Research Article

Robson Ricardo de Araujo*

The condition number associated with ideal lattices from odd prime degree cyclic number fields

https://doi.org/10.1515/jmc-2024-0022
received May 20, 2024; accepted November 08, 2024

Abstract: The condition number of a generator matrix of an ideal lattice derived from the ring of integers of an algebraic number field is an important quantity associated with the equivalence between two computational problems in lattice-based cryptography, the “Ring Learning With Errors (RLWE)” and the “Polynomial Learning With Errors (PLWE)”. In this work, we compute the condition number of a generator matrix of the ideal lattice from the whole ring of integers of any odd prime degree cyclic number field using canonical embedding.

Keywords: condition number, RLWE, PLWE, Abelian number fields, ideal lattices

MSC 2020: 11T71, 15A12, 11R20, 11C99

1 Introduction

The Ring Learning with Errors (RLWE) problem and the Polynomial Learning with Errors (PLWE) problem are the basis for some of the most promising post-quantum cryptographic protocols [1,2]. These problems are part of lattice-based cryptography since they arise from Learning with Errors (LWE) problem, which is at least as difficult to solve as the approximate shortest independent vector problem (α-SIVP). In turn, these problems are known to be NP-hard for certain α [3]. Although the decision version of RLWE has known security reduction for α-SVP, the advantage of PLWE is that it is more efficient and suitable for implementation. Essentially, RLWE is defined over the ring of integers of an algebraic number field $K = \mathbb{Q}(\alpha)$ through canonical embedding, whereas PLWE is defined over a quotient of a polynomial ring $\mathbb{F}_q[x]/(f(x))$ through coefficient embedding.

In some cases, the problems RLWE and PLWE are equivalent, which occurs when there is an algorithm that transforms a solution of one of them into a solution of the other, and *vice versa*, in polynomial time. The theoretical problem of the relation (in particular, the equivalence) between RLWE and PLWE was first described in [4]. Especially since then, it has been shown that RLWE and PLWE are equivalent or non-equivalent in several situations (e.g., [5–9]).

To determine the equivalence (or not) between RLWE and PLWE, an important quantity is the condition number associated with a generator matrix of the ideal lattice used in the RLWE construction. If K is an algebraic number field of degree n and O_K denotes its ring of integers, the *canonical embedding* of K consists of the map $\sigma_K : K \longrightarrow \mathbb{C}^n$ given by $\sigma_K(x) = (\sigma_1(x), \ldots, \sigma_n(x))$, for all $x \in O_K$, where $\sigma_1, \ldots, \sigma_n$ are the monomorphisms from K to $\mathbb{C}$. In this way, $\sigma_K(O_K)$ can be seen as a lattice in an n-dimensional Euclidean space H isomorphic to $\mathbb{R}^n$, where the lattice is understood to be a full-rank discrete additive subgroup of H (or $\mathbb{R}^n$). The lattice $\Lambda = \sigma_K(O_K)$ is said to be an *ideal lattice* and is associated with an $n \times n$ matrix $\mathbf{M}$ such that $\mathbf{v} \in \Lambda$ if and only if $\mathbf{v}^T = \mathbf{M} \cdot \mathbf{u}^T$ for some $\mathbf{u} \in \mathbb{Z}^n$. The matrix $\mathbf{M}$ is called a *generator matrix* of Λ. The *condition number*

*** Corresponding author: Robson Ricardo de Araujo,** Federal Institute of São Paulo, Av. Pastor José Dutra de Moraes, 239 - Distrito Industrial Antônio Zácaro - Catanduva - SP, 15808-305, Brazil, e-mail: robson.ricardo@ifsp.edu.br

of $\mathbf{M}$ (or, of K) is defined as the quantity $\mathrm{Cond}(\mathbf{M}) = ||\mathbf{M}||||\mathbf{M}^{-1}||$, where $||\mathbf{A}|| \coloneqq \sqrt{\mathrm{Tr}(\mathbf{A}^*\mathbf{A})}$ denotes the *Frobenius norm* of a matrix $\mathbf{A}$ (where $\mathbf{A}^*$ denotes the conjugate transpose of the complex matrix $\mathbf{A}$ and Tr denotes the trace of a matrix). The condition number is important in RLWE/PLWE equivalence because it measures the distortion caused in the transformation from one to the other when the algebraic structures involved are paired [8]. In these situations, the RLWE/PLWE equivalence is established if the condition number is $O(n^r)$ for some constant $r > 0$ depending only on the field K.

Let K be a cyclic number field of odd prime degree p. Since $K/\mathbb{Q}$ is an Abelian field extension, there is a cyclotomic field $\mathbb{Q}(\zeta_m)$ containing K according to the Kronecker–Weber theorem. The minimal m with this property is called the *conductor* of K. It is known that p is either unramified or ramified in O_K. If p is unramified in O_K, then the conductor of K is given by $m = \prod_{i=1}^{r} p_i$, where $r \geq 1$ and $p_1, \ldots, p_r$ are prime positive integer numbers such that $p_i \equiv 1 \pmod{p}$ for $i = 1, \ldots, r$ (unramified case). In turn, if p is ramified in O_K, then the conductor of K is given by $m = p^2 u$, where $u = 1$ or $u = \prod_{i=1}^{r} p_i$ with $r \geq 1$ and $p_1, \ldots, p_r$ are prime positive integer numbers such that $p_i \equiv 1 \pmod{p}$ (ramified case). In this context, algebraic lattices coming from $\mathbb{Z}$-modules of O_K through canonical embedding and their associated trace forms have recently been studied for different applications (e.g., [10–13]).

Our objective in this work is to compute the condition number of a generator matrix of the lattice $\sigma_K(O_K)$, where K is an odd prime degree cyclic number field. The unramified case is described in Section 2 – the condition number is given in Theorem 2.1. In turn, the condition number of K in the ramified case is available in Theorem 3.1, which is covered in Section 3. Finally, we conclude this work in Section 4 with suggestions for further research related to RLWE/PLWE equivalence for K.

2 The unramified case

Let K be a cyclic number field of prime degree $p > 2$. Suppose that p is unramified in the ring of integers O_K. This means that the conductor of K is given by $m = p_1 \ldots p_r$, where $r \geq 1$ and $p_1, \ldots, p_r$ are prime positive integer numbers satisfying $p_i \equiv 1 \pmod{p}$, for each $i = 1, \ldots, r$. Then, $K \subseteq \mathbb{Q}(\zeta_m)$, where ζ_m is an mth primitive root of unity. In this case, the Hilbert–Speiser theorem [14, Theorem 1.7] states that K has a normal integral basis: in fact, if $t \coloneqq \mathrm{Tr}_{\mathbb{Q}(\zeta_m)/K}(\zeta_m)$ and θ denotes a generator of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$, then $\{t, \theta(t), \ldots, \theta^{p-1}(t)\}$ is a $\mathbb{Z}$-basis of O_K.

Since $K/\mathbb{Q}$ is a Galois field extension of the odd degree, K is a totally real number field. Therefore, the monomorphisms from K to $\mathbb{C}$ are exactly the i-powers of θ for $i = 0, \ldots, p-1$ and have their images contained in $\mathbb{R}$. So, the canonical embedding associated with K can be defined as $\sigma_K(x) = (x, \theta(x), \ldots, \theta^{p-1}(x)) \in \mathbb{R}^n$, for all $x \in K$. Thus, a generator matrix of the lattice $\Lambda = \sigma_K(O_K)$ is given by

$$\mathbf{M}_K = (\theta^i(\theta^j(t)))_{i,j \in \{0,1,\ldots,p-1\}} = \begin{pmatrix} t & \theta(t) & \cdots & \theta^{p-1}(t) \\ \theta(t) & \theta^2(t) & \cdots & t \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{p-1}(t) & t & \ldots & \theta^{p-2}(t) \end{pmatrix}. \tag{1}$$

Also, in [11, Theorem 2.2], it is shown that

$$\mathrm{Tr}_K(t^2) = m + \frac{1-m}{p} \tag{2}$$

and for $i, j \in \{0, 1, \ldots, p-1\}$ with $i \neq j$,

$$\mathrm{Tr}_K(\theta^i(t)\theta^j(t)) = \frac{1-m}{p}. \tag{3}$$

Furthermore, in the following, we use the fact shown in [15, Lemma 2.3] that, for any $a, b \in \mathbb{C}$,

$$\det\begin{pmatrix} a & b & b & \cdots & b \\ b & a & b & \cdots & b \\ b & b & a & \cdots & b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \cdot & a \end{pmatrix}_{k\times k} = (a-b)^{k-1}(a+(k-1)b). \tag{4}$$

Finally, we are able to show the main theorem of this section:

Theorem 2.1. *If K is a cyclic number field of prime degree $p > 2$, where p is unramified in O_K, then the condition number of a generator matrix of $\Lambda = \sigma_K(O_K)$ is given by*

$$\mathrm{Cond}(\mathbf{M}_K) = \sqrt{1 + (p-1)\left(m + p - 1 + \frac{1}{m}\right)}, \tag{5}$$

where m is the conductor of K.

Proof. The matrix $\mathbf{G} \coloneqq \mathbf{M}_K^*\mathbf{M}_K = \mathbf{M}_K^T\mathbf{M}_K$ is the Gram matrix of Λ because K is a totally real number field. Since $\mathrm{Tr}_K(\theta^i(t)\theta^j(t)) = \mathrm{Tr}_K(t\theta^{j-i}(t))$ for all $i, j \in \{0, 1, \ldots, p-1\}$, $\theta^p(t) = \theta^0(t) = t$, and by (2) and (3), we have that

$$\mathbf{G} = \begin{pmatrix} \mathrm{Tr}_K(t^2) & \mathrm{Tr}_K(t\theta(t)) & \cdots & \mathrm{Tr}_K(t\theta^{p-1}(t)) \\ \mathrm{Tr}_K(t\theta(t)) & \mathrm{Tr}_K(t^2) & \cdots & \mathrm{Tr}_K(t\theta^{p-2}(t)) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}_K(t\theta^{p-1}(t)) & \mathrm{Tr}_K(t\theta^{p-2}(t)) & \cdots & \mathrm{Tr}_K(t^2) \end{pmatrix} = \begin{pmatrix} m + \dfrac{1-m}{p} & \dfrac{1-m}{p} & \cdots & \dfrac{1-m}{p} \\ \dfrac{1-m}{p} & m + \dfrac{1-m}{p} & \cdots & \dfrac{1-m}{p} \\ \vdots & \vdots & \ddots & \vdots \\ \dfrac{1-m}{p} & \dfrac{1-m}{p} & \cdots & m + \dfrac{1-m}{p} \end{pmatrix}. \tag{6}$$

So, $\|\mathbf{M}_K\| = \sqrt{\mathrm{Tr}(\mathbf{G})} = \sqrt{m(p-1)+1}$. To compute $\|\mathbf{M}_K^{-1}\|$, we observe that $\mathrm{Tr}((\mathbf{M}_K^{-1})^T\mathbf{M}_K^{-1}) = \mathrm{Tr}(\mathbf{G}^{-1})$, which corresponds to the sum of the eigenvalues of the symmetric matrix $\mathbf{G}^{-1}$ counted with multiplicity. Since the eigenvalues of $\mathbf{G}^{-1}$ are equal to the inverse of the eigenvalues of $\mathbf{G}$, $\|\mathbf{M}_K\|^{-1} = \mathrm{Tr}(\mathbf{G}^{-1}) = \sum_{i=1}^{p}\lambda_i^{-1}$, where $\lambda_1, \ldots, \lambda_p$ are the eigenvalues of $\mathbf{G}$. Thus, to complete this proof, we need to compute the eigenvalues of $\mathbf{G}$. By (4), denoting by $\mathbf{I}_p$ the $p \times p$ identity matrix, we have

$$\det(\mathbf{G} - x\mathbf{I}_p) = (m-x)^{p-1}(1-x), \tag{7}$$

whence it follows that the eigenvalues of $\mathbf{G}$ are $\lambda_1 = \lambda_2 = \ldots = \lambda_{p-1} = m$ and $\lambda_p = 1$. So, $\|\mathbf{M}_K^{-1}\| = 1 + (p-1)/m$. Therefore,

$$\mathrm{Cond}(\mathbf{M}_K) = \|\mathbf{M}_K\|\|\mathbf{M}_K^{-1}\| = \sqrt{(m(p-1)+1)\left(1 + \frac{p-1}{m}\right)}, \tag{8}$$

which completes this proof after a simple rearrangement of the last expression. □

3 The ramified case

Let K be a cyclic number field of prime degree $p > 2$. In this section, we suppose that p is ramified in the ring of integers O_K. In this case, the conductor of K is given by $m = p^2u$, where $u = 1$ or $u = p_1 \ldots p_r$ for some prime positive integer numbers $p_1, \ldots, p_r$ such that $p_i \equiv 1 \pmod p$, $i = 1, \ldots, r$. In this case, the Leopoldt theorem [16, Theorem 2] implies that K has an integral basis given by $B = \{1, \theta(t), \ldots, \theta^{p-1}(t)\}$, where θ is a generator of the cyclic Galois group $\mathrm{Gal}(K/\mathbb{Q})$ and $t \coloneqq \mathrm{Tr}_{\mathbb{Q}(\zeta_m)/K}(\zeta_m)$ (note that B is not a normal integral basis of K, which in fact is regarded by the Hilbert–Speiser theorem).

As commented in the previous section, the canonical embedding associated with K can be seen as $\sigma_K : K \longrightarrow \mathbb{R}^p$ defined by $\sigma_K(x) = (x, \theta(x), \ldots, \theta^{p-1}(x))$, for all $x \in K$. Then, a generator matrix of the ideal lattice $\Lambda = \sigma_K(O_K)$ is given by

$$\mathbf{M}_K = \begin{pmatrix} 1 & \theta(t) & \theta^2(t) & \ldots & \theta^{p-1}(t) \\ 1 & \theta^2(t) & \theta^3(t) & \cdots & t \\ 1 & \theta^3(t) & \theta^4(t) & \cdots & \theta(t) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & t & \theta(t) & \cdots & \theta^{p-2}(t) \end{pmatrix}. \tag{9}$$

Since m is not a squarefree integer, it is well known that

$$\mathrm{Tr}_K(t) = \mathrm{Tr}_{\mathbb{Q}(\zeta_m)}(\zeta_m) = 0. \tag{10}$$

Additionally, in [13], it is shown that

$$\mathrm{Tr}_K(t^2) = \frac{m(p-1)}{p} \tag{11}$$

and for $i, j \in \{0, \ldots, p-1\}$, $i \neq j$,

$$\mathrm{Tr}_K(\theta^i(t)\theta^j(t)) = \mathrm{Tr}_K(t\theta^{j-i}(t)) = -\frac{m}{p}. \tag{12}$$

With this setting, in the following theorem, we show the condition number of a generator matrix of $\sigma_K(O_K)$:

Theorem 3.1. *If K is a cyclic number field of prime degree $p > 2$, where p is ramified in O_K, the condition number of a generator matrix of $\Lambda = \sigma_K(O_K)$ is given by*

$$\mathrm{Cond}(\mathbf{M}_K) = \sqrt{2p^2\left(1 + \frac{1}{m}\right) - p\left(\frac{2}{m} + 6\right) + 7 + m - \frac{2}{p}(1 + m) + \frac{m}{p^2}}, \tag{13}$$

where m is the conductor of K.

Proof. The proof is similar to that presented for Theorem 2.1. In this case, due to formulas (10), (11), and (12), the Gram matrix of Λ, $\mathbf{G} = \mathbf{M}_K^T\mathbf{M}_K$, is given by

$$\mathbf{G} = \begin{pmatrix} p & \mathrm{Tr}_K(t) & \mathrm{Tr}_K(t) & \cdots & \mathrm{Tr}_K(t) \\ \mathrm{Tr}_K(t) & \mathrm{Tr}_K(t^2) & \mathrm{Tr}_K(t\theta(t)) & \cdots & \mathrm{Tr}_K(t\theta^{p-2}(t)) \\ \mathrm{Tr}_K(t) & \mathrm{Tr}_K(t\theta(t)) & \mathrm{Tr}_K(t^2) & \cdots & \mathrm{Tr}_K(t\theta^{p-3}(t)) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}_K(t) & \mathrm{Tr}_K(t\theta^{p-2}(t)) & \mathrm{Tr}_K(t\theta^{p-3}(t)) & \cdots & \mathrm{Tr}_K(t^2) \end{pmatrix} = \begin{pmatrix} p & 0 & 0 & \cdots & 0 \\ 0 & \frac{m(p-1)}{p} & -\frac{m}{p} & \cdots & -\frac{m}{p} \\ 0 & -\frac{m}{p} & \frac{m(p-1)}{p} & \cdots & -\frac{m}{p} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -\frac{m}{p} & -\frac{m}{p} & \cdots & \frac{m(p-1)}{p} \end{pmatrix}. \tag{14}$$

Thus, $||\mathbf{M}_K|| = \sqrt{\mathrm{Tr}(\mathbf{G})} = \sqrt{p(m+1) - 2m + m/p}$. Finally, to compute $||\mathbf{M}_K^{-1}|| = \sqrt{\mathrm{Tr}(\mathbf{G}^{-1})}$, we need the eigenvalues of $\mathbf{G}$. Using the Laplace expansion in combination with (4), we have that

$$\det(\mathbf{G} - x\mathbf{I}_p) = (p - x)(m - x)^{p-2}(m/p - x). \tag{15}$$

This implies that $\lambda_1 = p$, $\lambda_2 = \lambda_3 = \ldots = \lambda_{p-1} = m$, and $\lambda_p = m/p$ are the eigenvalues of $\mathbf{G}$. Consequently, their inverses are the eigenvalues of $\mathbf{G}^{-1}$. So,

$$||\mathbf{M}_K^{-1}|| = \sqrt{\mathrm{Tr}(\mathbf{G}^{-1})} = \frac{1}{p} + \frac{2(p-1)}{m}. \tag{16}$$

Therefore,

$$\mathrm{Cond}(\mathbf{M}_K) = \|\mathbf{M}_K\|\|\mathbf{M}_K^{-1}\| = \sqrt{\left(p(m+1) - 2m + \frac{m}{p}\right)\left(\frac{1}{p} + \frac{2(p-1)}{m}\right)} \tag{17}$$

from which the result follows after rearrangements in this expression. □

4 Conclusion and future research

Considering that K is an odd prime degree cyclic number field and σ_K is the canonical embedding associated with it, in this work, we have shown formulas for the condition number of a generator matrix of the lattice $\sigma_K(O_K)$ depending only on the degree and the conductor of K. If p not divides m, this condition number is presented in Theorem 2.1. In turn, if p divides m, the condition number is computed in Theorem 3.1.

As noted in the introduction of this work, the condition number of a generator matrix of an ideal lattice can be used in a cryptographic context related to the equivalence between the RLWE and PLWE problems. Although the quantities shown in this work indicate that RLWE and PLWE are equivalent for odd prime degree cyclic number fields, once the condition numbers computed here are of polynomial order, the non-monogenicity of these number fields (as shown in [17]) prevents the expected conclusion *a priori*. Thus, future research could investigate whether the RLWE and PLWE problems are equivalent in the context of odd prime degree cyclic number fields, which could lead to new studies related to RLWE/PLWE equivalence for non-monogenic number fields.

Acknowledgment: The author thanks the referee for her/his suggestions to improve this work.

Funding information: This work was supported by National Council for Scientific and Technological Development (CNPq) – Process 405842/2023-6 and by Federal Institute of São Paulo through its program PIPECT 2024.

Author contributions: The author has accepted responsibility for the entire content of this manuscript and approved its submission.

Conflict of interest: The author declares no competing interests.

Ethical approval: The conducted research is not related to either human or animals use.

Data availability statement: Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

References

[1] Stehlé D, Steinfeld R, Tanaka K, Xagawa K. Efficient public key encryption based on ideal lattices. Adv Cryptol-ASIACRYPT 2009 Lecture Notes in Comput Sci. 2009;5912:617–35. doi: https://doi.org/10.1007/978-3-642-10366-7_36.

[2] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. J Assoc Comput Mach. 2013;60:1–35. doi: https://doi.org/10.1145/2535925.

[3] Micciancio D. The shortest vector in a Lattice is hard to approximate to within some constant. SIAM J Comput. 2001;30:2008–35. doi: https://doi.org/10.1137/S0097539700373039.

[4] Rosca M, Stehlé D, Wallet A. On the ring-LWE and polynomial-LWE problems. Adv Cryptology-EUROCRYPT 2018 Lecture Notes Comput Sci. 2018;10820:146–73. doi: https://doi.org/10.1007/978-3-319-78381-9_6.

[5] Ducas L, Durmus A. Ring-(lwe) in polynomial rings. Public Key Cryptography - PKC 2012 Lecture Notes Comput Sci. 2012;7293:34–51. doi: https://doi.org/10.1007/978-3-642-30057-8_3.

[6] Blanco-Chacón I. On the RLWE/PLWE equivalence for cyclotomic number fields. Appl Algebr Eng Comm. 2022;33:53–71. doi: https://doi.org/10.1007/s00200-020-00433-z.

[7] Blanco-Chacón I, López-Hernanz L. RLWE/PLWE equivalence for the maximal totally real subextension of the $2^r pq$-th cyclotomic field. Adv Math Commun. 2022;13:1–32. doi: https://doi.org/10.3934/amc.2022093.

[8] Blanco-Chacón I. RLWE/PLWE equivalence for totally real cyclotomic subextensions via quasi-Vandermonde matrices. J Algebra Appl. 2022;21:2250218. doi: https://doi.org/10.1142/S0219498822502188.

[9] DiScala AJ, Sanna C, Signorini E. RLWE and PLWE over cyclotomic fields are not equivalent. Appl Algebr Eng Comm. 2022;22:174–8. doi: https://doi.org/10.1007/s00200-022-00552-9.

[10] Nunes JVL, Interlando JC, Neto TPN, Lopes JOD. New p-dimensional lattices from cyclic extensions. J Algebra Appl. 2017;16:1750186. doi: https://doi.org/10.1142/S0219498817501869.

[11] de Oliveira EL, Interlando JC, Neto TPN, Lopes JOD. The integral trace form of cyclic extensions of odd prime degree. Rocky Mt J Math. 2017;47:1075–88.

[12] de Araujo RR, Costa SIR. Well-rounded algebraic lattices in odd prime dimension. Arch Math. 2019;112:139–48. doi: https://doi.org/10.1007/s00013-018-1232-7.

[13] de Araujo RR, Chagas ACMM, Andrade AA, Neto TPN. Trace form associated to cyclic number fields of ramified odd prime degree. J Algebra Appl. 2020;19:2050080. doi: https://doi.org/10.1142/S0219498820500802.

[14] Johnston H. Notes on Galois module. 2016. University of Exeter; https://empslocal.ex.ac.uk/people/staff/hj241/GM_CourseNotes109.pd.

[15] Di Scala AJ, Sanna C, Signorini E. On the condition number of the Vandermonde matrix of the nth cyclotomic polynomial. J Math Cryptol. 2021;15:174–8. doi: https://doi.org/10.1515/jmc-2020-0009.

[16] Lettl G. The ring of integers of an Abelian number field. J Reine Angew Math. 1990;404:162–70. doi: https://doi.org/10.1515/crll.1990.404.162.

[17] Gras M. Non monogénéité de laanneau des entiers des extensions cycliques de Q de degré premier l ≥ 5. J Number Theory. 1986;23:347–53. doi: https://doi.org/10.1016/0022-314X(86)90079-X.