About the Use of Class Groups in Cryptology

Alexandre Gélin

Laboratoire de Mathématiques de Versailles
UVSQ – CNRS – Université Paris-Saclay

Journées du LMV – Versailles

15/05/2018

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$ $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic s.t.

$$\mathbf{K} \simeq \mathbf{Q}[X] / \langle T \rangle$$

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$ $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic s.t.

$$\mathbf{K} \simeq \mathbf{Q}[X]/\langle T \rangle$$

$\mathscr{O}_{\mathbf{K}}$ denotes the ring of integers of $\mathbf{K}$ and $\mathbf{Z}[X]/\langle T \rangle \subset \mathscr{O}_{\mathbf{K}}$

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$ $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic s.t.

$$\mathbf{K} \simeq \mathbf{Q}[X]/\langle T \rangle$$

$\mathscr{O}_{\mathbf{K}}$ denotes the ring of integers of $\mathbf{K}$ and $\mathbf{Z}[X]/\langle T \rangle \subset \mathscr{O}_{\mathbf{K}}$

Among the interesting structures:

- Group of ideals

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$ $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic s.t.

$$\mathbf{K} \simeq \mathbf{Q}[X]/\langle T \rangle$$

$\mathscr{O}_{\mathbf{K}}$ denotes the ring of integers of $\mathbf{K}$ and $\mathbf{Z}[X]/\langle T \rangle \subset \mathscr{O}_{\mathbf{K}}$

Among the interesting structures:

- Group of ideals

Definition. **Ideals:** additive subgroups of $\mathscr{O}_{\mathbf{K}}$ stable under multiplication

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$ $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic s.t.

$$\mathbf{K} \simeq \mathbf{Q}[X]/\langle T \rangle$$

$\mathscr{O}_{\mathbf{K}}$ denotes the ring of integers of $\mathbf{K}$ and $\mathbf{Z}[X]/\langle T \rangle \subset \mathscr{O}_{\mathbf{K}}$

Among the interesting structures:

- Group of ideals

Definition. **Ideals:** additive subgroups of $\mathscr{O}_{\mathbf{K}}$ stable under multiplication

Example. $\langle \alpha \rangle = \{\alpha \cdot x \mid x \in \mathscr{O}_{\mathbf{K}}\}$ for $\alpha \in \mathscr{O}_{\mathbf{K}}$

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite-degree extension of $\mathbf{Q}$ $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic s.t.

$$\mathbf{K} \simeq \mathbf{Q}[X]/\langle T\rangle$$

$\mathscr{O}_{\mathbf{K}}$ denotes the ring of integers of $\mathbf{K}$ and $\mathbf{Z}[X]/\langle T\rangle \subset \mathscr{O}_{\mathbf{K}}$

Among the interesting structures:

- Group of ideals

  Quotient by principal ideals $\Longrightarrow$ class group $Cl(\mathscr{O}_{\mathbf{K}})$

Definition. **Ideals:** additive subgroups of $\mathscr{O}_{\mathbf{K}}$ stable under multiplication

Example. $\langle\alpha\rangle = \{\alpha \cdot x \mid x \in \mathscr{O}_{\mathbf{K}}\}$ for $\alpha \in \mathscr{O}_{\mathbf{K}}$

Why do we study class groups ?

Why do we study class groups ?

Why do we study class groups ?

- Because Gauss did!

Why do we study class groups ?

- Because Gauss did!
- Beautiful mathematical challenge

Why do we study class groups ?

- Because Gauss did!
- Beautiful mathematical challenge
- Finite group $\Longrightarrow$ Applications in Cryptology

Outline

Subexponential L-notation : $L_N(0) \approx (\log N)^c$ $L_N(1) \approx N^c$

$$L_N(\alpha) = \exp\Big((c+o(1))(\log N)^{\alpha}(\log\log N)^{1-\alpha}\Big) \qquad \text{for } c>0$$

1969 Shanks: quadratic number fields in $O\left(|\Delta_{\mathbf{K}}|^{\frac{1}{5}}\right)$

1989 Hafner and McCurley: quadratic number fields in $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$

1990 Buchmann: all number fields with fixed degree in $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$

2014 Biasse and Fieker: all number fields in $L_{|\Delta_{\mathbf{K}}|}\left(\frac{2}{3}+\varepsilon\right)$ in general and $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$ if $n \leq \left(\log|\Delta_{\mathbf{K}}|\right)^{\frac{3}{4}-\varepsilon}$

2017 *G.*: many cases, most of them between $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{3}\right)$ and $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$, worst case in $L_{|\Delta_{\mathbf{K}}|}\left(\frac{3}{5}\right)$

Index calculus

1. **Factor base**
   Fix a factor base composed of small elements
2. **Relation collection**
   Collect some relations between those small elements, corresponding to linear equations
3. **Linear algebra**
   Deduce the sought result performing linear algebra on the system built

The factor base

$$\mathscr{B} = \{\text{prime ideals in } \mathscr{O}_{\mathbf{K}} \text{ of norm below } B\}$$

B is determined such that $\mathscr{B}$ **generates the whole class group**

The factor base

$$\mathscr{B} = \{\text{prime ideals in } \mathscr{O}_{\mathbf{K}} \text{ of norm below } B\}$$

B is determined such that $\mathscr{B}$ **generates the whole class group**

Minkowski's bound: every class contains an ideal of norm smaller than

$$M_{\mathbf{K}} = \sqrt{|\Delta_{\mathbf{K}}|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}$$

The factor base

$$\mathscr{B} = \{\text{prime ideals in } \mathscr{O}_{\mathbf{K}} \text{ of norm below } B\}$$

B is determined such that $\mathscr{B}$ **generates the whole class group**

Minkowski's bound: every class contains an ideal of norm smaller than

$$M_{\mathbf{K}} = \sqrt{|\Delta_{\mathbf{K}}|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}$$

Bach's bound: assuming ERH, classes of ideals of norm less than $12\left(\log|\Delta_{\mathbf{K}}|\right)^2$ generate the class group

The factor base

$$\mathscr{B} = \{\text{prime ideals in } \mathscr{O}_{\mathbf{K}} \text{ of norm below } B\}$$

B is determined such that $\mathscr{B}$ **generates the whole class group**

Minkowski's bound: every class contains an ideal of norm smaller than

$$M_{\mathbf{K}} = \sqrt{|\Delta_{\mathbf{K}}|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}$$

Bach's bound: assuming ERH, classes of ideals of norm less than $12\left(\log|\Delta_{\mathbf{K}}|\right)^2$ generate the class group

Practically

$$B = L_{|\Delta_{\mathbf{K}}|}\left(\beta, c_b\right)$$

Relation collection

$$\mathscr{B} = \left(\mathfrak{p}_1, \ldots, \mathfrak{p}_N\right)$$

Surjective morphism:

$$\begin{array}{ccccc} \mathbf{Z}^N & \longrightarrow & \mathscr{I} & \longrightarrow & Cl(\mathscr{O}_{\mathbf{K}}) \\ (e_1, \ldots, e_N) & \longmapsto & \prod_i \mathfrak{p}_i^{e_i} & \longmapsto & \left[\prod_i \mathfrak{p}_i^{e_i}\right] \end{array}$$

$$Cl(\mathscr{O}_{\mathbf{K}}) \quad \simeq \quad \mathbf{Z}^N \big/ \left\{(e_1, \ldots, e_N) \in \mathbf{Z}^N \mid \prod \mathfrak{p}_i^{e_i} = \langle \alpha \rangle \mathscr{O}_{\mathbf{K}}\right\}$$

Relation collection

$$\mathscr{B} = \left(\mathfrak{p}_1, \ldots, \mathfrak{p}_N\right)$$

Surjective morphism:

$$\begin{array}{ccccc} \mathbf{Z}^N & \longrightarrow & \mathscr{I} & \longrightarrow & Cl(\mathscr{O}_{\mathbf{K}}) \\ (e_1, \ldots, e_N) & \longmapsto & \prod_i \mathfrak{p}_i^{e_i} & \longmapsto & \left[\prod_i \mathfrak{p}_i^{e_i}\right] \end{array}$$

$$Cl(\mathscr{O}_{\mathbf{K}}) \quad \simeq \quad \mathbf{Z}^N \Big/ \left\{(e_1, \ldots, e_N) \in \mathbf{Z}^N \mid \prod \mathfrak{p}_i^{e_i} = \langle \alpha \rangle \mathscr{O}_{\mathbf{K}}\right\}$$

Idea:

1. Pick at random $\mathfrak{a} = \prod \mathfrak{p}_i^{a_i}$
2. Find a *reduced* ideal $\mathfrak{b}$ in the same class
3. If $\mathfrak{b}$ splits over $\mathscr{B}$ $\left(\Longleftrightarrow \mathfrak{b} = \prod \mathfrak{p}_i^{b_i}\right)$ then

$$\mathfrak{a} \cdot \mathfrak{b}^{-1} = \prod \mathfrak{p}_i^{a_i - b_i} \quad \text{is principal}$$

Linear algebra

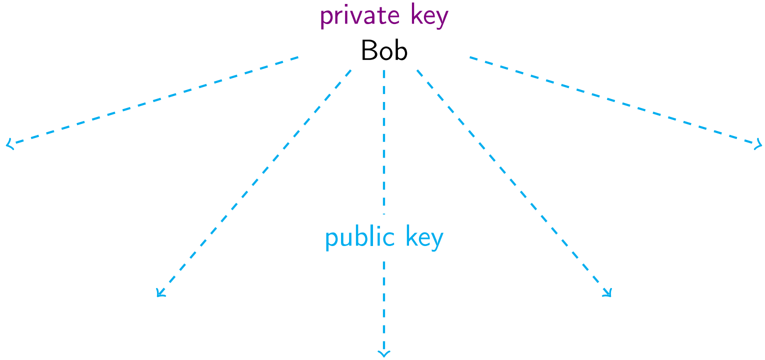
- Relations stored in a matrix of size about $N \times N$
- Structure of the class group given by the *Smith Normal Form* of the matrix
- First compute *Hermite Normal Form* with a premultiplier because we need kernel vectors
- Storjohann and Labahn algorithm, runtime in $N^{\omega+1}$ ($2 \leq \omega \leq 3$ exponent of matrix multiplication)

Outline

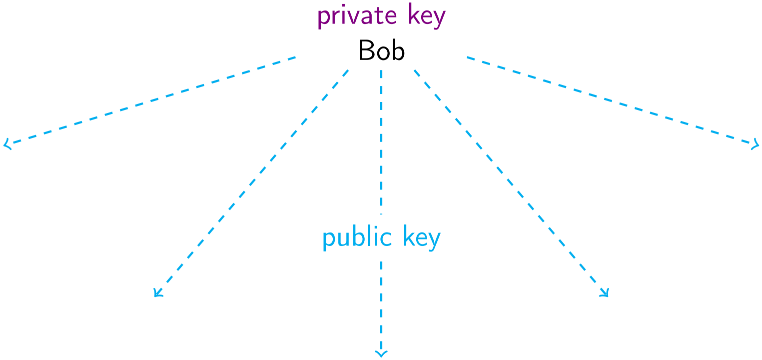
Public Key Cryptography

private key
Bob

Public Key Cryptography

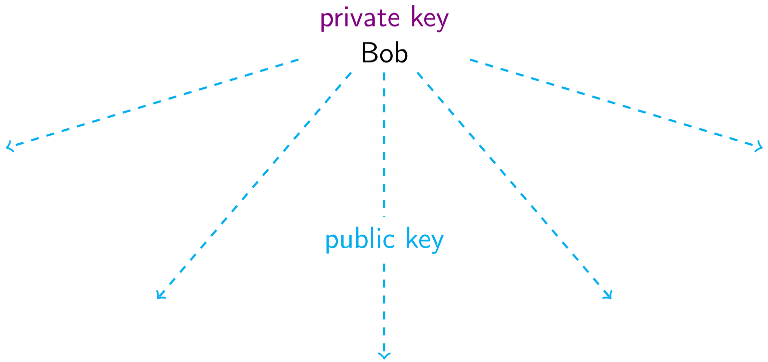


Public Key Cryptography



- Everyone uses the public key to encrypt

Public Key Cryptography



- Everyone uses the public key to encrypt
- Only Bob can decrypt thanks to his private key

The Principal Ideal Problem

Definition

The *Principal Ideal Problem* (PIP) consists in finding a generator of an ideal, assuming it is principal.

The Principal Ideal Problem

Definition

The *Short Principal Ideal Problem* (SPIP) consists in finding a short generator of an ideal, assuming it is principal.

The Principal Ideal Problem

Definition

The *Short Principal Ideal Problem* (SPIP) consists in finding a short generator of an ideal, assuming it is principal.

- Base of several cryptographical schemes ([SV10],[GGH13])

The Principal Ideal Problem

Definition

The *Short Principal Ideal Problem* (SPIP) consists in finding a short generator of an ideal, assuming it is principal.

- Base of several cryptographical schemes ([SV10],[GGH13])
- Two distinct phases:
  1. Given the $\mathbf{Z}$-basis of the ideal $\mathfrak{a} = \langle \boldsymbol{g} \rangle$, find a — not necessarily short — generator $\boldsymbol{g}' = \boldsymbol{g} \cdot \boldsymbol{u}$ for a unit $\boldsymbol{u}$
  2. From $\boldsymbol{g}'$, find a short generator of the ideal

The Principal Ideal Problem

Definition

The *Short Principal Ideal Problem* (SPIP) consists in finding a short generator of an ideal, assuming it is principal.

- Base of several cryptographical schemes ([SV10],[GGH13])
- Two distinct phases:
  1. Given the $\mathbb{Z}$-basis of the ideal $\mathfrak{a} = \langle \boldsymbol{g} \rangle$, find a — not necessarily short — generator $\boldsymbol{g}' = \boldsymbol{g} \cdot \boldsymbol{u}$ for a unit $\boldsymbol{u}$
  2. From $\boldsymbol{g}'$, find a short generator of the ideal

2014 - Campbell, Groves, and Sheperd:
Reduction in polynomial time for power-of-two cyclotomic fields
2016 - Cramer, Ducas, Peikert, and Regev:
Proof and extension to prime-power cyclotomic fields

FHE scheme – Smart and Vercauteren PKC 2010

Key Generation:

1. Fix the security parameter $N = 2^n$
2. Let $F(X) = X^N + 1$ be the polynomial defining the cyclotomic field $\mathbf{K} = \mathbf{Q}(\zeta_{2N})$
3. Set $G(X) = 1 + 2 \cdot S(X)$,
   for $S(X)$ of degree $N-1$ with coefficients in $\left[-2^{\sqrt{N}}, 2^{\sqrt{N}}\right]$,
   such that the norm $\mathcal{N}\left(\langle G(\zeta_{2N})\rangle\right)$ is prime
4. Set $\boldsymbol{g} = G(\zeta_{2N}) \in \mathcal{O}_{\mathbf{K}}$
5. Return the private key $\mathrm{sk} = \boldsymbol{g}$ and the public key $\mathrm{pk} = \mathrm{HNF}(\langle \boldsymbol{g} \rangle)$

FHE scheme – Smart and Vercauteren PKC 2010

Key Generation:

1. Fix the security parameter $N = 2^n$
2. Let $F(X) = X^N + 1$ be the polynomial defining the cyclotomic field $\mathbf{K} = \mathbf{Q}(\zeta_{2N})$
3. Set $G(X) = 1 + 2 \cdot S(X)$,
   for $S(X)$ of degree $N-1$ with coefficients in $\left[-2^{\sqrt{N}}, 2^{\sqrt{N}}\right]$,
   such that the norm $\mathcal{N}\left(\langle G(\zeta_{2N})\rangle\right)$ is prime
4. Set $\boldsymbol{g} = G(\zeta_{2N}) \in \mathcal{O}_{\mathbf{K}}$
5. Return the private key $\mathrm{sk} = \boldsymbol{g}$ and the public key $\mathrm{pk} = \mathrm{HNF}(\langle \boldsymbol{g} \rangle)$

Goal: Recover the private key from the public key

Outline of the algorithm [BEFGK17]

1. Perform a reduction from the cyclotomic field to its totally real subfield, allowing to work in smaller dimension
2. Then a descent makes the sizes of involved ideals decrease
3. Collect relations and run linear algebra to construct small ideals and a generator
4. Eventually run the derivation of the small generator from a bigger one

Outline of the algorithm [BEFGK17]

1. Perform a reduction from the cyclotomic field to its totally real subfield, allowing to work in smaller dimension
2. Then a descent makes the sizes of involved ideals decrease
3. Collect relations and run linear algebra to construct small ideals and a generator
4. Eventually run the derivation of the small generator from a bigger one

All the complexities are expressed as a function of the field discriminant $\Delta_{\mathbf{Q}(\zeta_{2N})} = N^N$, for $N = 2^n$. For instance,

$$L_{|\Delta_{\mathbf{K}}|}(\alpha) = 2^{N^{\alpha+o(1)}}$$

2. The descent

$$\begin{array}{c} \mathfrak{a}^+ = \mathfrak{a}^{(0)} \\ | \\ \mathfrak{b} \end{array}$$

Input ideal – Norm arbitrary large

2. The descent

$$\begin{array}{ll} \mathfrak{a}^+ = \mathfrak{a}^{(0)} & \text{Input ideal – Norm arbitrary large} \\ \Big| & \\ \mathfrak{b} & \text{Initial reduction – Norm: } L_{|\Delta_{\mathbf{K}}|}\left(\frac{3}{2}\right) \end{array}$$

2. The descent – Smoothness tests & Randomization

Heuristic

If $\mathcal{N}(\mathfrak{a}) \leq L_{|\Delta_{\mathbf{K}}|}(a)$, then $\mathfrak{a}$ is $L_{|\Delta_{\mathbf{K}}|}(b)$-smooth with probability

$$\mathscr{P} \geq L_{|\Delta_{\mathbf{K}}|}(a-b)^{-1}$$

Using ECM algorithm, each smoothness test costs $L_{|\Delta_{\mathbf{K}}|}\left(\frac{b}{2}\right)$

2. The descent – Smoothness tests & Randomization

Heuristic

If $\mathcal{N}(\mathfrak{a}) \leq L_{|\Delta_{\mathbf{K}}|}(a)$, then $\mathfrak{a}$ is $L_{|\Delta_{\mathbf{K}}|}(b)$-smooth with probability

$$\mathscr{P} \geq L_{|\Delta_{\mathbf{K}}|}(a-b)^{-1}$$

Using ECM algorithm, each smoothness test costs $L_{|\Delta_{\mathbf{K}}|}\left(\frac{b}{2}\right)$

Conclusion: $\mathfrak{b}$ is $L_{|\Delta_{\mathbf{K}}|}(1)$-smooth with probability $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)^{-1}$ and one test costs $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$

2. The descent – Smoothness tests & Randomization

Heuristic

If $\mathcal{N}(\mathfrak{a}) \leq L_{|\Delta_{\mathbf{K}}|}(a)$, then $\mathfrak{a}$ is $L_{|\Delta_{\mathbf{K}}|}(b)$-smooth with probability

$$\mathscr{P} \geq L_{|\Delta_{\mathbf{K}}|}(a-b)^{-1}$$

Using ECM algorithm, each smoothness test costs $L_{|\Delta_{\mathbf{K}}|}\left(\frac{b}{2}\right)$

Conclusion: $\mathfrak{b}$ is $L_{|\Delta_{\mathbf{K}}|}(1)$-smooth with probability $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)^{-1}$ and one test costs $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$

$\Longrightarrow$ We use $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$ ideals $\tilde{\mathfrak{a}} = \mathfrak{a}^{(0)} \prod \mathfrak{p}_i^{e_i}$ for small prime ideals $\mathfrak{p}_i$ and integers e_i to be sure to derive one $\tilde{\mathfrak{b}}$ that is $L_{|\Delta_{\mathbf{K}}|}(1)$-smooth

2. The descent

$$\mathfrak{a}^{+} = \mathfrak{a}^{(0)}$$

$$\mathfrak{a}_1^{(1)} \quad \mathfrak{a}_2^{(1)} \quad \cdots \quad \mathfrak{a}_{n_1}^{(1)}$$

Input ideal – Norm arbitrary large

Initial reduction – Norm: $L_{|\Delta_{\mathbf{K}}|}\left(\frac{3}{2}\right)$

2. The descent

$$\mathfrak{a}^+ = \mathfrak{a}^{(0)}$$

Input ideal – Norm arbitrary large

$$\mathfrak{a}_1^{(1)} \quad \mathfrak{a}_2^{(1)} \quad \cdots \quad \mathfrak{a}_{n_1}^{(1)}$$

Initial reduction – $L_{|\Delta_{\mathbf{K}}|}(1)$-smooth

2. The descent – Subsequent steps

We cannot reduce the norm using the same lattice-reduction

2. The descent – Subsequent steps

We cannot reduce the norm using the same lattice-reduction

Solution: Cheon's trick

- Use the coefficient embedding in the basis $(\zeta^i + \zeta^{-i})_i$
- Compute the HNF of the integral lattice
- Find a short vector in a sublattice of smaller dimension

2. The descent – Subsequent steps

We cannot reduce the norm using the same lattice-reduction

Solution: Cheon's trick

- Use the coefficient embedding in the basis $\left(\zeta^i + \zeta^{-i}\right)_i$
- Compute the HNF of the integral lattice
- Find a short vector in a sublattice of smaller dimension

Input: $\mathfrak{a}$ with $\mathcal{N}(\mathfrak{a}) \leq L_{|\Delta_{\mathbf{K}}|}(\alpha)$

2. The descent – Subsequent steps

We cannot reduce the norm using the same lattice-reduction

Solution: Cheon's trick

- Use the coefficient embedding in the basis $\left(\zeta^i + \zeta^{-i}\right)_i$
- Compute the HNF of the integral lattice
- Find a short vector in a sublattice of smaller dimension

Input: $\mathfrak{a}$ with $\mathcal{N}(\mathfrak{a}) \leq L_{|\Delta_{\mathbf{K}}|}(\alpha)$

Output: algebraic integer $\boldsymbol{v} \in \mathfrak{a}$ and ideal $\mathfrak{b} \subset \mathcal{O}_{\mathbf{K}^+}$ s.t. $\langle \boldsymbol{v} \rangle = \mathfrak{a} \cdot \mathfrak{b}$ and

$$\mathcal{N}(\mathfrak{b}) \leq L_{|\Delta_{\mathbf{K}}|}\left(\frac{2\alpha+3}{4}\right)$$

2. The descent – Subsequent steps

We cannot reduce the norm using the same lattice-reduction

Solution: Cheon's trick

- Use the coefficient embedding in the basis $\left(\zeta^i + \zeta^{-i}\right)_i$
- Compute the HNF of the integral lattice
- Find a short vector in a sublattice of smaller dimension

Input: $\mathfrak{a}$ with $\mathcal{N}(\mathfrak{a}) \leq L_{|\Delta_\mathbf{K}|}(\alpha)$

Output: algebraic integer $\boldsymbol{v} \in \mathfrak{a}$ and ideal $\mathfrak{b} \subset \mathcal{O}_{\mathbf{K}^+}$ s.t. $\langle \boldsymbol{v} \rangle = \mathfrak{a} \cdot \mathfrak{b}$ and

$$\mathcal{N}(\mathfrak{b}) \leq L_{|\Delta_\mathbf{K}|}\left(\tfrac{2\alpha+3}{4}\right) \qquad \rightsquigarrow L_{|\Delta_\mathbf{K}|}\left(\tfrac{2\alpha+1}{4}\right)\text{-smooth}$$

2. The descent – Subsequent steps

We cannot reduce the norm using the same lattice-reduction

Solution: Cheon's trick

- Use the coefficient embedding in the basis $\left(\zeta^i + \zeta^{-i}\right)_i$
- Compute the HNF of the integral lattice
- Find a short vector in a sublattice of smaller dimension

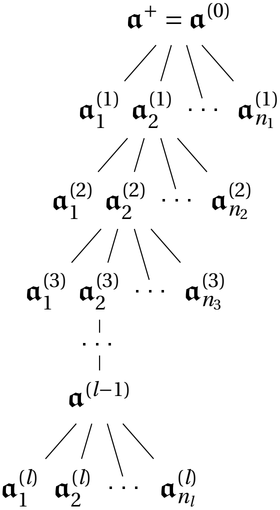
Input: $\mathfrak{a}$ with $\mathcal{N}(\mathfrak{a}) \le L_{|\Delta_{\mathbf{K}}|}(\alpha)$

Output: algebraic integer $\boldsymbol{v} \in \mathfrak{a}$ and ideal $\mathfrak{b} \subset \mathcal{O}_{\mathbf{K}^+}$ s.t. $\langle \boldsymbol{v} \rangle = \mathfrak{a} \cdot \mathfrak{b}$ and

$$\mathcal{N}(\mathfrak{b}) \le L_{|\Delta_{\mathbf{K}}|}\left(\tfrac{2\alpha+3}{4}\right) \qquad \rightsquigarrow L_{|\Delta_{\mathbf{K}}|}\left(\tfrac{2\alpha+1}{4}\right)\text{-smooth}$$

Cost: $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$ for lattice reduction & smoothness tests

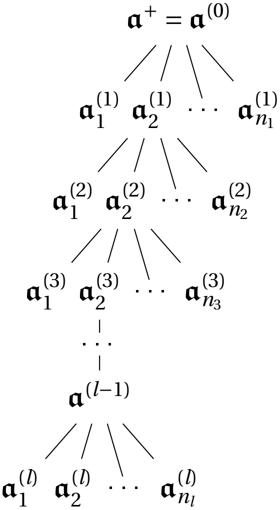
2. The descent



Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbf{K}}|}(1)$-smooth

2. The descent

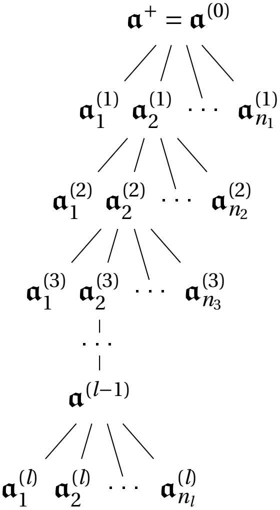


Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbf{K}}|}(1)$-smooth

First step – Norm: $L_{|\Delta_{\mathbf{K}}|}\left(\frac{5}{4}\right)$

2. The descent



Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbf{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbf{K}}|}\left(\frac{3}{4}\right)$-smooth

2. The descent

$\mathfrak{a}^+ = \mathfrak{a}^{(0)}$ — Input ideal – Norm arbitrary large

$\mathfrak{a}_1^{(1)} \quad \mathfrak{a}_2^{(1)} \quad \cdots \quad \mathfrak{a}_{n_1}^{(1)}$ — Initial reduction – $L_{|\Delta_{\mathbf{K}}|}(1)$-smooth

$\mathfrak{a}_1^{(2)} \quad \mathfrak{a}_2^{(2)} \quad \cdots \quad \mathfrak{a}_{n_2}^{(2)}$ — First step – $L_{|\Delta_{\mathbf{K}}|}\left(\frac{3}{4}\right)$-smooth

$\mathfrak{a}_1^{(3)} \quad \mathfrak{a}_2^{(3)} \quad \cdots \quad \mathfrak{a}_{n_3}^{(3)}$ — Second step – Norm: $L_{|\Delta_{\mathbf{K}}|}\left(\frac{9}{8}\right)$

$\cdots$

$\mathfrak{a}^{(l-1)}$

$\mathfrak{a}_1^{(l)} \quad \mathfrak{a}_2^{(l)} \quad \cdots \quad \mathfrak{a}_{n_l}^{(l)}$

2. The descent

$$\mathfrak{a}^+ = \mathfrak{a}^{(0)}$$

$$\mathfrak{a}_1^{(1)} \quad \mathfrak{a}_2^{(1)} \quad \cdots \quad \mathfrak{a}_{n_1}^{(1)}$$

$$\mathfrak{a}_1^{(2)} \quad \mathfrak{a}_2^{(2)} \quad \cdots \quad \mathfrak{a}_{n_2}^{(2)}$$

$$\mathfrak{a}_1^{(3)} \quad \mathfrak{a}_2^{(3)} \quad \cdots \quad \mathfrak{a}_{n_3}^{(3)}$$

$$\cdots$$

$$\mathfrak{a}^{(l-1)}$$

$$\mathfrak{a}_1^{(l)} \quad \mathfrak{a}_2^{(l)} \quad \cdots \quad \mathfrak{a}_{n_l}^{(l)}$$

Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_\mathbf{K}|}(1)$-smooth

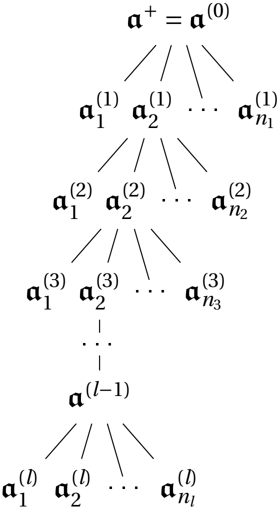
First step – $L_{|\Delta_\mathbf{K}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_\mathbf{K}|}\left(\frac{5}{8}\right)$-smooth

2. The descent

$\mathfrak{a}^+ = \mathfrak{a}^{(0)}$	Input ideal – Norm arbitrary large
$\mathfrak{a}_1^{(1)} \ \mathfrak{a}_2^{(1)} \ \cdots \ \mathfrak{a}_{n_1}^{(1)}$	Initial reduction – $L_{\lvert\Delta_{\mathbf{K}}\rvert}(1)$-smooth
$\mathfrak{a}_1^{(2)} \ \mathfrak{a}_2^{(2)} \ \cdots \ \mathfrak{a}_{n_2}^{(2)}$	First step – $L_{\lvert\Delta_{\mathbf{K}}\rvert}\left(\frac{3}{4}\right)$-smooth
$\mathfrak{a}_1^{(3)} \ \mathfrak{a}_2^{(3)} \ \cdots \ \mathfrak{a}_{n_3}^{(3)}$	Second step – $L_{\lvert\Delta_{\mathbf{K}}\rvert}\left(\frac{5}{8}\right)$-smooth
$\cdots$	
$\mathfrak{a}^{(l-1)}$	Last but one step – Norm: $\approx L_{\lvert\Delta_{\mathbf{K}}\rvert}(1)$
$\mathfrak{a}_1^{(l)} \ \mathfrak{a}_2^{(l)} \ \cdots \ \mathfrak{a}_{n_l}^{(l)}$	

2. The descent



Input ideal – Norm arbitrary large

Initial reduction – $L_{|\Delta_{\mathbf{K}}|}(1)$-smooth

First step – $L_{|\Delta_{\mathbf{K}}|}\left(\frac{3}{4}\right)$-smooth

Second step – $L_{|\Delta_{\mathbf{K}}|}\left(\frac{5}{8}\right)$-smooth

Last but one step – $\approx L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$-smooth

2. The descent

$\mathfrak{a}^+ = \mathfrak{a}^{(0)}$	Input ideal – Norm arbitrary large
$\mathfrak{a}_1^{(1)} \ \mathfrak{a}_2^{(1)} \ \cdots \ \mathfrak{a}_{n_1}^{(1)}$	Initial reduction – $L_{\lvert\Delta_{\mathbf{K}}\rvert}(1)$-smooth
$\mathfrak{a}_1^{(2)} \ \mathfrak{a}_2^{(2)} \ \cdots \ \mathfrak{a}_{n_2}^{(2)}$	First step – $L_{\lvert\Delta_{\mathbf{K}}\rvert}\left(\frac{3}{4}\right)$-smooth
$\mathfrak{a}_1^{(3)} \ \mathfrak{a}_2^{(3)} \ \cdots \ \mathfrak{a}_{n_3}^{(3)}$	Second step – $L_{\lvert\Delta_{\mathbf{K}}\rvert}\left(\frac{5}{8}\right)$-smooth
$\cdots$	
$\mathfrak{a}^{(l-1)}$	Last but one step – $\approx L_{\lvert\Delta_{\mathbf{K}}\rvert}\left(\frac{1}{2}\right)$-smooth
$\mathfrak{a}_1^{(l)} \ \mathfrak{a}_2^{(l)} \ \cdots \ \mathfrak{a}_{n_l}^{(l)}$	Last step – Norm: $L_{\lvert\Delta_{\mathbf{K}}\rvert}(1)$

2. The descent

$\mathfrak{a}^+ = \mathfrak{a}^{(0)}$	Input ideal – Norm arbitrary large
$\mathfrak{a}_1^{(1)}\ \mathfrak{a}_2^{(1)}\ \cdots\ \mathfrak{a}_{n_1}^{(1)}$	Initial reduction – $L_{\lvert\Delta_\mathbf{K}\rvert}(1)$-smooth
$\mathfrak{a}_1^{(2)}\ \mathfrak{a}_2^{(2)}\ \cdots\ \mathfrak{a}_{n_2}^{(2)}$	First step – $L_{\lvert\Delta_\mathbf{K}\rvert}\left(\frac{3}{4}\right)$-smooth
$\mathfrak{a}_1^{(3)}\ \mathfrak{a}_2^{(3)}\ \cdots\ \mathfrak{a}_{n_3}^{(3)}$	Second step – $L_{\lvert\Delta_\mathbf{K}\rvert}\left(\frac{5}{8}\right)$-smooth
$\cdots$	
$\mathfrak{a}^{(l-1)}$	Last but one step – $\approx L_{\lvert\Delta_\mathbf{K}\rvert}\left(\frac{1}{2}\right)$-smooth
$\mathfrak{a}_1^{(l)}\ \mathfrak{a}_2^{(l)}\ \cdots\ \mathfrak{a}_{n_l}^{(l)}$	Last step – $L_{\lvert\Delta_\mathbf{K}\rvert}\left(\frac{1}{2}\right)$-smooth

3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$

3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B

3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M

3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M

  Relation: principal ideal that splits on the factor base. Test ideals generated by $\boldsymbol{v} = \sum v_i(\zeta^i + \zeta^{-i})$ for $|v_i| \leq \log|\Delta_{\mathbf{K}}|$

3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_\mathbf{K}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M

  Relation: principal ideal that splits on the factor base. Test ideals generated by $\boldsymbol{v} = \sum v_i(\zeta^i + \zeta^{-i})$ for $|v_i| \leq \log|\Delta_\mathbf{K}|$

  Norm below $L_{|\Delta_\mathbf{K}|}(1) \Longrightarrow L_{|\Delta_\mathbf{K}|}\left(\frac{1}{2}\right)$-smooth ideals in $L_{|\Delta_\mathbf{K}|}\left(\frac{1}{2}\right)$

3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M

$$\begin{pmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \vdots \\ \boldsymbol{v}_{Q|\mathscr{B}|} \end{pmatrix} \begin{matrix} \rightarrow \\ \rightarrow \\ \vdots \\ \rightarrow \end{matrix} \begin{pmatrix} M_{1,1} & \cdots & M_{1,|\mathscr{B}|} \\ M_{2,1} & \cdots & M_{2,|\mathscr{B}|} \\ \vdots & & \vdots \\ M_{Q|\mathscr{B}|,1} & \cdots & M_{Q|\mathscr{B}|,|\mathscr{B}|} \end{pmatrix} \Longrightarrow \forall\, i, \langle \boldsymbol{v}_i \rangle = \prod_{j=1}^{|\mathscr{B}|} \mathfrak{p}_j^{M_{i,j}}$$

3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M
- A N-dimensional vector Y including all the valuations of the smooth ideals in the $\mathfrak{p}_i$

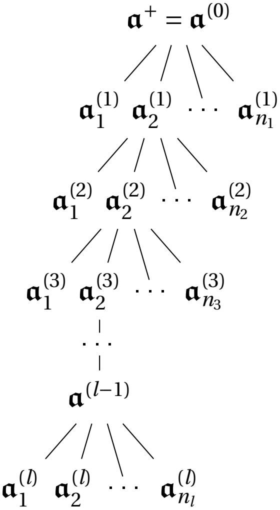
3. Solution for smooth ideals

Input: Bunch of prime ideals of norm below $B = L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$

Index Calculus Method:

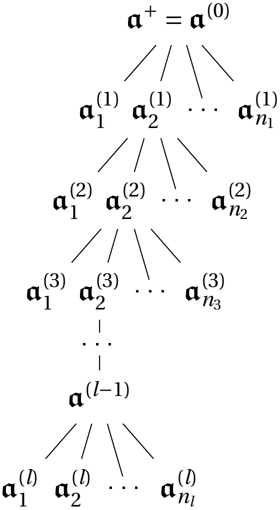
- Factor base: set of all prime ideals with norm below B
- Relation collection: construction of a full-rank matrix M
- A N-dimensional vector Y including all the valuations of the smooth ideals in the $\mathfrak{p}_i$
- A solution X of $MX = Y$ provides a generator of the product of the $L_{|\Delta_{\mathbf{K}}|}\left(\frac{1}{2}\right)$-smooth ideals

4. The backtracking



A generator for the product

4. The backtracking



A generator for the product

4. The backtracking

$$\mathfrak{a}^{+} = \mathfrak{a}^{(0)}$$

$$\mathfrak{a}_1^{(1)} \quad \mathfrak{a}_2^{(1)} \quad \cdots \quad \mathfrak{a}_{n_1}^{(1)}$$

$$\mathfrak{a}_1^{(2)} \quad \mathfrak{a}_2^{(2)} \quad \cdots \quad \mathfrak{a}_{n_2}^{(2)}$$

$$\mathfrak{a}_1^{(3)} \quad \mathfrak{a}_2^{(3)} \quad \cdots \quad \mathfrak{a}_{n_3}^{(3)}$$

$$\cdots$$

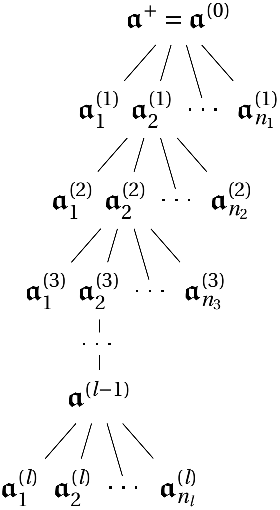
$$\mathfrak{a}^{(l-1)}$$

$$\mathfrak{a}_1^{(l)} \quad \mathfrak{a}_2^{(l)} \quad \cdots \quad \mathfrak{a}_{n_l}^{(l)}$$

A generator for the initial ideal

A generator for the product

4. The backtracking



A generator for the initial ideal

$\Uparrow$ ☺

A generator for the product

Thanks

Merci