Ring-LWE, Ideal Lattices and Class Numbers

Heiko Knospe

Technische Hochschule Köln

10 November 2025

Abstract

The Ring Learning with Errors (RLWE) problem is widely believed to be computationally hard and underpins many modern cryptographic constructions. Its security is supported by a reduction from worst-case problems on ideal lattices to average-case instances of RLWE.

We introduce ideal lattices arising from cyclotomic fields and explain the RLWE problem. We then explore methods to find mildly short vectors in ideal lattices, emphasizing the role of the plus and the minus class groups. We consider the growth of class numbers and discuss different parameter choices for RLWE that can influence the hardness of the underlying approximate shortest vector problem.

Topics

- Lattices and ideal lattices
- The Ring Learning with Errors (RLWE) problem
- The approximate Shortest Vector Problem (SVP) in ideal lattices
- Class numbers and new parameters for RLWE

Lattice

A lattice Λ is a discrete subgroup of an n-dimensional Euclidean vector space V. A full-rank lattice is defined by a basis $v_1, v_2, \ldots, v_n \in V$ such that

$$\Lambda = \{x_1 v_1 + x_2 v_2 + \cdots + x_n v_n \mid x_i \in \mathbb{Z}\}.$$

If B is the matrix whose columns are the coordinates of $v_1, \ldots, v_n$ in an orthonormal basis, then

$$\Lambda = \{Bx \mid x \in \mathbb{Z}^n\}.$$

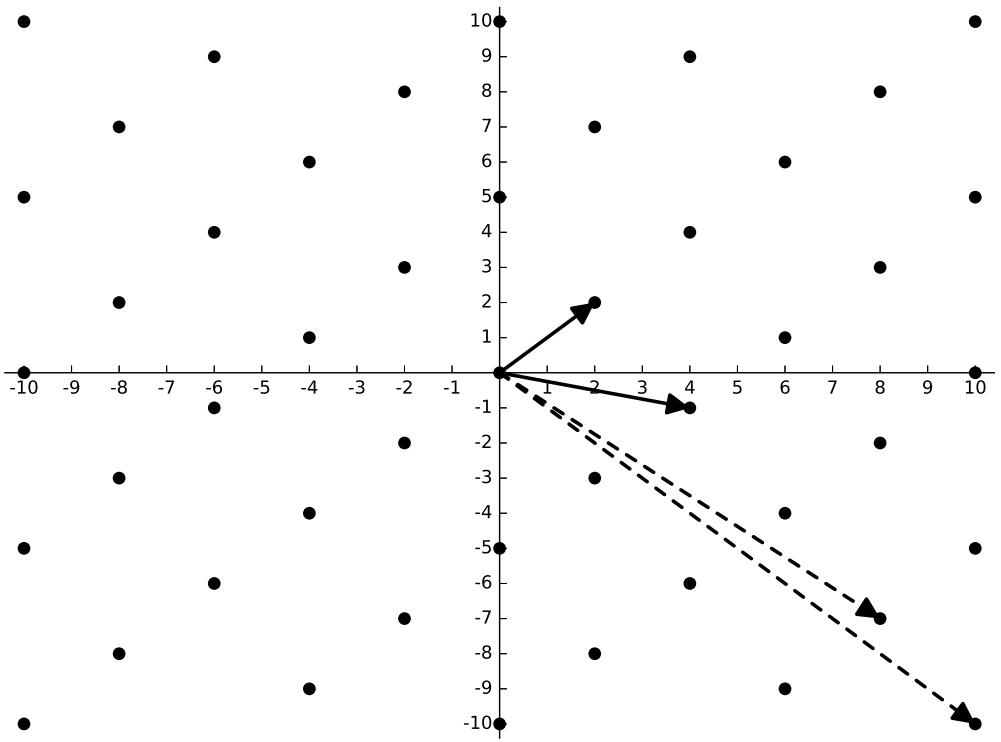
The space of all lattices can be identified with $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$.

Example: Different Bases of a Lattice

A lattice can admit many distinct bases. For example,

$$B_1 = \left\{ \begin{pmatrix} 4 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \end{pmatrix} \right\}, \quad B_2 = \left\{ \begin{pmatrix} 8 \\ -7 \end{pmatrix}, \begin{pmatrix} 10 \\ -10 \end{pmatrix} \right\}.$$

B_1 is illustrated with solid lines and B_2 with dashed lines.



Determinant and Lattice Volume

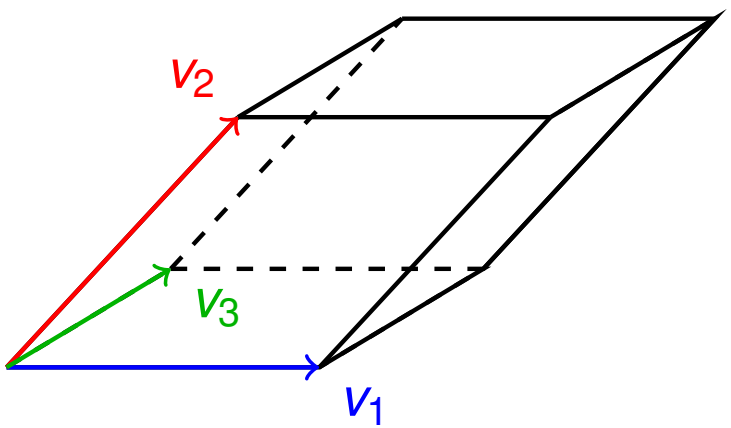
The basis $B = (v_1, \ldots, v_n)$ defines the fundamental parallelepiped

$$P = \{x_1 v_1 + \cdots + x_n v_n \mid x_i \in [0, 1)\}.$$

The lattice volume is the absolute determinant and can also be computed using the Gram matrix of inner products:

$$\det(\Lambda) = |\det(B)| = \sqrt{\det(v_i \cdot v_j)_{1 \leq i,j \leq n}}.$$

This quantity represents the volume of P and is invariant under a change of basis.



Dual Lattice

Definition

Given lattice Λ, the dual lattice is

$$\Lambda^* = \{y \in V \mid x \cdot y \in \mathbb{Z} \text{ for all } x \in \Lambda\}.$$

If Λ has basis matrix B, then

$$\Lambda^* = \{(B^T)^{-1}x \mid x \in \mathbb{Z}^n\},$$

and consequently,

$$\det(\Lambda^*) = \frac{1}{\det(\Lambda)}.$$

Computational Problems

The following lattice problems are considered to be hard, even for quantum computers:

1. **Shortest Vector Problem (SVP):** Find the shortest nonzero vector in Λ.
2. **Shortest Independent Vector Problem (SIVP):** Find n linearly independent lattice vectors each as short as possible.
3. **Closest Vector Problem (CVP):** Given $w \in V$, find the closest lattice vector to w.

Note: There are also easy lattice problems, such as testing membership in Λ.

Approximate Lattice Problems

Definition (Approximate SVP)

Let $\gamma \geq 1$. If v is the shortest lattice vector of Λ, any $w \in \Lambda$ satisfying

$$\|w\| \leq \gamma \|v\|$$

solves SVP_γ.

Approximations within polynomial $\gamma(n)$ remain computationally hard; exponential factor approximations are feasible in polynomial time.

Ideal Lattices

Let $K = \mathbb{Q}(\zeta_m)$ be the cyclotomic field of degree $n = \varphi(m)$. Its ring of integers is $R = O_K = \mathbb{Z}[\zeta_m]$. The canonical embedding

$$\sigma : K \to \mathbb{C}^n, \quad x \mapsto (\sigma_1(x), \ldots, \sigma_n(x)),$$

is defined by the $n = s_1 + 2s_2$ embeddings σ of K into $\mathbb{R}$ or $\mathbb{C}$. The image is contained in the subspace $H \cong K \otimes_{\mathbb{Q}} \mathbb{R} = K_{\mathbb{R}}$ of dimension n over $\mathbb{R}$ defined by $x_{s_1+s_2+j} = \overline{x_{s_1+j}}$.

The image of a fractional ideal $I \subset K$ is a lattice in H. We endow H with the inner product $< , >$ induced by $\mathbb{C}^n$. The inner product of $x, y \in K$ satisfies

$$Tr(x \cdot y) = < x, \overline{y} >$$

where $Tr : K \to \mathbb{Q}$ is the trace map. This defines an ℓ_2-norm on K.

Volume of Ideal Lattices

The ring of integers $R = O_K$ is a lattice of volume

$$\mathrm{vol}\,(R) = \sqrt{|\Delta_K|}$$

where $b_1, \ldots, b_n$ is an arbitrary $\mathbb{Z}$-basis of R and

$$\Delta_K = \det\big(\mathit{Tr}(b_i b_j)_{1 \le i,j \le n}\big)$$

denotes the absolute discriminant of K. For fractional ideal I,

$$\mathrm{vol}\,(I) = N(I)\sqrt{|\Delta_K|}\,.$$

Bounds on Shortest Vector Lengths

Define the root discriminant:

$$\delta_K = \mathrm{vol}\,(R)^{1/n} = \sqrt{|\Delta_K|}^{1/n}$$

For fractional ideal I, the shortest lattice vector length $\lambda_1(I)$ satisfies

$$\sqrt{n}\, N(I)^{1/n} \leq \lambda_1(I) \leq \sqrt{n}\, N(I)^{1/n}\, \delta_K$$

Proof.

Lower bound follows from the AM-GM inequality, and the upper bound follows from Minkowski's theorem. □

Note: The Gaussian heuristic estimates

$$\lambda_1(I) \approx \sqrt{n/(2\pi e)}\,\mathrm{vol}\,(I)^{1/n}.$$

Duality

Let I be a fractional ideal. The dual ideal $I^\vee$ is

$$I^\vee = \{x \in K \mid Tr(xI) \subset \mathbb{Z}\}.$$

The embedding relates the dual ideal $I^\vee$ to the conjugate of the dual lattice:

$$\sigma(I^\vee) = \overline{\sigma(I)^*}$$

For $R = \mathbb{Z}[\zeta_m]$, the dual ideal $R^\vee$ is the codifferent

$$R^\vee = \frac{1}{\Phi'_m(\zeta_m)} R,$$

where Φ_m denotes the m-th cyclotomic polynomial.

Example

$R^\vee = \frac{1}{2^{k-1}} R$ for $m = 2^k$ and $R^\vee = \frac{(1-\zeta_p)}{p} R$ if $m = p$ is prime.

Ring-LWE Problem

Let $K = \mathbb{Q}(\zeta_m)$ and $R = \mathbb{Z}[\zeta_m]$. Choose modulus $q \equiv 1 \pmod{m}$ of polynomial size in n. Set $R_q = R/(q)$ and $R_q^\vee = R^\vee/(qR^\vee)$. Sample a secret $s \in R_q^\vee$ uniformly at random. For random $a \in R_q$ and error $e \in K_\mathbb{R}/qR^\vee$ from a spherical Gaussian with parameter r, define

$$b = a \cdot s + e.$$

Search RLWE Problem: Given pairs (a, b), find s.

Decision RLWE Problem: Distinguish (a, b) from uniform random pairs.

Dual vs Non-Dual RLWE

RLWE initially uses the dual lattice $R^\vee$, but practical schemes often use a scaled RLWE variant with R:

Multiplying by a generator $t = \Phi'_m(\zeta_m)$ of the different ideal gives

$$b = as + e,$$

with $a, s \in R_q$ and e an elliptical Gaussian error.

For power-of-two cyclotomics, one has $t = \frac{m}{2}$. Hence scaling preserves spherical error shape.

Efficient Ring Multiplication via NTT

Since q splits completely in R, we have the Chinese Remainder decomposition

$$R_q \cong \prod_{i \in \mathbb{Z}_m^\times} R/\mathfrak{q}_i \cong \prod_{i \in (\mathbb{Z}/m\mathbb{Z})^\times} \mathbb{Z}_q,$$

where $\mathfrak{q}_i = (q, \zeta_m - \omega_m^i)$ and $\omega_m \in \mathbb{Z}_q$ is a primitive m-th root of unity.

This allows multiplication in R_q to be performed efficiently via the Number-Theoretic Transform (NTT).

Worst-case to average-case reduction for RLWE

RLWE has a worst-case to average-case reduction for *ideal lattices*.

Theorem (Lyubashevsky, Peikert, Regev)

Suppose RLWE is defined as above and assume that the error elements are drawn from a Gaussian distribution with parameter $r \geq 2\omega(\sqrt{\log(n)})$ *in each coordinate. There is a polynomial-time quantum reduction from the worst-case SVP problem on ideals in* K *to within approximation factor* $\tilde{O}(\sqrt{n}q/r)$ *to the average-case search RLWE problem.*

There is a similar reduction for the *decision RLWE problem*. This provides theoretical security grounding for RLWE-based cryptography.

Hardness of Ideal-SVP

Theorem (Cramer, Ducas, Wesolowski)

Ideal-SVP in the worst case can be solved in quantum polynomial time for approximation factor $\exp(\tilde{O}(\sqrt{n}))$.

This contrasts with an approximation factor $\exp(\Theta(n))$ for general lattices, revealing a hardness gap.

Recent Approaches to Ideal-SVP

Two major steps in recent attack approaches:

1. Solve the Principal Ideal Problem (PIP) — find short generators of principal ideals.
2. Solve the Close Multiple Problem (CMP) — reduce general ideals to principal ones via multiplication by short ideals.

These reduce Ideal-SVP to seemingly easier subproblems involving class groups and unit lattices.

Mildly short vectors in Ideals

Let $\mathfrak{a}$ be a given ideal. Find a small ideal integral $\mathfrak{b}$ and $\mathfrak{c}$ such that $\mathfrak{abc}$ is principal. Suppose one can solve CMP and $N(\mathfrak{bc}) \leq \exp(\tilde{O}(n^{1+c}))$ for $c < \frac{1}{2}$. Furthermore, suppose one can solve the principal ideal problem for $\mathfrak{abc}$ and find a generator g such that

$$\|g\| \leq N(\mathfrak{abc})^{1/n} \exp(\tilde{O}(\sqrt{n})) \leq N(\mathfrak{a})^{1/n} \exp(\tilde{O}(\sqrt{n}))$$

Then g solves the shortest vector problem for $\mathfrak{a}$ to within a sub-exponential approximation factor.

Principal Ideal Problem (PIP)

Given a principal ideal $\mathfrak{a} \subset R$, find a generator h such that

$$\|h\| \leq N(\mathfrak{a})^{1/n} \exp(\tilde{O}(\sqrt{n})).$$

1. Find any generator g.
2. Use the logarithmic embedding

$$Log : K^{\times} \to \mathbb{R}[G]/(1-\tau),$$

where τ denotes the complex conjugation. Let C be the multiplicative group of cyclotomic units. Then the lattice $Log(C)$ has full rank in a subspace of codimension 1 and a set of short generators. Find $u \in C \subset R^{\times}$ such that $Log(u)$ is close to $Log(g)$, which is a CVP problem in the lattice $Log(C)$. Then $Log(g) - Log(u) = Log(gu^{-1})$ is short and $h = gu^{-1}$ is a mildly short generator.

Close Multiple Problem (CMP)

Solve the Close Multiple Problem (CMP): given an ideal $\mathfrak{a}$, multiply by short ideals such that the product is a principal ideal.

The ideal class group $Cl(K) = I(K)/P(K)$ (fractional ideals modulo principal ideals) plays an important role in solving CMP.

Let $Cl(K^+)$ be the class group of the maximal real subfield $K^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ and define $Cl^-(K)$ by the exact sequence

$$1 \longrightarrow Cl^-(K) \longrightarrow Cl(K) \overset{N_{K/K^+}}{\longrightarrow} Cl(K^+) \longrightarrow 1.$$

We denote the associated class numbers by $h(K)$, $h^+(K)$ and $h^-(K) = h(K)/h^+(K)$.

Close Multiple Problem (CMP)

1. Given $\mathfrak{a}$, find a small ideal $\mathfrak{b}$ such that the class of $\mathfrak{ab}$ is in $Cl^-(K)$. To this end, multiply $\mathfrak{a}$ with random short ideals such that the product $\mathfrak{ab}$ lands in $Cl^-(K)$.
2. Construct an ideal $\mathfrak{c}$ such that $\mathfrak{abc}$ is principal. Use the fact that the Stickelberger ideal annihilates $Cl(K)$. The projected Stickelberger ideal gives a sublattice of $\mathbb{Z}[G]/(1+\tau)$ and has short generators. Find a set of short $\mathbb{Z}[G]$-generators of $Cl^-(K)$ and expand $\mathfrak{ab}$ (in quantum polynomial time) with respect to that factor base. Then reduce the coefficients using the Stickelberger lattice. This yields a short ideal $\mathfrak{b}'$ in the same class as $\mathfrak{ab}$. Define $\mathfrak{c} = (\mathfrak{b}')^{-1}$. Then $\mathfrak{abc}$ is a principal ideal.

Success depends on properties of plus and minus parts of class groups.

Plus Part $h^+(K)$

The plus part $h^+(K)$ often equals 1 and is notoriously difficult to compute.

Theorem (Sinnott)

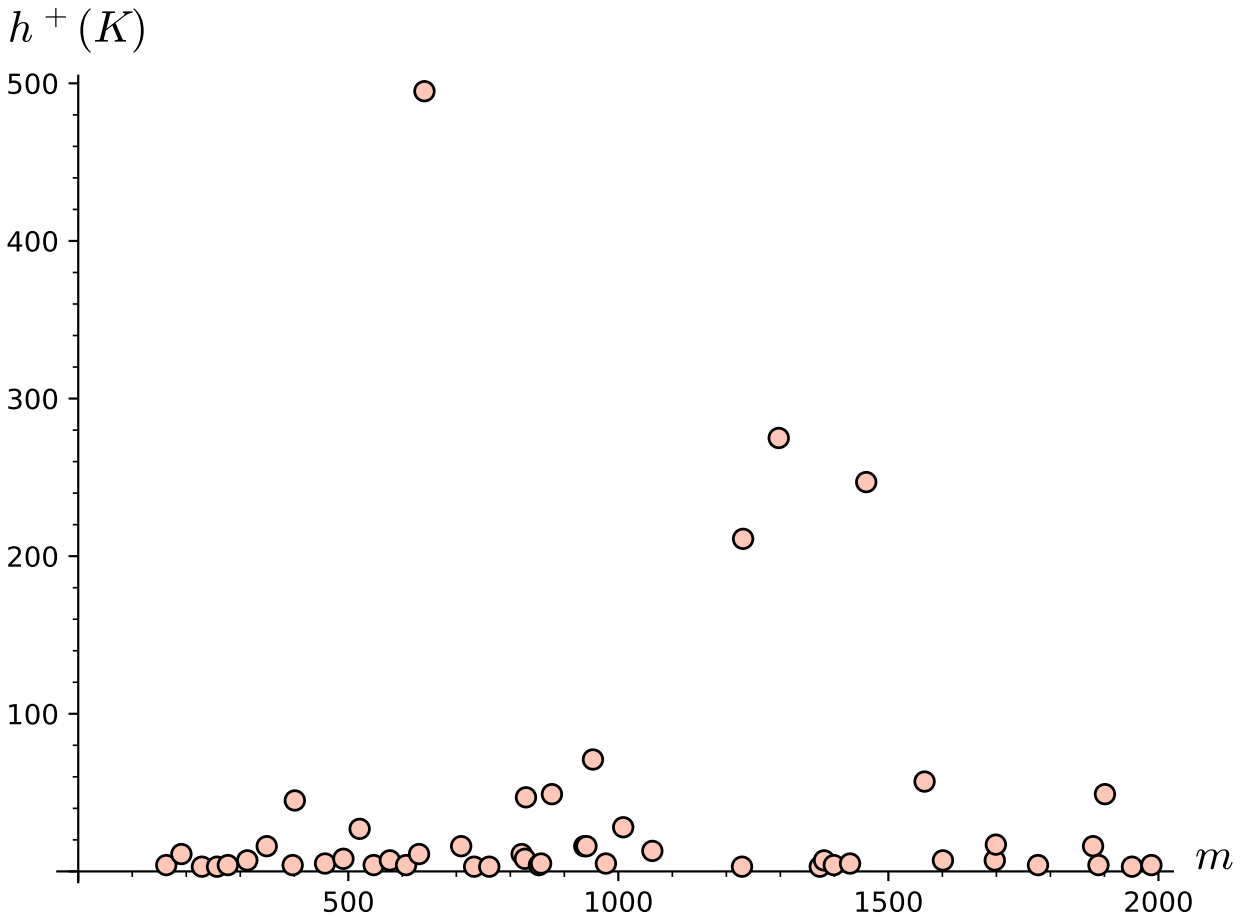
Let $K = \mathbb{Q}(\zeta_m)$ and let C^+ be the subgroup of cyclotomic units of K^+. Then C^+ is of finite index in $(R^+)^\times$ and

$$2^b h^+(K) = [(R^+)^\times : C^+],$$

where b depends on the number of distinct prime factors of m.

Numerical Results on $h^+(K)$

Computations by Schoof for primes $p < 10^5$ (up to a factor that is probably 1) suggest slow polynomial growth of $h^+(K)$.



Minus Part of the Class Number

The analytic class number formula gives:

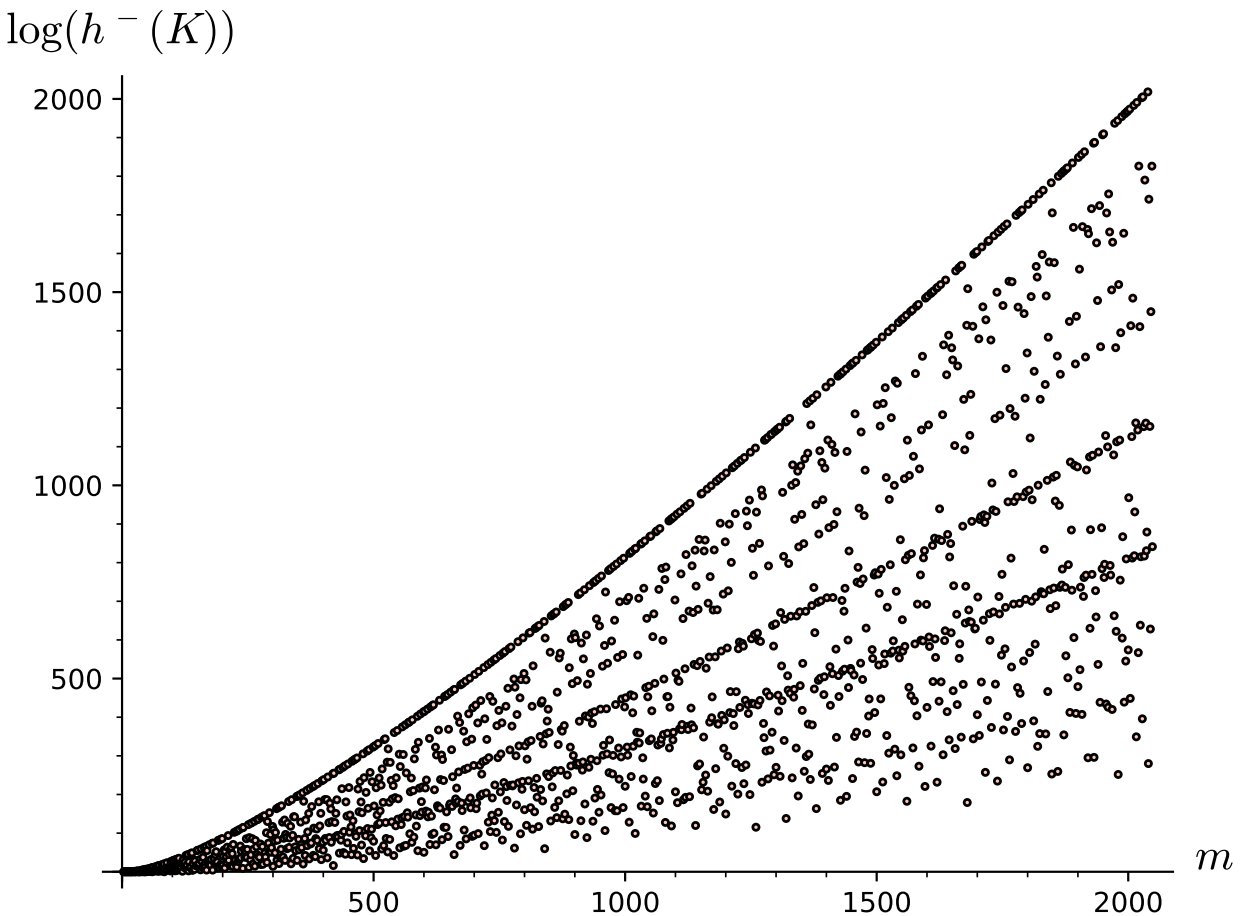
$$h^-(K) = Qw \prod_{\chi \text{ odd}} (-\frac{1}{2} B_{1,\chi})$$

where χ runs over odd Dirichlet characters of $Gal(K/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$ and $B_{1,\chi}$ are Bernoulli numbers. The constants Q and w depend on m:

$$Q = \begin{cases} 1 & \text{if } m = p^k \\ 2 & \text{otherwise} \end{cases} \quad \text{and} \quad w = \begin{cases} 2m & \text{if } m \text{ is odd} \\ \text{m} & \text{otherwise} \end{cases}$$

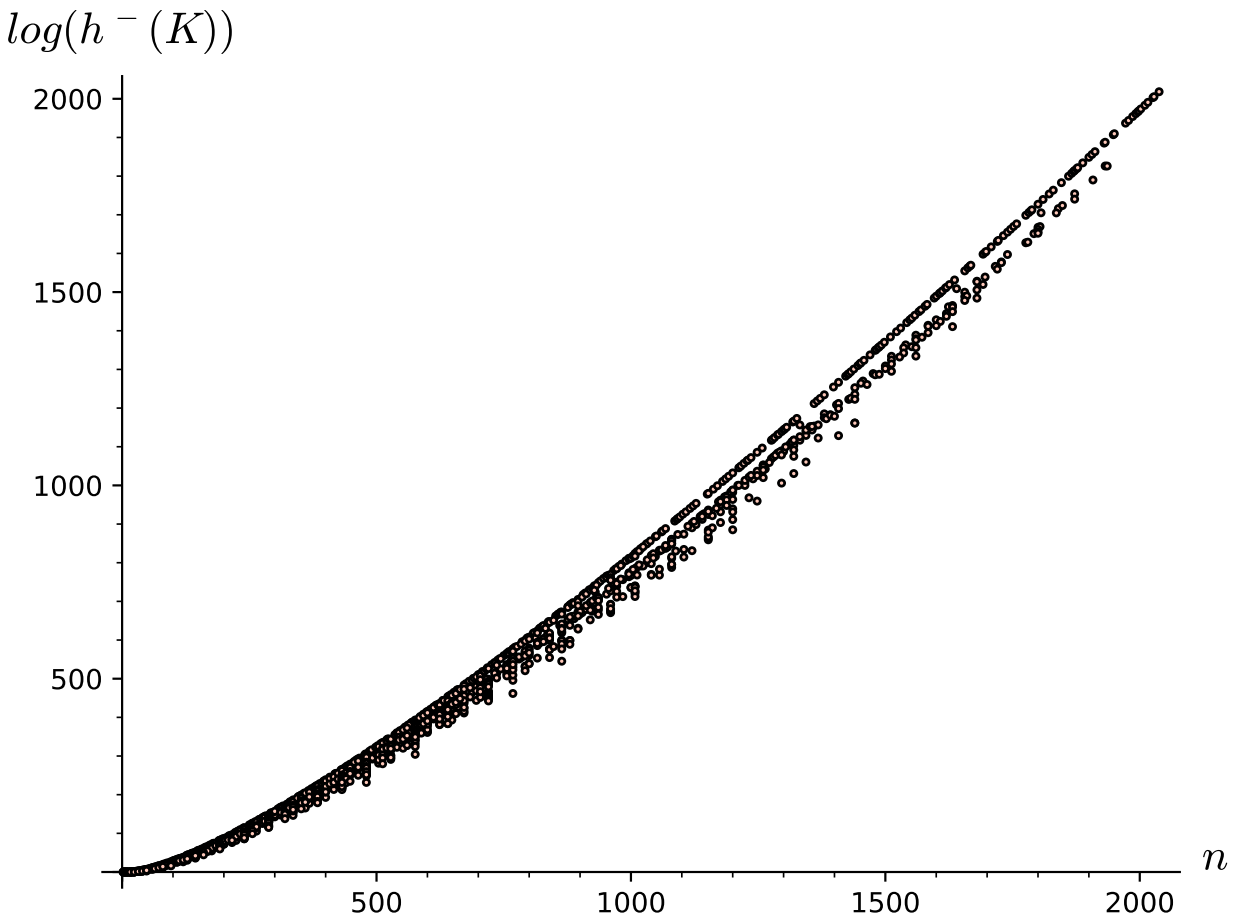
Numerical Results on $h^-(K)$

$\log(h^-(K))$ is bounded by $\tilde{O}(m)$.



Growth of $h^-(K)$

$h^-(K)$ depends more on $n = \varphi(m)$ than on m.



Growth of Class Numbers via Iwasawa Theory

Let p be a prime and $K = \mathbb{Q}(\zeta_m)$ with $p \mid m$ and $p^2 \nmid m$. Define $K_r = \mathbb{Q}(\zeta_{mp^r})$; the cyclotomic $\mathbb{Z}_p$-tower $K = K_0 \subset K_1 \subset K_2 \subset \dots$ is a classical setting of Iwasawa theory. The p-part of $h(K_r)$ grows as

$$p^{\lambda_p r + c}$$

for large r, where λ_p is the Iwasawa λ-invariant of the tower. Similarly, one defines λ_p^+ and λ_p^-.

Conjecture (Greenberg): $\lambda_p^+(K) = 0$.

For every fixed $\ell \neq p$, the ℓ-part of $Cl(K_r)$ remains bounded along the tower.

Lambda-Invariants

Let $K = \mathbb{Q}(\zeta_p)$. Then $\lambda_p^-(K) = 0$ if and only if $p \nmid h^-(K)$. In this case, p is called a **regular prime**, which plays an important role in the proof of Fermat's Last Theorem. It is predicted that $e^{-1/2} \approx 60.65\%$ of all primes are regular.

More generally, for $K = \mathbb{Q}(\zeta_m)$ with $p \mid m$ and $p^2 \nmid m$, the p-adic L-functions attached to Dirichlet characters χ of $Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ have associated Iwasawa invariants $\lambda_p(\chi)$, and $\lambda_p^-(K)$ aggregates the contributions from *odd* characters.

There is a conjecture (and numerical evidence) from Delbourgo and K. regarding the distribution of $\lambda_p(\chi)$-invariants.

RLWE Parameters with Power-of-Two Cyclotomics

Most RLWE-based cryptographic schemes use power-of-two cyclotomic fields $K = \mathbb{Q}(\zeta_{2^k})$ due to efficiency and simple structure. Usually,

$$h^+(K) = 1, \quad \text{and} \quad \lambda_2(K) = 0.$$

m	$\varphi(m)$	$h^+(K)$	$\log(h^-(K))$	Example q with $q \equiv 1 \bmod m$
256	128	1	43.79	3329, 7681
512	256	1	126.17	$3329^{\#}$, 8380417
1024	512	1^*	335.21	12289, $2^{60} - 2^{10} \cdot 512 \cdot 6700417$
2048	1024	1^*	841.34	12289, 18433, 40961

$^{\#}$: $q \equiv 1 \mod \frac{m}{2}$

*: Conjectural values

Alternative Parameters

Prime cyclotomic fields $K = \mathbb{Q}(\zeta_p)$ may offer harder Ideal-SVP problems:

$m = p$	$\varphi(m)$	$h^+(K)$	$\log(h^-(K))$	$\lambda_p^-(K)$	Example q
257	256	3	126.04	1	1543, 9767
401	400	45	238.64	1	3209, 4813
641	640	495	453.42	0	3847, 12821
1297	1296	275	1139.16	2	5189, 20753
3547	3546	16777	3996.52	0	21283

Summary and Open Problems

- Using cyclotomic rings other than power-of-two may strengthen Ideal-SVP hardness and cryptographic security.
- Large class numbers add complexity to attacks based on class group structure.
- No known efficient reduction from RLWE to Ideal-SVP.
- There are reductions from MLWE to RLWE and from Module-SVP to Ideal-SVP, but in practice MLWE schemes are becoming preferred.
- The dual and non-dual RLWE forms are equivalent but differ in error distribution properties.
- For prime cyclotomics, error distortion of non-dual RWLE forms complicates direct hardness assumptions.