Impossibility results for Module LLL based on Euclidean Division

Joël Felderhoff

1 Introduction

The security of cryptographic protocols is based on various algorithmic assumptions, the one providing security of the most widely implemented protocols at the time of the is the Discrete Logarithm on elliptic curves (whose extensive description can be found in [Gal12]). Those problems are known to be solved in polynomial time by a quantum attacker via Shor's algorithm [Sho94], which motivates the study of quantum-resistant security assumptions. This line of research has seen a further increase of interest because of the call for proposals of quantum-resistant cryptosystems of the American National Institute of Standardisation of Technology in 2017 [CSD17].

The most promising assumptions come from problems over lattices, namely variants of the Learning With Error problems [Reg05]. These assumptions, aside from being allegedly quantum-secure, allow to create advanced cryptographic primitives such as homomorphic encryption [Gen09] or Attribute Based Encryption [GVW15]. Those security assumptions have been used for creating quantum-resistant protocols and some of them are to be standardized by the NIST [CSD20].

Due to the cipher size of the protocols based on standard LWE assumptions, structured lattices are used in practical implementations (e.g., for most of the lattice-based NIST candidates), see for example NTRU [HPS98] or Ring-LWE [Reg10]. The structured lattice assumptions are hoped to offer the same level of security as the unstructured ones, while providing smaller cipher sizes and acceleration for the underlying algorithms.

The non-equivalence between the security assumptions on structured lattices and unstructured ones motivates the specific cryptanalysis of the latter. In particular we will focus here on module-lattices, that are a class of structured lattices coming from number theory which are used by the lattice-based NIST finalists.

1.1 State of the art

Module lattices specific algorithms have been described by various authors: in [FP96], Fieker and Pohst described an enumeration algorithm for module lattice along with a version of the LLL algorithm which did not give guarantees about the size of the output (while being faster than the unstructured LLL described in [LLL82]). Over the last few years, improvements on the specific cryptanalysis of Module lattices have been achieved. Specific algorithms to solve the approximate shortest vector problem in the case of rank-1 module lattices (also called ideal lattices) were proposed [CDW17, PMHS19, BRL20].

For the case of rank-2 and greater rank module lattices, there have been several partial attempts. In [KL17], Kim and Lee proposed a module-LLL algorithm in the case of biquadratic fields. In [LPMSW19] and [MSD20] two versions of a module-LLL algorithm were described for modules of rank $n \geq 2$. In both articles, the rank-2 case is identified as the main step to overcome in order to build a full module-LLL algorithm working at all rank.

1.2 Contributions

Our first contribution is Proposition 8 which states the existence of a low algebraic norm vector in the module $\mathcal{O}_K\vec{u} + \mathcal{O}_K\vec{v}$ given that the gap between $N(\vec{u})$ and $N(\vec{v})$ is large enough. Here $\mathcal{O}_K$ is the ring of integers of a number field K, $\vec{u}$ and $\vec{v}$ are vectors over K^2 and $N(\vec{u})$ and $N(\vec{v})$ denote the algebraic norms of $\vec{u}$ and $\vec{v}$, which correspond to the volumes of the lattice that they span. The new result does not rely on heuristic assumptions and gives bounds on the algebraic norm. It is not directly comparable as [LPMSW19, Cor 4.8].

The main work of this paper is the study of the main step of LLL algorithm (the Gauss-Lagrange algorithm) in the case of number fields. In the classical LLL [LLL82], this algorithm uses as a central operation the rounding of real numbers, that is to say the ability to find an integer at distance at most $\frac{1}{2}$ to any real number in reasonable time. This ability is closely related to the existence of the Euclidean division algorithm for $\mathbb{Q}$, which has an equivalent in some number fields. A natural way to try to extend the LLL algorithm to module lattices is then to focus on the case of fields that have a Euclidean Division algorithm for the algebraic norm.

We proved in Section 4 that a textbook generalisation of the Gauss Lagrange algorithm for fields with Euclidean division can lead to arbitrary bad output for rank-2 modules. We also investigate in Section 5 a more powerful Euclidean division oracle (namely one that does not only output an integer at algebraic distance at most 1, but indeed the closest possible), and prove that such oracle is not a good candidate for building a Module Gauss-Lagrange algorithm either.

These results could seem contradictory with [KL17] in which the authors describe an Euclidean division based module-LLL algorithm for biquadratic fields. In Section 6 we make an analysis of those results and prove that our results and the one of Kim and Lee are not in contradiction since the notion of size considered here and the one considered in [KL17] differ.

2 Generalities

2.1 Lattices

We start by recalling the basic definitions of the objects used in this paper. Proofs of the results presented in this section can be found in [Coh96].

Def 1. *A lattice is a discrete subgroup $\mathcal{L}$ of $\mathbb{R}^n$. It is given by m linearly independant vectors $b_1, \ldots, b_m$ called its basis. Then $\mathcal{L} = \sum_{i=1}^{m} \mathbb{Z} \cdot b_i$.*

If $m = n$, $\mathcal{L}$ is said full-rank.

In the latter, we will only consider full rank lattices. A lattice can have several basis, therefore it is important to study its invariants. One of them is its volume.

Def 2. *Let $\mathcal{L}$ be a full-rank lattice given by a basis $b_1, \ldots, b_n$. Then its volume is the quantity $|\det([b_1, \ldots, b_n])|$. This quantity is homogeneous to a volume in dimension n ($[\mathrm{L}]^n$) and is invariant by changing of basis, so it depends only on $\mathcal{L}$. The volume of $\mathcal{L}$ is denoted vol$(\mathcal{L})$.*

Another invariant for a lattice $\mathcal{L}$ is its shortest vector's length.

Def 3. *For a lattice $\mathcal{L}$ and a norm $\|\cdot\|$, the quantity $\lambda_{1,\|\cdot\|}(\mathcal{L})$ is defined to be $\inf\{\|x\|, x \in \mathcal{L} \setminus \{0\}\}$.*

By discreteness of $\mathcal{L}$, this quantity is achieved.

In the latter, if not precised otherwise, we use $\|\cdot\| = \|\cdot\|_2$. Lattices and their shortest vectors pays an important role in modern cryptography as several problems related to them are computationally hard.

Def 4. *Let $\gamma(n)$ a function of n, the γ-Approx Shortest Vector problem ask, given an integer n and basis of a full-rank lattice $\mathcal{L}$ in $\mathbb{Z}^n$, to find a vector $x \in \mathcal{L}$ such that $\|x\| \leq \gamma(n)\lambda_1(\mathcal{L})$.*

This problem have been studied for a wide range of $\gamma(n)$, for some (e.g., $\gamma(n) = \text{poly}(n)$) it is known to be NP-Complete and for other (e.g., $\gamma(n) = 2^{O(n)}$) it can be solved in polytime by the LLL algorithm [LLL82].

The volume of the lattice gives an approximation of how short a vector can be in a lattice. This result is given by the Minkowski's theorem.

Theorem 1 (Minkowski). *Let $\mathcal{L}$ be a full rank lattice in $\mathbb{R}^n$. Then $\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot vol(\mathcal{L})^{1/n}$.*

In order to be more precise about this bound, one can define a constant called the Hermite constant to control precisely the gap between $\lambda_1(\mathcal{L})$ and $\mathrm{vol}(\mathcal{L})^{1/n}$.

Def 5. *The (normalized) Hermite constant δ_n is defined as follow:*

$$\delta_n = \inf_L \left\{ \frac{\lambda_1(L)}{\det(L)^{1/n}} \right\},$$

where the infimum is taken over all lattices of rank n and exists by Minkowski's theorem.

It is known that this constant is $\Theta(\sqrt{n})$ (see [CS88]).

2.2 Number theory definitions

In practice in many cryptographic schemes, **structured** lattices are used. Structured lattices are often taken from number-theoretics objects. We here recall some number-theoretics facts and definitions, more detailled studies and proofs can be found in [Coh96].

Let K be a number field of degree $d = r_1 + 2r_2$, $\mathcal{O}_K$be its ring of integers. The field K embbeds in $\mathbb{C}^d$ via its canonical embedding

$$\begin{array}{rccc} \sigma : & K & \longrightarrow & \mathbb{C}^d \\ & x & \longmapsto & \sigma_i(x) \end{array}$$

with $\sigma_i : K \to \mathbb{R}$ for $i = 1 \ldots r_1$, $\sigma_i : K \to \mathbb{C}$ for $i = r_1 + 1 \ldots d$ and $\sigma_{r_1+i} = \overline{\sigma_{r_1+r_2+i}}$.

The span of $\sigma(K)$ is not $\mathbb{C}^d$ since the last $2r_2$ coordinates of σ have relations. It spans the subspace $E = \left\{ y \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}, y_{r_1+i} = \overline{y_{r_1+r_2+i}} \right\}$.

The **algebraic norm** is defined as $N_{K/\mathbb{Q}}(x) = \prod_{i=1}^d \sigma_i(x) \in \mathbb{Q}$. As this norm grows when d grows, it is useful to also define the **normalized algebraic norm** : $\widetilde{N_{K/\mathbb{Q}}} = |N_{K/\mathbb{Q}}|^{1/d}$ which is homogeneous to a distance.

The **discriminant** of the field Δ_K is then the volume of the image of $\mathcal{O}_K$ by σ[1] as a $\mathbb{Z}$-lattice. It is a the measure of a d dimensional volume, we define the **normalized discriminant** by $\widetilde{\Delta}_K = \Delta_K^{1/d}$, which is homogeneous to a distance.

In order to work in a complete space, we define $K_\mathbb{R} = K \otimes \mathbb{R} \cong E$. The field K is dense in $K_\mathbb{R}$ and all continuous constructions (namely $\sigma, N_{K/\mathbb{Q}}, \widetilde{N_{K/\mathbb{Q}}}$) can be extended to $K_\mathbb{R}$.

The ring $K_\mathbb{R}$ is not a field, since it contains zero-divisor (any element which has a zero coefficient is a zero divisor) so a different notion of linear independance is needed.

Def 6. *A familly $b_1, \ldots, b_n$ in ${K_\mathbb{R}}^m$ is said to be $K_\mathbb{R}$-linearly independat if there exist no $\alpha_1, \ldots, \alpha_n \in K_\mathbb{R}$ not all equal to zero such that $\sum_{i=1}^n \alpha_i \cdot b_i = 0$.*[2]

The l_p norms of elements of $K_\mathbb{R}$ are defined as $\|x\|_p = \|\sigma(x)\|_p$. Usual inequalities applies for those norms.

Proposition 2. *If $x \in K_\mathbb{R}$, then $\widetilde{N_{K/\mathbb{Q}}}(x) \leq \|x\|_\infty$ and $\widetilde{N_{K/\mathbb{Q}}}(x) \leq \frac{1}{\sqrt{d}} \|x\|_2$.*

Proof. The first inequality comes from the fact that $N_{K/\mathbb{Q}}(x)$ is the product of all the coordinates of x, the second is the arithmetico-geometric inequality. □

From now on, when the context is clear we shall denote $N_{K/\mathbb{Q}}$ by N.

Proposition 3. *The quantities $\widetilde{N}$ and $\|\cdot\|_\infty$ are not equivalent. In fact, an element of $K_\mathbb{R}$ can have an arbitrarily large l_p norm with fixed algebraic norm if $r_1 + r_2 > 1$.*

Proof. As $r_1 + r_2 > 1$, by Dirichlet's unit theorem ${\mathcal{O}_K}^\times$ is an infinite discrete group, hence the l_p norms of their elements are unbounded, but for all $x \in {\mathcal{O}_K}^\times$, we have that $|\widetilde{N}(x)| = 1$. □

[1] in the litterature, such as in [LPMSW19], the discriminant is defined to be Δ_K^2. Our choice is made for the sake of homogeneity

[2] This definition is stronger than the fact that any b_i is not in the span of the others.

Proposition 4. *If $r_1+r_2 > 1$, the algebraic norm does not follow the triangular inequality: there exist $x, y \in K_{\mathbb{R}}$ such that $\frac{N(x+y)}{N(x)+N(y)}$ is arbitrarily large.*

Proof. In this paper, we will give our proofs in the case $K_{\mathbb{R}} \cong \mathbb{R}^2$. Our proofs can be extended to any field as long as $r_1 + r_2 > 1$.

Let $\varepsilon > 0$, and take $x = \begin{bmatrix} \varepsilon \\ 1/\varepsilon \end{bmatrix}$ and $y = \begin{bmatrix} 1/\varepsilon \\ \varepsilon \end{bmatrix}$.

Then $N(x) = N(y) = 1$, and the algebraic norm of the sum $N(x+y) = (\varepsilon + 1/\varepsilon)^2 \to_{\varepsilon\to 0} \infty$ can be as large as wanted. □

The above example shows exactly the kind of pathological cases that can occur with the algebraic norm: when the vectors are not balanced, the additive behavior of the algebraic norm becomes erratic.

We can define a notion of balanced elements of $K_{\mathbb{R}}$ in the following way.

Def 7. *Let $\gamma \geq 1$. An element $x \in K_{\mathbb{R}}$ is said γ-**balanced** if $\|x\|_\infty \leq \gamma \cdot \widetilde{N}(x)$*

These elements are the elements “on which $\widetilde{N}$ and $\|\cdot\|_\infty$ are equivalent”. Then the (normalized) algebraic norm is sub-linear for those elements.

Proposition 5. *If $x, y \in K_{\mathbb{R}}$ are γ-balanced, then*

$$\widetilde{N}(x+y) \leq \gamma \cdot \left(\widetilde{N}(x) + \widetilde{N}(y)\right)$$

Proof. Let x, y two γ-balanced element of $K_{\mathbb{R}}$, then

$$\widetilde{N}(x+y) \leq \|x+y\|_\infty \leq \|x\|_\infty + \|y\|_\infty \leq \gamma \cdot \left(\widetilde{N}(x) + \widetilde{N}(y)\right)$$

□

It is argued in [CDPR16] that if K is a cyclotomic field, then for any $x \in K$, it is possible to find an element $u \in \mathcal{O}_K{}^\times$ such that ux is γ-reduced.

Theorem 6 ([CDPR16])**.** *(Heuristic) Take $K = \mathbb{Q}(\zeta_m)$ with $m = p^k$ a prime power and $x \in K$. Then there exists a classical subexponential/quantum polytime algorithm outputing $u \in \mathcal{O}_K{}^\times$ such that ux is $\exp\left(\widetilde{O}(\sqrt{m})\right)$-balanced.*

2.3 Module Lattices

If K is a field of degree d and $\mathcal{O}_K$ its ring of integers, then take $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ fractional ideals and $b_1, \ldots, b_n \in K_{\mathbb{R}}{}^m$ $K_{\mathbb{R}}$-linearly independant, then $M = \sum_{i=1}^n \mathfrak{b}_i \cdot b_i$ is a module lattice. We call n its rank and m its coordinate dimension. We call $(\mathfrak{b}_i, b_i)_{i=1\ldots n}$ a pseudo-basis of M.

In the following, we will always assume that the considered modules are finitely generated and torsion free. The module M can be embedded into $\mathbb{C}^{dm}$ via the cannonical embedding. We can then define the l_p norm of any element of M.

We can also define the algebraic norm of elements of M in the following way:

$$N(x) = \prod_{i=1}^{d} \sqrt{\sum_{j=1}^{m} |\sigma_i(x_j)|^2},$$

so that if $d = 1$, then $N(x) = \|x\|_2$, and if $m = 1$, then $N(x) = N_{K/\mathbb{Q}}(x)$.

3 Rank-2 SVP

In order to create a proper LLL algorithm for module lattices, we have to find a way to make an algorithm similar to Gauss-Lagrange reduction work in the case of module lattices. The central step of the algorithm is to take two vectors and to reduce one relatively to the other.

3.1 For $\mathbb{Z}$: the Gauss-Lagrange algorithm

In order to find short vectors in a $\mathbb{Z}$ lattice spanned by the basis $v_1 = \begin{bmatrix} a \\ b \end{bmatrix}, v_2 = \begin{bmatrix} c \\ d \end{bmatrix}$ with $\|v_1\| < \|v_2\|$, the Gauss-Lagrange algorithm is often used. The procedure is summarised in Algorithm 3.1.

Algorithm 3.1 Gauss-Lagrange algorithm

```
1: procedure GAUSS-LAGRANGE($v_1, v_2 \in \mathbb{Z}^2$ with $\|v_2\|_2 < \|v_1\|_2$)
2:     Let $B_1 = \|v_1\|_2^2$
3:     Let $B_2 = \|v_2\|_2^2$
4:     while $B_2 < B_1$ do
5:         Swap $v_1$ and $v_2$
6:         $B_1 \leftarrow B_2$
7:         Let $\mu \leftarrow \langle v_1, v_2 \rangle / B_1$
8:         $v_2 \leftarrow v_2 - \lfloor \mu \rceil \cdot v_1$                ▷ Reduction of $v_2$ by $v_1$
9:         Let $B_2 = \|v_2\|_2^2$
10:    return $v_1, v_2$
```

One can note that the main part of the algorithm is to compute the **reduction of v_2 by v_1**. This is done by taking the closest integer of $\langle v_1, v_2 \rangle / \|v_1\|^2$. This step can be rewritten as follows: if $\begin{matrix} r_1 = B_1^2 & r_{12} = \langle v_1, v_2 \rangle \\ 0 & r_2 = B_2^2 \end{matrix}$ is the R factor of the QR factorisation of v_1, v_2, then Step 8 of Alg 3.1 is making the Euclidean division of $r_{1,2}$ by r_1. Hence in order to find shorts vector in rank-2 $\mathcal{O}_K$ lattices, a possible approach would be to generalize the Gauss-Lagrange algorithm for the algebraic norm.

3.2 General results for $\mathcal{O}_K$-lattices

In [LPMSW19, Section 4], the R part of the QR representation of $b_1, b_2 \in {K_\mathbb{R}}^2$ is taken, and a short algebraic norm vector is found by taking combinations of b_1 and b_2 with coefficients in $\mathfrak{b}_1$ and $\mathfrak{b}_2$.

Namely, the following 2×2 matrix:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \text{ with } a, b, c \in K_\mathbb{R}$$

is considered and they try to find $(u, v) \in \mathfrak{b}_1 \times \mathfrak{b}_2$ such that the vector $\begin{bmatrix} u \cdot a + v \cdot b \\ v \cdot c \end{bmatrix}$ has small algebraic norm.

We are going to study these rank-2 $\mathcal{O}_K$-modules. To simplify our study, we can apply [Coh00, Corollary 1.2.25] in order to suppose that $\mathfrak{b}_1 = \mathcal{O}_K$. In the context of our use of rank-2 $\mathcal{O}_K$-modules (a divide and swap algorithm in the module-LLL algorithm of [LPMSW19]), we will have $N(a) > N(c)N(\mathfrak{b}_2)$, we can then divide all the columns of M by a for the normalization. The module we will be looking at in the remaining will then be of this form:

$$\mathcal{O}_K \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \mathfrak{a} \begin{bmatrix} b \\ c \end{bmatrix} \text{ with } b, c \in K_\mathbb{R} \text{ and } N(\mathfrak{a})N(c) < 1$$

We will be looking for a vector in this module-lattice whose algebraic norm is < 1. The first thing to ask is if finding such a vector $X = \begin{bmatrix} u + vb \\ vc \end{bmatrix}$ is possible. Then if it is possible, what are the values for u, v that we can consider?

We first need to link the (normalized) algebraic norm of a vector to its infinite norm, it is summarized in the following lemma.

Lemma 7. *If $x \in {K_{\mathbb{R}}}^m$, then $\widetilde{N}(x) \leq \sqrt{m}\,\|x\|_\infty$.*

Proof. We have that:

$$N(x) = \prod_{i=1}^{d} \sqrt{\sum_{j=1}^{m} |\sigma_i(x_j)|^2} \leq \prod_{i=1}^{d} \sqrt{\sum_{j=1}^{m} \|x\|_\infty^2} = \prod_{i=1}^{d} \sqrt{m}\,\|x\|_\infty$$
$$= \left(\sqrt{m}\,\|x\|_\infty\right)^d$$

By taking the dth root we get $\widetilde{N}(x) \leq \sqrt{m}\,\|x\|_\infty$. □

That leads us to Proposition 8.

Proposition 8. *Consider the $\mathcal{O}_K$-module $M = \begin{bmatrix}1\\0\end{bmatrix} + \mathfrak{a}\begin{bmatrix}b\\c\end{bmatrix}$.*

Then if $\widetilde{N}(c) < \frac{d}{\widetilde{N}(\mathfrak{a})\cdot\delta_{2d}^2\cdot\widetilde{\Delta}_K^2}$, there exist $x \in M$ such that $\widetilde{N}(x) < \sqrt{2}\,\|x\| < 1$.

I.e., there exist $u, v \in \mathcal{O}_K \times \mathfrak{a}$ such that $1 \leq \widetilde{N}(v) < \frac{\delta_{2d}^2}{d}\cdot\widetilde{N}(\mathfrak{a})\cdot\widetilde{\Delta}_K^2$ and

$$\widetilde{N}\left(\begin{bmatrix}u+v\cdot b\\ v\cdot c\end{bmatrix}\right) < \sqrt{2}\cdot\left\|\begin{bmatrix}u+v\cdot b\\ v\cdot c\end{bmatrix}\right\|_\infty < 1$$

Proof. Consider the rank-2 $\mathcal{O}_K$-module $M_t = \mathcal{O}_K\begin{bmatrix}1\\0\end{bmatrix} + \mathfrak{a}\begin{bmatrix}b\\t\cdot c\end{bmatrix}$ where $t > 0$ is to be chosen later.

The volume of M_t as a $\mathbb{Z}$-lattice is $N(tc)\cdot\Delta_K\cdot N(\mathfrak{a})\Delta_K = \Delta_K^2\cdot N(\mathfrak{a})t^d\cdot N(c)$.

By Minkowski's theorem, there exists $(u, v) \in (\mathcal{O}_K, \mathfrak{a}) \setminus \{(0,0)\}$ such that

$$\left\|\begin{bmatrix}u+v\cdot b\\ v\cdot tc\end{bmatrix}\right\|_\infty \leq \delta_{2d}\left(t^d\cdot N(\mathfrak{a})\cdot N(c)\cdot\Delta_K^2\right)^{\frac{1}{2d}} = \delta_{2d}\sqrt{t\cdot\widetilde{N}(\mathfrak{a})\cdot\widetilde{N}(c)\cdot\widetilde{\Delta}_K^2}$$

. In particular, we can choose $t = \frac{d}{\delta_{2d}^2\cdot\widetilde{N}(\mathfrak{a})\cdot\widetilde{N}(c)\cdot\widetilde{\Delta}_K^2}$ which is > 1 by hypothesis, and then $\left\|\begin{bmatrix}u+v\cdot b\\ v\cdot tc\end{bmatrix}\right\|_\infty < 1/\sqrt{2}$.

We know that $\left\|\begin{bmatrix}u+v\cdot b\\ v\cdot c\end{bmatrix}\right\|_\infty \leq \left\|\begin{bmatrix}u+v\cdot b\\ v\cdot tc\end{bmatrix}\right\|_\infty < 1/\sqrt{2}$, since $t \geq 1$. And then by Lemma 7, we get

$$\widetilde{N}\left(\begin{bmatrix}u+v\cdot b\\ v\cdot c\end{bmatrix}\right) \leq \sqrt{2}\cdot\left\|\begin{bmatrix}u+v\cdot b\\ v\cdot c\end{bmatrix}\right\|_\infty < 1.$$

Now let us bound $\widetilde{N}(v)$.

First, if $v = 0$, then $\left\|\begin{bmatrix}u+v\cdot b\\ v\cdot tc\end{bmatrix}\right\|_\infty = \|u\|_\infty$ and $N\left(\begin{bmatrix}u+v\cdot b\\ v\cdot tc\end{bmatrix}\right) = N(u) \in \mathbb{Z}$. as $|N(u)| \leq \|u\|_\infty^d < 1$, we have $u = 0$, which is a contradiction with $(u, v) \neq (0, 0)$. So $v \neq 0$, and hence as $v \in \mathcal{O}_K$, we have $\widetilde{N}(v) \geq 1$.

On the other hand, we have $\|vtc\|_\infty < 1/\sqrt{2}$ and hence, by Lemma 7, we have $\widetilde{N}(vtc) < 1$.

We know that $\widetilde{N}(vtc) = t\cdot\widetilde{N}(v)\cdot\widetilde{N}(c) = \frac{\widetilde{N}(v)\cdot\widetilde{N}(c)\cdot d}{\delta_{2d}^2\cdot\widetilde{N}(\mathfrak{a})\cdot\widetilde{N}(c)\cdot\widetilde{\Delta}_K^2}$, hence

$$\widetilde{N}(v) < \frac{\delta_{2d}^2}{d}\cdot\widetilde{N}(\mathfrak{a})\cdot\widetilde{\Delta}_K^2$$

which concludes the proof. □

The bound on the algebraic norm of v in Prop 8 is not tight. In fact in order to create a Gauss-Lagrange reduction for two elements of an $\mathcal{O}_K$-module, we would like to find v with the smallest possible algebraic norm. The extreme case being $v \in {\mathcal{O}_K}^\times$. We say that K admits rank-2 Euclidean division in one step if for any vectors b_1, b_2 we can find u, v such as in Prop 8 with $v \in {\mathcal{O}_K}^\times$. This is a very strong condition, namely it implies the fact that K is Euclidean for the algebraic norm (see Section 4).

The result of Proposition 8 should be put in relation with Corollary 4.8 of [LPMSW19] which gives the same kind of result. This proposition is rephrased next in order to match the notations of this article.

Proposition 9 ([LPMSW19], Cor 4.8 (Heuristic))**.** *Let $\varepsilon = 2^{-\widetilde{O}(\log(\widetilde{\Delta_K}))}$. There exists an algorithm which given as input $b \in K_{\mathbb{R}}$ and $\mathfrak{a}$ an ideal of $\mathcal{O}_K$, output $(u,v) \in \mathcal{O}_K \times \mathfrak{a}$ such that*

$$\|u+bv\|_\infty \leq \varepsilon$$
$$\|v\|_\infty \leq 2^{\widetilde{O}(d\log(\rho(\mathcal{O}_K)))/d}$$

where $\rho(\mathcal{O}_K)$ is the covering radius of $\mathcal{O}_K$ seen as a $\mathbb{Z}$-lattice.

Let us rephrase Proposition 8 in the same way.

Proposition 10 ([LPMSW19], Cor 4.8 (Heuristic))**.** *Let $b \in K_{\mathbb{R}}$ and $\mathfrak{a}$ an ideal of $\mathcal{O}_K$. There exists $(u,v) \in \mathcal{O}_K \times \mathfrak{a}$ such that*

$$\widetilde{N}(u+bv) \leq \|u+bv\|_\infty < 1/\sqrt{2}$$
$$\widetilde{N}(v) < \frac{\delta_{2d}^2}{d} \cdot \widetilde{N}(\mathfrak{a}) \cdot \widetilde{\Delta}_K^2$$

where $\rho(\mathcal{O}_K)$ is the covering radius of $\mathcal{O}_K$ seen as a $\mathbb{Z}$-lattice.

One can see that those two results are quite similar, but [LPMSW19, Cor. 4.8] gives bounds on the l_∞ norm, is heuristic and constructive and Proposition 8 gives a worst bound on $\|u+bv\|_\infty$ but is not heuristic and bound on the algebraic norm of v. The bound of Proposition 8 is thought asymptotically better than the one of [LPMSW19, Cor. 4.8], since $\widetilde{O}(d\log(\rho(\mathcal{O}_K))) = \Omega(\log \Delta_K)$ [LPMSW19, p.8].

One may ask whether the bound on the algebraic norm of v of Proposition 8 is optimal, but more work seems required to answer this question.

4 The case of Euclidean fields

For the following, we are going to need the definition of a field **Euclidean for the algebraic norm** (or **Euclidean Field**). An overview of those can be found in [Lez12].

Def 8. *The field K is* ***Euclidean for the algebraic norm*** *if for any $x \in K$, there is an integer $k \in \mathcal{O}_K$ such that $|N(x-k)| < 1$.*

The fact of being Euclidean implies in particular that the ring of integers $\mathcal{O}_K$ is principal.

With those definitions, we can now prove the claimed proposition about the Euclidianity of fields that admits rank-2 Euclidean division in one step.

Proposition 11. *If for any $b, c \in K$ such as in Proposition 8 there exists $u \in \mathcal{O}_K$ and $v \in {\mathcal{O}_K}^\times$ such that $\widetilde{N}\left(\begin{bmatrix} u+v\cdot b \\ v\cdot c\end{bmatrix}\right) < 1$, then K is Euclidean for the algebraic norm.*

Proof. Take any $x \in K$. Let $c \in K \setminus \{0\}$ such that $\widetilde{N}(c) < \frac{d}{\delta_{2d}^2 \cdot \widetilde{\Delta}_K^2}$ (for example we can take $1/n$ for a large enough $n \in \mathbb{Z}_{\geq 0}$). Then there exists $u \in \mathcal{O}_K$ and $v \in {\mathcal{O}_K}^\times$ such that $\widetilde{N}\left(\begin{bmatrix} u+v\cdot x \\ v\cdot c\end{bmatrix}\right) < 1$. In particular, we have $\widetilde{N}(u+v\cdot x) < 1$ and then $N(u+v\cdot x) < 1$.

As $v \in {\mathcal{O}_K}^\times$, we have $N(u+v\cdot x) = N(v^{-1}\cdot(u+v\cdot x)) = N(v^{-1}u + x)$. We can then take $k = -v^{-1}u$ and we have $N(x-k) < 1$. □

The notion of Euclideanity can be encapsuled in a constant depending only on the considered field.

Def 9 ([Lez12])**.** *Let $x \in K$, the* ***Euclidean minimum*** *of x, denote $m_K(x)$ is the infimum of the function $k \mapsto |N(x-k)|$ where k runs over $\mathcal{O}_K$. This definition extends by continuity to any $x \in K_{\mathbb{R}}$ and is then denoted $m_{K_{\mathbb{R}}}(x)$.*

*The **Euclidean minimum** of K, denoted $\mathfrak{M}_K$ is equal to the quantity $\sup_{x\in K} m_K(x)$.*
*The **Euclidean minimum** of $K_{\mathbb{R}}$, denoted $\mathfrak{M}_{K_{\mathbb{R}}}$ is equal to the quantity $\sup_{x\in K_{\mathbb{R}}} m_{K_{\mathbb{R}}}(x)$.*

If $r_1 + r_2 > 1$, the two Euclidean minimum $\mathfrak{M}_K$ and $\mathfrak{M}_{K_{\mathbb{R}}}$ in fact coincide [Lez12, Th 2.7].

From now on in this section, we assume that the field K is **Euclidean for the algebraic norm**, with **Euclidean minimum** $\mathfrak{M}_K < 1$. In order to place ourselves in interesting cases, we will assume that the rank of the units of $\mathcal{O}_K$ is greater than 1 (i.e., that $r_1 + r_2 \geq 2$). We will also assume that we have access to an oracle ED (for Euclidean Division) that on input $x \in K$ returns such a $k \in \mathcal{O}_K$. This oracle extends to $K_{\mathbb{R}}$ by density and discreteness of $\mathcal{O}_K$(the fact that $\mathfrak{M}_K < 1$ enable us to consider that for any $x \in K_{\mathbb{R}}, ED(x) < 1$).

One thing we would want from ED is for it to preserve the balanceness of the elements of K. Namely, if x is balanced (of small l_p norm relatively to its normalized algebraic norm), then we would like ED(x) to be balanced. This is not possible to ask for, as summarised in the Proposition 12.

Proposition 12. *If the field K is such that $r_1+r_2 > 1$, for any $1 > \varepsilon > 0$, there exists $x \in K_{\mathbb{R}}$ with $\widetilde{N}(x) < \sqrt{2}\varepsilon$ and $\|x\|_\infty < 2\varepsilon$, such that a valid output for $ED(x)$ is k of algebraic norm 1 and of l_∞ norm $> 1/\varepsilon$.*

Proof. Without loss of generality, we restrict ourselve to the case $r_1 + r_2 = 2$.

First, take a $u \in \mathcal{O}_K{}^\times$, then $u = \begin{bmatrix} M \\ 1/M \end{bmatrix}$. As in Proposition 3, we can take $M > 1/\varepsilon$. Then let $x = \begin{bmatrix} 1/M \\ 2/M \end{bmatrix} \in K_{\mathbb{R}}$. Then u is a legitimate output of ED(x) as $|N(x-u)| = (M - 1/M)\cdot(1/M) = 1 - 1/M^2 < 1$.

Then the four following facts hold:

- $\widetilde{N}(x) < \sqrt{2}\varepsilon$.
- $\|x\|_\infty < 2\varepsilon$.
- $N(u) = 1$.
- $\|u\|_\infty > 1/\varepsilon$.

This complete the proof. □

In order to have more clarity, the Landau notation will be used in the following. The previous proposition can be rephrased as follows:

Proposition 13. *If the field K is such that $r_1 + r_2 > 1$, for any $1 > \varepsilon > 0$, there exists $x \in K_{\mathbb{R}}$ with $\widetilde{N}(x) = O(\varepsilon)$, $\|x\|_\infty = O(\varepsilon)$ such that a valid output for $ED(x)$ is k of algebraic norm 1 and of l_∞ norm $\Omega(1/\varepsilon)$.*

Proposition 13 explains that the quotient by the Euclidean division of a balanced element of $K_{\mathbb{R}}$ can be unbalanced. The same proof can be adapted to prove the same fact for the remainder.

Proposition 14. *If $r_1 + r_2 > 1$, for any $1 > \varepsilon > 0$, there exists $x \in K_{\mathbb{R}}$ with $\widetilde{N}(x) = O(\varepsilon)$ and $\|x\|_\infty = O(\varepsilon)$, such that a valid output for $ED(x)$ is k of algebraic norm 1 and such that $\|x - k\|_\infty = \Omega(1/\varepsilon)$.*

We are now going to try to anyway use the ED oracle to have a Lagrange-Gauss' algorithm for rank-2 $\mathcal{O}_K$-modules.

The setup is the same as before, we are considering the matrix:

$$\begin{bmatrix} 1 & b \\ 0 & c \end{bmatrix},$$

and we want to find $u, v \in \mathcal{O}_K$ such that $\widetilde{N}\left(\begin{bmatrix} u + v\cdot b \\ v \cdot c \end{bmatrix}\right) < 1$.

The most natural way to do so, as we know that K is Euclidean for the algebraic norm, is to take $v = 1$ and $u = ED(b)$. This leads to Algorithm 4.1. However, this algorithm does not output a vector with smaller algebraic norm in all cases.

Proposition 15. *If $r_1 + r_2 > 1$, for all $1 > \varepsilon > 0$ there exists $b, c \in K_{\mathbb{R}}$ with $\widetilde{N}(b) = O(\varepsilon)$, $\widetilde{N}(c) = O(1)$, $\|b\|_\infty = O(\varepsilon)$ and $\|c\|_\infty = O(1)$ such that a possible output of Algorithm 4.1 on (b, c) is X with $N(X) = \Omega(1/\varepsilon)$.*

Algorithm 4.1 Reduction by ED of b by 1

```
procedure EUCLIDEAN_DIVISION($b, c \in K_{\mathbb{R}}$)
    Let $u$ be the output of $ED(b)$
    return $\begin{bmatrix} b-k \\ c \end{bmatrix}$
```

Proof. Let $\varepsilon > 0$. By Proposition 14, we can find a pair b, k with $\widetilde{N}(b) = O(\varepsilon)$, $\|b\|_{\infty} = O(\varepsilon)$ such that k is a possible output for ED(b) and $b - k = \begin{bmatrix} \varepsilon \\ \Omega(1/\varepsilon) \end{bmatrix}$. We take $c = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ an element of $K_{\mathbb{R}}$ of very small l_p and algebraic norm.

So $N\left(\begin{bmatrix} b-k \\ c \end{bmatrix}\right)^2 = (\varepsilon^2 + 1)(\Omega(1/\varepsilon^2) + 1) = \Omega(1/\varepsilon^2)$.

On input b, c, Algorithm 4.1 will output a vector of large algebraic norm. □

These propositions should not be seen as a simple existence statements but more as a descriptions of the pathological cases that can occur and make Algorithm 4.1 unusable in practice. Namely, if $k - b$ is very unbalanced the algorithm does not work. This leads us to an updated version of Algorithm 4.1, namely Algorithm 4.2, where the number $b - k$ is balanced by multiplying it by an element of $\mathcal{O}_K{}^{\times}$.

Algorithm 4.2 Reduction by ED of b by 1 with balancing

```
procedure BALANCED_EUCLIDEAN_DIVISION($b, c \in K_{\mathbb{R}}, \gamma > 1$)
    Let $k$ be the output of $ED(b)$
    Find $u \in \mathcal{O}_K{}^{\times}$ such that $u \cdot (b-k)$ is $\gamma$-balanced.
    return $\begin{bmatrix} u \cdot (b-k) \\ u \cdot c \end{bmatrix} = uk \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + u \cdot \begin{bmatrix} b \\ c \end{bmatrix}$
```

Unfortunately, Algorithm 4.2 also has pathological cases.

Proposition 16. *If $r_1 + r_2 > 1$, for all $1 > \varepsilon > 0$, for all $\gamma > 1$, there exists $b, c \in K_{\mathbb{R}}$ with $\widetilde{N}(b) = O(\varepsilon)$, $\widetilde{N}(c) = O(1)$, $\|b\|_{\infty} = O(\varepsilon)$ such that the output of Algorithm 4.2 on (b, c, γ) is X with $N(X) = \Omega(1/\varepsilon)$.*

Proof. Fix a $\gamma > 1$ and let $\varepsilon > 0$. By Proposition 14, we can find a pair b, k with $\widetilde{N}(b) = O(\varepsilon)$, $\|b\|_{\infty} = O(\varepsilon)$ such that $ED(b) = k$ and $b - k = \begin{bmatrix} \varepsilon \\ \Omega(1/\varepsilon) \end{bmatrix}$.

We assume that $(b - k) = u^{-1}\begin{bmatrix} x \\ y \end{bmatrix}$ with $u \in \mathcal{O}_K{}^{\times}$, $xy < 1$ and such that $\begin{bmatrix} x \\ y \end{bmatrix}$ is balanced, namely $x, y \leq \gamma \cdot xy < \gamma$. In particular we have $x, y \geq 1/\gamma$.

Take $0 < a < 1$. Let $c = u^{-1}\begin{bmatrix} a\varepsilon \\ 1/\varepsilon \end{bmatrix}$. Then $N(c) = a = O(1)$ and

$$N\left(\begin{bmatrix} u \cdot (b-k) \\ u \cdot c \end{bmatrix}\right)^2 = ((a\varepsilon)^2 + x^2)(1/\varepsilon^2 + y^2) > x^2 \cdot (1/\varepsilon^2 + y^2) > 1/\gamma^2 \cdot (1/\varepsilon^2 + 1/\gamma^2) = \Omega(1/\varepsilon^2) \text{ since } \gamma \text{ is fixed.}$$

On input b, c, Algorithm 4.2 will output a vector of algebraic norm $\Omega(1/\varepsilon)$. □

Here again, we can see that the objection for the output to have a output with small algebraic norm is that even if $u \cdot (b - k)$ is balanced then if $u \cdot c$ is not, the algorithm can go wrong. One may then wonder if it is possible to find $u \in \mathcal{O}_K$ which will balance both $b - k$ and c at the same time. But again this is not possible.

Proposition 17. *For all $M > 0$ large enough, there exists $(x, y) \in K_{\mathbb{R}}{}^2$ with algebraic norm equal to 1 such that for any $u \in \mathcal{O}_K{}^{\times}$ either ux or uy has l_2 norm $\Omega(M)$.*

Proof. Let $M > 0$ and take $x = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $y = \begin{bmatrix} M^2 \\ 1/M^2 \end{bmatrix}$. Then x and y have algebraic norm equal to 1. The area of the parallelogram $(0, u \cdot x, \cdot(x+y), \cdot y)$ is $A = \|x\|_2 \cdot \|y\|_2 \cdot |\sin(x,y)|$. The angle between x and y goes to $\pi/4$ when M grows, so for M large enough we have that $A \geq \|x\|_2 \cdot \|y\|_2 /4 = (\sqrt{M^4 + 1/M^4})(\sqrt{2})/4 = \Omega(M^2)$.

The matrices of the multiplication by elements of ${\mathcal{O}_K}^\times$ are unimodular, hence they preserve the areas. For any $u \in {\mathcal{O}_K}^\times$, the area of the parallelogram $(0, x, x+y, y)$ is equal to $\|ux\|_2 \|uy\|_2 |\sin(ux, uy)| \leq \|ux\|_2 \|uy\|_2$. We then have the inequalities:

$$\|ux\|_2 \|uy\|_2 \geq \|ux\|_2 \|uy\|_2 |\sin(ux, uy)| = A \geq \Omega(M^2)$$

Then either $\|ux\|_2$ or $\|uy\|_2$ is greater than $\Omega(M)$. □

5 Minimum-based Euclidean division

In this work, the definition of ED(x) gives us any number at a distance at most 1 of x, which is a not the strongest condition possible. One could think that a more powerful oracle could lead to better results.

Proposition 18. *For any $x \in K$, the minimum of the function $k \mapsto |N(x-k)|$ is reached.*

Proof. Let $x = p/q$ be an element of K with $p \in \mathcal{O}_K$ and $q \in \mathcal{O}_K \setminus \{0\}$. The set $\{N(x-k), k \in \mathcal{O}_K\}$ is contained inside the discrete set $\{N(k/q), k \in \mathcal{O}_K\} \subset \frac{1}{N(q)}\mathbb{Z}$. Then by positiveness and by discreteness of $\{N(x-k), k \in \mathcal{O}_K\}$, the minimum of the fuction $k \mapsto |N(x-k)|$ is reached. □

Let us then define an oracle giving one of the best possible k.

Def 10. *Let ED' be an oracle that, on input x, return some $k \in \mathcal{O}_K$ such that $|N(x-k)|$ is minimal. If multiple choices are possible, then the oracle arbitrarily chooses one of them.*

With this definition in particular, the proof of Proposition 12 does not hold anymore since the condition $|N(x-k)| < 1$ is not sufficient. However, this new Euclidean division oracle does not suffice to hope for a good divide and swap algorithm.

5.1 Properties of the min-Euclidean division

First, let's introduce some notation. We define the algebraic norm integer-circle centered on $x \in K_\mathbb{R}$ of radius $r > 0$ to be the set of integers at fixed "algebraic distance" r of x: $\mathcal{C}^N_{\mathcal{O}_K}(x,r) = \{y \in \mathcal{O}_K, |N(x-y)| = r\}$. Let us first state some properties of those sets.

Proposition 19. *For any $x \in K_\mathbb{R}$ and any $r > 0$, the following holds:*

$$\forall k \in \mathcal{O}_K,\ \ \mathcal{C}^N_{\mathcal{O}_K}(x+k,r) = \mathcal{C}^N_{\mathcal{O}_K}(x,r) + k \tag{1}$$

$$\forall u \in {\mathcal{O}_K}^\times,\ \ \mathcal{C}^N_{\mathcal{O}_K}(ux,r) = u^{-1} \cdot \mathcal{C}^N_{\mathcal{O}_K}(x,r) \tag{2}$$

Proof. Let $x \in K_\mathbb{R}$ and $r > 0$.

For Eq 1, take $k \in \mathcal{O}_K$.

$$\begin{aligned} \mathcal{C}^N_{\mathcal{O}_K}(x,r) + k &= \{k + k', k' \in \mathcal{O}_K, |N(x-k')| = r\} \\ &= \{k + k', k' \in \mathcal{O}_K, |N(x+k-(k+k'))| = r\} \\ &= \{k' \in \mathcal{O}_K, |N(x+k-k')| = r\} \\ &= \mathcal{C}^N_{\mathcal{O}_K}(x+k,r) \end{aligned}$$

For Eq 2, take $u \in {\mathcal{O}_K}^{\times}$.

$$\begin{aligned} u^{-1} \cdot \mathcal{C}^N_{\mathcal{O}_K}(x,r) &= \left\{u^{-1} \cdot k,\ k \in \mathcal{O}_K, |N(x-k)| = r\right\} \\ &= \left\{u^{-1} \cdot k,\ k \in \mathcal{O}_K, |N(u \cdot x - u \cdot k)| = r\right\} \\ &= \left\{u^{-1} \cdot u \cdot k, k \in \mathcal{O}_K,\ |N(u \cdot x - k)| = r\right\} \\ &= \{k \in \mathcal{O}_K,\ |N(u \cdot x - k)| = r\} = \mathcal{C}^N_{\mathcal{O}_K}(ux, r) \end{aligned}$$

□

It is important to notice that $\mathcal{C}^N_{\mathcal{O}_K}(x,r)$ does **not behave like a circle** in the traditional sense. In particular, if $r_1 + r_2 > 1$ they can be unbounded: for example $\mathcal{C}^N_{\mathcal{O}_K}(0,1) = {\mathcal{O}_K}^{\times}$. We are able to state a more general proposition:

Proposition 20. *If $r_1 + r_2 > 1$, then for any $x \in K$ the set $\mathcal{C}^N_{\mathcal{O}_K}(x,r)$ is either empty or infinite.*

Proof. Let $x = p/q \in K$ with $(p,q) \in \mathcal{O}_K \times \mathcal{O}_K \setminus \{0\}$ and $r > 0$ such that $\mathcal{C}^N_{\mathcal{O}_K}(x,r)$ is not empty. Let $k \in \mathcal{C}^N_{\mathcal{O}_K}(x,r)$, by Prop 19, up to taking $x' = x - k$, we can assume $0 \in \mathcal{C}^N_{\mathcal{O}_K}(x,r)$. Let us rewrite $\mathcal{C}^N_{\mathcal{O}_K}(x,r)$.

$$\mathcal{C}^N_{\mathcal{O}_K}(x,r) = \{k \in \mathcal{O}_K, |N(x-k)| = |N(x)|\} = \{k \in \mathcal{O}_K, |N(1 - k/x)| = 1\}.$$

The set $\mathcal{C}^N_{\mathcal{O}_K}(x,r)$ can therefore be put in bijection with the set $1 + \frac{1}{x}\mathcal{O}_K \bigcap \mathcal{C}^N_K(0,1)$.

A subset of this set is $1 + \frac{1}{x}\mathcal{O}_K \bigcap \mathcal{C}^N_{\mathcal{O}_K}(0,1) = 1 + \frac{q}{p}\mathcal{O}_K \bigcap {\mathcal{O}_K}^{\times}$ which contains $1 + q\mathcal{O}_K \bigcap {\mathcal{O}_K}^{\times}$.

We are going to show that for any $q \in \mathcal{O}_K \setminus \{0\}$, the set $(1 + q\mathcal{O}_K) \bigcap {\mathcal{O}_K}^{\times}$ is infinite.

Let $u \in {\mathcal{O}_K}^{\times}$ be a unit which is not a root of unity (it exists since $r_1 + r_2 > 1$). The set $\left\{u^k, k \in \mathbb{Z}\right\}$ is therefore infinite. The set $\mathcal{O}_K / q\mathcal{O}_K$ is finite, so there exists $k_1 < k_2$ such that $u^{k_1} = u^{k_2} \mod q$ i.e., $u^{k_2 - k_1} = 1 \mod q$ i.e., $u^{k_2-k_1} \in 1 + q\mathcal{O}_K$. Therefore, we have found $v = u^{k_2 - k_1} \in {\mathcal{O}_K}^{\times} \bigcap 1 + q\mathcal{O}_K$ hence $v^k \in {\mathcal{O}_K}^{\times} \bigcap (1 + q\mathcal{O}_K)$ for all $k \in \mathbb{Z}$, therefore ${\mathcal{O}_K}^{\times} \bigcap (1 + q\mathcal{O}_K)$ is infinite since v is not a root of unity.

Then $(1 + \frac{1}{x}\mathcal{O}_K) \bigcap {\mathcal{O}_K}^{\times}$ is infinite, hence $1 + \frac{1}{x}\mathcal{O}_K \bigcap \mathcal{C}^N_K(0,1)$ is infinite, and finaly $\mathcal{C}^N_{\mathcal{O}_K}(x,r)$ is infinite, which concludes the proof. □

Note that the proof of Prop 20 gives a way to build an infinite number of elements of $\mathcal{C}^N_{\mathcal{O}_K}(x,r)$ in polynomial time in $N_{K/\mathbb{Q}}(x)$. The action of ED'(x) can therefore be seen as taking an arbitrary element in the set $\mathcal{C}^N_{\mathcal{O}_K}(x, m_K(x))$ where $m_K(x) = \min_{k \in \mathcal{O}_K} |N(x-k)|$ is the Euclidean minimum of x, as defined in [Lez12]. Note that this proposition does not apply to elements of $K_{\mathbb{R}}$, therefore in order to find elements with unique Euclidean norm we must restrict ourselve to elements of $K_{\mathbb{R}} \setminus K$.

5.2 Arbitrarily bad Euclidean divisions for ED'

In this section we do not need to assume K Euclidean anymore since we use ED' which uses "argmin" instead of the condition "< 1". We are going to postulate the existence of an element $y \in K_{\mathbb{R}}$ such that $\mathcal{C}^N_{\mathcal{O}_K}(y, m_K(y)) = \{0\}$. This statement is discussed in Section 5.3.

Theorem 21. *Let $\varepsilon > 0$, then there exists an $x_\varepsilon \in K_{\mathbb{R}}$ with $N(x) = O_\varepsilon(1)$, $\|x_\varepsilon\| = O_\varepsilon(1)$ and such that the unique valid output k of ED'(x_ε) verifies $\|x_\varepsilon - k\| = \Omega_\varepsilon(1/\varepsilon)$.*

First, we are going to find an element of K which is arbitrarily large and with unique output for ED' equal to 0.

Lemma 22. *For all $\varepsilon > 0$, there exists $y_\varepsilon \in K_{\mathbb{R}}$ with 0 as unique possible output for ED'(y_ε), $N(y_\varepsilon) = O_\varepsilon(1)$ and such that $\|y_\varepsilon\| = \Omega_\varepsilon(1/\varepsilon)$.*

Proof. Take y the element of $K_{\mathbb{R}}$ such that $\mathcal{C}^N_{\mathcal{O}_K}(y, m_K(y)) = \{0\}$. Its norm does not depend on ε and $k = \text{ED'}(y)$. By the infinity of ${\mathcal{O}_K}^\times$, there exists $u_\varepsilon \in {\mathcal{O}_K}^\times$ such that $\|u_\varepsilon(y-k)\| > 1/\varepsilon$.

Since y has unique Euclidean divisor 0, it is the same for $u_\varepsilon \cdot y$ by Proposition 19. We then define $y_\varepsilon = u_\varepsilon \cdot y$. □

Now with this "arbitrarily bad" element, we can prove the theorem.

Proof of Theorem 21. Let $\varepsilon > 0$. For any $k \in \mathcal{O}_K$ we have that k is the unique valid output for ED'$(k - y_\varepsilon)$. Now let k_ε be the closest integer to y_ε in l_∞ norm. Since $\mathcal{O}_K$ is a lattice, we have that $\|k_\varepsilon - y_\varepsilon\| = O_\varepsilon(1)$ and hence $N(k_\varepsilon - y_\varepsilon) = O_\varepsilon(1)$.

Furthermore, we have that k_ε is the unique valid output for ED'$(k_\varepsilon - y_\varepsilon)$. Then by taking $x = k_\varepsilon - y_\varepsilon$, we have x of bounded algebraic and l_p norms whose output $x - ED'(x) = y_\varepsilon$ can be of arbitrary large l_p norm. □

We can note that the results we have here are not as strong as the ones in Section 4 since x cannot be as small as we want, but they applies in all fields, and not only in the Euclidean ones.

5.3 Constructing element with unique Euclidean divisor

During our study of ED', the question of finding elements of $K_{\mathbb{R}}$ such that the output of ED' is unique occurred. It turns out that constructing an element with unique Euclidean divisor is not trivial, since Proposition 20 gives that any element of K has an infinite number of "minimal Euclidean Divisors". One could then restrict themselve to transcendental numbers.

Proposition 23. *If $x \in \mathbb{C}$ (seen as an element of $K_{\mathbb{R}}$via the embedding $x \mapsto (x, \ldots, x)$) is transcendental, then for any $r > 0$, the set $\mathcal{C}^N_{\mathcal{O}_K}(x, r)$ has cardinal 0 or 1.*

Proof. Let $x \in \mathbb{C}$ transcendental and $r > 0$ such that $\mathcal{C}^N_{\mathcal{O}_K}(x, r) \neq \emptyset$. As for any $k \in \mathcal{O}_K$, $\mathcal{C}^N_{\mathcal{O}_K}(x + k, r) = \mathcal{C}^N_{\mathcal{O}_K}(x, r) + k$ and for any $k \in \mathcal{O}_K, k + x$ is transcendental, we can assume $0 \in \mathcal{C}^N_{\mathcal{O}_K}(x, r)$, hence $r = |N(x)|$.

Then let $k \in \mathcal{O}_K$ such that $r = |N(x)| = \pm N(x-k)$. Let $P(Y) = (N(Y) - N(Y-k))(N(Y) + N(Y-k))$, then it is a polynomial with coefficients in $\mathbb{Z}$ of degree d, and $P(x) = 0$. Hence, as x is transcendental $P = 0$, so either $N(X) = N(X-k)$ or $N(X) = -N(X-k)$. The sign of the bigger coefficient implies that $N(X) \neq -N(X-k)$, so $N(X) = N(X-k)$. Hence the roots of $N(X)$ and $N(X-k)$ coincide, and the roots of the polynomial $N(X-a)$ are exactly the embeddings of a in $\mathbb{C}$. As the embeddings of 0 are all equal to 0, $k = 0$, hence $|\mathcal{C}^N_{\mathcal{O}_K}(x, r)| = 1$ □

In order to construct a number with unique Euclidean division, one must then find $x \in \mathbb{C}$ transcendental such that its Euclidean minimum is reached. In order to do so, a first approach would be to take elements very close to 0 in l_p norm and to try to prove that the "closest" integer in algebraic norm to those elements is 0. This approach do not succeed easily, as summarised in the next proposition.

Proposition 24. *If $r_1 + r_2 > 1$, for every $\varepsilon > 0$ there exist an element $x \in K$ with $\|x\|_2 < \varepsilon$ such that $N(x) > m_K(x)$.*

Proof. We are doing the proof with $r_1 + r_2 = 2$, but it generalize for greater rank of ${\mathcal{O}_K}^\times$.

Let $\varepsilon > 0$. Let $\varepsilon_1, \varepsilon_2 > 0$ to be determined later. Let $u \in {\mathcal{O}_K}^\times = \begin{bmatrix} \varepsilon_1 \\ 1/\varepsilon_1 \end{bmatrix}$. We are going to look at the open inside of $\mathcal{C}^N_{\mathcal{O}_K}(u, \varepsilon_2)$, which we call $\mathcal{D}^N(u, \varepsilon_2) = \{x \in K_{\mathbb{R}}, |N(u - x)| < \varepsilon_2\}$. The intersection of this set with the x axis is equal to the open segment $(\epsilon_1(1 - \epsilon_2), \epsilon_1(1 + \epsilon_2))$.

On can choose ϵ_1 such that for any ϵ_2 sufficiently small, the segment $(\epsilon_1(1 - \epsilon_2), \epsilon_1(1 + \epsilon_2))$ lies into the open ball of radius ε, which we are going to call $B_{l_2}(0, \varepsilon)$. Once ϵ_1 is fixed, we are goig to fix ϵ_2 in order to place ourselve in a situation looking like Fig 1. Namely we want that there exist points inside the set $X_{\varepsilon_1, \varepsilon_2} = \left(B_{l_2}(0, \varepsilon) \bigcap \mathcal{D}^N(u, \varepsilon_2)\right) \setminus \mathcal{D}^N(0, \varepsilon_2)$.

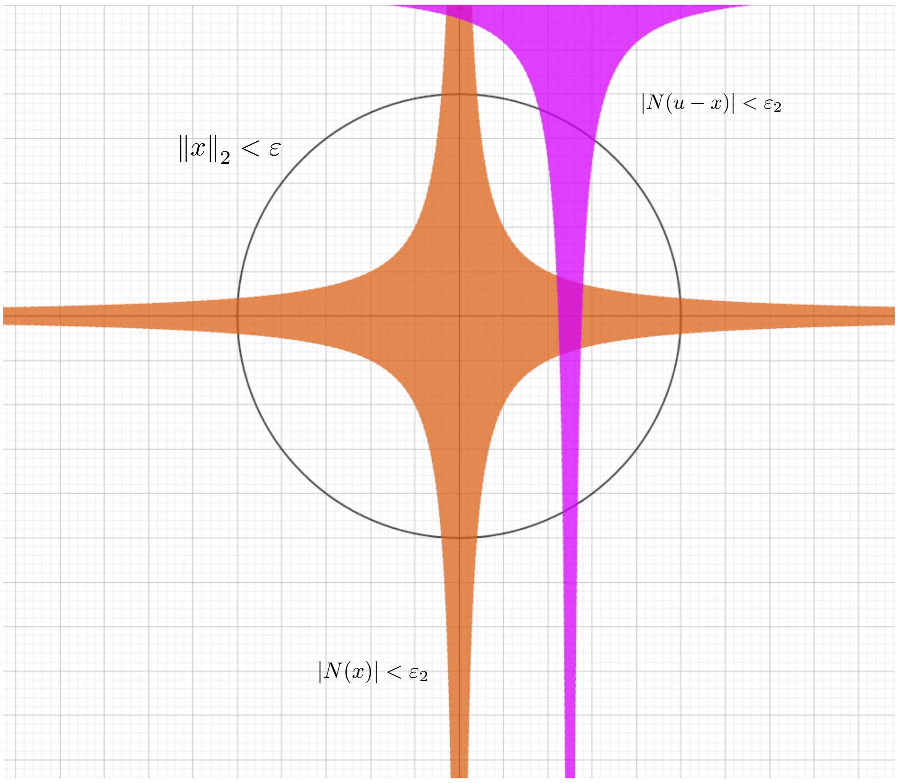

Figure 1: $\mathcal{D}^N(u, \varepsilon_2)$, $\mathcal{D}^N(0, \varepsilon_2)$ and $B_{l_2}(0, 2\epsilon_2)$.

Since when ε_2 goes to 0 (with $\varepsilon, \varepsilon_1$ fixed), the set $\mathcal{D}^N(u, \varepsilon_2) \bigcap \mathcal{D}^N(0, \varepsilon_2)$ converges to the set $\{(\varepsilon_1, 0)\}$ and hence $X_{\varepsilon_1,0}$ is not empty, for ε_2 small enough, $X_{\varepsilon_1,\varepsilon_2}$ is an open non-empty set.

As $X_{\varepsilon_1,\varepsilon_2}$ is open and non-empty, by density of K in $K_{\mathbb{R}}$ it contains an element of K, let us call it x. This element verifies $\|x\|_2 < \varepsilon$ and $|N(x-u)| < \varepsilon_2$, in particular $m_K(x) < \varepsilon_2$. But as $x \notin \mathcal{D}^N(0, \varepsilon_2)$, it also verifies $|N(x)| > \varepsilon_2 > m_K(x)$, which concludes the proof. □

Corollary 25. *There exist a sequence x_n of elements of K converging to 0 such that for all n, $N(x_n) > m_K(x_n)$.*

In particular, Proposition 24 show that the strategy of taking small elements $K_{\mathbb{R}}$in order to find an element with unique Euclidean divisor equal to zero do not work.

6 Module LLL in biquadratic Euclidean fields

A attempt to use the Lagrange algorithm in module lattices was made in [KL17]. They succeeded for certain fields and for a certain norm to have a LLL-type algorithm. This seems to contradict our study but in the next section we will explain the differences between their algorithm and the one we are trying to create.

In [KL17], a LLL-type algorithm is described for biquadratic Euclidean number fields, namely fields of the form $K = \mathbb{Q}(\sqrt{-\alpha}, \sqrt{\beta})$ with $\alpha > 0$ and β such that K is Euclidean with respect to the algebraic norm (which works for some small values of α and β, see [KL17]).

6.1 Other notions of LLL reduction

Let $K = \mathbb{Q}(\sqrt{-\alpha}, \sqrt{\beta})$ with α and β such that K is Euclidean as before, and define the complex subfield $K_0 = \mathbb{Q}(\sqrt{-\alpha})$. The extension K/K_0 is of degree two and of galois group $Gal(K/K_0) = \{id, \theta\}$ where θ is the conjugation $\sqrt{\beta} \mapsto -\sqrt{\beta}$. Then the following is a bilinear form over K^n:

$$\forall x, y \in K^n : B(x, y) = \sum_{i=1}^{n} x_i \theta(y_i)$$

Now, it is important to notice that for all $x \in K$, $B(x, x) \in K_0$, so B induces a quadratic form $q_B : K^n \to K_0$. This quadratic form is degenerate as we will see in Section 6.2.

Then the norm of any element of K^n is defined as $\|B(x, x)\|$, where for any element $x = a + b\sqrt{-\alpha} \in K_0$, $\|x\|^2 = N_{K_0/\mathbb{Q}}(x) = a^2 + \alpha \cdot b^2$.

In [KL17], a whole LLL algorithm is presented for any $\mathcal{O}_K$-module of dimension n but in this work we are only going to focus on $n = 2$.

6.2 Degeneracy of $B(\cdot, \cdot)$

Kim and Lee already noted that the quadratic form $x \mapsto B(x, x)$ was degenerate but did not provide specific examples of isotropic vectors. We provide here a way to construct arbitrary large (in norm and in bit-size) vectors that are annihilated by $x \mapsto B(x, x)$.

We can take an unit u as large as we want in norm or bit-size such that $N_{K/K_0}(u) = -1$. Then the vector $\begin{bmatrix} u \\ 1 \end{bmatrix}$ is isotropic and has arbitrarily large norm.

Example 26. *For $\beta = 2$ and any α, the algebraic integer $(1 + \sqrt{2})^n$ is an unit of algebraic norm $(-1)^n$ with l_p norm growing exponentially with n.*

This degeneracy of the function B implies that the vector size in $K_{\mathbb{R}}$ and the notion of size needed by the LLL-type algorithm of [KL17] totally differ from the one we are considering in this paper and which is also considered in [LPMSW19].

6.3 The difference with Module-LLL

As the notion of size differs, the notion of LLL-reducedness differs too.

Proposition 27. *There exists $x \in K^2$ such that $\|B(x, x)\| = 4$ and the l_2 norm of x is arbitrarily large.*

Proof. As K has infinite unit group, there exist u arbitrarily large, and then the vector $x = \begin{bmatrix} u \\ 1 \end{bmatrix}$ has a l_2 norm arbitrarily large. Since u is invertible in $\mathcal{O}_K$, the algebraic norm relatively to K_0 of u is an element of $\mathcal{O}_{K_0}^{\times}$. This unit group is finite and hence contains only roots of unity. The degree of $K_0/\mathbb{Q}$ beging 2, up to taking u^2 instead of u, we can assume that $N_{K/K_0}(u) = 1$. Therefore $B(x, x) = 1 + 1 = 2$, hence $\|B(x, x)\| = 4$. □

One could note that this result implies that the bit size of the small elements of K and the norm of $B(\cdot, \cdot)$ are non-corelated. An example

The Lovasz condition between [KL17] and [LPMSW19] hence differs. Take $b_1 = \begin{bmatrix} b_{11} \\ b_{12} \end{bmatrix}$ and $b_2 = \begin{bmatrix} b_{21} \\ b_{22} \end{bmatrix}$ two vectors of ${\mathcal{O}_K}^2$. Let us give an explicit writing the LLL-reduceness condition for the two papers for the case $n = 2$.

LLL condition in [KL17]:

Lovasz condition:

$$\begin{aligned} & \|B(b_2, b_2)\|^2 \geq A \cdot \|B(b_1, b_1)\|^2 \\ \Leftrightarrow\ & \|b_{21}\theta(b_{21}) + b_{22}\theta(b_{22})\|^2 \geq A \cdot \|b_{11}\theta(b_{11}) + b_{12}\theta(b_{12})\|^2 \\ \Leftrightarrow\ & \left\|N_{K/K_0}(b_{21}) + N_{K/K_0}(b_{22})\right\|^2 \geq A \cdot \left\|N_{K/K_0}(b_{11}) + N_{K/K_0}(b_{12})\right\|^2 \end{aligned}$$

Size reduceness condition:

$$N_{K/\mathbb{Q}}\left(\frac{B(b_2, b_1)}{B(b_1, b_1)}\right) \leq \mathfrak{M}(K).$$

Where $\mathfrak{M}(K)$ is the Euclidean minimum of K (this is a positive real which is less than 1, see [KL17] for a precise definition).

Lovatz condition in [LPMSW19]:

$$|N_{K/\mathbb{Q}}(b_2)|^2 \geq A \cdot |N_{K/\mathbb{Q}}(b_1)|^2$$
$$\Leftrightarrow |N_{K/\mathbb{Q}}(|b_{21}|^2 + |b_{22}|^2)| \geq A \cdot |N_{K/\mathbb{Q}}(|b_{11}|^2 + |b_{12}|^2)|.$$

With this explicit description, we can then construct a basis which is size-reduced and Lovasz-reduced for the LLL-type algorithm of [KL17] but not for the one of [LPMSW19].

Let $l \geq 1$ such that $1/(l+1)^2 < \mathfrak{M}(K)$ and a unit u of arbitrarily large l_p-norm. Then take $b_1 = \begin{bmatrix} u \\ n \end{bmatrix}$ and $b_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Then $N(b_1)$ can be arbitrarily larger than $N(b_2)$ so $[b_1, b_2]$ does not fit the Lovatz condition in [LPMSW19].

On the other hand, $B(b_1, b_1) = l+1$ and $B(b_2, b_1) = \theta(u)$, hence $N_{K/\mathbb{Q}}\left(\frac{B(b_2,b_1)}{B(b_1,b_1)}\right) = 1/(l+1)^2 < \mathfrak{M}(K)$ (Size reduceness condition) and $B(b_2, b_2) = 1$ so for $A > n+1$, the Lovasz condition of [KL17] is satified. Therefore the basis $[b_1, b_2]$ is reduced in the sense of [KL17].

References

[BRL20] Olivier Bernard and Adeline Roux-Langlois. Twisted-phs: Using the product formula to solve approx-svp in ideal lattices. page 53, 2020. 1

[CDPR16] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. *Recovering Short Generators of Principal Ideals in Cyclotomic Rings*, volume 9666 of *Lecture Notes in Computer Science*, page 559–585. Springer Berlin Heidelberg, 2016. 4

[CDW17] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to ideal-svp. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017*, Lecture Notes in Computer Science, page 324–348. Springer International Publishing, 2017. 1

[Coh96] Henri Cohen. *A course in computational algebraic number theory*. Graduate texts in mathematics. Springer, 3rd, corr. print edition, 1996. 2, 3

[Coh00] Henri Cohen. *Advanced Topics in Computional Number Theory*, volume 193 of *Graduate Texts in Mathematics*. Springer New York, 2000. 5

[CS88] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups*, volume 290 of *Grundlehren der mathematischen Wissenschaften*. Springer New York, 1988. 3

[CSD17] Information Technology Laboratory Computer Security Division. Post-quantum cryptography — csrc — csrc, Jan 2017. 1

[CSD20] Information Technology Laboratory Computer Security Division. Round 3 submissions - post-quantum cryptography — csrc — csrc, 2020. 1

[FP96] C. Fieker and M. E. Pohst. *On lattices over number fields*, volume 1122 of *Lecture Notes in Computer Science*, page 133–139. Springer Berlin Heidelberg, 1996. 1

[Gal12] Steven D. Galbraith. *Mathematics of Public Key Cryptography.* Cambridge University Press, 2012. 1

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st annual ACM symposium on Symposium on theory of computing - STOC '09*, page 169, Bethesda, MD, USA, 2009. ACM Press. 1

[GVW15] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. *Journal of the ACM*, 62(6):45:1–45:33, Dec 2015. 1

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. Ntru: A ring-based public key cryptosystem. In Joe P. Buhler, editor, *Algorithmic Number Theory*, Lecture Notes in Computer Science, page 267–288. Springer, 1998. 1

[KL17] Taechan Kim and Changmin Lee. Lattice reductions over euclidean rings with applications to cryptanalysis. In Máire O'Neill, editor, *Cryptography and Coding*, Lecture Notes in Computer Science, page 371–391. Springer International Publishing, 2017. 1, 2, 13, 14, 15

[Lez12] Pierre Lezowski. *Questions d'euclidianité.* PhD thesis, Université Bordeaux, 2012. 7, 8, 11

[LLL82] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, Dec 1982. 1, 2

[LPMSW19] Changmin Lee, Alice Pellet-Mary, Damien Stehlé, and Alexandre Wallet. *An LLL Algorithm for Module Lattices*, volume 11922 of *Lecture Notes in Computer Science*, page 59–90. Springer International Publishing, 2019. 1, 2, 3, 5, 6, 7, 14, 15

[MSD20] Tamalika Mukherjee and Noah Stephens-Davidowitz. *Lattice Reduction for Modules, or How to Reduce ModuleSVP to ModuleSVP*, volume 12171 of *Lecture Notes in Computer Science*, page 213–242. Springer International Publishing, 2020. 1

[PMHS19] Alice Pellet-Mary, Guillaume Hanrot, and Damien Stehlé. Approx-svp in ideal lattices with preprocessing. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, Lecture Notes in Computer Science, page 685–716. Springer International Publishing, 2019. 1

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. page 37, 2005. 1

[Reg10] Oded Regev. *Learning with Errors over Rings*, volume 6197 of *Lecture Notes in Computer Science*, page 3–3. Springer Berlin Heidelberg, 2010. 1

[Sho94] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, page 124–134. IEEE Comput. Soc. Press, 1994. 1