Générateurs courts d'idéaux principaux dans certaines extensions de Kummer réelles

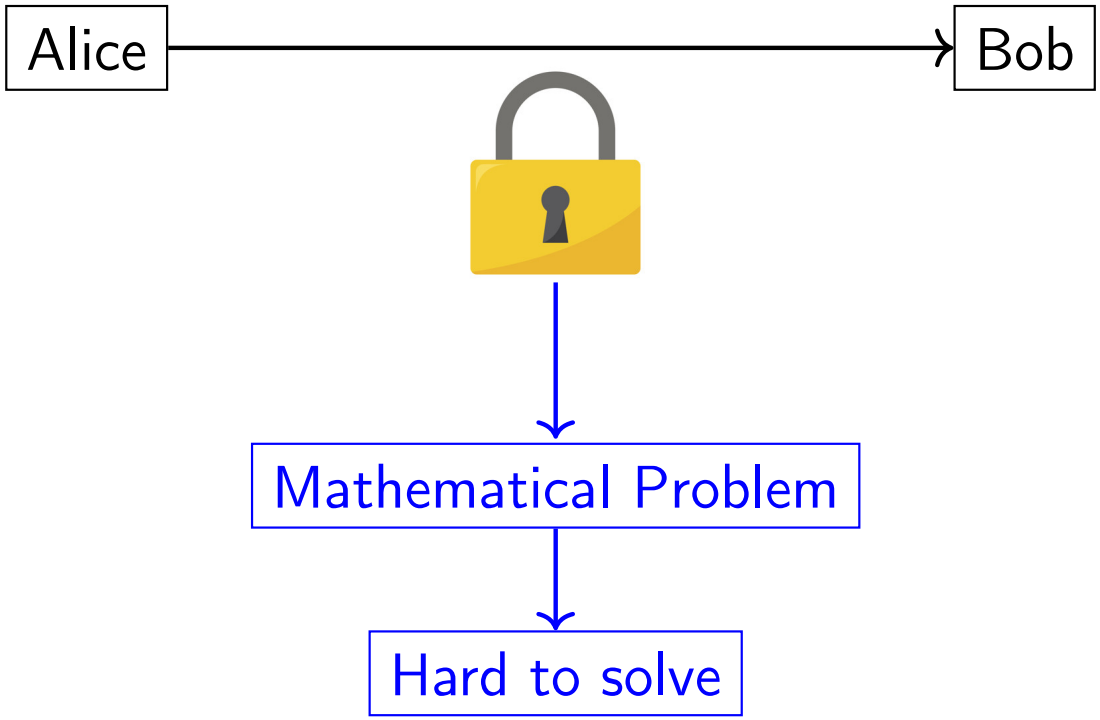
Andrea LESAVOUREY Thomas PLANTARD Willy SUSILO

School of Computing and Information Technology
University of Wollongong

Outline

1. Motivation
   - Cryptography
   - Lattice-based cryptography
2. Recalls
   - Lattices
   - Cryptography and ideal lattices
3. Relative real Kummer extensions
   - General framework
   - Results

Cryptography



Post-quantum cryptography

- ⋆ Two main mathematical problems : Factorization and Discrete Logarithm.
- ⋆ Quantum computers break these problems (Shor 1994)
- ⋆ The American National Security Agency (NSA) announced they were considering quantum computers as a real threat and were moving towards post-quantum cryptography.
- ⋆ April 2016 : The American National Institute for Standards and Technology (NIST) announced it will launch a call for standardization for post-quantum cryptosystems.
  $\longrightarrow$ now in Round 2.

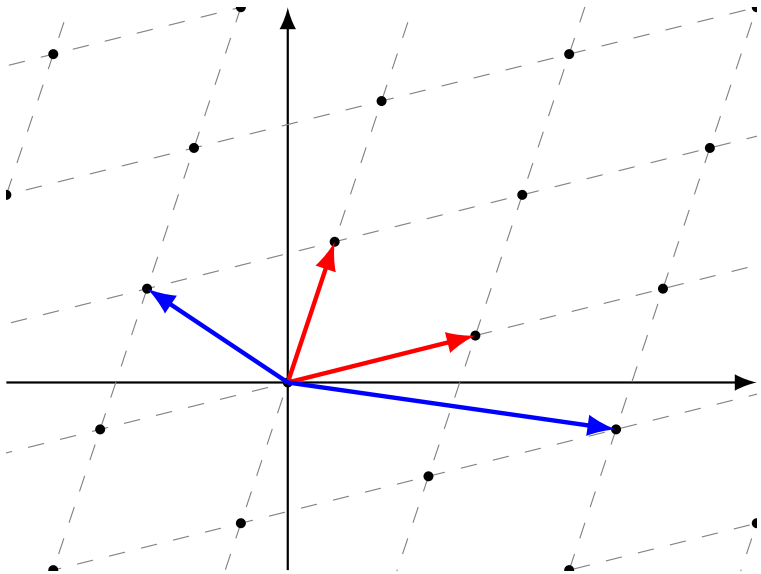
Lattice-based cryptography

- ⋆ One family of post-quantum cryptography is based on euclidean lattices.
- ⋆ For efficiency reasons we use structured lattices e.g. ideal lattices.
- ⋆ In Round 2 candidates: 9 over 17 KEMs/Encryption and 3 over 9 Signature schemes are based on lattices

General Context

Definition

We call lattice any discrete subgroup $\mathcal{L}$ of $\mathbb{R}^n$ where n is a positive integer i.e. a free $\mathbb{Z}$-submodule of $\mathbb{R}^n$

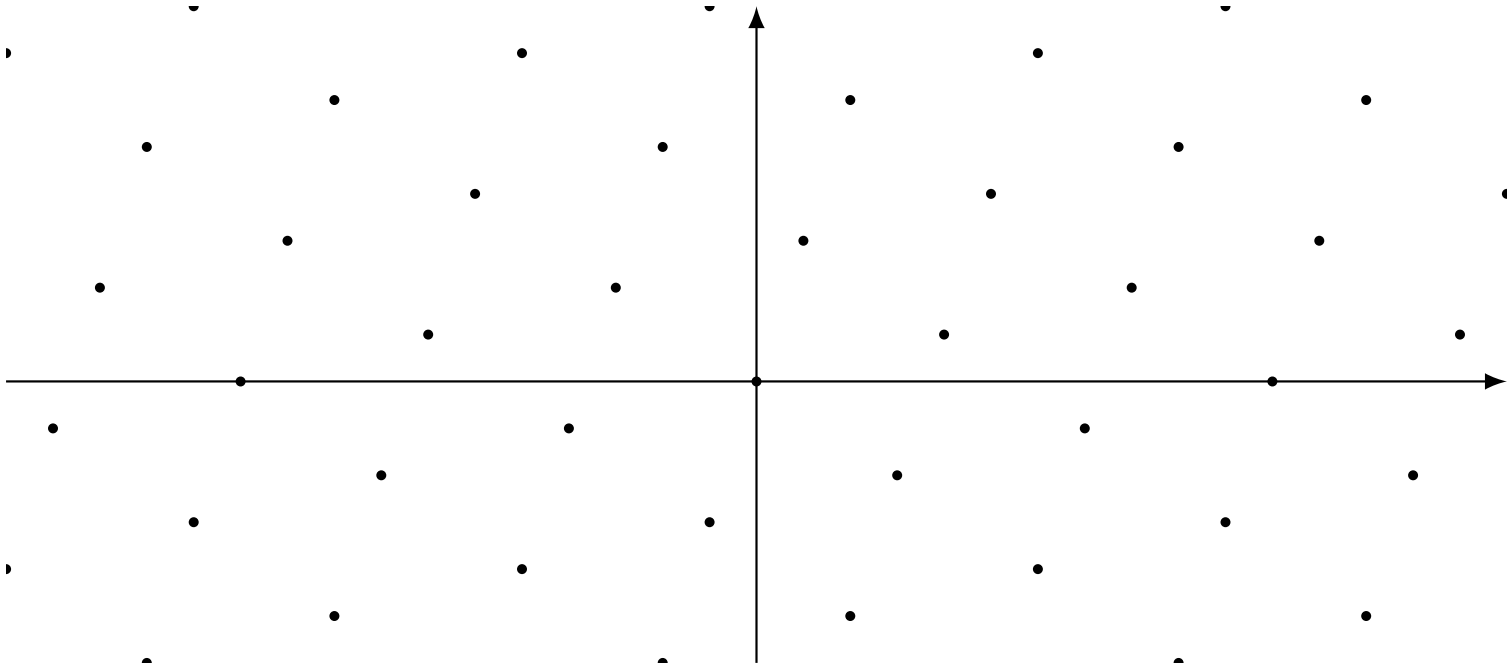


Any set B of free vectors which generates $\mathcal{L}$ is called a basis.

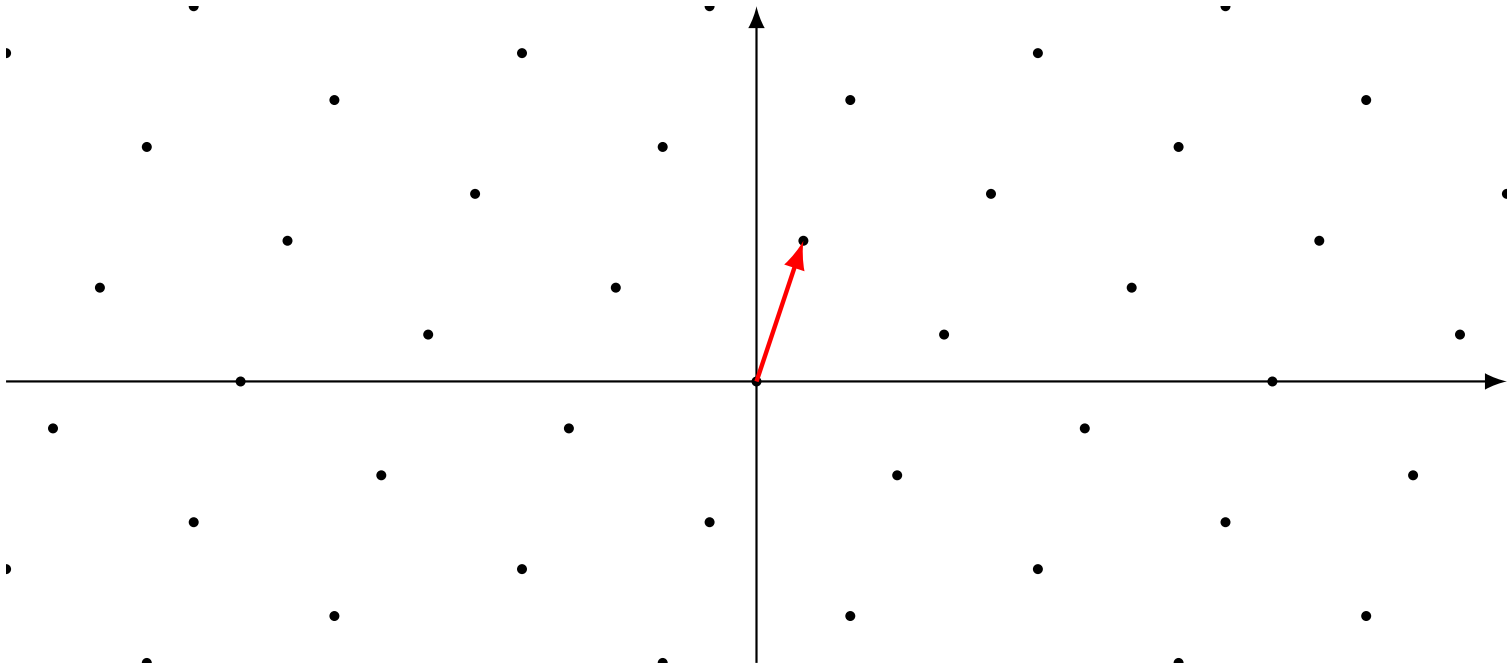
There are infinitely many bases.

Some are considered better than others : orthogonality, short vectors

Problems on lattices

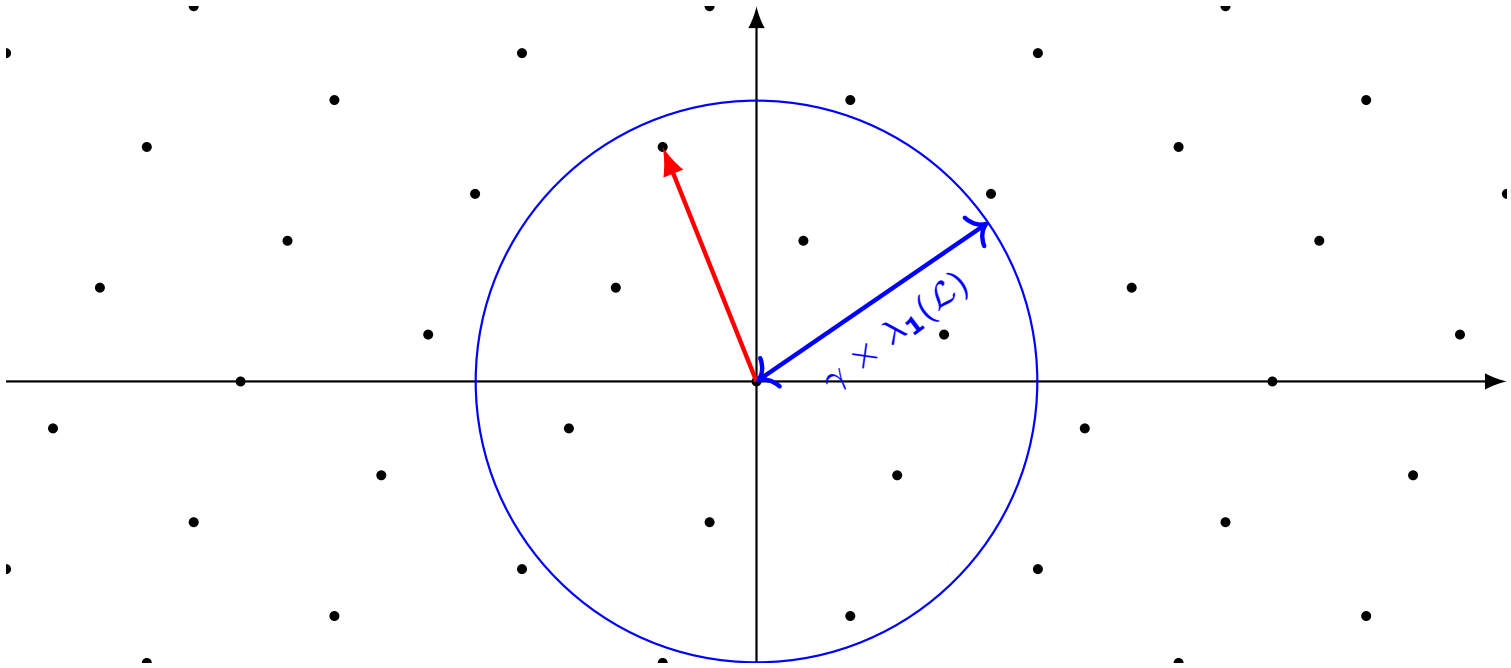


Problems on lattices



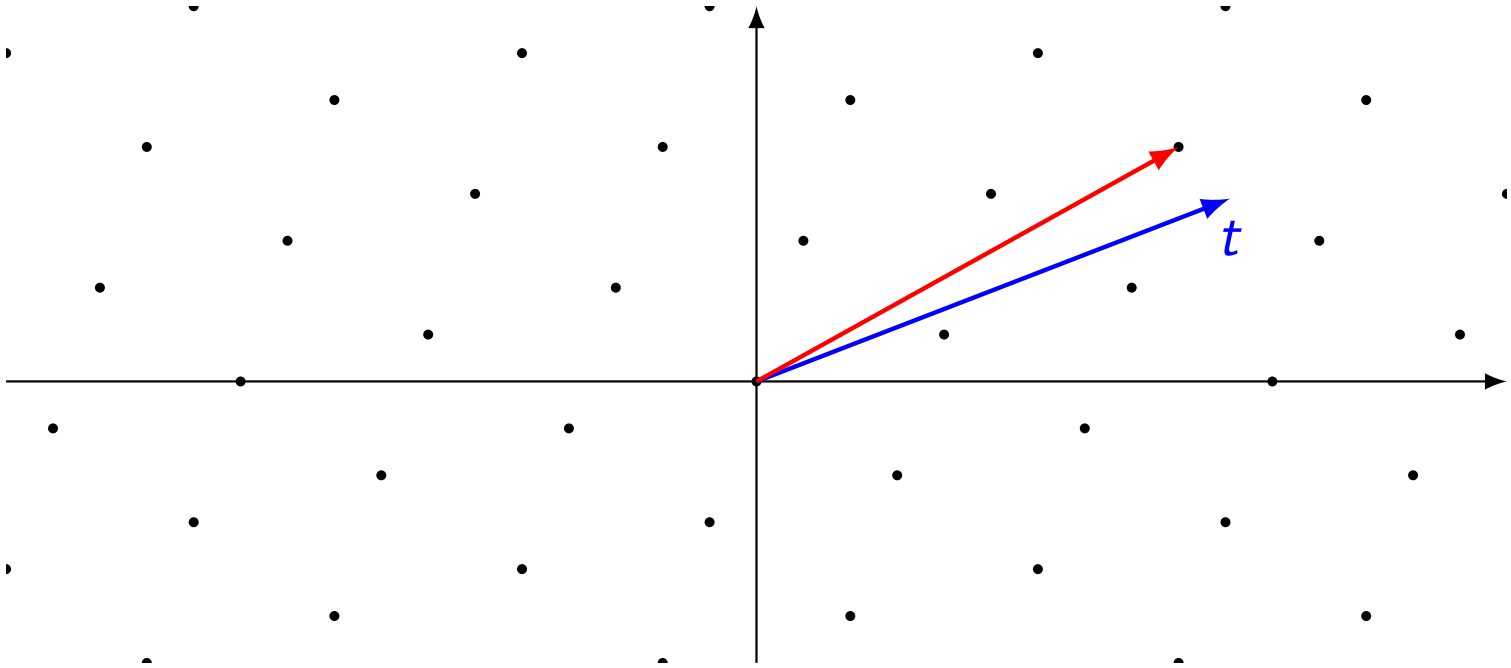
Shortest Vector Problem (SVP) : Find the shortest vector of $\mathcal{L}$.
Note $\lambda_1(\mathcal{L})$ its norm.

Problems on lattices



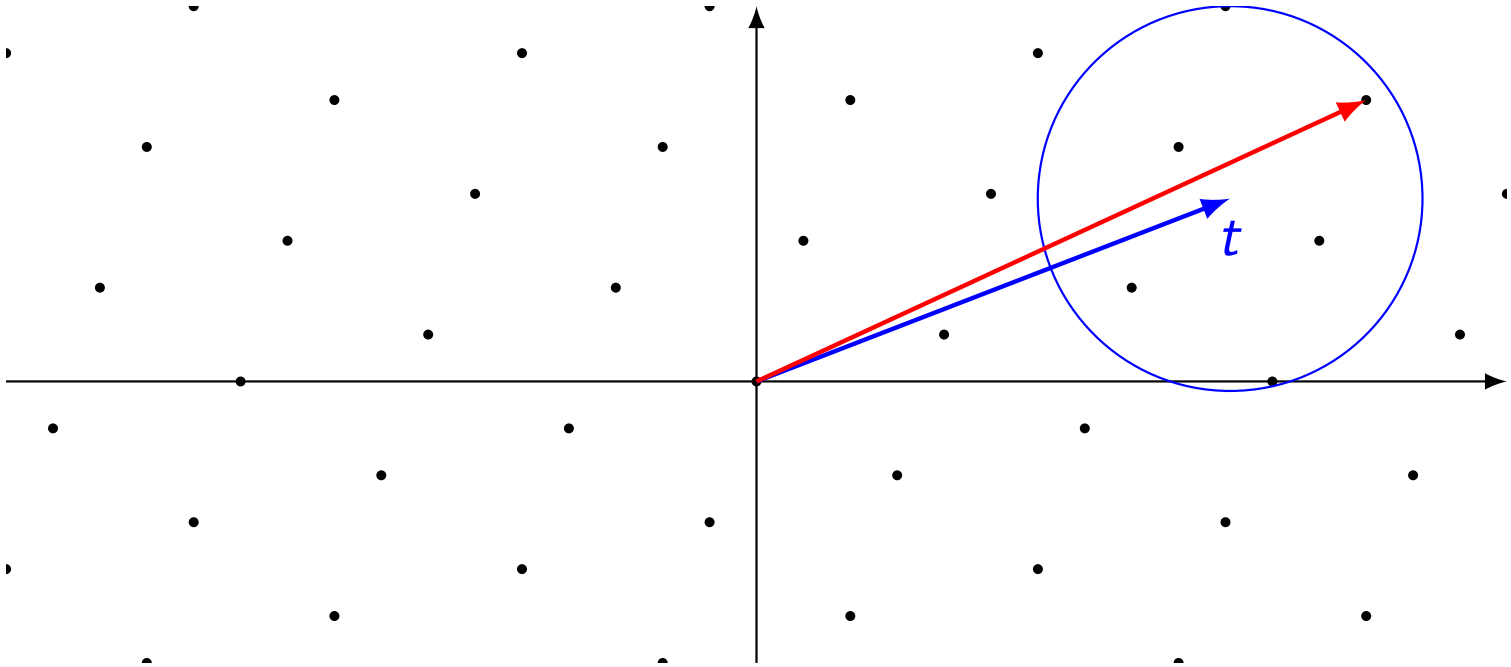
γ-Approximate Shortest Vector Problem (γ-SVP) : Find a vector of $\mathcal{L}$ with norm less than $\gamma \times \lambda_1(\mathcal{L})$

Problems on lattices



Closest Vector Problem (CVP): Given t a target vector, find a vector of $\mathcal{L}$ closest to t

Problems on lattices



Approximate Closest Vector Problem (γ-CVP): Given t a target vector, find a vector of $\mathcal{L}$ within distance $\gamma \times d(t, \mathcal{L})$ of t

Ideal lattices

We consider here several objects :

- K a number field i.e. a finite extension of $\mathbb{Q}$
  $K \simeq \dfrac{\mathbb{Q}[X]}{(P(X))}$

- $\mathcal{O}_K$, the ring of integers of K
  $\mathcal{O}_K = \{x \in K \mid \exists Q(X) \in \mathbb{Z}[X] \text{ monic }, Q(x) = 0\}$

- $\mathcal{O}_K^\times$ the group of units of $\mathcal{O}_K$ (or K)
  $\mathcal{O}_K^\times = \left\{u \in \mathcal{O}_K \mid u^{-1} \in \mathcal{O}_K\right\}$

- I an ideal of $\mathcal{O}_K$ i.e. an additive subgroup stable by multiplication.
  - ◇ principal ideals : generated by an element i.e $g\mathcal{O}_K$

Log-unit lattice

Let r_1 be the number of real embeddings of K and $2r_2$ be the number of complex embeddings. We have $n = r_1 + 2r_2$.

Consider the Log morphism defined on $K \setminus \{0\}$ by

$$\mathrm{Log}(x) := (\log|\sigma_i(x)|)_{i=1,\ldots,n}.$$

$$\mathcal{O}_K^\times \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} \times \mathbb{Z}^{r_1+r_2-1}.$$

$\mathrm{Log}(\mathcal{O}_K^\times)$ is a lattice of rank $r_1 + r_2 - 1$.

Cryptography and ideal lattices

Consider K and $\mathcal{O}_K$ as before. Moreover let $I = g\mathcal{O}_K$ be a principal ideal where g is supposed to be short as a vector.

We are focusing on cryptosystems such that :

- $\star$ I is public, given by integral basis for example
- $\star$ g is private.

Cryptography and ideal lattices

An attack on such a cryptosystem can be decomposed in two steps :

1. Find a generator $h = gu$ of I ($u \in \mathcal{O}_K^\times$) Can be done in polynomial time with a quantum computer
2. Find g given h.

The second step can be viewed as a search for a unit v such that hv is short : it is a reducing phase Kind of problem which seems to resist more to quantum computers

Cryptography and ideal lattices

In order to solve this problem, a standard approach is to use the Log-unit lattice :

$$\mathrm{Log}\,(h) = \mathrm{Log}\,(gu) = \mathrm{Log}\,(g) + \mathrm{Log}\,(u) \in \mathrm{Log}\,(g) + \mathrm{Log}(\mathcal{O}_K^\times).$$

$\mathrm{Log}(g)$ small : error

Can be seen as a CVP.

Cramer, Ducas, Peikert, Regev (2016):

The cyclotomic field $K = \mathbb{Q}(\zeta_m)$
Not use the full group $\mathcal{O}_K^\times$ but subgroup of so called cyclotomic units

$$C = < \pm\zeta_m; c_j := \frac{\zeta_m^j - 1}{\zeta_m - 1} \mid \gcd(j, m) = 1 >$$

$\mathrm{Log}\, C$ is a sublattice $\mathrm{Log}\, O_K^\times$: close enough
$[\mathcal{O}_K^\times : C]$ very small

Multiquadratic fields

Bauch, Bernstein, de Valence, Lange, van Vredendaal (2017):

The multiquadratic field associated with $d_1, \ldots, d_n$ is
$K := \mathbb{Q}\left(\sqrt{d_1}, \ldots, \sqrt{d_n}\right)$.

Subgroup generated by the units of all the quadratic subfields : full rank sublattice with an Orthogonal Basis but Too far away

- Compute the full unit group
- Compute the generator of a principal ideal
- Attack a cryptosystem

General framework

Consider a number field extension K/k such that $K = k(\sqrt[p]{m_1}, \sqrt[p]{m_2})$ and $I = (g)$ an ideal of K.

$\forall x \in K^* : x^p = x_1 x_2 \dots x_{p+1}$ with each x_i being in a subfield of the form $K_i = k(\sqrt[p]{M_i})$ with $M_i \notin k^p$.

$$(\mathcal{O}_K^\times)^p < \mathcal{O}_{K_1}^\times \mathcal{O}_{K_2}^\times \dots \mathcal{O}_{K_{p+1}}^\times < \mathcal{O}_K^\times$$

$$g^p \in I_1 I_2 \dots I_{p+1} < I$$

Procedures for units and PIP

1. Compute units (resp. generator) of $p+1$ subfields (resp. ideals in subfields)

2. Detect p powers

3. Compute corresponding roots

4. Reduce the family.

Procedures for units and PIP

1. Compute units (resp. generator) of $p+1$ subfields (resp. ideals in subfields)

2. Detect p powers

3. Compute corresponding roots

4. Reduce the family.

Computations in subfields need to be efficient enough!

Our work

We considered number fields of the form:

$\mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r})$ i.e. $k = \mathbb{Q}$

$\mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r}, \sqrt[q]{n_1}, \ldots, \sqrt[q]{n_s})$ i.e. $k = \mathbb{Q}(\sqrt[q]{n_1}, \ldots, \sqrt[q]{n_s})$

Experimental Results

One exponent

Defining sequence	Exponent	Dimension	Percentage of success	Time for $\mathcal{O}_K^\times$ (s)
$(2,3)$	5	25	59.3	1.130
$(3,5)$	5	25	75.1	1.420
$(5,7)$	5	25	99.99	2.830
$(2,3)$	7	49	74.8	9.970
$(3,5)$	7	49	99.9	20.740
$(5,7)$	7	49	99.9	139.970
$(2,3)$	11	121	69.2	1411.950
$(2,3)$	13	169	–	3,269.1000
$(2,3,5)$	5	125	70.63	99.170
$(3,5,7)$	5	125	95.71	175.090
$(5,7,11)$	5	125	100.0	715.500
$(2,3,5,7,11)$	3	243	74.81	314.460
$(3,5,7,11,13)$	3	243	100.0	–
$(5,7,11,13,17)$	3	243	100.0	–

Table: Experimental results for Kummer extension of $\mathbb{Q}$ with one exponent

Experimental results

Two exponents

Sequence of L	Sequence of K	Exponent of L	Exponent of K	Dimension	Success	Time for $\mathcal{O}_K^\times$ (s)
$(2,3)$	$(5,7)$	2	3	36	46.2	6.56
$(2,3)$	$(7,11)$	2	3	36	43.2	7.40
$(2,3)$	$(5,7)$	2	5	100	48.5	535.74
$(2,3,5)$	$(11,7)$	3	2	108	19.6	82.10

Table: Experimental results for Kummer extension K/L with two exponents

Leads for future work

- Improve work to have more data: programming, ideal norm computation, $p-$root computation, proof for experimental results
- Generalise the approach to other families of number fields
- *Biasse, van Vredendaal (2018):* Same general framework to compute $S-$units and class groups in multiquadratic fields: could help implement algorithms of *Hanrot, Pellet-Mary, Stehlé (2019)* to solve ISVP.
- Can we use the structure of studied Kummer extensions to solve ISVP?

Thank you for your attention.