Non-Equivalence of Ring Learning With Errors and Polynomial Learning With Errors over Cyclotomic Number Fields

Carlo Sanna

(joint work with Antonio Di Scala and Edoardo Signorini)

Group of Cryptography and Number Theory

Department of Mathematical Sciences

Politecnico di Torino

March 30, 2022

Contents

Post-Quantum Cryptography (1/2)

The first and most widely used Public Key Cryptosystem is RSA, which was invented by Rivest, Shamir, and Adleman in 1977.
(An equivalent cryptosystem was developed in secret by Clifford Cocks in 1973 for the British signals intelligence agency and declassified in 1997.)

The security of RSA is based on difficulty of the **Factorization Problem**, in particular, the problem of finding two prime numbers p and q given their product $n = pq$.

No efficient (classical) algorithm to factorize large integers n is known.

However, in 1994 Peter Shor invented a quantum algorithm, now known as **Shor's algorithm**, that can efficiently factorize n via a quantum computer.

Post-Quantum Cryptography (2/2)

Due to the recent progress and the large investments into the development of quantum computing, the actual implementation of Shor's algorithm seems more imminent than ever and constitutes a real threat to RSA.

Consequently, a lot of effort is put into **Post-Quantum Cryptography**, that is, asymmetric cryptography designed to be resistant even against attacks using quantum computers.

Candidates for Post-Quantum Cryptography includes:

- Multivariate Cryptography
- Code-based Cryptography
- Hash-based Cryptography
- Lattice-based Cryptography
- Supersingular Elliptic Curve Isogeny Cryptography

Lattice-Based Cryptography (1/2)

Lattice-Based Cryptography relies its security on the difficulty of problems related to lattices, that is, subsets of $\mathbb{R}^n$ of the form $\{\sum_{i=1}^{k} x_i v_i : x_i \in \mathbb{Z}\}$ where $v_1, \ldots, v_k \in \mathbb{R}^n$.

It began in 1996 with the seminal work of Ajtai, who gave the first collision-resistant hash function on random lattices.

Since then, numerous lattice-based encryption and digital signature schemes have been proposed.

In particular, lattice-based proposals are the most numerous in the final phase of the NIST post-quantum standardization process, with finalist in both key encapsulation (CRYSTALS-Kyber, NTRU, SABER) and digital signature schemes (CRYSTALS-Dilithium, FALCON).

Lattice-Based Cryptography (2/2)

The main building block of lattice-based cryptographic schemes is the Learning With Errors (LWE) problem, which, roughly speaking, consists of retrieving a secret vector from a noisy random sample of matrix products.

Learning With Errors (LWE) Problem

Let $n, m, q \in \mathbb{N}$ and D be a probability distribution over $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$.

Given m samples $(\boldsymbol{a}_i, \boldsymbol{a}_i \cdot \boldsymbol{s} + e_i)$ where $\boldsymbol{a}_i \in \mathbb{Z}_q^n$ are uniformly distributed random vectors, $e_i \in \mathbb{Z}_q$ are D-distributed random errors ($i = 1, \ldots, m$), and $\boldsymbol{s} \in \mathbb{Z}_q^n$ is a secret vector; Find the secret vector $\boldsymbol{s}$.

LWE-based schemes have solid theoretical security bases but require the ciphertext or the public key to be nearly quadratic respect to the security parameters. To overcome this, variants of LWE working over $\mathbb{Z}_q[X]/(f)$, $f \in \mathbb{Z}_q[X]$, instead of $\mathbb{Z}_q^n$ have been introduced.

RLWE & PLWE

In 2009, Stehlé et al. introduced the Polynomial-LWE (PLWE) variant using power-of-two degree cyclotomic polynomials.

In 2010, Lyubashevsky et al. introduced the Ring-LWE (RLWE) variant over the ring of integers of a number field.

The advantage of RLWE is the provable-security by hard computational problems, as for LWE.

PLWE is preferable in implementations, where the modular arithmetic between polynomials can be efficiently implemented.

Therefore, it is interesting to study for which families of polynomials f the RLWE and PLWE problems are equivalent, that is, every solution of RLWE can be turned in polynomial time into a solution of PLWE, and vice versa, incurring in a noise increase that is polynomial in $\deg(f)$.

Short Elements

Let $K = \mathbb{Q}(\alpha)$ be a monogenic number field of degree m, and let $f \in \mathbb{Z}[X]$ be the minimal polynomial of α over $\mathbb{Q}$, so that $K \cong \mathbb{Z}[X]/(f)$.

The geometric notion of **short element** derives from a choice of a norm on K by embedding the number field in $\mathbb{C}^m$.

RLWE uses the **canonical embedding** (or **Minkowski embedding**) $\sigma : K \to \mathbb{C}^m$, where σ_i $(i = 1, \ldots, m)$ are all the embeddings of K in $\mathbb{C}$.

PLWE uses the **coefficient embedding**, which maps each $x \in \mathcal{O}_K$ to the vector $(x_0, \cdots, x_{m-1}) \in \mathbb{Z}$ of its coefficients respect to the power basis $1, \alpha, \ldots, \alpha^{m-1}$ of $\mathcal{O}_K$ as a $\mathbb{Z}$-module.

As a linear map, the canonical embedding has a matrix representation $V_f \in \mathbb{C}^{m \times m}$, so that $\sigma(x) = V_f \cdot (x_0, \ldots, x_{m-1})^\intercal$ for each $x \in \mathcal{O}_K$.

Vandermonde Matrix

Precisely, V_f is the **Vandermonde matrix** of f, which is defined as

$$V_f := \begin{pmatrix} 1 & \alpha_0 & \alpha_0^2 & \cdots & \alpha_0^{m-1} \\ 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{m-1} & \alpha_{m-1}^2 & \cdots & \alpha_{m-1}^{m-1} \end{pmatrix},$$

where $\alpha_0, \ldots, \alpha_m$ are the roots of f (which are distinct, since f is irreduc.).

We have that

$$\det(V_f) = \prod_{0 \le i < j < m} (\alpha_i - \alpha_j) \neq 0.$$

Hence, V_f is invertible.

Equivalence Between RLWE and PLWE

Let $\|\cdot\|$ be any fixed norm on $\mathbb{C}^m$ (since all such norms are equivalent).

For the equivalence between RLWE and PLWE, it is important to determine when, whether $\|x\|$ is small, then so is $\|\sigma(x)\|$, and vice versa.

This notion is quantified by V_f having a small condition number $\mathrm{Cond}(V_f)$.

The **condition number** of an invertible matrix $A \in \mathbb{C}^{m\times m}$ is defined as

$$\mathrm{Cond}(A) := \|A\| \, \|A^{-1}\|$$

where $\|A\| := \sqrt{\mathrm{Tr}(A^* A)} = \sqrt{\sum_{i,j} |a_{i,j}|^2}$ denotes the **Frobenius norm** of A and A^* is the conjugate transpose of A.

RLWE and PLWE are **equivalent** over a family of polynomials $\mathcal{F}$ if

$$\mathrm{Cond}(V_f) \leq C_{\mathcal{F}} \, (\deg(f))^{E_{\mathcal{F}}}, \qquad \text{for all } f \in \mathcal{F},$$

where $C_{\mathcal{F}}, E_{\mathcal{F}} > 0$ are constants depending only on the family $\mathcal{F}$.

Some Results on the Equivalence

Equivalence of RLWE and PLWE has been proved for various families of polynomials. The greatest interest concerns cyclotomic polynomials, which, for efficiency reasons, are among the most used in cryptographic applications.

Miruna Rosca, Damien Stehlé, and Alexandre Wallet,
On the Ring-LWE and Polynomial-LWE Problems,
EUROCRYPT 2018-37th Annual International Conference on the Theory and Applications.

Damien Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa,
Efficient public key encryption based on ideal lattices,
International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2009, pp. 617–635.

Cyclotomic Polynomials

Let us recall that the nth cyclotomic polynomial is defined as

$$\Phi_n(X) := \prod_{\substack{1 \le k \le n \\ \gcd(n,k)=1}} \left(X - \mathrm{e}^{2\pi \boldsymbol{i} k/n}\right),$$

that is, $\Phi_n(X)$ is the monic polynomial having as roots the primitive nth roots of unity.

It can be proved that Φ_n has integer coefficients and is irreducible over $\mathbb{Q}$. In fact, Φ_n is the minimal polynomial of each primitive nth root of unity.

In what follows, let $m := \varphi(n)$ be the degree of Φ_n, where φ is the Euler totient function, and let $\zeta_0, \ldots, \zeta_{m-1}$ be the primitive nth roots of unity (in some fixed order), where, to ease the notation, the dependency on n is omitted.

Vandermonde Matrices of Cyclotomic Polynomials

Thus the Vandermonde matrix of Φ_n is

$$V_n := V_{\Phi_n} = \begin{pmatrix} 1 & \zeta_0 & \zeta_0^2 & \cdots & \zeta_0^{m-1} \\ 1 & \zeta_1 & \zeta_1^2 & \cdots & \zeta_1^{m-1} \\ 1 & \zeta_2 & \zeta_2^2 & \cdots & \zeta_2^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_{m-1} & \zeta_{m-1}^2 & \cdots & \zeta_{m-1}^{m-1} \end{pmatrix}.$$

The main difficulty in the study of V_n is that the sequence of powers

$$1, \quad \zeta_j, \quad \zeta_j^2, \quad \zeta_j^3, \quad \ldots$$

is periodic with period length n, but V_n has only m columns and $m < n$.

Note that $\|V_n\| = m$, since $|\zeta_j| = 1$. Therefore, computing the condition number $\mathrm{Cond}(V_n) := \|V_n\| \, \|V_n^{-1}\|$ amount to computing $\|V_n^{-1}\|$.

The Power-of-Two Case

The case of n a power of 2 is well known and completely understood.

Proposition

For $n = 2^k$ the matrix V_n is a scaled isometry: $V_n V_n^* = m\,\mathrm{Id}_n$, where Id_n is the $n \times n$ identity matrix. Furthermore, $\mathrm{Cond}(V_n) = m$.

Proof: Since $n = 2^k$, we have that $m = 2^{k-1}$ and $\zeta_i^m = -1$ for each i. Hence, the product of the ith row of V_n and the jth column of V_n^* is equal to m if $i = j$, and it is equal to

$$\sum_{k=0}^{m-1} \left(\zeta_i \overline{\zeta_j}\right)^k = \frac{\left(\zeta_i \overline{\zeta_j}\right)^m - 1}{\zeta_i \overline{\zeta_j} - 1} = 0$$

if $i \neq j$; so that $V_n V_n^* = m\,\mathrm{Id}_n$ and consequently $\mathrm{Cond}(V_n) = m$. □

Corollary

RLWE and PLWE over the polynomial family $(\Phi_{2^k})_{k \geq 1}$ are equivalent.

Some Upper Bounds on Cond(V_n) (1/2)

Iván Blanco-Chacón,
On the RLWE/PLWE equivalence for cyclotomic number fields,
Applicable Algebra in Engineering, Communication and Computing (2020).

Theorem (Blanco-Chacón, 2020)

Let $n = p_1 \cdots p_k$, where $p_1 < \cdots < p_k$ are prime numbers. Then

$$\mathrm{Cond}(V_n) \leq 2p_1 \cdots p_k n^{2^k + 2^{k-1} + k + 2}.$$

Corollary

For every fixed $k \geq 1$, RLWE and PLWE over the polynomial family $(\Phi_{p_1 \cdots p_k})_{p_1 < \cdots < p_k}$ are equivalent.

Some Upper Bounds on Cond(V_n) (2/2)

For small k, Blanco-Chacón provided sharper upper bounds:

Theorem (Blanco-Chacón, 2020)

Let $p_1 < p_2 < p_3$ be prime numbers and let $e_1, e_2, e_3 \geq 1$ be integers.

For $n = p_1^{e_1}$ we have that

$$\mathrm{Cond}(V_n) \leq 4\varphi(p_1)m,$$

for $n = p_1^{e_1} p_2^{e_2}$ we have that

$$\mathrm{Cond}(V_n) \leq 2\varphi(p_1 p_2)m^2,$$

and for $n = p_1^{e_1} p_2^{e_2} p_3^{e_3}$ we have that

$$\mathrm{Cond}(V_n) \leq 2\big(\varphi(p_1 p_2 p_3)\big)^2 m^2.$$

Reduction to Squarefree Numbers

Antonio J. Di Scala, C. S., and Edoardo Signorini,
On the condition number of the Vandermonde matrix of the *n*th cyclotomic polynomial, *Journal of Mathematical Cryptology (2020)*.

Theorem (Di Scala, S., Signorini, 2020)

For every positive integer n, we have

$$\mathrm{Cond}(V_n) = \frac{n}{\mathrm{rad}(n)}\,\mathrm{Cond}(V_{\mathrm{rad}(n)}),$$

where $\mathrm{rad}(n)$ *is the product of the prime factors of* n.

Hence, in the study of $\mathrm{Cond}(V_n)$, it suffices to consider only **squarefree** n, that is, numbers of the form $n = p_1 \cdots p_k$, where $p_1 < \cdots < p_k$ are primes.

Exact Formula for $\mathrm{Cond}(V_n)$ when $n = p^k$ and $n = 2^k p^h$

Theorem (Di Scala, S., Signorini, 2020)

For $n = p^k$, with $k \geq 1$ and p a prime number, and for $n = 2^k p^h$, with $k, h \geq 1$ and p an odd prime number, we have that

$$\mathrm{Cond}(V_n) = \sqrt{2\,(1 - 1/p)}\, m.$$

Note that this exact formula improves the previous upper bound for $n = p^k$

$$\mathrm{Cond}(V_n) \leq 4(p-1)m,$$

given by Blanco-Chacón.

Non-Equivalence of RLWE and PLWE over (Φ_n)

Antonio J. Di Scala, C. S., and Edoardo Signorini,
RLWE and PLWE over cyclotomic fields are not equivalent,
Applicable Algebra in Engineering, Communication and Computing (accepted) arXiv: `https://arxiv.org/abs/2201.04365`.

Theorem (Di Scala, S., Signorini, 2020)

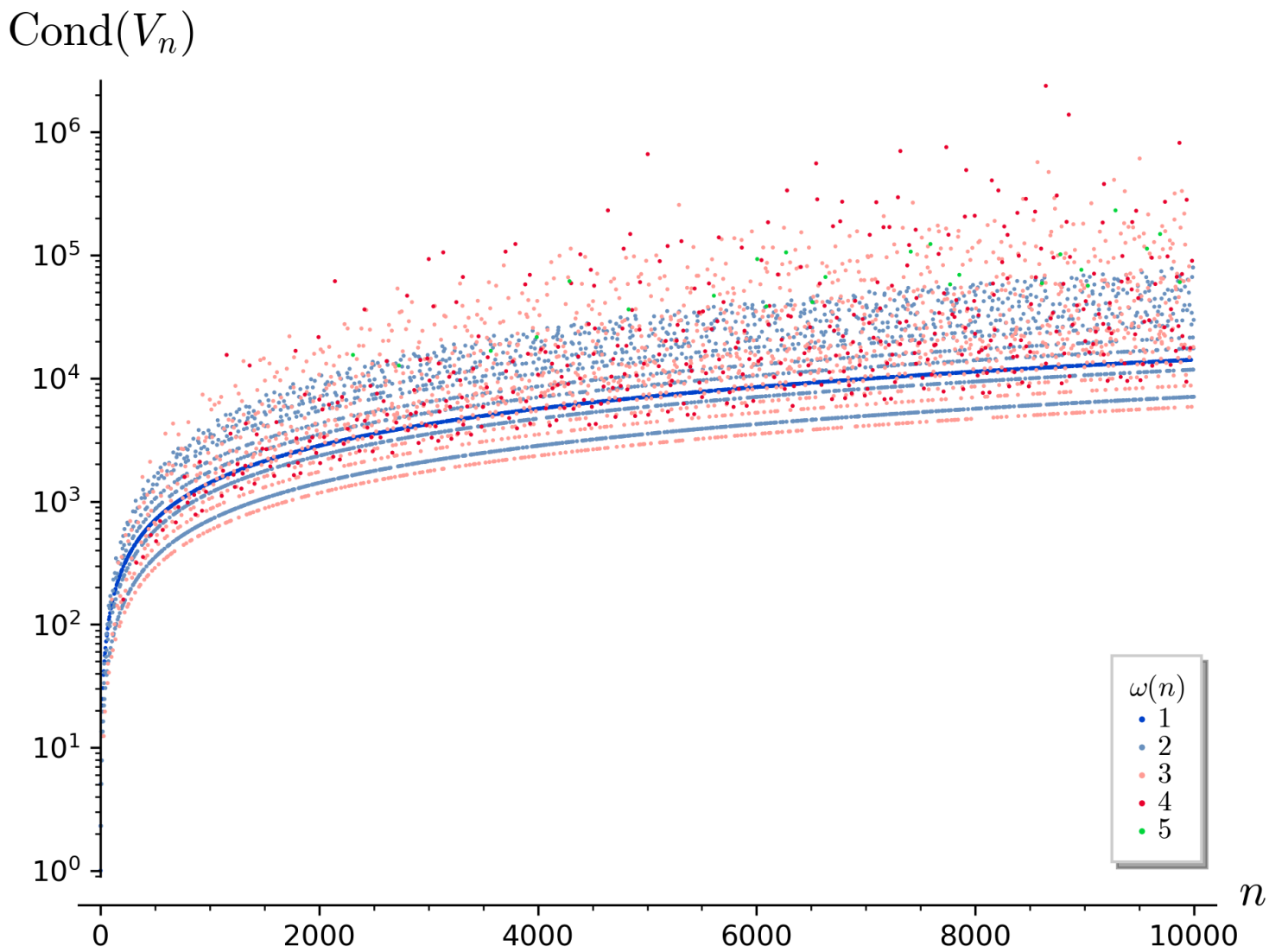
There exist infinitely many positive integers n such that

$$\mathrm{Cond}(V_n) > \exp\left(n^{\log 2 / \log\log n}\right)/\sqrt{n}.$$

In particular, for every $E > 0$, we have that $\mathrm{Cond}(V_n) \neq O\left(n^E\right)$.

Corollary

RLWE and PLWE over cyclotomic fields are not equivalent.



A plot of Cond(V_n) with n squarefree, $1 < n < 10000$. The data is partitioned according to the number $\omega(n)$ of prime factors of n.

(Edoardo Signorini: `https://github.com/edoars/cyclovandermonde`)

Ramanujan's Sums

The **Ramanujan's sum** modulo n is the arithmetic function c_n defined by

$$c_n(t) := \sum_{j=0}^{m-1} \zeta_j^t, \qquad \text{for all } t \in \mathbb{Z}.$$

(Recall that $\zeta_0, \ldots, \zeta_{m-1}$ are the primitive nth roots of unity.)

Ramanujan's sums appear frequently and are important objects in both Analytic and Algebraic Number Theory.

It is easy to check that c_n is an even periodic function with period length n. Furthermore, it holds the *von Sterneck formula*

$$c_n(t) = \mu\left(\frac{n}{(n,t)}\right) \frac{\varphi(t)}{\varphi\left(\frac{n}{(n,t)}\right)}$$

where μ is the Möbius function and (n,t) denotes the greatest common divisor. In particular, $c_n(t)$ is an integer.

Gram Matrix of V_n

Let $G_n := V_n^* V_n$ be the **Gram matrix** of V_n. Then we have

$$G_n = \begin{pmatrix} c_n(0) & c_n(1) & \cdots & c_n(m-1) \\ c_n(1) & c_n(0) & \cdots & c_n(m-2) \\ \vdots & \vdots & \ddots & \vdots \\ c_n(m-1) & c_n(m-2) & \cdots & c_n(0) \end{pmatrix} = \big(c_n(i-j)\big)_{0 \le i,j < m}.$$

In particular, G_n is a symmetric Toeplitz matrix with integer entries.

Let $\lambda_1, \ldots, \lambda_m$ be the eigenvalues of G_n, which are real and positive, since G_n is the Gram matrix of an invertible matrix. Then

$$\mathrm{Cond}(V_n) = \|V_n\| \|V_n^{-1}\| = m\sqrt{\mathrm{Tr}(G_n^{-1})} = m\sqrt{\sum_{i=1}^{m} \frac{1}{\lambda_i}}.$$

Hence, studying $\mathrm{Cond}(V_n)$ is equivalent to studying the eigenvalues of G_n.

Reduction to Squarefree Numbers

The characteristic polynomials of G_n and $G_{\mathrm{rad}(n)}$ are related by:

Lemma

For every positive integer n, we have

$$\det(G_n - x\,\mathrm{Id}_m) = h^m \det\left(G_{n'} - \frac{x}{h}\,\mathrm{Id}_{m'}\right)^h$$

where $n' := \mathrm{rad}(n)$, $m' := \varphi(n')$, and $h := n/n'$.

Proof (Sketch): von Sterneck formula yields that $G_n = h\,G_{n'} \otimes \mathrm{Id}_h$. Then one uses $\det(A \otimes B) = \det(A)^s \det(B)^t$, for $A \in \mathbb{C}^{t\times t}$ and $B \in \mathbb{C}^{s\times s}$. $\square$

Thus the eigenvalues of G_n are the eigenvalues of $G_{\mathrm{rad}(n)}$ multiplied by h both in values and multiplicities. Hence, from the previous considerations, it follows that

$$\mathrm{Cond}(V_n) = \frac{n}{\mathrm{rad}(n)}\,\mathrm{Cond}(V_{\mathrm{rad}(n)}).$$

The Cases $n = p^k$ and $n = 2^k p^h$

Further work with von Sterneck formula shows that G_{2n} and G_n have the same eigenvalues, for every odd positive integer n.

Therefore, the computation of the condition number $\mathrm{Cond}(V_n)$ for $n = p^k$ and $n = 2^k p^h$ is reduced to the computation of $\mathrm{Cond}(V_p)$.

Since

$$G_p = \begin{pmatrix} p-1 & -1 & -1 & \cdots & -1 \\ -1 & p-1 & -1 & \cdots & -1 \\ -1 & -1 & p-1 & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & \cdots & p-1 \end{pmatrix}$$

a bit of computation shows that the eigenvalues of G_p are p and 1, with respective multiplicities $p-2$ and 1.

From this, one gets the formulas for $\mathrm{Cond}(V_{p^h})$ and $\mathrm{Cond}(V_{2^k p^h})$.

The Proof of the Lower Bound for Cond(V_n)

The main difficulty in proving a lower bound for Cond(V_n) is that the entries of V_n^{-1} are sums of roots of unity, and in such sums a lot of "cancellation" can happen. Hence, such sums can be very small, despite having a lot of addends, which makes them difficult to bound from below.

This is strictly related to the fact that the coefficients of the cyclotomic polynomials are usually small, despite being sums of many roots of unity. For instance, expanding the product

$$\Phi_{105}(X) := \prod_{\substack{1 \le k \le 105 \\ \gcd(105,k)=1}} \left(X - \mathrm{e}^{2\pi \boldsymbol{i} k/105}\right),$$

one gets that the coefficient of X^7 in $\Phi_{105}(X)$ is the sum of

$$\binom{48}{7} = 73,629,072$$

roots of unity. Despite that, such coefficient is equal to -2.
(This example is due to D. H. Lehmer (1966).)

Continuing V_n

Let

$$W_n := \begin{pmatrix} 1 & \zeta_0 & \zeta_0^2 & \cdots & \zeta_0^{mn-1} \\ 1 & \zeta_1 & \zeta_1^2 & \cdots & \zeta_1^{mn-1} \\ 1 & \zeta_2 & \zeta_2^2 & \cdots & \zeta_2^{mn-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_{m-1} & \zeta_{m-1}^2 & \cdots & \zeta_{m-1}^{mn-1} \end{pmatrix}$$

be the $m \times mn$ matrix obtained by "continuing" V_n to the right.

Lemma

We have $W_n W_n^* = mn\,\mathrm{Id}_m$.

Proof: The product of the ith row of W_n and the jth column of W_n^* is

$$\sum_{k=0}^{mn-1} \left(\zeta_i \overline{\zeta_j}\right)^k = \begin{cases} mn & \text{if } i = j; \\ 0 & \text{if } i \neq j. \end{cases}$$

(This is the orthogonality of roots of unity.) $\square$.

Coefficients of Φ_n

Let $a_n(j)$ denote the coefficient of X^j in $\Phi_n(X)$, that is,

$$\Phi_n(X) = \sum_{j=0}^{m} a_n(j) X^j.$$

The study of the coefficients of the cyclotomic polynomials has a very long history, which goes back at least to Gauss.

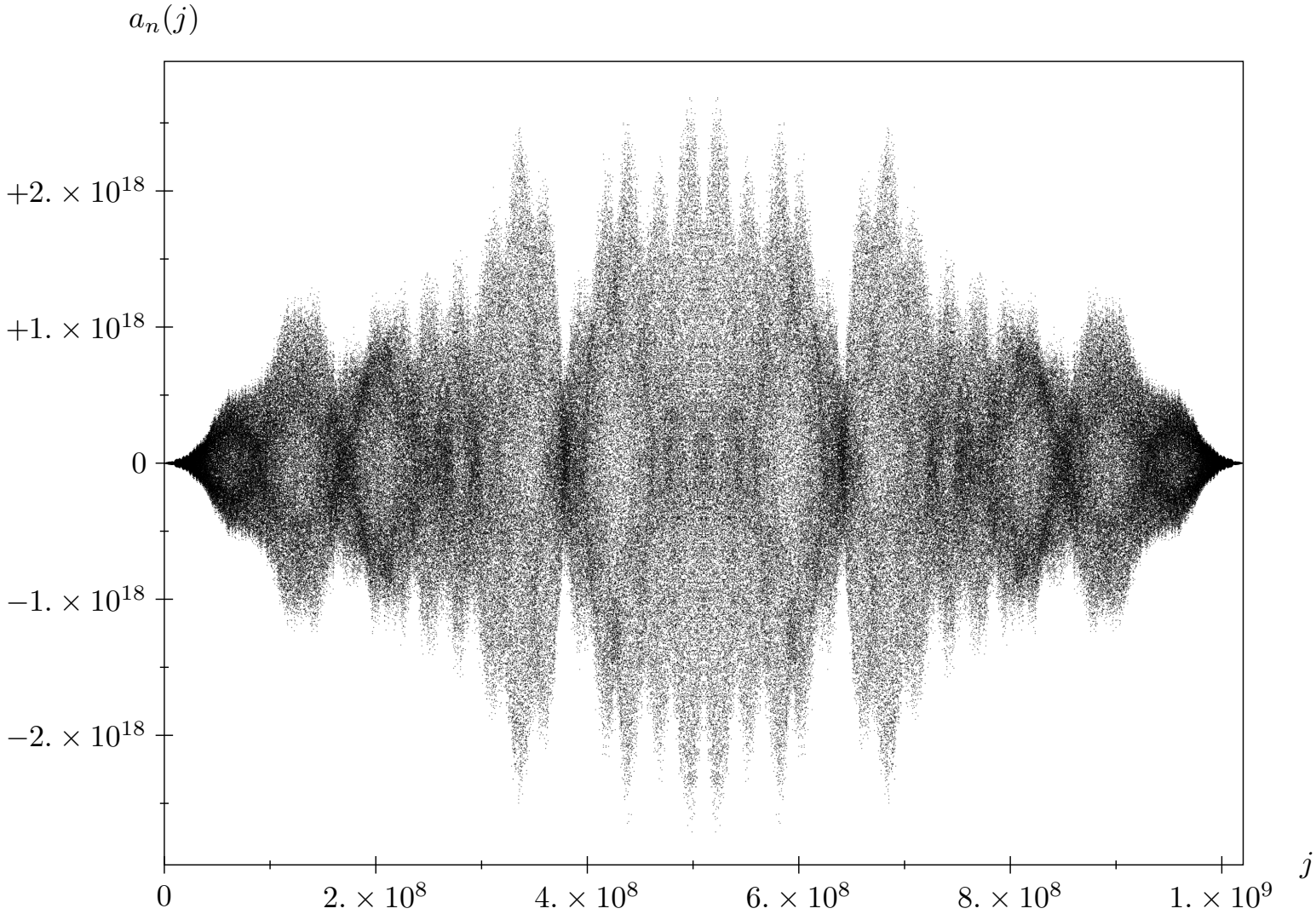
Let $A(n)$ be the maximum of the absolute values of $a_n(0), \ldots, a_n(m-1)$.

Theorem (Vaughan, 1974)

We have $A(n) > \exp\left(n^{\log 2 / \log\log n}\right)$ *for infinitely many positive integers* n.


Robert C. Vaughan, **Bounds for the coefficients of cyclotomic polynomials**, *Michigan Mathematical Journal (1974).*


C. S., **A survey on coefficients of cyclotomic polynomials**, *Expositiones Mathematicae (accepted)* https://arxiv.org/abs/2111.04034.



A plot of the coefficients of $\Phi_n(X)$ for $n = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$. The $\varphi(n) + 1 = 1,021,870,081$ coefficients were computed using the program SPS4_64 of Arnold and Monagan. Then the plot was produced by selecting a random sample of 500,000 coefficients.

Companion Matrix of Φ_n

Let C_n be the **companion matrix** of Φ_n, which is the $m \times m$ matrix

$$C_n := \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_n(0) \\ 1 & 0 & \cdots & 0 & -a_n(1) \\ 0 & 1 & \cdots & 0 & -a_n(2) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_n(m-1) \end{pmatrix},$$

and let

$$S_n := \left(\mathrm{Id}_m \mid C_n^m \mid C_n^{2m} \mid \cdots \mid C_n^{(n-1)m} \right)$$

be the $m \times mn$ matrix given by juxtapositioning the first n powers of C_n^m.

Lemma

We have $V_n^{-1} W_n = S_n$.

A Formula for $\|V_n^{-1}\|$

Lemma

We have $\|V_n^{-1}\|^2 = \frac{1}{mn}\sum_{k=0}^{n-1}\|C_n^{km}\|^2$.

Proof: From $W_n W_n^* = mn\,\mathrm{Id}_m$ and $V_n^{-1}W_n = S_n$, it follows that

$$mn\|V_n^{-1}\|^2 = mn\,\mathrm{Tr}\big(V_n^{-1}(V_n^{-1})^*\big) = \mathrm{Tr}\big(V_n^{-1}W_nW_n^*(V_n^{-1})^*\big) = \mathrm{Tr}(S_nS_n^*).$$

Then, by the definition of S_n, we have that

$$\mathrm{Tr}(S_nS_n^*) = \mathrm{Tr}\left(\left(\mathrm{Id}_m \mid C_n^m \mid \cdots \mid C_n^{(n-1)m}\right)\begin{pmatrix}\mathrm{Id}_m\\ \hline (C_n^m)^*\\ \hline \vdots\\ \hline \left(C_n^{(n-1)m}\right)^*\end{pmatrix}\right)$$

$$= \sum_{k=0}^{n-1}\mathrm{Tr}\big(C_n^{km}(C_n^{km})^*\big) = \sum_{k=0}^{n-1}\|C_n^{km}\|^2. \quad \square$$

Powers of the Companion Matrix C_n

Lemma

Let k be a positive integer and let

$$C := \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_{k-1} \end{pmatrix} \in \mathbb{C}^{k \times k}.$$

Then, for every integer $j \in [1, k]$, the $(k-j)$th column of C^j is equal to $\begin{pmatrix} c_0 & c_1 & \cdots & c_{k-1} \end{pmatrix}^\mathsf{T}$. (Note: The first column if the 0th.)

Proof: Actually, a stronger claim holds: For every integer $j \in [1, k]$, the 0th, 1th, ..., $(k-j)$th columns of C^j are equal to the $(j-1)$th, jth, ..., $(k-1)$th columns of C, respectively. This follows easily by induction on j.

The Lower Bound for Cond(V_n)

Putting all together, we get that

$$\|V_n^{-1}\|^2 = \frac{1}{mn}\sum_{k=0}^{n-1}\|C_n^{km}\|^2 \geq \frac{1}{mn}\|C_n^m\|^2 \geq \frac{1}{mn}\sum_{j=0}^{m-1}|a_n(j)|^2 \geq \frac{1}{mn}A(n)^2.$$

where in the second inequality we used the previous lemma (since $m < n$). In turn, this implies that

$$\mathrm{Cond}(V_n) = \|V_n\|\,\|V_n^{-1}\| = m\,\|V_n^{-1}\| \geq \sqrt{\frac{m}{n}}\,A(n) \geq \frac{1}{\sqrt{n}}\,A(n).$$

As a consequence, Vaughan's lower bound for $A(n)$ yields that

$$\mathrm{Cond}(V_n) > \exp\left(n^{\log 2/\log\log n}\right)/\sqrt{n},$$

for infinitely many positive integers n.

Conclusions

We settled the question of the equivalence between RLWE and PLWE over cyclotomic fields by answering it negatively.

Therefore, from both a practical and a theoretical point of view, future investigations have to keep in mind that, in general, over cyclotomic fields, results on RLWE cannot be translated into results on PLWE, and vice versa, unless further restrictions on the polynomials $\Phi_n(X)$ are imposed.

Some natural questions for future research are the following:

Question 1

Is there an "explicit formula" for $\mathrm{Cond}(V_{pq})$, with $p < q$ prime numbers?

Question 2

What is the maximal order of $\mathrm{Cond}(V_n)$ as $n \to +\infty$?