Ideal lattices in multicubic fields

Andrea LESAVOUREY Thomas PLANTARD Willy SUSILO

School of Computing and Information Technology
University of Wollongong

Outline

Outline

Post-quantum cryptography

⋆ Two main mathematical problems : Factorization and Discrete Logarithm.

Post-quantum cryptography

- ⋆ Two main mathematical problems : Factorization and Discrete Logarithm.
- ⋆ Quantum computers break these problems (Shor 1994)

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.

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.

Related art

We are interested in the following problem : Given a principal ideal of a number field K find a short generator of K. (SG-PIP)

- *Cramer, Ducas, Peikert, Regev (2016):* quantum polynomial-time or classical $2^{n^{2/3+\epsilon}}$-time algorithm to solve Short Generator Principal Ideal Problem (SG-PIP) on cyclotomic fields

- *Bauch, Bernstein, de Valence, Lange, van Vredendaal (2017):* classical polynomial-time algorithm to solve SG-PIP on a class of multiquadratic fields

Outline

General Context

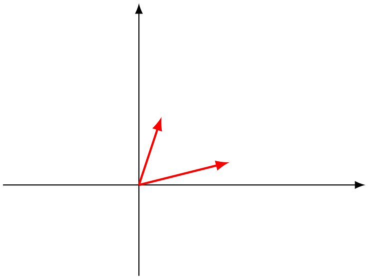
Definition

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 $\mathbb{R}^n$

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 $\mathbb{R}^n$

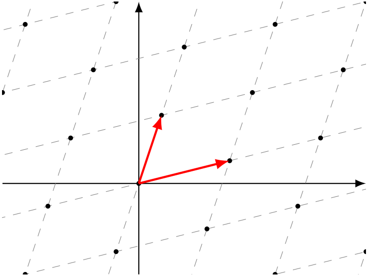


Any set B of free vector which generates $\mathcal{L}$ is called a basis.

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 $\mathbb{R}^n$

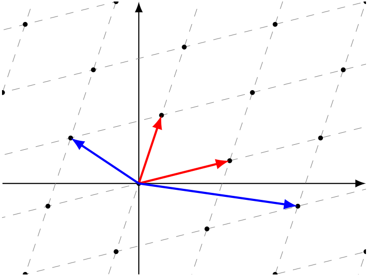


Any set B of free vector which generates $\mathcal{L}$ is called a basis.

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 $\mathbb{R}^n$

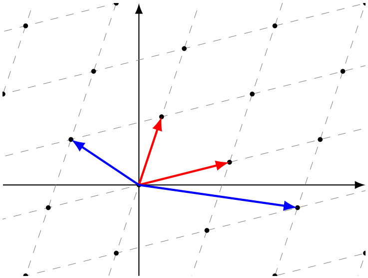


Any set B of free vector which generates $\mathcal{L}$ is called a basis.

There are infinitely many basis

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 $\mathbb{R}^n$

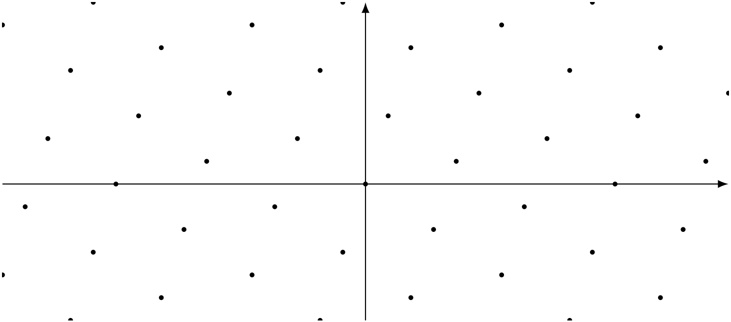


Any set B of free vector which generates $\mathcal{L}$ is called a basis.

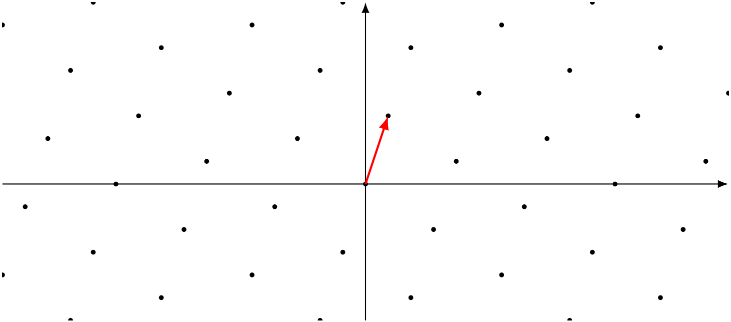
There are infinitely many basis

Some are consider better than others : orthogonality, short vectors

Problems on lattices

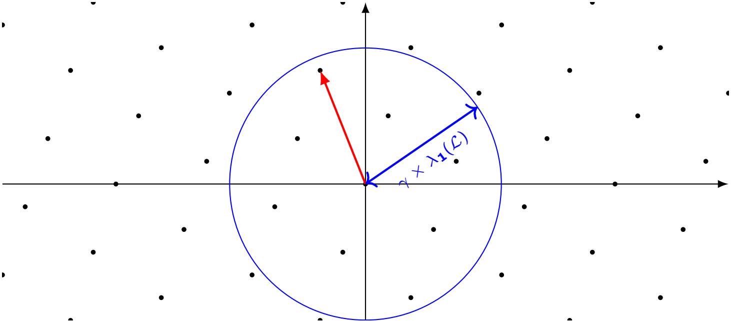


Problems on lattices



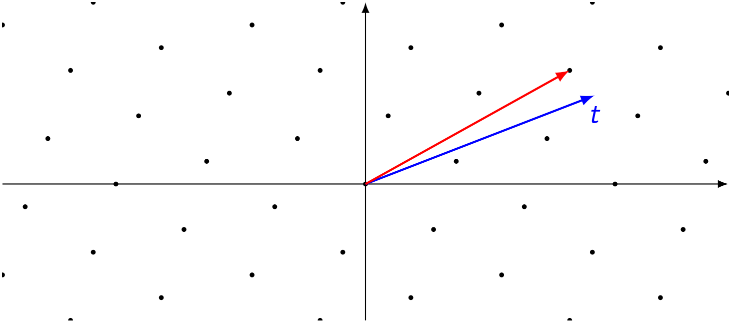
Shortest Vector Problem (SVP) : Find the shortest vector of $\mathcal{L}$.
Note $\lambda_1(\mathcal{L})$ its norm.

Problems on lattices



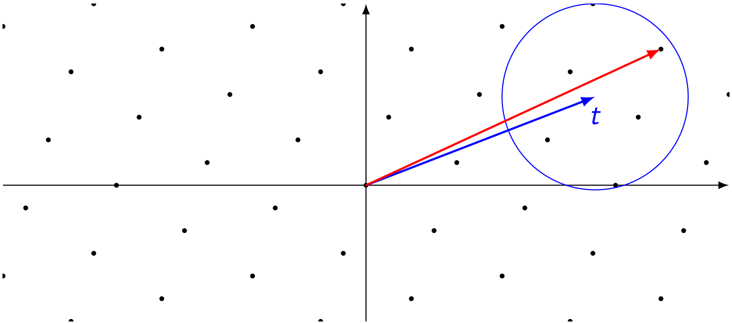
γ-Approximate Shortest Vector Problem (γ-SVP) : Find a vector of $\mathcal{L}$ with norm less than $\gamma \times \lambda_1(\mathcal{L})$

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 :

Ideal lattices

We consider here several objects :

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

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

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)
  $\mathcal{O}_K^\times = \left\{u \in \mathcal{O}_K \mid u^{-1} \in \mathcal{O}_K\right\}$

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 $\mathcal{O}_K^\times$ 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 $n = r_1 + 2r_2$.

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

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

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

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

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

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

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

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

$\mathrm{Log}(\mathcal{O}_K^\times)$ 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.

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

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 :

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

1. Find a generator $h = gu$ of I $(u \in \mathcal{O}_K^\times)$

Cryptography and ideal lattices

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

1. Find a generator $h = gu$ of I $(u \in \mathcal{O}_K^\times)$
2. Find g given h.

Cryptography and ideal lattices

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

1. Find a generator $h = gu$ of I ($u \in \mathcal{O}_K^\times$)

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

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

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 :

Cryptography and ideal lattices

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

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

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.

Cyclotomic fields

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

Cyclotomic fields

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

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

Cyclotomic fields

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

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

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

Multiquadratic fields

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

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

Outline

1. Motivation
   - Cryptography
   - Lattice-based cryptography
2. Recalls
   - Lattices
   - Cryptography and ideal lattices
   - Cyclotomic and multiquadratic fields
3. Our work
   - General Framework
   - Procedures
   - Results

- $\star$ $K = \mathbb{Q}(\sqrt[3]{d_1}, \ldots, \sqrt[3]{d_n})$
- $\star$ $[K : \mathbb{Q}] = 3^n \iff \prod_{i=1}^{n} d_i^{\alpha_i}$ is not a cube, for all $(\alpha_i)_i \in [\![0, 2]\!]^n$
- $\star$ K is **not Galois**, every complex embedding σ is given by its action on $\sqrt[3]{d_i} \mapsto \zeta_3^{\beta_i} \sqrt[3]{d_i}$ with $(\beta_i)_i \in [\![0, 2]\!]^n$

K is a multicubic field as before.

The Galois closure of K is $\widetilde{K} = K(\zeta_3)$

$\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq \langle \tau \rangle \ltimes \langle \tilde{\sigma} \mid \sigma \in \mathrm{Hom}(K, \mathbb{C}) \rangle \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \ltimes \left(\frac{\mathbb{Z}}{3\mathbb{Z}}\right)^n$

- τ is the complex conjugaison
- $\tilde{\sigma}$ is the extension of σ which action is trivial on ζ_3.

With the Galois correspondence : if F is a subfield of K then $H(F) \simeq \langle \tau \rangle \ltimes \langle \tilde{\sigma}^{(1)}, \dots, \tilde{\sigma}^{(r)} \rangle$

Action of morphisms

- $\sigma \in \mathrm{Hom}(K, \mathbb{C}) \iff \underline{\beta} \in \mathbb{F}_3^n$

- Cubic subfield $\iff \underline{\alpha} \in \mathbb{F}_3^n \setminus \{0\} \mathrm{mod}[2]$
  $\iff$ hyperplane in $\mathbb{F}_3^n$

- σ action on $CF(\underline{\alpha})$ given by $\sum_{i=1}^n \alpha_i \beta_i$ in $\mathbb{F}_3$ i.e. $\underline{\beta} \in H_{\underline{\alpha}}(t)$ for $t \in \mathbb{F}_3$.

Units

Multiquadratic Fields

- $\star$ $\mathcal{O}_K^\times \simeq \mathbb{Z}^{2^n-1}$
- $\star$ For Quadratic subfields : one fundamental unit $\epsilon_{\underline{\alpha}}$
- $\star$ $U = \langle -1, \epsilon_{\underline{\alpha}} \mid \underline{\alpha} \rangle$ subgroup of finite index
- $\star$ $\{\mathrm{Log}(\epsilon_{\underline{\alpha}}) \mid \underline{\alpha}\}$ is an orthogonal basis of $\mathrm{Log}(U)$

Multicubic Fields

- $\star$ $\mathcal{O}_K^\times \simeq \mathbb{Z}^{\frac{3^n-1}{2}}$
- $\star$ For Cubic subfields : one fundamental unit $\epsilon_{\underline{\alpha}}$
- $\star$ $U = \langle -1, \epsilon_{\underline{\alpha}} \mid \underline{\alpha} \rangle$ subgroup of finite index
- $\star$ $\{\mathrm{Log}(\epsilon_{\underline{\alpha}}) \mid \underline{\alpha}\}$ is an orthogonal basis of $\mathrm{Log}(U)$

Computing the units

Compute units from the Multiquadratic or Multicubic units :
more efficient procedure and better geometry

How is it done though?
Use relative norms.

Multiquadratic Fields

Lemma

Let σ and τ two independant elements of $\mathrm{Gal}(K,\mathbb{C})$. For all $x \in K^*$ we have $x^2 \in K_\sigma K_\tau K_{\sigma\tau}$.

$$(O_K^\times)^2 \subseteq O_{K_\sigma}^\times O_{K_\tau}^\times O_{K_{\sigma\tau}}^\times$$

Multicubic Fields

Lemma

Let σ_1 and σ_2 two independant elements of $\mathrm{Hom}(K,\mathbb{C})$. For all $x \in K^*$ we have $x^3 \in K_{\tilde{\sigma_1}} K_{\tilde{\sigma_2}} K_{\tilde{\sigma_1}\tilde{\sigma_2}} K_{\tilde{\sigma_1}^2\tilde{\sigma_2}}$.

$$(O_K^\times)^3 \subseteq O_{K_{\tilde{\sigma}}}^\times O_{K_{\tilde{\tau}}}^\times O_{K_{\tilde{\sigma}\tilde{\tau}}}^\times O_{\tilde{\sigma}^2\tilde{\tau}}^\times$$

Computing the units
General Procedure

Multiquadratic Fields

1. Compute a subgroup such that $(O_K^\times)^2 \subset U \subset O_K^\times$
   Recursive computation
2. Compute $O_K^\times$ from U
   Detection of squares and **computation of square-roots**

Multicubic Fields

1. Compute a subgroup such that $(O_K^\times)^3 \subset U \subset O_K^\times$
   Recursive computation
2. Compute $O_K^\times$ from U
   Detection of cubes and **computation of cube-roots**

Solving the PIP
General Procedure

Recall that we consider $I = g\mathcal{O}_K$ a principal ideal. We want to find a generator h.

Multiquadratic Fields

1. Compute a generator of I^2

   Recursive computation on relative norms of I

2. Deduce a generator of I

   Detection of an associate which is a square and **computation of square-roots**

Multicubic Fields

1. Compute a generator of I^3

   Recursive computation on relative norms of I.

2. Deduce a generator of I

   Detection of an associate which is a cube and **computation of cube-roots**

Given $S = \langle x_1, \ldots, x_m \rangle < K^*$ find $(e_1, \ldots, e_m)$ s.t. $x_1^{e_1} x_2^{e_2} \cdots x_m^{e_m}$ is a cube.

1. Find p such that :
   - $\diamond$ $p \equiv 1 \bmod 3$
   - $\diamond$ every d_i has a cube root in $\mathbb{F}_p$
   - $\diamond$ coefficients of every x_j can be reduced modulo p

   $\Longrightarrow \phi_p : S \longrightarrow \mathbb{F}_p^*$ reduction morphism

2. Compose ϕ_p with $t \longmapsto t^{\frac{p-1}{3}}$ obtaining $\chi_p : S \longrightarrow \mathbb{F}_3$

Detecting cubes

Consider $S = \langle x_1, \ldots, x_m \rangle < K^*$.

1. Find $\chi_1, \ldots, \chi_r$ sufficiently enough characters.
2. Compute M the character matrix $[\chi_j(x_i)]_{i,j}$.
3. Find K the kernel of M in $\mathbb{F}_3$.

Consider $K = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_n})$ and $L = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_{n-1}})$. Let $h = g^2$. Then if we write $g = g_0 + g_1\sqrt{d_n}$ and $h = h_0 + h_1\sqrt{d_n}$ we have :

$$h_0 = g_0^2 + d_n g_1^2$$

$$h_1 = 2g_0 g_1$$

$$\mathrm{N}_{K/L}(g) = \sqrt{\mathrm{N}_{K/L}(h)} = g_0^2 - g_1^2 d$$

Compute recursively in L and solve the a sign problem.

Consider $K = \mathbb{Q}(\sqrt[3]{d_1}, \dots, \sqrt[3]{d_n})$ and $L = \mathbb{Q}(\sqrt[3]{d_1}, \dots, \sqrt[3]{d_{n-1}})$. Let $h = g^3$. Then if we write $g = g_0 + g_1 \sqrt[3]{d_n} + g_2 \sqrt[3]{d_n}^2$ and $h = h_0 + h_1 \sqrt[3]{d_n} + h_2 \sqrt[3]{d_n}^2$ we have :

$$h_0 = g_0^3 + g_1^3 d_n + g_2^3 d_n^2 + 6 g_0 g_1 g_2 d_n$$

$$y_1 = 3(g_0^2 g_1 + g_1^2 g_2 d_n + g_2^2 g_0 d_n)$$

$$y_2 = 3(g_0^2 g_2 + g_1^2 g_0 + g_2^2 g_1 d_n)$$

$$\mathrm{N}_{K/L}(g) = g_0^3 + g_1^3 d_n + g_2^3 d_n^2 - 3 g_0 g_1 g_2 d_n.$$

Cube Roots

How we do it

Consider $\mathbf{v}_l$ the column vector of $(b_i)_i$ computed in $\mathbb{R}$ up to a given precision l.

Let $M_l = [\mathbf{v}_l \mid C \cdot I_N]$ and $L_l, U_l = \mathrm{LLL}(M_l)$.

Consider $\mathbf{x} = [x_l \mid \mathbf{0} \mid B]$ with B an upper bound of the norms of the row vectors of L_l.

Compute $R = \mathrm{LLL}\left(\left[\begin{array}{c} L_l \mid \mathbf{0} \\ \hline \mathbf{x} \end{array}\right]\right)$

Cube root candidate : $\dfrac{1}{C}(R_{N+1,2}, \ldots, R_{N+1,N+1})$

Cube Roots

Precision needed : experiments suggest $N\|y\|_2$

Complexity : polynomial in N and length of $\|y\|_2$.

Cons : heuristic method.

Experimental Results

Computation of units

First prime	2	3	5	7	11	13	17	19	23	29
$\mathcal{O}_K^\times$ (times in s)	0.260	0.260	0.260	0.270	0.290	0.350	0.330	0.360	0.480	0.320
`CubeRoot` (times in s)	0.010	0.010	0.010	0.010	0.000	0.050	0.060	0.070	0.180	0.010
# cube roots	3	3	1	1	1	1	1	2	3	1
Average logarithm of the Norm of cubes	3	18	31	45	24	215	270	175	162	70

First prime	2	3	5	7	11	13	17	19	23	29
$\mathcal{O}_K^\times$ (times in s)	2.110	2.250	2.490	4.500	2.780	18.780	4.060	24.810	9.230	24.420
`CubeRoot` (times in s)	0.060	0.180	0.350	2.310	0.350	15.980	1.020	16.540	5.950	16.490
# cube roots	3	4	3	4	2	5	4	5	4	3
Average logarithm of the Norm of cubes	13	29	46	127	83	404	112	398	313	781

Table: Times and data for Algorithm for number fields defined by consecutive primes for $n = 2$ and 3

First prime	2	3	5	7	11	13	17
$\mathcal{O}_K^\times$ (times in s)	39.670	71.160	157.460	873.670	7479.250	9862.540	29308.850
`CubeRoot` (times in s)	19.220	47.270	130.240	832.780	7370.470	9271.600	28425.140
# cube roots	14	12	10	11	11	11	13
Average logarithm of the Norm of cubes	29	75	168	533	1090	2178	3295

First prime	2	3	5
$\mathcal{O}_K^\times$ (times in s)	16026.410	87701.680	566029.130
`CubeRoot` (times in s)	15246.560	85036.150	562127.470
# cube roots	36	36	48
Average logarithm of the Norm of cubes	63	199	531

Table: Times and data for Algorithm for number fields defined by consecutive primes for $n = 4$ and 5

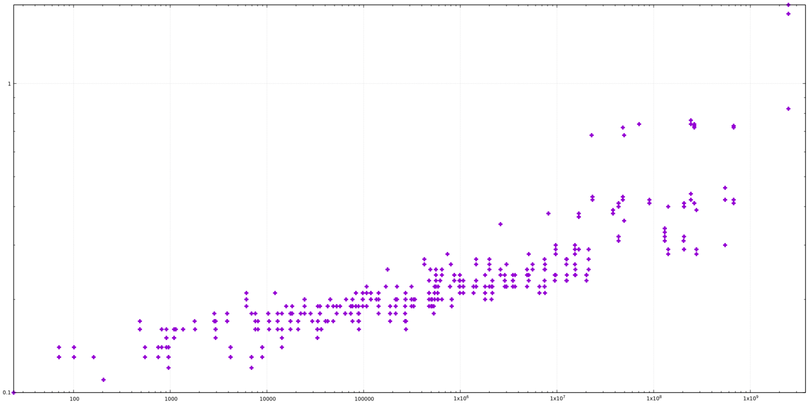


Figure: Times in seconds to compute $\mathcal{O}_K^\times$ in function of the product of the regulators of the cubic subfields of K for $n = 2$. (Axes are in logarithmic scales.)

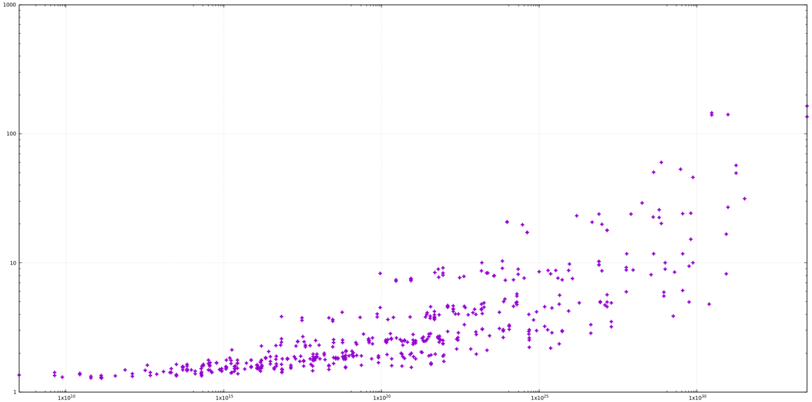


Figure: Times in seconds to compute $\mathcal{O}_K^\times$ in function of the product of the regulators of the cubic subfields of K for $n = 3$. (Axes are in logarithmic scales.)

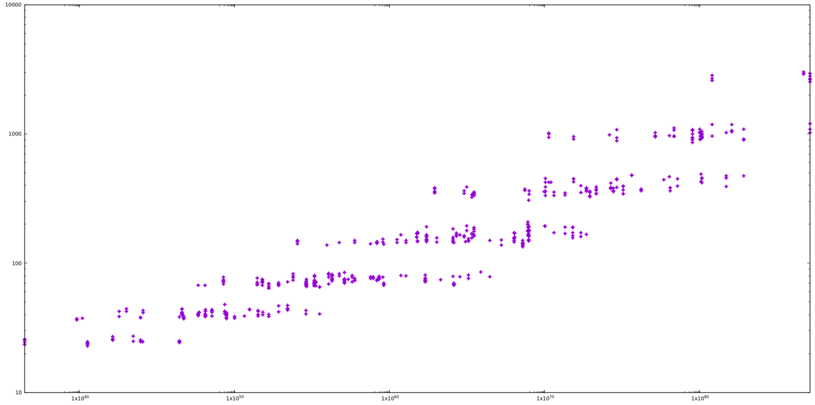


Figure: Times in seconds to compute $\mathcal{O}_K^\times$ in function of the product of the regulators of the cubic subfields of K for $n = 4$. (Axes are in logarithmic scales.)

Experimental Results

Solving the SGPIP

First prime	2	3	5	7	11	13	17	19	23	29
Consecutive	35.20	90.80	98.40	98.20	100.0	100.0	99.70	99.80	100.0	100.0
	46.20	91.50	98.40	98.20	100.0	100.0	99.70	99.80	100.0	100.0
Arithmetic	69.90	95.10	98.60	97.40	100.0	99.80	100.0	99.80	100.0	100.0
	75.20	95.10	98.60	97.40	100.0	99.80	100.0	99.80	100.0	100.0

First prime	2	3	5	7	11	13	17	19	23	29
Consecutive	46.00	93.30	100.0	99.91	100.0	100.0	100.0	100.0	100.0	100.0
	46.40	93.30	100.0	99.91	100.0	100.0	100.0	100.0	100.0	100.0
Arithmetic	84.10	99.59	100.0	99.50	100.0	n/a	n/a	n/a	n/a	n/a
	84.10	99.59	100.0	99.50	100.0	n/a	n/a	n/a	n/a	n/a

First prime	2	3	5	7	11	13	17	19
Consecutive	64.20	99.91	100.0	100.0	100.0	100.0	100.0	100.0
	64.20	99.91	100.0	100.0	100.0	100.0	100.0	100.0
Arithmetic	95.00	100.0	100.0	100.0	100.0	n/a	n/a	n/a
	95.00	100.0	100.0	100.0	100.0	n/a	n/a	n/a

Table: Percentages of keys recovered for $n = 2$, 3 and 4

Leads for future work

- *Biasse, van Vredendaal (2018):* Same general framework to compute $S-$units and class groups in multiquadratic fields

- If we consider exponents p bigger than 3 : the unit group of subfields of degree p will not be computed by a single fundamental unit anymore $\Longrightarrow$ we do not start with an orthogonal basis

- Can we find other algebraic relations to take advantage of?

Thank you for your attention.