ON HERMITIAN DECOMPOSITION LATTICES AND THE MODULE-LIP PROBLEM IN RANK 2

• • •

THOMAS ESPITAU* AND HEORHII PLIATSOK*

Abstract. In this short note, we introduce a specific class of rank two lattices over CM fields endowed with additional symmetries, which are involved in the decomposition of algebraic integers in Hermitian squares. As an application, we show an elementary reduction from the module-LIP problem in rank 2 over a CM or totally real number field to the finding of a square basis in such lattices.

1. Introduction

One of the most famous results in elementary number theory is Fermat's two-square theorem.

Theorem (Fermat, 1640)**.** *An odd prime p is a sum of two integral squares if and only if it is congruent to 1 modulo 4.*

While its initial proof is purely arithmetic and relies on the elegant idea of infinite descent, a more geometric proof relying on Minkowski's first theorem briefly states as follows:

The direct implication is clear from modular arithmetic, so let choose p to be a prime congruent to 1 modulo 4, so that -1 is a square modulo p; hence, there exists an integer u such that $-1 \equiv u^2 \mod p$. Consider the plane lattice $\Lambda_u = \begin{pmatrix} 1 & 0 \\ u & p \end{pmatrix} \mathbb{Z}^2$. It has covolume p, so that by Minkowski's first theorem, there exists a non-zero lattice vector x with (squared) norm smaller than $\frac{4}{3}\mathit{vol}(\Lambda_u) = \frac{4p}{3}$. However, the squared norm of any element in Λ_u must be divisible by p, implying that $\|x\|^2 = p$. By construction, this norm is a sum of squared integers.

From this seemingly simple proof, we can make a few observations:

- The lattice Λ_u is cocyclic, i.e. of the form $\{x, y \in \mathbb{Z}^2 \mid xu \equiv y \pmod p\}$.

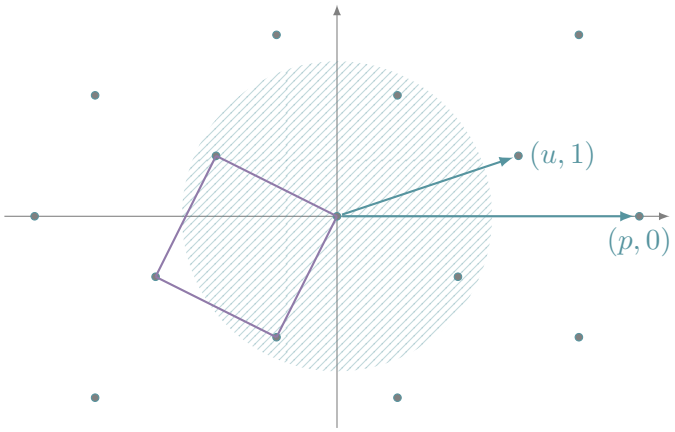

FIGURE 1. Example of the lattice obtained for $p = 5$, with $u = 2$. The hatched disk is the Minkowski bound. Note that the lattice Λ_u is a rotation/scaling of $\mathbb{Z}^2$, the square of minimal vectors being highlighted.

- Since $u^2 \equiv -1 \pmod{p}$, then Λ_u is stable under the symmetry $(x, y) \mapsto (-y, x)$, which is of order 4, indeed, for $ux \equiv y$, we find by multiplying by u on both sides $-x \equiv uy$, i.e. $(-y, x) \in \mathcal{L}_u$.
- Thus, taking (a, b) to be the shortest element of this lattice, which norm is $a^2 + b^2 = p$, the sublattice $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mathbb{Z}^2$ has a covolume p by determinant computation, meaning this matrix is actually a basis of Λ_u. This means that the lattice Λ_u is *isometric* to $\sqrt{p}\mathbb{Z}^2$.

See Figure 1 for a small exemple, where we can observe the square structure of the lattice Λ_u and the ball of radius being Minkowski's bound.

In this note, we propose to study some algebraic generalizations of such lattices. They arise naturally in study of two-squares decomposition over a totally real number field and more importantly in *hermitian squares* decomposition over the maximal order of a CM field— i.e. decomposing an element as $\alpha\bar{\alpha} + \beta\bar{\beta}$ for some algebraic integer α and β.

We introduce lattices playing the same role as the Λ_u in the proof of Fermat's theorem. Their geometry is now more subtle, but we still retrieve some interesting properties. In particular, these lattices—now modules of rank two in the CM field—exhibit an exceptional symmetry of order 4, namely $(x, y) \mapsto (-\bar{y}, \bar{x})$. We discuss further the algorithmic reduction of such lattices, and, in particular, show that in the totally real case, we can rely on a method of Lenstra and Silverberg [9] to retrieve the shortest vectors in deterministic polynomial time.

As an application of this preliminary work, we show a perhaps surprising Cook reduction between the so-called module-LIP ([11]) problem over CM fields and the problem of finding short vectors in these highly symmetric lattices coming from decompositions. Informally, this problem aims at recovering a (secret) basis of a (public) lattice of prescribed (public) Gram-matrix. We can state this reduction as:

Theorem. *There exists a Cook reduction from the ($\mathcal{O}_k^2$-)module-LIP over CM field problem to a shortest vector problem on a rank two lattice with explicit symmetry group, with exactly one call to the latter oracle.*

We extend this result to any free modules over k, at the cost of requiring a mild randomization.

Theorem. *There exists a probabilistic polynomial time reduction — in the input data, the log-discriminant of k and the residue at 1 of the zeta function of k^+— from the (free-)module-LIP over CM field problem to a shortest vector problem on a rank two lattice with explicit symmetry group, with exactly one call to the latter oracle.*

For a totally real field, these results readily give a deterministic polynomial time algorithm for this problem, simplifying the approach of [11]: there exists a deterministic polynomial time algorithm for $\mathcal{O}_k^2$-module-LIP over totally real fields.

2. On hermitian decomposition lattices

2.0.1. Let us fix a CM-field or a totally real field k of absolute degree d and k^+ its maximal totally real subfield. We will denote by $\mathcal{O}_k$ and $\mathcal{O}_{k^+}$ their respective rings of integers—k^+ classically being k itself when totally real. The cone of totally positive element is denoted by k^{++}. The complex conjugation of k is denoted by $\bar{\cdot}$—being the identity map in the totally real case. We write $k_{\mathbf{R}}$ for the scalar extension $k \otimes_{\mathbf{Q}} \mathbf{R}$. We write Δ_k for its discriminant.

2.0.2. We say that a $k_{\mathbf{R}}$-bilinear form $g : k_{\mathbf{R}}^n \times k_{\mathbf{R}}^n \to k_{\mathbf{R}}$ is non-degenerate when $g(x, x) = 0$ if and only if $x = 0$, and is positive definite if $g(x, x) \in k_{\mathbf{R}}^{++}$ for all $x \in k_{\mathbf{R}}^n \setminus \{0\}$. Mildly abusing terminology, an *hermitian form* is a non-degenerate positive definite $k_{\mathbf{R}}$-bilinear form g which is hermitian with respect to the involution, that is: $g(x, y) = \overline{g(y, x)}$ for any $x, y \in k_{\mathbf{R}}$. We will focus on the *standard* form $(x, y) \mapsto x_1\bar{y_1} + x_2\bar{y_2}$ and generically denote the corresponding k-norm $\|(x_1, y_1)\|_k^2 = x_1\bar{x_1} + x_2\bar{x_2}$. In the following, we will always see lattices as projective

modules embedded in $k_{\mathbf{R}}^n$ for some rank n, so their Hermitian form is—unless explicitly stated otherwise—the standard form.

For a complete reference on algebraic number theory and its related algorithms, we let the reader refer to [5, Chapter 4-6] and [1].

2.1. **Hermitian decomposition in squares and lattices.**

2.1.1. We are interested in the decomposition of a totally real positive element into a sum of two Hermitian squares, in the following sense.

Definition 2.1. *Let $g \in \mathcal{O}_{k^+}$, we say that g admits an* Hermitian decomposition in two squares *if there exists $(\alpha, \beta) \in \mathcal{O}_k^2$ such that $g = \alpha\overline{\alpha} + \beta\overline{\beta}$. This decomposition is* primitive *if in addition, $\alpha\mathcal{O}_k + \beta\mathcal{O}_k = \mathcal{O}_k$.*

When k is totally real, this corresponds verbatim to a decomposition in two integral squares.

2.1.2. Analogously to the importance of the root of -1 modulo a prime in Fermat's theorem, we introduce the following class of integers for studying Hermitian decompositions modulo g.

Definition 2.2. *For a totally positive element $g \in \mathcal{O}_{k^+}$, we say that an element $u \in \mathcal{O}_k$ is an* Hermitian root of -1 modulo g *if $u\bar{u} = -1 \pmod{g}$.*

Further, we will refer to u simply as a *root* when there is no possible ambiguity; notice that this is a (square)-root of -1 for totally real fields.

Note that such elements are usually far from being unique in the CM case. Indeed, their cardinality is controlled by a simple product of curves of degree 2 in residue fields.

Lemma 2.1. *Let $\beta \in \mathcal{O}_k$ be a totally negative element such that $k \cong k^+[x]/(x^2 - \beta)$. Consider the decomposition of the ideal $g\mathcal{O}_k$ into prime factors $g\mathcal{O}_k = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ and assume that $\mathfrak{p}_i \neq \mathfrak{p}_j$ for $i \neq j$. Then the number of Hermitian roots modulo g is exactly $\prod_{i=1}^{s} |\mathcal{C}_{\beta^2}(\mathcal{O}_k/\mathfrak{p}_i)|$, where for $\mathbb{F}$ being a finite field of characteristic p and an element $a \in \mathbb{F}$, we define the following curve:*

$$\mathcal{C}_a(\mathbb{F}) := \{(x, y) \in \mathbb{F}^2 | x^2 + ay^2 = -1\}$$

Proof. By the Chinese Remainder Theorem, we decompose the residue field at g as $\mathcal{O}_k/g \cong \mathcal{O}_k/\mathfrak{p}_1 ... \mathcal{O}_k/\mathfrak{p}_s$. We see that there is a bijection between the set of Hermitian roots of -1 modulo g and the elements of form $(u_1, ..., u_s) \in \mathcal{O}_k/\mathfrak{p}_1 ... \mathcal{O}_k/\mathfrak{p}_s$ such that every u_i is an Hermitian root modulo $\mathfrak{p}_i$. Consequently, it is enough to find the number of Hermitian roots in the ring

of the form $\mathcal{O}_k/\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_k$. Note that $\mathcal{O}_k/\mathfrak{p}$ is a finite field and that $u\overline{u} = (x+\beta y)(x-\beta y) = x^2+\beta^2 y^2 = -1 \pmod g$ defines a bijection between the set of Hermitian roots modulo $\mathfrak{p}$ and $\mathcal{C}_\beta(\mathcal{O}_k/\mathfrak{p})$. ::

As a byproduct, this means that we can assert the existence of such root as a product of Hilbert symbols an Hermitian root of -1 modulo g exists if and only if $\prod_{i=1}^{s}(\beta^2,-1)_{\mathcal{O}_k/\mathfrak{p}_i}$.

Exemple. *In the case when $k = \mathbb{Q}(i)$; $\mathcal{O}_k = \mathbb{Z}[i]$ and $g = p$ is a prime number, by Gauss summation technique, the curve $\mathcal{C}_1(\mathbb{F}_p)$ has exactly $p - \left(\frac{-1}{p}\right)$ points.*

2.1.3. We now introduce our main geometric object of interest.

Definition 2.3. *For a totally positive element $g \in \mathcal{O}_{k^+}$ and an Hermitian root u modulo g, the (g-)*Hermitian decomposition lattice *at root u is the cocyclic lattice consisting of vectors mod g-orthogonal to u in $\mathcal{O}_k^2$, that is to say*

$$\Lambda_u := \left\{(\alpha,\beta) \in \mathcal{O}_k^2 \,|\, u\alpha \equiv \beta \pmod g\right\}$$

Remark. *We can slightly generalize this definition to define the lattice as*

$$\Lambda_{u,v} := \left\{(\alpha,\beta) \in \mathcal{O}_k^2 \,|\, u\alpha \equiv v\beta \pmod g\right\},$$

for some u, v such that $u\bar{u} \equiv -v\bar{v} \pmod g$—which is equivalent when u or v is inversible $\pmod g$, as their quotient is an Hermitian root of -1. In the general case, this does not change the rest of the following discussion and especially their algorithmic reduction properties, as these lattices will have exactly *the same symmetries as the standard decomposition lattices. As such, we stick to this definition for the sake of clarity of exposition.*

As a cocyclic lattice modulo g, this lattice is of determinant $g\mathcal{O}_k$ and a simple basis, in Hermite Normal Form over $\mathcal{O}_k$, is given as the columns of the matrix $\begin{pmatrix} 1 & 0 \\ u & g \end{pmatrix}$. Indeed, fix $(\theta,\rho) \in \Lambda_u$. As by definition $u\theta = \rho \pmod g$, there exists $\delta \in \mathcal{O}_k$ such that $\rho = u\theta + g\delta$. Therefore $(\theta,\rho) = (\theta, u\theta+g\delta) = \delta(0,g) + \theta(1,u)$ and we conclude by equality of determinants.

2.1.4. Note that an Hermitian decomposition lattice possesses a nontrivial automorphism, called *conjugate rotation* given by $\sigma : \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \longrightarrow \begin{pmatrix}-\overline{\beta}\\ \overline{\alpha}\end{pmatrix}$. Indeed, for any $(\alpha,\beta) \in \Lambda_u$, we have $u\alpha \equiv \beta \pmod g$, so that $\bar{u}\bar{\alpha} \equiv \bar{\beta}$ and so by multiplying by $-u$ on both sides: $-\bar{\beta}u \equiv -u\bar{u}\bar{\alpha} \equiv \alpha \pmod g$ —the conjugation action being compatible with the projection modulo g as g is totally

real. Remark that for any $x \in k^2$, $\sigma(u)$ is k-orthogonal to u for the standard Hermitian form $\langle x, y\rangle = x^T \bar{y}$.

2.1.5. We say that an Hermitian decomposition lattice admits a *square basis* if there exists a vector $x = (\alpha, \beta) \in \Lambda_u$ such that $(x, \sigma(x))$ is a basis of Λ_u, that is:

$$\Lambda_u = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mathcal{O}_k \perp \begin{pmatrix} -\overline{\beta} \\ \overline{\alpha} \end{pmatrix} \mathcal{O}_k.$$

These bases link the decomposition lattices and the Hermitian decompositions in the following sense:

Lemma 2.2. *If an Hermitian decomposition lattice Λ_u admits a square basis given by vector (α, β) then g admits an Hermitian decomposition $g = \alpha\overline{\alpha} + \beta\overline{\beta}$.*

Proof. As being a basis of the decomposition lattice, we have $g\mathcal{O}_k = \det(\Lambda_u) = (\alpha\overline{\alpha} + \beta\overline{\beta})\mathcal{O}_k$. ::

Remark that when a decomposition lattice admits a square basis, then the conjugate lattice $\overline{\Lambda_u} = \{\alpha, \beta \in \mathcal{O}_k \,|\, \bar{\alpha}u \equiv \bar{\beta} \pmod g\} = \{\alpha, \beta \in \mathcal{O}_k \,|\, \alpha\bar{u} \equiv \beta \pmod g\} = \Lambda_{\bar{u}}$ also admits a square basis. We conjecture that this result is far more general and that all decomposition lattices are isometric (this is trivially the case when they admit a square basis):

Conjecture 1. *Let k be a CM field, $g \in \mathcal{O}_{k^+}$ and u, v two Hermitian roots of -1 modulo g, then $\Lambda_u \cong \Lambda_v$.*

Remark. *This conjecture is true when k is totally real and g is a prime. Indeed, in this case, being a Hermitian root of -1 modulo g is just being a square root in the residue field $\mathcal{O}_k/(g)$, so that there are only two such elements in the field, say u and $-u$. Hence, there are only two different latices, $\Lambda_{\pm u}$, and the isometry between the two is given by the linear transformation $(x, y) \mapsto (x, -y)$.*

The converse result of Lemma 2.2, i.e. that every decomposition lattice gives rise to a square basis is a natural but (apparently) complex question. It is the case over the integers and over the Gaussian integers for instance, but we were unable to (dis)prove it for general CM fields. A possible obstruction comes from the gap between the length of the second vector of a reduced basis and the shortest length in the lattice. More precisely, if we take $x = (\alpha, \beta)$ to be the shortest vector of Λ_u, then by action of the conjugate rotation, $(x, \sigma(x))$ is a basis of a *sublattice* X of Λ_u, so that its determinant is *only* a multiple of $\det(\Lambda_u)$. It is tempting to think that since x is one of

the shortest vectors of Λ_u, any basis of the form (x, y) for y having a larger norm should be itself a sublattice of X. For "small" enough number rings (for instance the Gaussian integers or rings of integers of cyclotomics of small conductor) we can indeed conclude, thanks to Minkowski's first theorem. We quantify this smallness by the following generalized Hermite constant (also called multiplicative Icaza-Humbert constant, from [8]), defined as:

$$\gamma(k, n) := \sup_{\mathcal{L}} \min_{x \in \mathcal{L}} N(\|x\|_k^2)^{\frac{1}{n}}$$

where X varies in the moduli space of $\mathcal{O}_k$-lattices of unit determinant and $\|\cdot\|$ is the norm of k^+—in this formalism we recover a $\mathbf{Z}$ lattice by pushforward as taking the Euclidean norm as the composition of $\|.\|_k^2$ by the absolute trace of k.

Proposition 2.1. *Suppose that the generalized Hermite constant $\gamma(k, 2)$ is* strictly *smaller than 2, then any decomposition lattice over k admits a square basis.*

Proof. Let k be such a CM field, write d for its degree and take Λ_u a decomposition lattice for $g \in \mathcal{O}_{k^+}$. Then, taking $x = (\alpha, \beta)$ as a shortest vector, and writing X the sublattice spanned by x and $\sigma(x)$, we have that $\det(X)$ must be a multiple of g. But by orthogonality of x and $\sigma(x)$, $\det(X) = (\alpha\bar{\alpha} + \beta\bar{\beta})$, so that by taking norms of their generators, we have $\frac{N(\alpha\bar{\alpha}+\beta\bar{\beta})}{N(g)} \in \mathbf{N}$. But by definition of generalized Hermite constant, we find: $N(\alpha\bar{\alpha} + \beta\bar{\beta}) \leqslant \gamma(k, 2)N(g)$, so that the ratio $\frac{N(\alpha\bar{\alpha}+\beta\bar{\beta})}{N(g)}$ must be equal to 1. ∷

Remark. *The proposition's hypothesis applies for instance to:*

- $\mathbf{Z}$*: this recovers the geometric proof of Fermat's two square theorem.*
- $\mathbf{Z}[i]$*: this is the complex analog of Fermat's two squares theorem. As a byproduct, it gives a very intuitive proof of Lagrange's four-squares theorem (as decomposing each Hermitian factor $x\bar{x}$ in a sum of two squares itself).*

2.2. **Effective Reduction of Decomposition Lattices.**

2.2.1. Assume that a given decomposition lattice Λ_u admits a square basis. To find the corresponding Hermitian decomposition, we need to explicitly determine this basis. This is an instance of the so-called module-svp problem for a very particular kind of rank 2 lattice over $\mathcal{O}_k$, endowed with the conjugate rotation. Computationally speaking, we always assume that the ring of integers of k and k^+ has been computed and is polynomially represented, so that computations in the field, ring of integers and with ideals are polynomial time—see for instance [1] for a survey on standard representation techniques.

2.2.2. *Using Pushforward to* $\mathbf{Z}$. We can always forget about the additional structure and look at the decomposition lattice $\mathcal{L}_u$ as a $\mathbf{Z}$-lattice. Thereof, we both forget its symmetry σ and the algebraic structure coming as $\mathcal{O}_k$-module. Solving the shortest vector problem in such a lattice would have complexity $O(2^{2d}\text{Poly}(d, B, \log \Delta_k))$ where d is the absolute degree of k and B is a bound on the bit representation of the elements g, u and on the ring of integers of k.

In the special case where k is a power-of-two cyclotomic—i.e. such that the $\mathbf{Z}$-lattice corresponding to the order $\mathcal{O}_k$ for the canonical embedding is hypercubic— a better solution is possible. Because a square basis of a decomposition lattice is k-orthogonal, the pushforward of this basis over the integers $\mathbf{Z}$ is an orthogonal basis, i.e., the corresponding $\mathbf{Z}$-lattice is *hypercubic*. From the results of [2]—using basis reduction—and [6]—using Gaussian sampling, we know that the time complexity of recovering an orthogonal basis in such a lattice is $2^{\frac{n}{2}+o(1)}\text{Poly}(n, B)$, where n is the rank and B is an absolute bound on the bit representation of the lattice. In our setting, this amounts to recovering the square basis in time $O(2^d\text{Poly}(d, B, \log \Delta_k))$ the field we are working in.

2.2.3. *Applying the Lenstra-Silverberg Framework.* When k is totally real, we can rely on a much more powerful technique, introduced by Gentry and Szydlo in [7] and generalized by Lenstra and Silverberg [10]. However, we will see that this framework fails very shortly to work on all CM fields.

Recall that a CM-order is a $\mathbf{Z}$-order A such that:

(1) it has no non-zero nilpotent elements;
(2) it is equipped with an automorphism $\bar{\cdot}$ commuting with all morphisms from A to $\mathbf{C}$.

The so-called *standard* A-lattice is the $A-$module endowed with the Euclidean form $\text{Tr}_A(x\bar{x})$. The main theorem of [10] is as follows, where an A-lattice is a $\mathbf{Z}$-module $\mathcal{L}$ with an A-module structure such that the inner product of $\mathcal{L}$ satisfies $\langle ax, y\rangle = \langle x, \bar{a}y\rangle$.

Theorem 2.1. *There is a deterministic polynomial-time algorithm that, given a CM-order A and an A-lattice $\mathcal{L}$, decides whether or not $\mathcal{L}$ is A-isomorphic with the standard A-lattice, and if so, computes such an A-isomorphism.*

Let us now try to realize Λ_u as some rank 1 A-lattice for a good ring A. First, note that the rotation σ is naturally of order 4 as $\sigma \circ \sigma = -\text{Id}$, giving decomposition lattices a *complex structure*. This is a *complex structure* on the module. As such, following [9], it seems natural to

construct the *modified* group ring $A = \mathcal{O}_k[\iota]/(\iota^2 = -1)$, and write the square basis $\begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix}$ as the element $\alpha + \iota\beta$. As the complex embeddings of the ring are of the form[1] $x + \iota y \mapsto \varphi(x) \pm \varphi(y)$ for $\varphi : \mathcal{O}_k \mapsto \mathbf{C}$ it is straightforward to check that A is a CM-order for the linear extension of the conjugation of $\mathcal{O}_k$ with $\bar{\iota} = -\iota$.

Remark. *When k is a totally real field, this corresponds exactly to giving a complex structure on k^2, and the matrix $\begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$ is a linear representation of the complex number $\alpha + i\beta$ in $M_{2,2}(k)$.*

We have the following norm compatibility between the norm on Λ_u and the standard norm of A.

$$\forall x = (\alpha, \beta) \in \Lambda_u, \|x\|_{\mathbf{Z}}^2 = \mathrm{Tr}_k(\alpha\bar{\alpha} + \beta\bar{\beta}) = \mathrm{Tr}_A\Big((\alpha + \iota\beta)\overline{(\alpha + \iota\beta)}\Big). \tag{1}$$

From this observation, we now want to realize Λ_u as a rank 1 A-module. Given a generic element $t + \sigma r \in A$, we have $(t + \iota r) \cdot (\alpha + \iota\beta) = (t\alpha - r\beta) + \iota(r\alpha + t\beta)$, with $u\alpha \equiv \beta \pmod{g}$.

2.2.4. Hence, when k is totally real we have

$$u(t\alpha - r\beta) \equiv t(u\alpha) - r(u\beta) \equiv t\beta - r\alpha \pmod{g}.$$

Indeed, we have the additional relation $-\beta u \equiv \alpha \pmod{g}$ from multiplying by u the relation $\alpha u \equiv \beta \pmod{g}$. As such Λ_u is a A lattice of rank 1 and can be seen as an ideal lattice of A. By definition of A, we have $\Lambda_u \otimes_A \overline{\Lambda_u} \equiv \Lambda_u \cdot \overline{\Lambda_u} = g^2 A$, so that $\frac{1}{g}\Lambda_u$ is isometric to the standard A lattice. In addition a polynomial representation of a $\mathbf{Z}$-basis of the CM order A can be computed in polynomial time as quadratic extension of the order $\mathcal{O}_k$, which we assumed to be polynomially represented (for instance, by relying on [3] in the relative quadratic case). Putting all together with the Lenstra-Silverberg theorem, we find:

Theorem 2.2. *For any totally real field k, any totally positive element g and u a root of -1 modulo g, such that the decomposition lattice Λ_u of g admits a square basis, there exists a deterministic polynomial time algorithm—in the input basis representation and log discriminant of k—computing a square basis of Λ_u.*

[1] By classical ring theory, there are exactly $2[k : \mathbf{Q}]$ such morphisms and we exhibit such number of them. It is indeed clear that each of the $(\varphi \pm \varphi)_\varphi$ are distinct by evaluation.

2.2.5. However, when k is a CM-field, we do not have this extra relation and we can only write the following modular equality:

$$u(t\alpha - r\beta) \equiv t(u\alpha) - r(u\beta) \equiv t\beta - r\alpha \pmod{g},$$

forbidding the identification as an A-module. We are *very close* to being in the setting of a lattice of a CM-order, described by Lenstra and Silverberg but not quite there. To get a proper A-module structure, it is tempting to modify the multiplication law of A to be

$$(t + \iota r) \cdot (\alpha + \iota\beta) = (t + \iota r)(\overline{\alpha} + \iota\overline{\beta}) \tag{2}$$

but this action is non-commutative, excluding us from the CM-order framework.

The main obstruction in this construction essentially lies in the observation that conjugation and conjugate rotation do not commute. Writing explicitly the action of these maps in k^2 reveals that the group they span is exactly D_8, the dihedral group formed as the semi-direct product of $\mathbf{Z}/4\mathbf{Z}$ (spanned by the conjugate rotation) and $\mathbf{Z}/2\mathbf{Z}$ (the conjugation) [2]. Hence, pushing forward to the integers, we find that the decomposition lattices are $\mathbf{Z}[D_{2d}]$ group rings. To fall back into the framework of [10] and [9], we would need to find a *non-commutative* variant of these algorithms. An alternative insight is that the ring A would lie in the *cyclic algebra* $(-1,-1)_{-1} = k[\zeta,\iota]/(\zeta^2 = -1, \iota^2 = -1, \zeta\iota = (-1)\iota\zeta)$, i.e. would correspond to a quaternion order over k^+. In the vein of the Gentry-Szydlo algorithm, this would correspond to finding a generator of a quaternionic ideal knowing its reduced norm. Finding such a non commutative Gentry-Szydlo algorithm or a dihedral Lenstra-Silverberg algorithm seems to be the two faces of the same coin, and we let understanding the interplay between these two approaches as a future exciting open problem[3].

3. A reduction of module-LIP

As an application of these objects, we show a reduction from the module-LIP problem in rank 2 to the computation of an Hermitian decomposition in squares with prescribed hermitian root, or equivalently to the reduction of a given decomposition lattice.

[2] A quick geometric consideration reveals that this is no surprise: the conjugate rotation acts as a "rotation" of angle $\pi/2$ in k^2 and the conjugation is a reflection orthogonal to σ^2. This is the textbook geometric definition of the dihedral group of order 8.

[3] It appears that Chevignard et al. reached similar conclusions starting from the Gentry-Szydlo viewpoint [4].

3.1. **On the module-LIP problem.** Following the work of [11], we first reproduce the definition of the so called module-lip.

Definition 3.1 (wcsMLIP). *For B a pseudo-basis of a module-lattice $M \subset k_{\mathbf{R}}^{\ell}$ with associated pseudo-Gram matrix $\mathbf{G}$, the worst-case search module-Lattice Isomorphism Problem with parameter k and B denoted by wcsMLIP$_k(B)$ is, given as input any pseudo-Gram matrix $\mathbf{G}' \sim \mathbf{G}$, to find a congruence matrix between $\mathbf{G}$ and $\mathbf{G}'$.*

We detail how to deal with the free case of this problem, as it carries all the geometric insight and main ideas of the reduction. Handling the ideals (i.e. pseudo bases) appearing in the projective case is more of a technicality and does not seem to be of interest in the global understanding of the problem. It is an *arithmetic* complication, but not a geometric one. See Section 3.3.3 for a discussion on this point. In the following, we will refer to the problem as free-module-LIP.

3.2. **Exploiting the complex structure and symplecticity: a reduction to the hermitian decomposition.**

3.2.1. We can readily see that when B is the identity matrix, the module-LIP problem boils down to recovering the integral factorization of a (pseudo) Gram-matrix $\mathbf{G}$ into $\mathbf{A}^T\overline{\mathbf{A}}$, knowing the lattice $\mathbf{A}\cdot\mathcal{O}_k^2$ is $\mathcal{O}_k^2$ itself. Thus in the following, let us denote this (Secret) matrix by $A \in \mathcal{O}_k^{2\times 2}$ and the (public)key Gram matrix by G, with named coefficients as:

$$A := \begin{pmatrix} \alpha & \theta \\ \beta & \rho \end{pmatrix}, \qquad G := \begin{pmatrix} g_{00} & g_{10} \\ g_{01} & g_{11} \end{pmatrix}$$

3.2.2. Our reduction is elementary and geometric. We exploit the fact that thanks to the Gram-Schmidt orthogonalization process, we can decompose any basis in the decomposition lattice attached to *only* its first vector. This is an avatar of the fact that a unimodular rank 2 module is necessarily *symplectic* for the determinant form, and as such we can fully describe it using a single primitive vector [4].

[4]From this perspective it is quite natural to interpret this result from the decomposition theory of hermitian forms. Recall that given an hermitian form h over a real vector space V with complex structure J gives rise to a symplectic form $\omega = -\mathrm{Im}(h)$ and a symmetric bilinear form $g = -\mathrm{Re}(h)$, related by $\omega(x, y) = g(J(x), y)$. In dimension 2, there is a unique symplectic structure up to scaling, the determinant form. We can see that for h being the standard hermitian form and ω being the determinant, J will correspond to the conjugate rotation introduced earlier. Hence it is no surprise that this symmetry will play a pivotal role thanks to the sympleciticity of rank 2 modules of determinant 1.

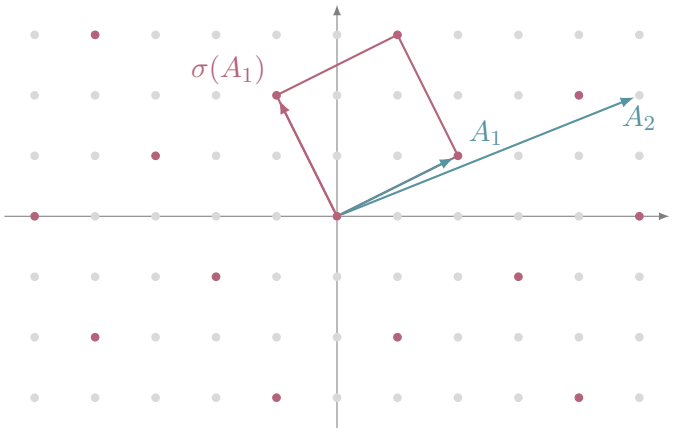

FIGURE 2. An example of the reduction for the matrix $A = \begin{pmatrix} 2 & 5 \\ 1 & 2 \end{pmatrix}$ spanning $\mathbf{Z}^2$. The corresponding Gram matrix is $\begin{pmatrix} 5 & 12 \\ 12 & 29 \end{pmatrix}$ and the corresponding decomposition lattice Λ_2 with its square basis $(A_1, \sigma(A_1))$

3.2.3. Let us make this intuition formal. The vectors $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ and $\begin{pmatrix} -\overline{\beta} \\ \overline{\alpha} \end{pmatrix}$ form an orthogonal basis of the vector space k^2 for the standard Hermitian product.

Let us denote by (x, y) the coordinates of the vector $\begin{pmatrix} \theta \\ \rho \end{pmatrix}$ in this basis, that is:

$$\begin{pmatrix} \theta \\ \rho \end{pmatrix} = x \begin{pmatrix} \alpha \\ \beta \end{pmatrix} + y \begin{pmatrix} -\overline{\beta} \\ \overline{\alpha} \end{pmatrix}$$

Taking inner product with the vector $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ on the left-hand side and the right-hand side gives:

$$\theta\overline{\alpha} + \rho\overline{\beta} = \left\langle \begin{pmatrix} \theta \\ \rho \end{pmatrix}, \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \right\rangle = \left\langle x \begin{pmatrix} \alpha \\ \beta \end{pmatrix} + y \begin{pmatrix} -\bar{\beta} \\ \bar{\alpha} \end{pmatrix}, \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \right\rangle = x(\alpha\overline{\alpha} + \beta\overline{\beta})$$

By definition, $\theta\overline{\alpha} + \rho\overline{\beta} = g_{10}$ and $\alpha\overline{\alpha} + \beta\overline{\beta} = g_{00}$, we must have $x = \frac{g_{10}}{g_{00}}$. Moreover, remark that by bilinearity of the (matrix) determinant, we must have $y = \frac{1}{g_{00}}$, since:

$$1 = \det \begin{pmatrix} \alpha & \theta \\ \beta & \rho \end{pmatrix} = y \det \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} = g_{00}$$

As such, we obtained the following matrix decomposition, using the fact that the dual basis of $\begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}$ is exactly $\frac{1}{g_{00}} \begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix}$:

$$\begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix} \begin{pmatrix} \alpha & \theta \\ \beta & \rho \end{pmatrix} = \begin{pmatrix} 1 & \frac{g_{10}}{g_{00}} \\ 0 & g_{00} \end{pmatrix} \tag{3}$$

This now entails the preliminary remark we made: it is enough to find only (α, β) in order to fully recover the full matrix A as there is a simple linear relation given by public data derived from g.

Since the lattice spanned by A is $\mathcal{O}_k$, transposing Equation (3) and passing to a module equality over $\mathcal{O}_k^2$ gives:

$$\begin{pmatrix} 1 & 0 \\ -g_{10}^* & g_{00} \end{pmatrix} \mathcal{O}_k^2 = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix} \mathcal{O}_k^2$$

As such, $\begin{pmatrix} 1 & 0 \\ -g_{10}^* & g_{00} \end{pmatrix} \mathcal{O}_k^2$ is exactly the Hermitian decomposition lattice for the element $g_{00} \in \mathcal{O}_{k^+}$ with Hermitian root modulo g_{00} being $u := -g_{10}^*$. Indeed, as $\det(G) = \det(A)\det(A)^* = 1$ one obtains $g_{00}g_{11} - g_{10}g_{10}^* = 1$. Taking the equation modulo g_{00} shows that $-g_{10}^*$ is indeed an Hermitian root. Note that as this Hermitian decomposition lattice admits a square basis, by construction, and falls back to Section 2.2. We illustrate an example over $k = \mathbf{Q}$ in Figure 2.

3.2.4. Now that we understand the geometry of the problem and we identify that the full information is contained in a *single* Hermitian decomposition problem, we can state our reduction and prove it in a very elementary way, at the cost of losing all of the geometric insight.

Theorem 3.1. *There exists a Cook reduction from the $\mathcal{O}_k^2$-*module-LIP *problem to a shortest vector problem on an Hermitian decomposition lattice with square basis, with exactly* one *call to the latter oracle.*

Proof. Let $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ being the first vector for the basis A and write:

$$\begin{aligned} -\alpha\overline{g_{01}} &\equiv -\alpha\bar{\alpha}\gamma + \alpha\bar{\beta}\delta \pmod{g_{00}} \\ &\equiv -\beta\bar{\beta}\gamma + \alpha\bar{\beta}\delta \pmod{g_{00}} \\ &\equiv -\bar{\beta}\underbrace{(\alpha\delta - \beta\gamma)}_{=\det(A)=1} \pmod{g_{00}} \end{aligned}$$

This defines an decomposition lattice Λ, defined by the public elements g_{00} and g_{01}. We can explicit its Hermite Normal form and call the oracle on it to recover its square basis. We then retrieve the remaining column of A by elementary linear algebra, as stated in Equation (3). All in all, this gives the following reduction:

(1) Parse the input G as $\begin{pmatrix} g_{00} & g_{01} \\ g_{10} & g_{11} \end{pmatrix}$
(2) Construct the basis $T = \begin{pmatrix} 1 & 0 \\ -\overline{g_{01}} & g_{00} \end{pmatrix}$
(3) Call the reduction oracle on the lattice spanned by the column of T and write (α, β) for the first column of its output.
(4) Set $x = \frac{g_{01}}{g_{00}}$ and $y = g_{00}^{-1}$.
(5) Return the matrix $A = \begin{pmatrix} \alpha & x\alpha - y\bar{\beta} \\ \beta & x\beta + y\bar{\alpha} \end{pmatrix}$.

The reduction being polynomial-time is clear from just using elementary matrix manipulations before and after calling the oracle. ::

Remark. *A similar reduction, but using quaternions and using an oracle to the principal ideal problem has been independently discovered by Chevignard et al.*[4]. *Their main relation (lem 3.4) is (un)surprisingly similar to our Equation (3), when seeing the matrix* $\begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix}$ *as the left regular representation of* $\overline{\alpha + j\beta}$.

3.3. **Generalizations.**

3.3.1. *Dealing with non-unit determinants.* From now on, we assume the Gram matrix G to be primitive, that is to say that its Gram ideal—defined as the ideal spanned by all the different norms appearing in the module[5]—to be trivial. Dealing with a non trivial ideal is possible but requires dealing with ideal inversion and thereof pseudo-bases (see Section 3.3.3 for a discussion on this point).

Remark that in the proof of Theorem 3.1, we end up with the modular equality $-\alpha\bar{g}_{01} \equiv \beta \det(A) \pmod{g_{00}}$. This was not an issue as we assumed $\det(A)$ to be 1. Now, suppose we want to treat the general case and let A spans any free lattice. If g_{01} or $\det(A)$ is invertible modulo g_{00}, we can write this equation as $-\alpha\bar{g}_{01}\det(A)^{-1} \equiv \beta \pmod{g_{00}}$ (or equivalently, $-\beta\bar{g}_{01}^{-1}\det(A) \equiv \alpha \pmod{g_{00}}$). We can see by direct computation that the element

[5]See [11, Sec 4.1] for a definition of this ideal, which adapts to the CM case directly.

$u = g_{01}\det(A)^{-1}$ satisfies $u\bar{u} \equiv -1 \pmod{g_{00}}$, since we have by definition of the determinant of the Gram matrix $G : \det(A)\overline{\det(A)} = g_{00}g_{11} - g_{01}\bar{g_{01}}$. Hence, this modular equation defined a decomposition lattice and the same reduction applies *mutatis mutendis*.

However, in this generic case, we might not have invertibility and this argument fails. If this is the case, the lattice defined by the modular equation $-\alpha\bar{g}_{01} \equiv \beta\det(A) \pmod{g_{00}}$ might not be of determinant g_{00} in k^2 and the short basis of this lattice would not be α, β themselves, as expected. However, we can randomize the instance so that the coefficients of matrix G behave nicely. In practice, we only need to ensure that the ideals generated by elements g_{00} and g_{01} are coprime to be able to perform usual quotient arithmetic. Nevertheless, we present a different version of randomization, which is closer in spirit to the one presented in [11]. The main idea is to randomize G until g_{00} and g_{11} become generators of two different prime ideals. [11] claims that this happens (heuristically) with sufficiently high probability for totally real number fields, as per Assumption 1 of [11].

Our approach rely on that if we suppose g_{00} and g_{01} to span prime ideals of k, elementary ideal arithmetic allows to conclude that g_{01} is invertible modulo g_{00}.

Lemma 3.1. *If g_{00} and g_{11} are generators of two different prime ideals of $\mathcal{O}_k$, then the ideal generated by g_{01} is coprime with the ideal g_{00}. Therefore g_{01} and $\det(A)$ are invertible modulo g_{00}.*

Proof. Indeed, assume that the ideal g_{00} divides the ideal g_{01}. First note that $\overline{g_{00}} = g_{00}$ divides $\overline{g_{01}}$. As we have the relation

$$g_{00}g_{11} = g_{01}\overline{g_{01}} + \det(A)\overline{\det(A)}$$

it means that g_{00} divides $\det(A)$ or $\overline{\det(A)}$. In turns, this implies that $\overline{g_{00}} = g_{00}$ divides $\overline{\det(A)}$ or $\det(A)$ respectively. Remark that the right-hand side contains the ideal g_{00}^2 in its prime decomposition. We conclude that necessarily the ideals g_{11} and g_{00} are equal, which contradicts the assumption. ::

We explicit the randomization as follows (recall that we assumed the matrix G to be primitive).

(1) Using algorithm `GaussianGram` from [11, Lem. 3.8] distribution, generate two linearly independent sufficiently short vectors (u, v) and (x, y) such that h_{00} and h_{11} are non-equal prime ideals, where we set $h_{00} := (u^*, v^*)^T G(u, v)$ and $h_{11} := (x^*, y^*)^T G(x, y)$
(2) Define matrix $H := \begin{pmatrix} u^* & v^* \\ x^* & y^* \end{pmatrix} G \begin{pmatrix} u & x \\ v & y \end{pmatrix}$

Note that there is a slight difference between our randomization and the one described in [11] at step 1. Indeed, in the later paper, it is required for h_{00} and h_{11} to be generators of prime ideals of $\mathcal{O}_{k^+}$ only. In our case, we require h_{00} and h_{11} to be generators of prime ideals of $\mathcal{O}_k$, which is a stronger condition. However $k^+ \subset k$ is a degree 2 Galois extension, so by Chebotarev's density theorem the density of unramified inert ideals is $\frac{1}{2}$. This taken into account, the probabilistic analysis of [11] applies in this case almost without change. We, therefore, state an identical assumption to [11, Assumption 1] up to changing the overhead polynomial factor P to take the conditioning on being inert into account. As we are only dealing with coarse-grained complexity, we do not care about the precise degree of this polynomial.

Assumption 1 (adapted from [11])**.** *There exists some absolute polynomial P (with non-negative coefficients) such that the following holds. Let k be a CM field of degree d, $M \subseteq \mathcal{O}_k^2$ be a free module of rank 2, and $s > 0$ be a real number such that $s \geqslant \eta_{1/2}(M)$, the smoothing parameter. Assume $I = \mathcal{G}(M)$, the Gram ideal of the module M to be trivial. Let $(z_1, z_2)^T \leftarrow D_{M,s}$ and $q = z_1 z_1^* + z_2 z_2^*$. Then*

$$\Pr(q \text{ is prime }) \geqslant \frac{1}{\rho_{k^+} \cdot \log(s) \cdot P(d)},$$

where ρ_{k^+} is the residue of the Dedekind zeta function of k^+ at 1, the probability being taken on the random bits used for the subroutine `GaussianGram`*.*

Remark. *In practice, we strongly believe that the probability of obtaining a matrix such that g_{00} and g_{01} generate coprime ideals is actually very high. Indeed, if we assume that these two elements behave randomly enough, we would expect them to be coprime with probability around $\zeta_k(2)^{-1}$, fro ζ_k the Dedekind zeta function of the field. However, since the distribution of these two elements is very peculiar, we have no hope to formally prove such a result and only rely on heuristics.*

Proposition 3.1 (under Assumption 1)**.** *Let k be a CM field. There exists a randomized Cook reduction—polynomial in the input matrix G, the logarithm of the discriminant of k and the residue ρ_{k^+}, from the free, primitive,* module-LIP *problem over k to the shortest vector problem on an Hermitian decomposition lattice, with exactly* one *call to the latter oracle.*

Proof. The reduction starts by randomizing the instance G using the technique just introduced. Call H the resulting Gram-matrix. Now, H satisfies the conditions of Lemma 3.1 by construction. We can apply the proof of Theorem 3.1 *mutatis mutendis* by inverting $\det(A)$ and setting $u = g_{01} \det(A)^{-1}$ modulo g_{00}. Writing the yielded Gram root B of H, a Gram root A of matrix

G can now be found by the simple multiplication $A = B\begin{pmatrix} u & x \\ v & y \end{pmatrix}^{-1}$. The correctness of this reduction is clear from the previous discussion. Under Assumption 1, the expected number of randomization is polynomial in the representation of the number field, and the value of the residue ρ_{k^+}, as all ideals appearing will be polynomially representable by construction (see [11, Sec 4.1, Lem 3.2]). Classically, the primality testing can be done in polynomial time by relying on prime ideal factorization and polynomial-time integer prime testing (see [5, Sec 6.2.5]). All linear algebra steps are of course polynomial-time in the input data. ∷

3.3.2. *Gram-factorization.* If also given a factorization oracle over $\mathbf{Z}$, we can even solve a slightly harder problem, where the lattice spanned by A is *not* given. Instead, we look for an integral factorization of the Gram matrix G into $A^T\overline{A}$. This is the so-called *Gram-decomposition problem* in [11]. Remark in our reduction of Proposition 3.1, we only need to handle the determinant of A, hence it is sufficient to first reviver it from the determinant of G and finish the reduction.

As such, write $\det(A) = d$ and $\det(G) = g$, by construction one has $g = d\bar{d}$. The first step of our reduction requires to find such d given g. We rely on a norm-solving algorithm introduced by Howgrave-Graham and Szydlo for cyclotomic number rings of conductor a power of two. A detailed description of this algorithm is given as Algorithm 2.1 of [11] for any CM field.

Lemma 3.2 (Howgrave–Graham-Szydlo from [11])**.** *Let k be a CM field. Given access to an integer factorization oracle, there exists a deterministic polynomial-time algorithm—in the representation of the field and of input—solving norm equations of the form $d\bar{d} = g$ for any $g \in k^{++}$.*

Assume from now on that we already computed d such that $g = d\bar{d}$, that is to say that we already know the determinant of the matrix A, and we can use our previous reduction.

Putting together the reduction of Proposition 3.1, the use of the Howgrave-Graham-Szydlo algorithm gives the following.

Proposition 3.2 (under Assumption 1)**.** *There exists a randomized Cook reduction—polynomial in the input matrix G, the logarithm of the discriminant of k and the residue ρ_{k^+} from the (primitive)* Gram-decomposition problem *over $\mathcal{O}_k^2$ to the shortest vector problem on an Hermitian decomposition lattice and integer factorization, with exactly* one *call to these latter oracles.*

3.3.3. *Projective modules.* To deal with the most general version of module-LIP, we shall not restrain to free modules, but to *projective* modules. This essentially amounts to restricting the coefficient space to fractional ideals of $\mathcal{O}_k$, i.e. using so-called *pseudo-bases* instead of bases in

the terminology of [5]. In particular, this allows us to avoid assuming that the gram matrix is primitive by dividing by the Gram-ideal itself. As this is more of an arithmetic technicality and does not carry any useful geometric insight for the understanding of the problem, we let this generalization as a possibly interesting research direction.

3.3.4. Thanks to the applicability of the Lenstra-Silverberg algorithm as shown in Section 2.2.4, we have a deterministic polynomial-time algorithm to instantiate the reduction oracle, as by construction of the decomposition lattice has a square basis. Since the reduction is itself deterministic, we therefore have a deterministic polynomial time algorithm for the (free)-module-LIP algorithm in the totally real case. This retrieves the result given in [11], and removes the heuristics and the probabilistic elements that were artifacts of the randomization technique used. As this is not the main objective of this note, we let the details and formalization to future work and only indicate this result as a substantiated claim.

Claim 1. *There exists a Cook reduction from the $\mathcal{O}_k^2$-module-LIP problem to a shortest vector problem on an Hermitian decomposition lattice, with exactly one call to the latter oracle.*

References

[1] Karim Belabas. Topics in computational algebraic number theory. *Journal de théorie des nombres de Bordeaux*, 16(1):19–63, 2004.

[2] Huck Bennett, Atul Ganju, Pura Peetathawatchai, and Noah Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? In *Advances in Cryptology – EUROCRYPT*. Springer-Verlag, 2023.

[3] Johannes A. Buchmann and Hendrik W. Lenstra. Approximating rings of integers in number fields. *Journal de Théorie des Nombres de Bordeaux*, 6(2):221–260, 1994.

[4] Clémence Chevignard, Guilhem Mureau, Alice Pellet-Mary, and Alexandre Wallet. A reduction from hawk to the principal ideal problem in a quaternion algebra. *Personal communication*, 2024.

[5] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer Publishing Company, Incorporated, 2010.

[6] Léo Ducas. Provable lattice reduction of $\mathbb{Z}^n$ with blocksize n/2. *Designs, Codes and Cryptography*, 92(4), 2024.

[7] Craig Gentry and Mike Szydlo. Cryptanalysis of the revised ntru signature scheme. In *Advances in Cryptology—EUROCRYPT*, pages 299–320. Springer, 2002.

[8] Maria I. Icaza. Hermite constant and extreme forms for algebraic number fields. *Journal of the London Mathematical Society*, 55(1):11–22, 1997.

[9] Hendrik W Lenstra and Alice Silverberg. Lattices with symmetry. *Journal of Cryptology*, 30, 2017.

[10] Hendrik W Lenstra Jr and Alice Silverberg. Testing isomorphism of lattices over cm-orders. *SIAM Journal on Computing*, 48(4), 2019.

[11] Guilhem Mureau, Alice Pellet-Mary, Georgii Pliatsok, and Alexandre Wallet. Cryptanalysis of rank-2 module-lip in totally real number fields. In *Advances in Cryptology – EUROCRYPT 2024*, pages 226–255, 2024.

* PQShield, France, * IRISA, Rennes

Email address: thomas@espitau.com