alpha_0) \geq B = N(\beta_0) \). Define an algorithm, which computes

\[
\alpha_{n+1} = \beta_n, \quad \beta_{n+1} = \alpha_n - \left\lfloor \frac{(\alpha_n, \beta_n)}{N(\beta_n)} \right\rfloor \beta_n,
\]

and terminates whenever \( N(\beta_k) \geq N(\alpha_k) \) for some \( k \). Then \( k(A, B) \in O\left(\log \log \frac{A}{B\varphi}\right) \) as \( A/B \to \varphi \), where \( \varphi = (1+\sqrt{5})/2 \). In case if \( B = \lfloor A/\varphi \rfloor \), then \( k(A) \in O\left(\log \frac{A}{\lfloor A/\varphi \rfloor}\right) \) as \( A \to \infty \), where \( \{x\} \) denotes the fractional part of \( x \).

**Proof.** Let us estimate the difference between the norms of quaternions \( \alpha_n \) and \( \beta_{n+1} \):
Ideal Class Group Algorithms in the Ring of Integral Quaternions

\[ N(\alpha_n) - N(\beta_{n+1}) = N(\beta_n) \left[ \frac{(\alpha_n, \beta_n)_x}{N(\beta_n)} \right] \left( 2 \left( \frac{(\alpha_n, \beta_n)_x}{N(\beta_n)} \right) - \left\lfloor \frac{(\alpha_n, \beta_n)_x}{N(\beta_n)} \right\rfloor \right) \geq 0. \]

Note that the difference can be either less than, or greater than, or equal to \( N(\beta_n) \). Consider the first case. Then

\[ \left\lfloor \frac{2(\alpha_n, \beta_n)_x}{N(\beta_n)} \right\rfloor - \left\lfloor \frac{(\alpha_n, \beta_n)_x}{N(\beta_n)} \right\rfloor < 1. \]

Note that for the function \( f(x) = |2x - \lfloor x \rfloor| \) the inequality \( 0 \leq f(x) < 1 \) holds only for \(-1 < x < 1\). Therefore, \(-1 < (\alpha_n, \beta_n)_x/N(\beta_n) < 1\), and \( \lfloor (\alpha_n, \beta_n)_x/N(\beta_n) \rfloor = \pm 1 \), depending on the sign of \( (\alpha_n, \beta_n)_x \). We do not consider the case \( \lfloor (\alpha_n, \beta_n)_x/N(\beta_n) \rfloor = 0 \), because it indicates the termination of our algorithm. Suppose that \( (\alpha_n, \beta_n)_x \geq 0 \) (we can prove the opposite case analogously). Then

\[ \alpha_{n+1} = \beta_n, \quad \beta_{n+1} = \alpha_n - \left\lfloor \frac{(\alpha_n, \beta_n)_x}{N(\beta_n)} \right\rfloor \beta_n = \alpha_n - \beta_n; \]

\[ \alpha_{n+2} = \beta_{n+1} = \alpha_n - \beta_n, \quad \beta_{n+2} = \alpha_{n+1} - \left\lfloor \frac{(\alpha_{n+1}, \beta_{n+1})_x}{N(\beta_{n+1})} \right\rfloor \beta_{n+1}. \]

Let us simplify the integer occurring in \( \beta_{n+2} \):

\[ \left\lfloor \frac{(\alpha_{n+1}, \beta_{n+1})_x}{N(\beta_{n+1})} \right\rfloor = \left\lfloor \frac{(\beta_n, \alpha_n - \beta_n)_x}{N(\alpha_n) - 2(\alpha_n, \beta_n)_x + N(\beta_n)} + \frac{1}{2} \right\rfloor = \left\lfloor \frac{N(\alpha_n) - N(\beta_n)}{2(N(\alpha_n) - 2(\alpha_n, \beta_n)_x + N(\beta_n))} + \frac{1}{2} \right\rfloor. \]

If we now look closer at the difference under the floor sign, we notice that it actually varies from 0 to 1/2, excluding 1/2, because \( N(\alpha_n) > N(\beta_n) \). This allows us to conclude that the integer we have been computing is actually zero, and therefore \( \beta_{n+2} = \alpha_{n+1} = \beta_n \). Summarizing, we have

\[ \alpha_n, \alpha_{n+1} = \beta_n, \quad \alpha_{n+2} = \alpha_n - \beta_n; \]

\[ \beta_n, \beta_{n+1} = \alpha_n - \beta_n, \quad \beta_{n+2} = \beta_n. \]

We conclude that whenever the norm of \( N(\alpha_n) \) gets reduced by less than \( N(\beta_n) \), our algorithm will terminate either on the \((n+1)\)-st, or on the \((n+2)\)-nd iteration.

Now, consider the second case, when \( N(\alpha_n) - N(\beta_{n+1}) \geq N(\beta_n) \). Let us assume the worst case, when on each iteration of the algorithm the norm of
\( N(\alpha_n) \) gets reduced exactly by \( N(\beta_n) \). Denote \( A_n = N(\alpha_n) \), \( B_n = N(\beta_n) \), and let \( f_n \) for natural \( n \) denote the \( n \)-th element of the Fibonacci sequence, i.e. \( f_1 = 1 \), \( f_2 = 1 \), \( f_{n+2} = f_{n+1} + f_n \). Then on the first six iterations, our algorithm produces the result, demonstrated in the table below. Note that the 4th column demonstrates which inequality has to be satisfied in order for the algorithm to proceed to the next iteration, and the 5th column demonstrates an interval, which \( A/B \) belongs to if two consecutive iterations did not result in a termination of the algorithm.

| \( n \) | \( A_n \) | \( B_n \) | \( A_n > B_n \) | Interval for \( A/B \) |
|---|---|---|---|---|
| 1 | \( A \) | \( B \) | \( f_1A > f_2B \) | \( \frac{f_1}{f_2} \geq \frac{A}{B} \geq \frac{f_2}{f_3} \) |
| 2 | \( B \) | \( A - B \) | \( f_3B > f_2A \) | \( \frac{f_3}{f_2} \geq \frac{A}{B} \geq \frac{f_2}{f_1} \) |
| 3 | \( f_1A - f_2B \) | \( f_3B - f_2A \) | \( f_3A > f_4B \) | \( \frac{f_3}{f_2} \geq \frac{A}{B} \geq \frac{f_4}{f_3} \) |
| 4 | \( f_3B - f_2A \) | \( f_3A - f_4B \) | \( f_5B > f_4A \) | \( \frac{f_5}{f_4} \geq \frac{A}{B} \geq \frac{f_4}{f_5} \) |
| 5 | \( f_5A - f_4B \) | \( f_5B - f_4A \) | \( f_5A > f_6B \) | \( \frac{f_5}{f_4} \geq \frac{A}{B} \geq \frac{f_6}{f_5} \) |
| 6 | \( f_7B - f_6A \) | \( f_7A - f_6B \) | \( f_7B > f_6A \) | \( \frac{f_7}{f_6} \geq \frac{A}{B} \geq \frac{f_6}{f_7} \) |

Table 1

In general, it is not hard to show that, depending on the parity of \( n \), for \( n > 2 \) we get

- \( n \) is odd: \( \alpha_n = f_{n-2}A - f_{n-1}B \), \( \beta_n = f_nB - f_{n-1}A \);
- \( n \) is even: \( \alpha_n = f_{n-1}B - f_{n-2}A \), \( \beta_n = f_{n-1}A - f_nB \).

Using the famous relation \( f_{n-1}f_{n+1} - f_n^2 = (-1)^n \), which holds for any \( n \geq 2 \), we can demonstrate that an interval, defined on the iteration \( 2m+2 \), is a subset of an interval, defined on the iteration \( 2m \):

\[
\left[ \frac{f_{2m+2}}{f_{2m}}; \frac{f_{2m+3}}{f_{2m+2}} \right] \subset \left[ \frac{f_{2m}}{f_{2m-1}}; \frac{f_{2m+1}}{f_{2m}} \right].
\]

So as we can see, our interval gets shorter with each iteration, and our algorithm terminates whenever \( A/B \) falls out of the interval.

But we can go even further: recall that \( \lim_{n \to \infty} \frac{f_{n+1}}{f_n} = \varphi \), where \( \varphi \), known as the golden ratio, is equal to \((1+\sqrt{5})/2\). Since this sequence converges, any subsequence of it must converge as well, which implies that \{\(f_{2m}/f_{2m-1}\)\}_{m=1}^{\infty} and \{\(f_{2m+1}/f_{2m}\)\}_{m=1}^{\infty} both tend to \( \varphi \). But the first sequence is monotonously increasing, while the second one is monotonously decreasing. It means that each interval of the form \([f_{2m}/f_{2m-1} ; f_{2m+1}/f_{2m}]\) must contain \( \varphi \). As a consequence, we can see that the closer \( A/B \) to \( \varphi \), the more iterations our algorithm has to perform.
There are two separate cases arise at this point: when \( A/B \) is less than, or greater than \( \varphi \). If \( A/B < \varphi \), then \( A/B < \varphi < f_{2m+1}/f_{2m} \) is true for any \( m \), which means that the algorithm cannot terminate at the even iteration. Analogously, if \( A/B > \varphi \), then \( f_{2m}/f_{2m-1} < \varphi < A/B \), and the algorithm cannot terminate at the odd iteration.

Note that we expect out algorithm to terminate when \( A_k \geq B_k \) for some \( k \). Assume that \( A/B > \varphi \), which means that \( k = 2m \) for some positive integer \( m \). Recall the exact formula for the \( n \)-th element of the Fibonacci sequence:

\[
 f_n = \frac{\varphi^n - (1 - \varphi)^n}{\sqrt{5}}.
\]

Then for \( n \), satisfying \( A/B \geq f_{2m+1}/f_{2m} \), we have

\[
 \frac{A}{B} \geq \frac{\varphi^{2m+1} - (1 - \varphi)^{2m+1}}{\varphi^{2m} - (1 - \varphi)^{2m}},
\]

If we now take the logarithm on both parts of the inequality above, we shall get

\[
 (2m+1) \ln \varphi + \ln \left(1 + \left(\frac{\varphi - 1}{\varphi}\right)^{2m+1}\right) - 2m \ln \varphi - \ln \left(1 - \left(\frac{\varphi - 1}{\varphi}\right)^{2m}\right) \leq \ln \frac{A}{B};
\]

Since \( \ln(1 + x) \approx x \) for \( x \ll 1 \), and \( ((\varphi - 1)/\varphi)^{2m} \) tends to zero as \( m \) goes to infinity, then for big values of \( m \) the following inequality holds:

\[
 \left(\frac{\varphi - 1}{\varphi}\right)^{2m+1} + \left(\frac{\varphi - 1}{\varphi}\right)^{2m} \leq \ln \frac{A}{B\varphi},
\]

which, in turn, results in

\[
 \left(\frac{\varphi - 1}{\varphi}\right)^{2m} \leq \frac{\varphi}{2\varphi - 1} \ln \frac{A}{B\varphi}.
\]

If we now take the logarithm on both sides of the inequality above, we shall obtain

\[
 k = 2m \geq \frac{\ln \frac{2\varphi - 1}{\varphi \ln(A/(B\varphi))}}{\ln \frac{\varphi}{\varphi - 1}}.
\]

Let

\[
 a = \left(\ln \frac{\varphi}{\varphi - 1}\right)^{-1} \approx 1.039, \quad b = \frac{\ln \frac{2\varphi - 1}{\varphi \ln(A/(B\varphi))}}{\ln \frac{\varphi}{\varphi - 1}} \approx 0.336.
\]
Then

\[ k \geq -a \ln \ln \frac{A}{B \varphi} + b, \]

which means that for any even \( k \), which satisfies the inequality above, the relation \( A/B \geq f_{k+1}/f_k \) holds. In other words, the closest even integer greater than \( -a \ln \ln A/(B \varphi) + b \) will be the least upper bound for \( k \), which allows us to conclude that \( k(A, B) \in O \left( \log \log \left| \log \frac{A}{B \varphi} \right| \right) \) as \( A/B \to \varphi \). Here we used the module sign because in case if \( A/B < \varphi \), the value of \( \ln \ln \frac{A}{B \varphi} \) is negative. We also expect the value \( \ln \left| \ln \frac{A}{B \varphi} \right| \) to be negative.

Now, let’s see how bad our algorithm will perform, if we will make \( A/B \) as close to \( \varphi \) as possible. If \( A/B > \varphi \), this happens when \( B = \lfloor A/\varphi \rfloor \). In this case,

\[ \ln \ln \frac{A/\varphi}{\lfloor A/\varphi \rfloor} = \ln \ln \left( 1 + \frac{\{A/\varphi\}}{\lfloor A/\varphi \rfloor} \right) \approx \ln \frac{\{A/\varphi\}}{\lfloor A/\varphi \rfloor} = -\ln \frac{\lfloor A/\varphi \rfloor}{\{A/\varphi\}}. \]

We conclude that in this case

\[ k \geq a \ln \frac{\lfloor A/\varphi \rfloor}{\{A/\varphi\}} + b, \]

and therefore \( k(A) \in O \left( \log \frac{A}{\{A/\varphi\}} \right) \) as \( A \) approaches infinity.

**Remark 4.19.** From the theorem [4.18], it follows that the algorithm [4.17] executes in \( O \left( \log \log \frac{N(v_1)}{N(v)}\varphi \right) \), assuming that \( N(v_1) \geq N(v) \). If \( N(v_1)/N(v) \) approximates \( \varphi \) in the best possible manner, i.e. \( N(v) = \lfloor N(v_1)/\varphi \rfloor \), then the algorithm works in \( O \left( \log \frac{N(v_1)}{\lfloor N(v_1)/\varphi \rfloor} \right) \).

## 5 Generalizing the result of Fermat

Recall the Fermat factorization method: suppose that we know a couple of different representations of a positive integer \( m \) as a sum of two squares:

\[ m = x_0^2 + y_0^2 = x_1^2 + y_1^2, \quad x_0 \geq y_0 \geq 0, \quad x_1 \geq y_1 \geq 0, \quad x_0 > x_1. \]

Then \( 1 < \gcd(x_0y_1 - y_0x_1, m) < m \) [CP05, Sec. 5.6.2]. Same formula holds if we know a couple of different representations of \( m \) as the sum of a square and a doubled square: \( m = x_0^2 + 2y_0^2 = x_1^2 + 2y_1^2 \).

The result of Fermat is a special case of the theory, introduced in this paper. Consider a quadratic order \( \mathcal{O}(\mu) \) with \( \mu = xi + yj + zk \), where
\[ N(\mu) = x_0^2 + y_0^2 + z_0^2 \] is composite. Then by the theorem \[3.4\], the pseudo generator of an ambiguous ideal \( \langle \rho \rangle_R \) has to divide \( (2/r)\mu \) from the right, and therefore \( N(\rho) \) has to divide \( (2/r)^2m \). Since \( \rho \) satisfies the relation \( (3.3) \) for some \( \mu' = x_1i + y_1j + z_1k \) of the same norm as \( \mu \), it is evident that for any three squares representation of an integer there exists another three squares representation, which allows us to factor \( (2/r)^2m \). The following couple of theorems demonstrate that for quaternions \( \mu = xi + yj \) and \( \mu = xi + yj + yk \) and an ambiguous ideal \( \langle \rho \rangle_R \), \( \mu' \) has to be of a certain form.

**Theorem 5.1.** Consider a quadratic order \( \mathcal{O}(\mu) \), where \( \mu = x_0i + y_0j + z_0k \), and exactly one of the coefficients \( x_0, y_0, z_0 \) is equal to zero. The equivalence class \( \langle \rho \rangle_R \) is ambiguous if and only if for the quaternion \( \mu' = \rho\rho^{-1} = x_1i + y_1j + z_1k \) exactly one of the coefficients \( x_1, y_1, z_1 \) is zero.

**Proof.** \( \Rightarrow \) Let \( \langle \rho \rangle_R \) be an ambiguous ideal, which belongs to the order \( \mathcal{O}(\mu) \), where \( \mu = x_0i + y_0j + m = N(\mu) = x_0^2 + y_0^2 \). Note that in here we have picked \( \mu \) so that \( z_0 = 0 \), but in general we can zero out any of the coefficients by replacing \( \mathcal{O}(\mu) \) with a suitable quadratic order of the form \( \mathcal{O}(\varepsilon\mu) \) for some unit \( \varepsilon \).

By the theorem \[3.4\], \( \rho \) has to divide \( (2/r)\mu = 2\mu \) from the right, i.e. \( 2\mu = \rho' \rho \) for some integral quaternion \( \rho' \). Then \( 2\mu' = 2(x_1i + y_1j + z_1k) = \rho(2\mu)\rho^{-1} = \rho\rho' \). Let us demonstrate that \( z_1 = 0 \).

First of all, notice that \( 2\mu i = -x_0 - y_0k \) is an element of the ring of Gaussian integers \( \mathbb{Z}[k] \). Since \( \mathbb{Z}[k] \) is a unique factorization domain \[\text{[Mol11, Chap. 1],}\] the quaternion \( 2\mu i \) of norm \( 2m = N(\rho')N(\rho) \) can be uniquely represented as the product of two integral quaternions \( r = p_0 + q_0k \) and \( r' = p_1 + q_1k \), which are also in \( \mathbb{Z}[k] \), and \( N(r) = N(\rho') \), \( N(r') = N(\rho') \):

\[ 2\mu i = \rho' \rho i = r'r. \]

Since \( 2\mu = r'(-ri) \), put

\[ \rho = -ri = -p_0i + q_0j, \quad \rho' = r' = p_1 + q_1k. \]

Then \( \mu' = \rho\rho' \) has \( z_1 = 0 \).

\( \Leftarrow \) Let \( \mu = x_0i + y_0j, \mu' = x_1i + y_1j \), and \( N(\mu) = N(\mu') \). Once again, we have picked our \( \mu \) and \( \mu' \) so that \( z_0 = z_1 = 0 \), but this is not necessary, as we can always find suitable quaternions \( \varepsilon_0\mu\varepsilon_0^{-1} \) or \( \varepsilon_1\mu'\varepsilon_1^{-1} \) for some units \( \varepsilon_0, \varepsilon_1 \), which would make \( z_0 = z_1 = 0 \).

\[2\text{The necessary condition was proved by Mikhail N. Kubensky.}\]
By the theorem 4.12, an integral quaternion \( \rho' = (\mu + \mu')/d \), where \( d \) is the greatest integral divisor of \( \mu + \mu' \), is a right pseudo generator of a primitive ideal \([N(\rho), b + \mu]\) \( \subseteq \mathcal{O}(\mu) \) for some integer \( b \). Since \( \rho' \) is a right pseudo generator of an ideal, then \( \rho = i\rho' \) is a pseudo generator of the same ideal:

\[
\rho = i\rho' = \frac{-(x_0 + x_1) + (y_0 + y_1)k}{d}.
\]

Obviously, we have \((\mu, \rho) = 0\), which means that the relation (4.3) takes the form

\[
\Re(\rho)b = t\Re(\xi)\frac{N(\rho)}{t},
\]

where \( t \) is defined as in step 2 of the algorithm 4.6. Since \( \gcd(\Re(\rho), N(\rho)/t) = 1 \) (otherwise \( \rho \) would not be primitive), we have \( b = kN(\rho)/t \) for an integer \( k = t\Re(\xi)/\Re(\rho) \). It implies that the \( \mathbb{Z} \)-basis of \( \langle \rho \rangle_R \) takes the form \([N(\rho), kN(\rho)/t + \mu]\). In turn, this ideal is equivalent to \([N(\rho), \frac{t-1}{t}N(\rho) + \mu]\), which is ambiguous.

**Theorem 5.2.** Consider a quadratic order \( \mathcal{O}(\mu) \), where \( \mu = x_0i + y_0j + z_0k \), and exactly two of the coefficients \( x_0, y_0, z_0 \) are equal to each other in their absolute value. The equivalence class \([\langle \rho \rangle_R]\) is ambiguous if and only if for the quaternion \( \mu' = \rho\mu\rho^{-1} = x_1i + y_1j + z_1k \) exactly two of the coefficients \( x_1, y_1, z_1 \) are equal to each other in their absolute value.

**Proof.** \((\Rightarrow)\) If we have \( \mu = x_0i + y_0(j + k) \), then \( \mu i = -x_0 + y_0(j - k) \) belongs to the ring \( \mathbb{Z}[j - k] \), which is isomorphic to \( \mathbb{Z}[\sqrt{-2}] \). Since \( \mathbb{Z}[\sqrt{-2}] \) is a unique factorization domain, the same reasoning as in the proof of the theorem 5.1 can be applied to demonstrate the desirable result.

\((\Leftarrow)\) The sufficient condition can be proved using almost the same reasoning as in the theorem 5.1. The only contrast between two proves would be in the difference of initial quaternions \( \mu \) and \( \mu' \).

**6 Some relations, which characterize an ideal**

In this section, we present three formulas, which characterize a primitive ideal \( \langle \rho \rangle_R = [a, b + \omega] \) in the quadratic order \( \mathcal{O}(\mu) \). The first formula that we are about to introduce has the same form as (4.3), except that \( \rho \) gets replaced by \( \xi \), which satisfies \( b + \omega = \xi\rho \). To prove it, we first need to demonstrate the following proposition.
Proposition 6.1. Consider $\langle \rho \rangle_R = [a, b + \omega]$ in the quadratic order $O(\mu)$. Then $(\omega, \xi) = (\omega', \xi)$, where $\omega' = \rho \omega^{-1}$, and $\xi$ satisfies the relation $b + \omega = \xi \rho$.

Proof. Consider two equalities: $\xi(b + \omega) = \xi^2 \rho$ and $(b + \omega')\xi = \rho \xi^2$. Since every quaternion satisfies the relation (3.1), we have

$$\xi(b + \omega) = \xi^2 \rho = (2\Re(\xi)\xi - N(\xi)) \rho = 2\Re(\xi)(b + \omega) - N(\xi)\rho;$$

$$\xi(b + \omega') = \rho \xi^2 = \rho (2\Re(\xi)\xi - N(\xi)) = 2\Re(\xi)(b + \omega') - N(\xi)\rho.$$

Let us subtract the second equation from the first one:

$$\xi(b + \omega) - (b + \omega')\xi = 2\Re(\xi)(\omega - \omega');$$

$$\xi\omega - \omega'\xi = 2\Re(\xi)(\omega - \omega').$$

Consider the quaternion on the left side of the equation:

$$\xi\omega - \omega'\xi = \left(\Re(\xi) + \bar{\xi}\right) (\Re(\omega) + \bar{\omega}) - (\Re(\omega') + \bar{\omega'}) \left(\Re(\xi) + \bar{\xi}\right) =$$

$$= \Re(\xi)\Re(\omega) - \Re(\xi)\Re(\omega') + \left(\bar{\xi}\omega - \bar{\omega}\xi\right) + \Re(\xi)\bar{\omega} + \Re(\omega)\bar{\xi} - \Re(\xi)\bar{\omega'} - \Re(\omega')\bar{\xi}.$$

Since $\Re(\omega) = \Re(\omega')$,

$$\xi\omega - \omega'\xi = \left(\bar{\xi}\omega - \bar{\omega}\xi\right) + \Re(\xi)(\bar{\omega} - \bar{\omega'}) = 2\Re(\xi)(\omega - \omega').$$

Applying the relation (4.1), we obtain

$$-(\omega, \xi) + [\xi, \omega] + (\omega', \xi) - [\omega', \xi] + \Re(\xi) \left(\bar{\omega} - \bar{\omega'}\right) = 2\Re(\xi) (\omega - \omega').$$

Since the quaternion on the right has a zero real part, if we now take the real part on both sides of the equation above, we get $(\omega, \xi) = (\omega', \xi).$  \hfill $\Box$
Proposition 6.2. If a primitive ideal \([a, b + \omega] = \langle \rho \rangle_R\) belongs to the quadratic order \(O(\mu)\), then

\[
(6.1) \quad (\omega, \xi) + \Re(\xi) \left( b + \frac{r - 1}{r} \right) = \Re(\rho)N(\xi).
\]

where \(\xi\) is an integral quaternion, which satisfies the relation \(b + \omega = \xi\rho\), and an integer \(r\) is defined as in (3.2).

Proof. If we use the fact from proposition 6.1 that \((\omega, \xi) = (\omega, \xi')\), the relation (6.1) can be shown in the same manner as in the proof of the proposition 4.5.

Next two relations follow from the fact that an integral quaternion \(\omega + \omega'\) will always be a root of the the equation \(\rho\omega = \omega'\rho\). By the proposition 4.4, \((\omega + \omega', \omega) = (\omega + \omega', \omega')\). It follows that

\[
\left(\frac{\omega + \omega'}{2}, \omega\right) = \left(\frac{\omega + \omega'}{2}, \frac{\omega + \omega'}{2}\right) = \frac{m + (\mu, \mu')}{r^2},
\]

since \((\omega, \omega) = (\omega', \omega') = m/r^2\), where \(m = N(\mu) = N(\mu')\). If we now apply the 2nd relation from the system (4.4), we shall obtain

\[
\left(\frac{\omega + \omega'}{2}, \frac{\omega + \omega'}{2}\right) = \left(\Re(\xi)\bar{\rho} + \Re(\rho)\bar{\xi} + \frac{r - 1}{r}, \Re(\xi)\bar{\rho} + \Re(\rho)\bar{\xi} + \frac{r - 1}{r}\right) =
\]

\[
= \Re(\rho)^2(\xi, \xi) + 2\Re(\rho)\Re(\xi)(\rho, \xi) + \Re(\xi)^2(\rho, \rho);
\]

\[
\left(\frac{\omega + \omega'}{2}, \omega\right) = \left(\Re(\xi)\bar{\rho} + \Re(\rho)\bar{\xi} + \frac{r - 1}{r}, \omega\right) =
\]

\[
= \Re(\xi)(\omega, \rho) + \Re(\rho)(\omega, \xi) = \frac{\Re(\xi)(\mu, \rho) + \Re(\rho)(\mu, \xi)}{r}.
\]

In the end, we obtain the following couple of relations:

\[
(6.2) \quad \frac{m + (\mu, \mu')}{r} = \Re(\xi)(\mu, \rho) + \Re(\rho)(\mu, \xi);
\]

\[
(6.3) \quad \frac{m + (\mu, \mu')}{r^2} = \Re(\rho)^2(\xi, \xi) + 2\Re(\rho)\Re(\xi)(\rho, \xi) + \Re(\xi)^2(\rho, \rho).
\]
7 Number of ambiguous classes, characterized by the equation $\rho \mu = -\mu \rho$

From the theorem 4.12 we know that each ideal gets generated by a couple of quadratic orders. Among these ideals, some of them get generated by orders $\mathcal{O}(\mu)$ and $\mathcal{O}(-\mu)$. In our research, we were interested in the following question: how many nontrivial ambiguous ideals get generated by such quadratic orders? To answer it, we have written a program, which counts up to some bound $N$ how many integers, which satisfy certain parameters mentioned below, have at least one ambiguous ideal of that form.

First of all, we have to emphasize that it is not always the case that $\mathcal{O}(\mu)$ and $\mathcal{O}(-\mu)$ are not equivalent. Normally, if $m = x^2 + y^2 + z^2$ and $x, y, z$ are all distinct and non-zero, out of a single three squares representation we can produce 48 different, including the original one. These representations can be obtained by switching signs and by permuting $x, y, z$. On the other hand, if $\mu = xi + yj + zk$, there exist exactly 12 equivalent quadratic orders of the form $\mathcal{O}(\epsilon \mu \bar{\epsilon})$. Now it is not hard to observe that if $x, y, z$ are different and non-zero, quaternions $\mu, -\mu, \tilde{\mu}$ and $-\tilde{\mu}$, where $\tilde{\mu} = xi + zj + yk$, will form quadratic orders, which are not equivalent to each other.

There are two special cases arise at this point: if $\mu = xi + yj + zk$ and $y = z$, then $\tilde{\mu} = \mu$, i.e. quadratic orders, generated by these quaternions, are equivalent. Analogous observation can be made when $x = z$ or $x = y$. If $\mu = xi + yj + zk$ and $z = 0$, then $-\mu = k\mu \bar{k}$, which means that $\mathcal{O}(\mu)$ and $\mathcal{O}(-\mu)$ are equivalent to each other. Once again, analogous observation can be made when $x = 0$ or $y = 0$.

As a result, we have decided to avoid two squares representations, for they will always generate trivial ambiguous ideals. We can also argue that the case $\mu = xi + yj + zk$ when $y = z$ will also produce a trivial result. Recall the theorem 4.15. In its proof, we have demonstrated how to compute the $\mathbb{Z}$-module $[v, v_1]$, which fully characterizes the set of solutions to the equation $\rho \mu = -\mu \rho$. If we would follow the procedure described in that proof, we could notice that $v = j - k$. Because $\mathcal{O}(\mu)$ and $\mathcal{O}(-\mu)$ are not equivalent, the norm $N(v) = 2$ is the smallest, which means that $\langle v \rangle_R$ is reduced. When $m \equiv 3 \pmod{8}$, from the theorem 4.12 we know that such an ideal does not belong to $\mathcal{O}(\mu)$. In the opposite case, from the theorem 3.4 we know that $N(v) = 2$ has to divide $(2/r^2)m = 4m$, which obviously corresponds to the trivial case. This is why we ignore those $\mu = xi + yj + zk$ with $y = z$, as well as the cases when $x = y$ or $x = z$, which produce the trivial result for
the same reason.

The table below demonstrates our computational data. In our experiment, we were considering only those integers, which are a) squarefree; b) not prime; and c) not congruent to 7 mod 8 (since these integers cannot be represented as a sum of three squares). Let us denote the set of those integers as $\Sigma$. Among the elements of $\Sigma$, our algorithm was looking for those $m$, which have at least one quaternion $\mu = xi + yj + zk$ with the norm $m = N(\mu)$, s.t. quadratic orders $\mathcal{O}(\mu)$ and $\mathcal{O}(-\mu)$ generate a non-trivial ambiguous ideal. We denote this set as $A$. The 4th column demonstrates what is the percentage of elements of $A$ in respect to the number of elements of $\Sigma$. The 5th column shows an integer less than $N$, which has the maximal number $M$ of non-trivial ambiguous ideals, generated by $\rho\mu = -\mu\rho$. The number $M$ is indicated in brackets. Finally, the 6th column gives an example of an element $m = x^2 + y^2 + z^2$ in $A$ and a three squares representation $(x,y,z)$, which generates an ambiguous ideal, while the 7th column gives an example of an integer, which is in $\Sigma \setminus A$.

| $N$  | # $\Sigma$ | # $A$ | %   | Max #     | E.g. $A$       | E.g. $\Sigma \setminus A$ |
|------|------------|------|-----|----------|----------------|---------------------------|
| 10^4 | 379        | 151  | 39.84 | 645 (4)  | 21 (4,2,1)     | 6                         |
| 10^4 | 44145      | 1853 | 44.70 | 2310 (8) | 1001 (26,15,10)| 1002                      |
| 10^5 | 43464      | 20584| 47.36 | 90321 (32)| 10001 (98,19,6)| 10003                     |
| 10^5 | 447767     | 220308| 49.20| 899745 (64)| 1000002 (281,121,80)| 100001                   |
| 10^5 | 4567729    | 2302087| 50.40| 899745 (64)| 10000001 (770,630,101)| 10000006                 |

Table 2

There are two interesting tendencies that we can notice in this table. First of all, the overall percentage of numbers which have ambiguous ideals generated by $\rho\mu = -\mu\rho$ is growing. Second, each integer less than $N$, which has a maximal number $M$ of such an ambiguous classes, has $M$ equal to some power of 2. We can look closer at this sequence, and ask: is there a relation between the number of these ambiguous classes, and the ideal class group? The following table demonstrates that such a correlation seem to exist:

| $N$ | $M$ | $\Delta$ | $h_\Delta$ | $Cl_\Delta$ |
|-----|-----|----------|------------|-------------|
| 21  | 1   | -84      | 4          | 2 2         |
| 105 | 2   | -420     | 8          | 2 2 2       |
| 645 | 4   | -2580    | 16         | 4 2 2       |
| 2310| 8   | -9240    | 32         | 4 2 2 2     |
| 10605| 16 | -42420    | 64         | 4 4 2 2     |
| 90321| 32 | -361284  | 256        | 8 4 2 2 2   |
| 899745| 64 | -3598980 | 512        | 8 4 2 2 2 2 |

Table 3
Here $\Delta$ denotes the discriminant of a maximal quadratic order of an imaginary number field $\mathbb{Q}(\sqrt{-N})$, $h_\Delta$ is the class number, and $Cl_\Delta$ denotes the ideal class group. Following the definition [JW09, Sec. 7.1], we write the structure of each ideal class group as a direct product of cyclic subgroups, i.e.

$$Cl_\Delta \cong C(m_1) \times \ldots \times C(m_s),$$

where the positive integers $m_1, \ldots, m_s$ (which are presented in the 5th column) satisfy $m_1 \geq 1$, $m_{j+1} | m_j$ for $1 \leq j < s$, and $C(x)$ denotes the cyclic group of order $x$. As we can notice, for each $N$, the corresponding value of $h_\Delta$ is a power of 2, and the class group is non-cyclic.

8 A new approach to find a divisor of a class number

Fix the squarefree integer $m \not\equiv 7 \pmod{8}$, and consider a maximal quadratic order $O$ with discriminant $\Delta$ of an imaginary number field $\mathbb{Q}(\sqrt{-m})$. If the class number $h_\Delta = ef$ for some positive integers $e, f$, there exists a subgroup $A$ of the ideal class group $Cl_\Delta$, which consists of $f$ equivalence classes with reduced ideals $a_1, a_2, \ldots, a_f$ as their representatives. If we now generate an integral quaternion $\mu_1$ s.t. $\mu_1^2 = -m$ and replace $\sqrt{-m}$ in the $\mathbb{Z}$-basis of each ideal $a_i$ (where $1 \leq i \leq f$) with $\mu_1$, then we will “move” the subgroup $A$ from $O$ to $O(\mu_1)$. By the theorem 4.12, each ideal $a_i$ in $O(\mu_1)$ generates some quadratic order $O(\mu_i)$ by means of relation (3.3). Moreover, by the theorem 4.14, we know that all $\mu_1, \ldots, \mu_f$ are distinct, in a sense that no two integral quaternions from this set generate equivalent quadratic orders. Hence, there exists a bijective correspondence between $a_1, \ldots, a_f$ and $f$ distinct equivalence classes of quadratic orders with $O(\mu_1), \ldots, O(\mu_f)$ taken as their representatives (assuming that initially all ideals belong to $O(\mu_1)$) [Ven4, §18].

Now, pick an ideal $a \in A$ of order $f > 1$, i.e. $f$ is the smallest positive integer s.t. $[a]^f = 1$ holds.\[^3\] Then $a$ in $O(\mu)$ generates a new quadratic order, $O(\mu')$. Replacing $\mu$ in the $\mathbb{Z}$-basis of $a$ with $\mu'$, we will “move” $a$ to $O(\mu')$. Once again, $a$ in $O(\mu')$ generates a new quadratic order $O(\mu'')$. If we now proceed in this fashion, at some point our $a$ will return to $O(\mu)$, where $[a]$ denotes the equivalence class of $a$, and 1 denotes the unit in $Cl_\Delta$, which is simply $[O]$.\[^3\]
generating a cycle of length $f$ [Ven4, §19]. This cycle will run through all of the $O(\mu_1), \ldots, O(\mu_f)$, which were mentioned in the previous paragraph.

Consider a problem of finding the length $f$ of a cycle, which is equivalent to the problem of finding the order of $a$. Observe that for any quaternion $\mu_i$ for $1 \leq i \leq f$, a quadratic order $O(\mu_i)$ is equivalent to some quadratic order $O(\mu'_i)$, where $\mu'_i = \varepsilon \mu_i \Xi$ for some unit $\varepsilon$ has either all non-negative, or all non-positive coefficients. We shall call $O(\mu)$ positive if the first case holds, and negative if the second case holds.\footnote{Note that for the quaternion $\mu = xi + yj + zk$, where exactly one of the coefficients $x, y, z$ is equal to zero, the order $O(\mu)$ is both positive and negative.}

**Definition 8.1.** Consider an ideal $a$ in $O(\mu_1)$, which generates a cycle $O(\mu_1), \ldots, O(\mu_f)$. Let $a$ satisfy the separation property if each $O(\mu_i)$ is positive (negative) when $1 \leq i \leq \lfloor f/2 \rfloor$, and negative (positive) when $\lfloor f/2 \rfloor < i \leq f$. Then we call $a$ separated in $O(\mu_1)$.

It is not hard to demonstrate that if we know an ideal, which satisfies the separation property in some $O(\mu_1)$, then we can find the length $f$ of its cycle in polynomial time. The idea is to find borders between positive and negative quadratic orders. As you can notice, there exist exactly two of them: between $O(\mu_{\lfloor f/2 \rfloor})$ and $O(\mu_{\lfloor f/2 \rfloor + 1})$, and between $O(\mu_f)$ and $O(\mu_1)$.

Suppose that $a$ is separated in a positive order $O(\mu_1)$. Then, using the right pseudo generator of $a$, we compute $O(\mu_2)$ generated by $a$ in $O(\mu_1)$, $O(\mu_4)$ generated by $a^2$ in $O(\mu_2)$, and so on, until for some $n$ we obtain a negative order $O(\mu_n)$ generated by $a^{n/2}$ in $O(\mu_{n/2})$. We conclude that $n/2 < d \leq n$. Now we shall move backwards, and try to tighten this interval. We “move” our ideal $a$ to $O(\mu_n)$, and now consider its left pseudo generator, which will direct us towards $O(\mu_1)$. Once again, we compute $O(\mu_{n-1})$ generated by $a$ in $O(\mu_n)$, $O(\mu_{n-3})$ generated by $a^2$ in $O(\mu_{n-1})$, and so on, until for some $m$ we get a positive order $O(\mu_{n-m})$ generated by $a^{(m+1)/2}$ in $O(\mu_{n+1-(m+1)/2})$. We conclude that $n-m < d \leq n+1-(m+1)/2$. If we proceed in this fashion, then on each iteration an interval which $d$ belongs to will get smaller and smaller, until it reaches the size where we can check the sign of each order in the interval.

On the picture below, we introduce an example for $f = 12$. Here, our distance to the border was found in three steps, which are demonstrated by arrows. Initially, the only thing we know about $d$ is that $d \geq 1$. After three jumps to the left on the first step, we conclude that $3 < d \leq 7$. On the second step, after two jumps to the right, we conclude that $4 < d \leq 6$. Finally, on the third step we find $4 < d \leq 5$, which means that $d = 5$.\footnote{Note that for the quaternion $\mu = xi + yj + zk$, where exactly one of the coefficients $x, y, z$ is equal to zero, the order $O(\mu)$ is both positive and negative.}
Note that above we have found a distance from \( \mu_1 \) to only one of the borders. So what about the other border? We could find it analogously if from the very beginning we would start to compute quaternions, generated by \( a, a^2 \), etc. not with the right pseudo generator of \( a \), but with the left pseudo generator.

There is one problem that may occur during our computations: for the reason that on each iteration we double the size of our step, it may happen that the step becomes bigger than the length of a cycle. If this happens, our procedure may result in wrong computations, or even in an infinite loop. Fortunately, there exists an upper bound on the size of a class number of an imaginary number field [Coh93, Sec. 5.10.1]. In particular, we know that

\[
h_\Delta < \frac{1}{\pi} \sqrt{|\Delta|} \ln |\Delta| \text{ if } \Delta < -4.
\]

As soon as our step becomes greater than the value above, we can simply pick a different \( \mathcal{O}(\mu_1) \), for example by replacing it with its right (or left) neighbour.

Let us give an example of an ideal, which satisfies the property described above. Let \( a = [23, -2 + \sqrt{-893}] \) be an ideal in \( \mathcal{O} \) of \( \mathbb{Q}(\sqrt{-893}) \). If we now fix \( \mu_1 = 29i + 4j + 6k \) (note that \( 893 = 29^2 + 4^2 + 6^2 \)), and then “move” \( a \) to \( \mathcal{O}(\mu_1) \), i.e. \( a = [23, -2 + \mu_1] \), then \( a \) would generate the following cycle:
Another separated ideal is $[18, 1 + \mu_1]$, where $\mu_1 = 42i + 14j + k$ (1961 = $42^2 + 14^2 + 1^2$). It generates the following cycle:

\[
\begin{align*}
\mu_8 &= -30i - 10j - 31k & \mu_1 &= 42i + 14j + k \\
\mu_7 &= -26i - 14j - 33k & \mu_2 &= 18i + 26j + 31k \\
\mu_6 &= -30i - 10j - 31k & \mu_3 &= 26i + 18j + 31k \\
\mu_5 &= -10i - 30j - 31k & \mu_4 &= 14i + 42j + k
\end{align*}
\]

If we consider the same quadratic order $O(\mu_1)$, and pick an ideal $b = [5, 2 + \mu_1]$, we can notice that $[b] = [\mathfrak{a}]^3$ does not satisfy the separation property:

\[
\begin{align*}
\mu_8 &= -26i - 14j - 33k & \mu_1 &= 42i + 14j + k \\
\mu_7 &= 26i + 18j + 31k & \mu_2 &= 14i + 42j + k \\
\mu_6 &= -30i - 10j - 31k & \mu_3 &= -14i - 26j - 33k \\
\mu_5 &= -10i - 30j - 31k & \mu_4 &= 18i + 26j + 31k
\end{align*}
\]

Many questions arise at this point. First of all, do separated ideals exist in $O(\mu)$ for any squarefree $N(\mu)$? Second, can we say anything meaningful about their quantity? Third, how hard is it to find a separated ideal? Probably, these ideals satisfy some other interesting properties that need to be explored. We leave all these questions open, hoping to dedicate more time to the study of separated ideals in the near future.

\section{Conclusion}

In this paper, we have introduced four algorithms, which allow us to manipulate ideals in the ring of integral quaternions using only their pseudo generators, without ever mentioning their $\mathbb{Z}$-basis. In the future, we would like to extend our algorithms to the generalized quaternion algebras, possibly defined over a different field. We have also demonstrated the theorem, which shows that the Fermat’s number factoring technique, which uses two different representations of an integer as a sum of two squares, is a special case of the theory, presented in this paper. In general, if we have a single three squares representation for a composite integer $m = x_0^2 + y_0^2 + z_0^2$, there
must exist another three squares representation \( m = x_1^2 + y_1^2 + z_1^2 \), which can help us to factor \( m \). But the more interesting fact is that this is not always necessary, as sometimes a single three squares representation can produce a non-trivial factor of \( m \). This phenomenon was studied in the section 7.

There are multiple questions left open at this point. What is the necessary, or, even better, sufficient condition for an integer \( N \) to contain an ambiguous ideal, generated by the equation \( \rho \mu = -\mu \rho \)? Why each integer \( N \), with a number \( M \) of those ambiguous classes greater than any integer less than \( N \), has \( M \) being a power of 2? Why for each \( N \) that satisfy this property, the class number \( h_\Delta \) also turns out to be a power of 2? Finally, how can we find separated ideals within a certain ideal class group? We intend to explore all these questions in more depth in the future.

Acknowledgements

This research was done for the author’s Master’s thesis, which was submitted to the faculty of higher mathematics of the St. Petersburg National Research University of Information Technologies, Mechanics and Optics in June, 2013. The author would like to thank his supervisor, Mikhail Nikolayevich Kubensky, for his wise guidance. The author is also grateful to Dr. Matthew Greenberg (University of Calgary, Canada) and Robert Bateman (L’Institut Polytechnique des Sciences Avancées, France) for their thoughtful comments and the paper revision.

References

[BS09] J. Bobber, W. Stein, Quaternion Algebras, Sage reference manual, Available at http://www.sagemath.org/doc/reference/quat_algebras/sage/algebras/quatalg/quaternion_algebra.html, 2009.

[Buc07] J. Buchmann, U. Vollmer, Binary Quadratic Forms. An Algorithmic Approach, Springer-Verlag Berlin Heidelberg, 2007.

[CL83] H. Cohen, H. W. Lenstra, Jr., Heuristics on Class Groups of Number Fields, Number Theory, Lecture Notes in Mathematics 1068 (1983), Springer-Verlag, New York, 33–62.
[CL84] H. Cohen, H. W. Lenstra, Jr., *Heuristics on Class Groups*, Number Theory, Noordwijkerhout, Lectures Notes in Mathematics 1052 (1983), Springer-Verlag, New York, 26–36.

[Coh93] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, 1993.

[CP05] R. Crandall, C. Pomerance, *Prime Numbers. A Computational Perspective*, Springer Science + Business Media, Inc., 2nd edition, 2005.

[Gro85] E. Grosswald, *Representation of Integers as Sums of Squares*, Springer-Verlag, New York, 1985.

[Hur19] A. Hurwitz, *Vorlesungen Über die Zahlentheorie der Quaternionen*, Verlag von Julius Springer, Berlin, 1919.

[JW09] M. J. Jacobson, Jr., H. C. Williams, *Solving the Pell Equation*, Springer Science + Business Media, LLC, 2009.

[KM90] M. N. Kubensky, A. V. Malyshev, *Theory of Turns in Simple Central Algebras*, Acta Arithmetica 53 (1990), no. 5, 477–498 (in Russian).

[Koh05] D. Kohel, *Quaternion Algebras*, Sage reference manual, Available on the author’s website: [http://echidna.maths.usyd.edu.au/kohel/alg/doc/AlgQuat.pdf](http://echidna.maths.usyd.edu.au/kohel/alg/doc/AlgQuat.pdf) 2005.

[KV10] M. Kirschmer, J. Voight, *Algorithmic Enumeration of Ideal Classes for Quaternion Orders*, SIAM Journal on Computing 39 (2010), no. 5, 1714–1747.

[Mol11] R. A. Mollin, *Algebraic Number Theory*, Taylor and Francis Group, LLC, 2011.

[RS86] M. O. Rabin, J. O. Shallit, *Randomized Algorithms in Number Theory*, Communications on Pure and Applied Mathematics 39 (1986), S239–S256.

[Sch96] R. Scheidler, *Compact Representation in Real Quadratic Congruence Function Fields*, In Proc. Second Algorithmic Number Theory Symposium ANTS-II, Lecture Notes in Computer Science 1122 (1996), Springer, Berlin, 323–336.
[Ven1]  B. A. Venkov, *On the Arithmetic of Quaternions. First letter*, Izvestiya Rossiyskoy Akademii Nauk (1922), 205–220 (in Russian).

[Ven2]  B. A. Venkov, *On the Arithmetic of Quaternions. Second letter*, Izvestiya Rossiyskoy Akademii Nauk (1922), 221–246 (in Russian).

[Ven3]  B. A. Venkov, *On the Arithmetic of Quaternions. Third letter*, Izvestiya Akademii Nauk SSSR (1929), 535–562 (in Russian).

[Ven4]  B. A. Venkov, *On the Arithmetic of Quaternions. Fourth letter*, Izvestiya Akademii Nauk SSSR (1929), 489–504 (in Russian).

[Vig80]  M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions*, Springer-Verlag, Berlin, 1980.

[Voi10]  J. Voight, *The Arithmetic of Quaternion Algebras*. Available on the author’s website: [http://www.math.dartmouth.edu/~jvoight/crmquat/book/quat-modforms-041310.pdf](http://www.math.dartmouth.edu/~jvoight/crmquat/book/quat-modforms-041310.pdf), 2010.