Rigorous computation of class group and unit group

Koen de Boer[1] **Alice Pellet-Mary**[2] Benjamin Wesolowski[2]

[1] CWI and Leiden university [2] CNRS and Bordeaux university

ENSL/CWI/RHUL
joint online cryptography seminars

Main result

We describe a (Monte Carlo) algorithm

- computing the class group and unit group of a number field K
- provably correct (assuming ERH)

Motivations

Lattice-based cryptography: use structured lattices for efficiency

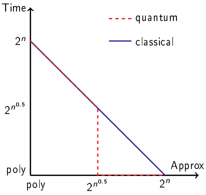
- module lattices
- ideal lattices (i.e., modules of dim 1)

Motivations

Lattice-based cryptography: use structured lattices for efficiency

- module lattices
- ideal lattices (i.e., modules of dim 1)

Cryptanalysis: recent algorithms computing short vectors in ideal lattices require to compute units and class groups



ideals lattices [CDW17]
(in cyclotomic fields)

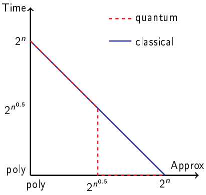
[CDW17] Cramer, Ducas, Wesolowski. Short stickelberger class relations and application to ideal-SVP. Eurocrypt.

Motivations

Lattice-based cryptography: use structured lattices for efficiency

- module lattices
- ideal lattices (i.e., modules of dim 1)

Cryptanalysis: recent algorithms computing short vectors in ideal lattices require to compute units and class groups



ideals lattices [CDW17]
(in cyclotomic fields)

Also: useful in algorithmic number theory

[CDW17] Cramer, Ducas, Wesolowski. Short stickelberger class relations and application to ideal-SVP. Eurocrypt.

History (algorithms computing units and class group)

Notation: $L_x(\alpha) = \exp\left(O(\log(x)^\alpha \cdot \log\log(x)^{1-\alpha})\right)$, K degree n and discriminant Δ_K

	Number fields	Complexity	Non heuristic
[HM89]	quadratic imaginary	$L_{\Delta_K}(1/2)$	✓

(all algorithms assume ERH)

[HM89] Hafner, McCurley. A rigorous subexponential algorithm for computation of class groups. Journal of the American mathematical society.

History (algorithms computing units and class group)

Notation: $L_x(\alpha) = \exp\left(O(\log(x)^{\alpha} \cdot \log\log(x)^{1-\alpha})\right)$, K degree n and discriminant Δ_K

	Number fields	Complexity	Non heuristic
[HM89]	quadratic imaginary	$L_{\Delta_K}(1/2)$	✓
[Buc88]	fixed degree n	$L_{\Delta_K}(1/2)$	✗

(all algorithms assume ERH)

[Buc88] Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. Séminaire de théorie des nombres.

History (algorithms computing units and class group)

Notation: $L_x(\alpha) = \exp\left(O(\log(x)^\alpha \cdot \log\log(x)^{1-\alpha})\right)$, K degree n and discriminant Δ_K

	Number fields	Complexity	Non heuristic
[HM89]	quadratic imaginary	$L_{\Delta_K}(1/2)$	✓
[Buc88]	fixed degree n	$L_{\Delta_K}(1/2)$	✗
[BF14]	arbitrary degree n	$L_{\Delta_K}(2/3+\varepsilon)$	✗

(all algorithms assume ERH)

[BF14] Biasse, Fieker. Subexponential class group and unit group computation in large degree number fields. LMS Journal of Computation and Mathematics.

History (algorithms computing units and class group)

Notation: $L_x(\alpha) = \exp\left(O(\log(x)^\alpha \cdot \log\log(x)^{1-\alpha})\right)$, K degree n and discriminant Δ_K

	Number fields	Complexity	Non heuristic
[HM89]	quadratic imaginary	$L_{\Delta_K}(1/2)$	✓
[Buc88]	fixed degree n	$L_{\Delta_K}(1/2)$	✗
[BF14]	arbitrary degree n	$L_{\Delta_K}(2/3+\varepsilon)$	✗
[BF14,Gel17] [BEF+17]	specific defining polynomial	as small as $L_{\Delta_K}(1/3)$	✗

(all algorithms assume ERH)

[Gel17] Gélin. Class group computations in number fields and applications to cryptology. PhD thesis.

[BEF+17] Biasse, Espitau, Fouque, Gélin, Kirchner. Computing generator in cyclotomic integer rings. Eurocrypt.

History (algorithms computing units and class group)

Notation: $L_x(\alpha) = \exp\left(O(\log(x)^\alpha \cdot \log\log(x)^{1-\alpha})\right)$, K degree n and discriminant Δ_K

	Number fields	Complexity	Non heuristic
[HM89]	quadratic imaginary	$L_{\Delta_K}(1/2)$	✓
[Buc88]	fixed degree n	$L_{\Delta_K}(1/2)$	✗
[BF14]	arbitrary degree n	$L_{\Delta_K}(2/3+\varepsilon)$	✗
[BF14,Gel17] [BEF+17]	specific defining polynomial	as small as $L_{\Delta_K}(1/3)$	✗
[BS16]	arbitrary degree n	quantum poly	✓

(all algorithms assume ERH)

[BS16] Biasse, Song. A polynomial time quantum algorithm for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

History (algorithms computing units and class group)

Notation: $L_x(\alpha) = \exp\left(O(\log(x)^\alpha \cdot \log\log(x)^{1-\alpha})\right)$, K degree n and discriminant Δ_K
ρ_K residue of the zeta function of K at 1

	Number fields	Complexity	Non heuristic
[HM89]	quadratic imaginary	$L_{\Delta_K}(1/2)$	✓
[Buc88]	fixed degree n	$L_{\Delta_K}(1/2)$	✗
[BF14]	arbitrary degree n	$L_{\Delta_K}(2/3+\varepsilon)$	✗
[BF14,Gel17] [BEF+17]	specific defining polynomial	as small as $L_{\Delta_K}(1/3)$	✗
[BS16]	arbitrary degree n	quantum poly	✓
This work	arbitrary degree n	$\rho_K(L_{\Delta_K}(1/2) + L_{n^n}(2/3))$	✓

(all algorithms assume ERH)

[BS16] Biasse, Song. A polynomial time quantum algorithm for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

Outline of the talk

Number fields and ideals

Number field: $K = \mathbb{Q}[X]/(X^n + 1)$ and $\mathcal{O}_K = \mathbb{Z}[X]/(X^n + 1)$ $(n = 2^k)$
(or K any number field)

Number fields and ideals

Number field: $K = \mathbb{Q}[X]/(X^n + 1)$ and $\mathcal{O}_K = \mathbb{Z}[X]/(X^n + 1)$ $(n = 2^k)$
(or K any number field)

Ideals: $I \subseteq \mathcal{O}_K$ s.t. for all $x, y \in I$ and $\alpha \in \mathcal{O}_K$

- $x + y \in I$
- $\alpha \cdot x \in I$

Number fields and ideals

Number field: $K = \mathbb{Q}[X]/(X^n + 1)$ and $\mathcal{O}_K = \mathbb{Z}[X]/(X^n + 1)$ $(n = 2^k)$
(or K any number field)

Ideals: $I \subseteq \mathcal{O}_K$ s.t. for all $x, y \in I$ and $\alpha \in \mathcal{O}_K$

- $x + y \in I$
- $\alpha \cdot x \in I$

e.g., $x \cdot \mathcal{O}_K := \{x \cdot y \mid y \in \mathcal{O}_K\}$ is a principal ideal

Number fields and ideals

Number field: $K = \mathbb{Q}[X]/(X^n + 1)$ and $\mathcal{O}_K = \mathbb{Z}[X]/(X^n + 1)$ $(n = 2^k)$
(or K any number field)

Ideals: $I \subseteq \mathcal{O}_K$ s.t. for all $x, y \in I$ and $\alpha \in \mathcal{O}_K$

- $x + y \in I$
- $\alpha \cdot x \in I$

e.g., $x \cdot \mathcal{O}_K := \{x \cdot y \,|\, y \in \mathcal{O}_K\}$ is a principal ideal

If you prefer:

$\mathcal{O}_K$	$\leftrightarrow$	$\mathbb{Z}$
$I \subseteq \mathcal{O}_K$	$\leftrightarrow$	$x \in \mathbb{Z}$ or $x \cdot \mathbb{Z}$
$I := \mathcal{O}_K$	$\leftrightarrow$	1 or $\mathbb{Z}$

Properties of ideals

Arithmetic properties:

- Multiplication / Inverse: $I \cdot J, \;\; I \cdot I^{-1} = \mathcal{O}_K$
- Divisibility: $x \in I \Leftrightarrow x \cdot \mathcal{O}_K = I \cdot J$ $\quad (6 \in 2 \cdot \mathbb{Z},\ 6 = 2 \cdot 3)$
- Unique factorization: $I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ $\quad (n_{\mathfrak{p}} \geq 0)$
- Size: $\mathcal{N}(I)$ $(\leftrightarrow |\mathbb{Z}/x\mathbb{Z}| = |x|$ for $x \in \mathbb{Z})$
- B-smooth: $I = \prod_{\mathcal{N}(\mathfrak{p}) \leq B} \mathfrak{p}^{n_{\mathfrak{p}}}$

Properties of ideals

Arithmetic properties:

- Multiplication / Inverse: $I \cdot J,\ \ I \cdot I^{-1} = \mathcal{O}_K$
- Divisibility: $x \in I \Leftrightarrow x \cdot \mathcal{O}_K = I \cdot J$ $(6 \in 2 \cdot \mathbb{Z},\ 6 = 2 \cdot 3)$
- Unique factorization: $I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ $(n_{\mathfrak{p}} \geq 0)$
- Size: $\mathcal{N}(I)$ $(\leftrightarrow |\mathbb{Z}/x\mathbb{Z}| = |x|$ for $x \in \mathbb{Z})$
- B-smooth: $I = \prod_{\mathcal{N}(\mathfrak{p}) \leq B} \mathfrak{p}^{n_{\mathfrak{p}}}$

Geometric properties:

- Embedding: $$\begin{aligned} \sigma : K &\to \mathbb{C}^n \\ x &\mapsto (\sigma_1(x), \cdots, \sigma_n(x)) \end{aligned}$$ (σ_i's are field morphisms)
- Lattices: $\sigma(I) \subset \mathbb{C}^n$ is a lattice (of rank n)
- Size: $\|x\| := \|\sigma(x)\|_2$ $(x \in \mathcal{O}_K)$

S-units

Notations:

- $\mathcal{S}$ is a finite set of prime ideals of $\mathcal{O}_K$
- Log : $K \to \mathbb{R}^n$ is the logarithmic embedding
  ($\mathrm{Log}(x) = (\log|\sigma_1(x)|, \cdots, \log|\sigma_n(x)|)$, with σ_i the complex embeddings of K)

S-units

Notations:

- $\mathcal{S}$ is a finite set of prime ideals of $\mathcal{O}_K$
- $\mathrm{Log} : K \to \mathbb{R}^n$ is the logarithmic embedding
  ($\mathrm{Log}(x) = (\log|\sigma_1(x)|, \cdots, \log|\sigma_n(x)|)$, with σ_i the complex embeddings of K)

Definition

The Log-$\mathcal{S}$-unit lattice is

$$\Lambda_{\mathcal{S}} := \left\{ \left(\mathrm{Log}(x), (-n_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{S}} \right) \,\middle|\, x\mathcal{O}_K = \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_{\mathfrak{p}}} \right\} \subset \mathbb{R}^n \times \mathbb{Z}^{|\mathcal{S}|}$$

(e.g., $\mathcal{S} = \{2, 3, 5\}$, $x = 6$, $\quad 6 = 2^1 \cdot 3^1 \cdot 5^0 \Rightarrow (\log(6), -1, -1, 0) \in \Lambda_S$)

S-units

Notations:

- $\mathcal{S}$ is a finite set of prime ideals of $\mathcal{O}_K$
- $\text{Log} : K \to \mathbb{R}^n$ is the logarithmic embedding
  ($\text{Log}(x) = (\log|\sigma_1(x)|, \cdots, \log|\sigma_n(x)|)$, with σ_i the complex embeddings of K)

Definition

The Log-$\mathcal{S}$-unit lattice is

$$\Lambda_{\mathcal{S}} := \left\{ \left(\text{Log}(x), (-n_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{S}} \right) \,\middle|\, x\mathcal{O}_K = \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_{\mathfrak{p}}} \right\} \subset \mathbb{R}^n \times \mathbb{Z}^{|\mathcal{S}|}$$

(e.g., $\mathcal{S} = \{2,3,5\}$, $x = 6$, $\quad 6 = 2^1 \cdot 3^1 \cdot 5^0 \Rightarrow (\log(6), -1, -1, 0) \in \Lambda_{\mathcal{S}}$)

Computing $\mathcal{S}$-units = computing a basis of $\Lambda_{\mathcal{S}}$
(or a generating set)

Theorem and applications

Theorem

Assuming ERH, there is a Monte Carlo algorithm which computes $\Lambda_{\mathcal{S}}$ in expected time polynomial in its input length, in ρ_K, in $L_{\Delta_K}(1/2)$ and in $L_{n^n}(2/3)$.

Reminder: ρ_K is the residue at 1 of ζ_K

Theorem and applications

Theorem

Assuming ERH, there is a Monte Carlo algorithm which computes $\Lambda_{\mathcal{S}}$ in expected time polynomial in its input length, in ρ_K, in $L_{\Delta_K}(1/2)$ and in $L_{n^n}(2/3)$.

Reminder: ρ_K is the residue at 1 of ζ_K

Applications: we can also compute

- unit group ($\mathcal{S} = \emptyset$)
- class-group ($\mathcal{S}$ generates Cl_K)
- generators of principal ideals
- class-group discrete logarithms

Outline of the talk

Computing a vector of $\Lambda_{\mathcal{S}}$

Definition: $\mathcal{S} = \{\text{prime } \mathfrak{p} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$ (for some B to be determined)

Computing a vector of $\Lambda_{\mathcal{S}}$

Definition: $\mathcal{S} = \{\text{prime } \mathfrak{p} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$ (for some B to be determined)

Algorithm `SampleVector`

1: **repeat**
2: Sample random $x \in \mathcal{O}_K$
3: **until** $x\mathcal{O}_K = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{n_\mathfrak{p}}$ for some $n_\mathfrak{p} \in \mathbb{Z}$
4: **return** $\big(\mathrm{Log}(x), (-n_\mathfrak{p})_\mathfrak{p}\big)$

Computing a vector of $\Lambda_\mathcal{S}$

Definition: $\mathcal{S} = \{\text{prime } \mathfrak{p} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$ (for some B to be determined)

Algorithm `SampleVector`

1: **repeat**
2: Sample random $x \in \mathcal{O}_K$
3: **until** $x\mathcal{O}_K = \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_\mathfrak{p}}$ for some $n_\mathfrak{p} \in \mathbb{Z}$
4: **return** $\big(\mathrm{Log}(x), (-n_\mathfrak{p})_\mathfrak{p}\big)$

Correctness: ✓

Computing a vector of $\Lambda_{\mathcal{S}}$

Definition: $\mathcal{S} = \{\text{prime } \mathfrak{p} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$ (for some B to be determined)

Algorithm `SampleVector`

1: **repeat**
2: Sample random $x \in \mathcal{O}_K$
3: **until** $x\mathcal{O}_K = \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_\mathfrak{p}}$ for some $n_\mathfrak{p} \in \mathbb{Z}$
4: **return** $\big(\mathrm{Log}(x), (-n_\mathfrak{p})_\mathfrak{p}\big)$

Correctness: ✓

Complexity: $O\Big(T_{\text{sample}} \cdot p_{\text{smooth}}^{-1} \cdot |\mathcal{S}|\Big)$

- T_{sample}: time to sample x
- p_{smooth}: probability that $x\mathcal{O}_K$ is smooth
- $|\mathcal{S}| = O(B)$: time to test smoothness

Computing a vector of $\Lambda_{\mathcal{S}}$

Definition: $\mathcal{S} = \{\text{prime } \mathfrak{p} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$ (for some B to be determined)

Algorithm `SampleVector`

1: **repeat**
2: Sample random $x \in \mathcal{O}_K$
3: **until** $x\mathcal{O}_K = \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_\mathfrak{p}}$ for some $n_\mathfrak{p} \in \mathbb{Z}$
4: **return** $\big(\mathrm{Log}(x), (-n_\mathfrak{p})_\mathfrak{p}\big)$

Correctness: ✓

Complexity: $O\Big(T_{\text{sample}} \cdot p_{\text{smooth}}^{-1} \cdot |\mathcal{S}|\Big)$

- T_{sample}: time to sample x
- p_{smooth}: probability that $x\mathcal{O}_K$ is smooth
- $|\mathcal{S}| = O(B)$: time to test smoothness

How to sample x? – Buchmann

Buchmann:

- sample random ideal $I = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{m_\mathfrak{p}}$
- $x = \texttt{Shortest\_Vector}(I)$ $\qquad (x \in I \Rightarrow x\mathcal{O}_K = I \cdot J)$

How to sample x? – Buchmann

Buchmann:

- sample random ideal $I = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{m_\mathfrak{p}}$
- $x = \texttt{Shortest\_Vector}(I)$ $\quad (x \in I \Rightarrow x\mathcal{O}_K = I \cdot J)$

$x\mathcal{O}_K$ smooth $\Leftrightarrow$ xI^{-1} smooth

($\Rightarrow$ the smaller $\mathcal{N}(xI^{-1})$, the better)

How to sample x? – Buchmann

Buchmann:

- sample random ideal $I = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{m_{\mathfrak{p}}}$
- $x = \texttt{Shortest\_Vector}(I)$ $\quad$ $(x \in I \Rightarrow x\mathcal{O}_K = I \cdot J)$

$x\mathcal{O}_K$ smooth $\Leftrightarrow$ xI^{-1} smooth

($\Rightarrow$ the smaller $\mathcal{N}(xI^{-1})$, the better)

Complexity: $2^{O(n)}$ (for $\texttt{Shortest\_Vector}(I)$)

How to sample x? – Buchmann

Buchmann:

- sample random ideal $I = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{m_\mathfrak{p}}$
- $x = \texttt{Shortest\_Vector}(I)$ $(x \in I \Rightarrow x\mathcal{O}_K = I \cdot J)$

$x\mathcal{O}_K$ smooth $\Leftrightarrow$ xI^{-1} smooth
($\Rightarrow$ the smaller $\mathcal{N}(xI^{-1})$, the better)

Complexity: $2^{O(n)}$ (for $\texttt{Shortest\_Vector}(I)$)

Subexponential only for fixed n

How to sample x? – Biasse-Fieker

Biasse-Fieker:

- sample random ideal $I = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{m_\mathfrak{p}}$
- $x = \mathrm{BKZ}_\beta(I)$ (blocksize β)

How to sample x? – Biasse-Fieker

Biasse-Fieker:

- sample random ideal $I = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{m_\mathfrak{p}}$
- $x = \mathrm{BKZ}_\beta(I)$ (blocksize β)

Complexity: $2^{O(\beta)}$ (can be subexponential)

How to sample x? – Biasse-Fieker

Biasse-Fieker:

- sample random ideal $I = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{m_\mathfrak{p}}$
- $x = \mathrm{BKZ}_\beta(I)$ (blocksize β)

Complexity: $2^{O(\beta)}$ (can be subexponential)

Shortness: $\|x\|_\infty \leq n^{n/\beta} \cdot \Delta_K^{1/(2n)} \cdot \mathcal{N}(I)^{1/n}$

How to sample x? – Biasse-Fieker

Biasse-Fieker:

- sample random ideal $I = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{m_\mathfrak{p}}$
- $x = \mathrm{BKZ}_\beta(I)$ (blocksize β)

Complexity: $2^{O(\beta)}$ (can be subexponential)

Shortness: $\|x\|_\infty \leq n^{n/\beta} \cdot \Delta_K^{1/(2n)} \cdot \mathcal{N}(I)^{1/n}$

$$\Rightarrow \quad \mathcal{N}(xI^{-1}) \leq n^{n^2/\beta} \cdot \sqrt{\Delta_K}$$

Intermediate summary

$\mathcal{S} := \{\text{prime } \mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq B\}$

Algorithm `SampleVector`

1: **repeat**
2: Sample random $I = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{m_\mathfrak{p}}$
3: $x \leftarrow \mathrm{BKZ}_\beta(I)$
4: **until** $xI^{-1} = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{n_\mathfrak{p}}$ for some $n_\mathfrak{p} \in \mathbb{Z}$
5: **return** $\big(\mathrm{Log}(x), (-n_\mathfrak{p} - m_\mathfrak{p})_\mathfrak{p}\big)$

Intermediate summary

$\mathcal{S} := \{\text{prime } \mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq B\}$

Algorithm `SampleVector`

1: **repeat**
2: Sample random $I = \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{m_\mathfrak{p}}$
3: $x \leftarrow \mathrm{BKZ}_\beta(I)$
4: **until** $xI^{-1} = \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_\mathfrak{p}}$ for some $n_\mathfrak{p} \in \mathbb{Z}$
5: **return** $\big(\mathrm{Log}(x), (-n_\mathfrak{p} - m_\mathfrak{p})_\mathfrak{p}\big)$

Complexity:

$$O\Big(T_{\text{sample}} \cdot p_{\text{smooth}}^{-1} \cdot |\mathcal{S}|\Big) = 2^{O(\beta)} \cdot B \cdot p_{\text{smooth}}^{-1}$$

Intermediate summary

$\mathcal{S} := \{\text{prime } \mathfrak{p} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$

Algorithm `SampleVector`

1: **repeat**
2: Sample random $I = \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{m_\mathfrak{p}}$
3: $x \leftarrow \mathrm{BKZ}_\beta(I)$
4: **until** $xI^{-1} = \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_\mathfrak{p}}$ for some $n_\mathfrak{p} \in \mathbb{Z}$
5: **return** $\big(\mathrm{Log}(x), (-n_\mathfrak{p} - m_\mathfrak{p})_\mathfrak{p}\big)$

Complexity:

$$O\Big(T_{\text{sample}} \cdot p_{\text{smooth}}^{-1} \cdot |\mathcal{S}|\Big) \;=\; 2^{O(\beta)} \cdot B \cdot p_{\text{smooth}}^{-1}$$

Smoothness probability

Notation: $p_{y,B}$ = proba that a uniformly random ideal of norm $\leq y$ is B-smooth

Smoothness probability

Notation: $p_{y,B}$ = proba that a uniformly random ideal of norm $\leq y$ is B-smooth

Asymptotically: $p_{y,B} \sim \rho(u) \approx u^{-u}$ (ρ Dickman function, $u = \log y / \log B$)

Smoothness probability

Notation: $p_{y,B}$ = proba that a uniformly random ideal of norm $\leq y$ is B-smooth

Asymptotically: $p_{y,B} \sim \rho(u) \approx u^{-u}$ (ρ Dickman function, $u = \log y / \log B$)

⚠ K fixed and B, u tending to infinity

Smoothness probability

Notation: $p_{y,B}$ = proba that a uniformly random ideal of norm $\leq y$ is B-smooth

Asymptotically: $p_{y,B} \sim \rho(u) \approx u^{-u}$ (ρ Dickman function, $u = \log y / \log B$)

⚠ K fixed and B, u tending to infinity

Heuristic: $p_{\text{smooth}} \approx u^{-u}$ where $u = \frac{\log \mathcal{N}(xI^{-1})}{\log B}$

Smoothness probability

Notation: $p_{y,B}$ = proba that a uniformly random ideal of norm $\leq y$ is B-smooth

Asymptotically: $p_{y,B} \sim \rho(u) \approx u^{-u}$ (ρ Dickman function, $u = \log y / \log B$)

⚠ K fixed and B, u tending to infinity

Heuristic: $p_{\text{smooth}} \approx u^{-u}$ where $u = \frac{\log \mathcal{N}(xI^{-1})}{\log B}$

2 assumptions hidden:

- the provable asymptotic bounds require huge B to be effective (roughly $B \gtrsim 2^{2^n}$)
- xI^{-1} is not a random ideal of bounded norm

Sampling one vector – summary

Algorithm `SampleVector`

```
repeat
    Sample random $I = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{m_\mathfrak{p}}$
    $x \leftarrow \mathrm{BKZ}_\beta(I)$
until $xI^{-1} = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{n_\mathfrak{p}}$ for some $n_\mathfrak{p} \in \mathbb{Z}$
return $\big(\mathrm{Log}(x), (-n_\mathfrak{p} - m_\mathfrak{p})_\mathfrak{p}\big)$
```

Complexity (heuristic):

$$2^{O(\beta)} \cdot B \cdot u^u \qquad \text{with } u = \frac{\log \mathcal{N}(xI^{-1})}{\log B} \leq \frac{n^2 \log n/\beta + \log|\Delta_K|/2}{\log B}$$

Sampling one vector – summary

Algorithm `SampleVector`

1: **repeat**
2: Sample random $I = \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{m_\mathfrak{p}}$
3: $x \leftarrow \mathrm{BKZ}_\beta(I)$
4: **until** $xI^{-1} = \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_\mathfrak{p}}$ for some $n_\mathfrak{p} \in \mathbb{Z}$
5: **return** $\left(\mathrm{Log}(x), (-n_\mathfrak{p} - m_\mathfrak{p})_\mathfrak{p}\right)$

Complexity (heuristic):

$$2^{O(\beta)} \cdot B \cdot u^u \qquad \text{with } u = \frac{\log \mathcal{N}(xI^{-1})}{\log B} \leq \frac{n^2 \log n/\beta + \log|\Delta_K|/2}{\log B}$$

Instantiating:

- $\beta = n^{2/3}$
- $B = L_{\Delta_K}(1/2) + L_{n^n}(2/3)$

Total complexity: $L_{\Delta_K}(1/2) + L_{n^n}(2/3)$

Computing the full lattice $\Lambda_{\mathcal{S}}$

Remark: One can efficiently approximate $\det(\Lambda_{\mathcal{S}}) = \mathrm{Reg}_K \cdot h_K$
($\mathcal{S}$ generates the class-group)

Computing the full lattice $\Lambda_{\mathcal{S}}$

Remark: One can efficiently approximate $\det(\Lambda_{\mathcal{S}}) = \mathrm{Reg}_K \cdot h_K$

($\mathcal{S}$ generates the class-group)

Algorithm `ComputeSUnits`

repeat

    $\boldsymbol{z}_i \leftarrow$ `SampleVector()`

until $\mathcal{L}((\boldsymbol{z}_i)_i)$ is a lattice with the desired rank and det

Compute a basis $\boldsymbol{B}$ of $\mathcal{L}((\boldsymbol{z}_i)_i)$ (linear algebra)

return $\boldsymbol{B}$

Computing the full lattice $\Lambda_{\mathcal{S}}$

Remark: One can efficiently approximate $\det(\Lambda_{\mathcal{S}}) = \mathrm{Reg}_K \cdot h_K$
($\mathcal{S}$ generates the class-group)

Algorithm `ComputeSUnits`

1: **repeat**
2: $\quad \boldsymbol{z}_i \leftarrow$ `SampleVector()`
3: **until** $\mathcal{L}((\boldsymbol{z}_i)_i)$ is a lattice with the desired rank and det
4: Compute a basis $\boldsymbol{B}$ of $\mathcal{L}((\boldsymbol{z}_i)_i)$ (linear algebra)
5: **return** $\boldsymbol{B}$

Correctness: ✓

Computing the full lattice $\Lambda_{\mathcal{S}}$

Remark: One can efficiently approximate $\det(\Lambda_{\mathcal{S}}) = \mathrm{Reg}_K \cdot h_K$

($\mathcal{S}$ generates the class-group)

Algorithm `ComputeSUnits`

1: **repeat**
2: $\quad \boldsymbol{z}_i \leftarrow$ `SampleVector()`
3: **until** $\mathcal{L}((\boldsymbol{z}_i)_i)$ is a lattice with the desired rank and det
4: Compute a basis $\boldsymbol{B}$ of $\mathcal{L}((\boldsymbol{z}_i)_i)$ (linear algebra)
5: **return** $\boldsymbol{B}$

Correctness: ✓

Heuristic: $O(B)$ vectors from `SampleVector()` generate $\Lambda_{\mathcal{S}}$ with good probability ($\mathrm{rk}(\Lambda_{\mathcal{S}}) = O(B)$)

Computing the full lattice $\Lambda_{\mathcal{S}}$

Remark: One can efficiently approximate $\det(\Lambda_{\mathcal{S}}) = \mathrm{Reg}_K \cdot h_K$

($\mathcal{S}$ generates the class-group)

Algorithm `ComputeSUnits`

1: **repeat**
2: $\quad \boldsymbol{z}_i \leftarrow$ `SampleVector()`
3: **until** $\mathcal{L}((\boldsymbol{z}_i)_i)$ is a lattice with the desired rank and det
4: Compute a basis $\boldsymbol{B}$ of $\mathcal{L}((\boldsymbol{z}_i)_i)$ (linear algebra)
5: **return** $\boldsymbol{B}$

Correctness: ✓

Heuristic: $O(B)$ vectors from `SampleVector()` generate $\Lambda_{\mathcal{S}}$ with good probability ($\mathrm{rk}(\Lambda_{\mathcal{S}}) = O(B)$)

Complexity: $\mathrm{poly}(B) = L_{\Delta_K}(1/2) + L_{n^n}(2/3)$

Heuristics – summary

Heuristic 1: $p_{\text{smooth}} \approx u^{-u}$ where $u = \frac{\log \mathcal{N}(xI^{-1})}{\log B}$

1.1. the asymptotic bounds hold even for smallish B's

1.2. xI^{-1} behaves like a uniform ideal of bounded norm

Heuristics – summary

Heuristic 1: $p_{\text{smooth}} \approx u^{-u}$ where $u = \frac{\log \mathcal{N}(xI^{-1})}{\log B}$

1.1. the asymptotic bounds hold even for smallish B's

1.2. xI^{-1} behaves like a uniform ideal of bounded norm

Heuristic 2: $O(B)$ vectors from `SampleVector()` generate $\Lambda_{\mathcal{S}}$ with good probability

Outline of the talk

Provable sampling in ideals [BDPW22]

Algorithm `SampleInIdeal`

1: sample random $I = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{m_{\mathfrak{p}}}$
2: $\boldsymbol{B} \leftarrow BKZ_{\beta}(I)$ ($\boldsymbol{B}$ reduced basis of I)
3: sample random $x \in I$ (using small basis $\boldsymbol{B}$)
4: **return** (x, I)

[BDPW22] de Boer, Ducas, Pellet-Mary, Wesolowski. Sampling ideals in a class: smooth, near-prime or otherwise.

Provable sampling in ideals [BDPW22]

Algorithm `SampleInIdeal`

1: sample random $I = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{m_{\mathfrak{p}}}$
2: $\boldsymbol{B} \leftarrow BKZ_\beta(I)$ ($\boldsymbol{B}$ reduced basis of I)
3: sample random $x \in I$ (using small basis $\boldsymbol{B}$)
4: **return** (x, I)

Theorem (ERH) [BDPW22]

For any infinite set $\mathcal{T}$ of ideals, it holds that

$$\Pr_{(x,I) \leftarrow \texttt{SampleInIdeal}} \left(xI^{-1} \in \mathcal{T} \right) \geq \frac{\delta_{\mathcal{T}}[n^{n^2/\beta} \cdot \sqrt{\Delta_K}]}{3}.$$

Definition: $\delta_{\mathcal{T}}[y] \approx \frac{|\{\mathfrak{a} \in \mathcal{T} \,|\, \mathcal{N}(\mathfrak{a}) \leq y\}|}{|\{\mathfrak{a} \text{ ideal} \,|\, \mathcal{N}(\mathfrak{a}) \leq y\}|}$ (density of $\mathcal{T}$ at y)

[BDPW22] de Boer, Ducas, Pellet-Mary, Wesolowski. Sampling ideals in a class: smooth, near-prime or otherwise.

Heuristic 1.2

Heuristic 1.2: xI^{-1} behaves like a uniform ideal of bounded norm

Can be proven using previous slide up to

- changing slightly the sampling procedure
- decreasing by 3 the success probability

Heuristic 1.1

Heuristic 1.1: $\delta_{\mathcal{S}}[y] \approx u^{-u}$ even for small B's $\quad (u = \log y / \log B)$

Heuristic 1.1

Heuristic 1.1: $\delta_{\mathcal{S}}[y] \approx u^{-u}$ even for small B's $\quad (u = \log y / \log B)$

- We could not prove it, but we proved

Lemma

For any $B \geq \Omega((n + \log \Delta_K)^3)$,

$$\delta_{\mathcal{S}}[y] \gtrsim u^{-u} \cdot \rho_K^{-1}.$$

Heuristic 1.1

Heuristic 1.1: $\delta_{\mathcal{S}}[y] \approx u^{-u}$ even for small B's $\quad (u = \log y / \log B)$

- We could not prove it, but we proved

Lemma

For any $B \geq \Omega((n + \log \Delta_K)^3)$,

$$\delta_{\mathcal{S}}[y] \gtrsim u^{-u} \cdot \rho_K^{-1}.$$

Discussion:

- for cyclotomic fields, $\rho_K = \mathrm{poly}(n)$

Heuristic 1.1

Heuristic 1.1: $\delta_{\mathcal{S}}[y] \approx u^{-u}$ even for small B's $(u = \log y / \log B)$

- We could not prove it, but we proved

Lemma

For any $B \geq \Omega((n + \log \Delta_K)^3)$,

$$\delta_{\mathcal{S}}[y] \gtrsim u^{-u} \cdot \rho_K^{-1}.$$

Discussion:

- for cyclotomic fields, $\rho_K = \mathrm{poly}(n)$
- there exist fields where $\rho_K = \exp(n)$

Heuristic 1.1

Heuristic 1.1: $\delta_{\mathcal{S}}[y] \approx u^{-u}$ even for small B's $(u = \log y / \log B)$

- We could not prove it, but we proved

Lemma

For any $B \geq \Omega((n + \log \Delta_K)^3)$,

$$\delta_{\mathcal{S}}[y] \gtrsim u^{-u} \cdot \rho_K^{-1}.$$

Discussion:

- for cyclotomic fields, $\rho_K = \mathrm{poly}(n)$
- there exist fields where $\rho_K = \exp(n)$
- is the bound tight?
  - If yes, this impacts also the heuristic algorithm

Heuristic 1 – summary

One can prove heuristic 1 up to

- changing slightly the sampling procedure (same asymptotic complexity)
- dividing p_{smooth} by ρ_K

Heuristic 1 – summary

One can prove heuristic 1 up to

- changing slightly the sampling procedure (same asymptotic complexity)
- dividing p_{smooth} by ρ_K

Theorem (ERH)

There is an algorithm `SampleVector` that computes $\boldsymbol{v} \in \Lambda_{\mathcal{S}}$ in time

$$\rho_K \cdot \Big(L_{\Delta_K}(1/2) + L_{n^n}(2/3) \Big).$$

Outline of the talk

Variation on `SampleVector`

Reminder

There is an algorithm `SampleVector` that

- computes $\boldsymbol{v} \in \Lambda_{\mathcal{S}}$
- in time

$$\rho_K \cdot \Big(L_{\Delta_K}(1/2) + L_{n^n}(2/3) \Big).$$

Variation on SampleVector

Reminder

There is an algorithm `SampleVector` that

- computes $x \in K$ and $(n_\mathfrak{p})_\mathfrak{p} \in \mathbb{Z}^{|\mathcal{S}|}$ such that $x\mathcal{O}_K = \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_\mathfrak{p}}$
- in time

$$\rho_K \cdot \Big(L_{\Delta_K}(1/2) + L_{n^n}(2/3) \Big).$$

Variation on `SampleVector`

Reminder

There is an algorithm `SampleVector` that

- takes as input an ideal I
- computes $x \in K$ and $(n_\mathfrak{p})_\mathfrak{p} \in \mathbb{Z}^{|\mathcal{S}|}$ such that $x\mathcal{O}_K = I \cdot \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_\mathfrak{p}}$
- in time

$$\rho_K \cdot \Big(L_{\Delta_K}(1/2) + L_{n^n}(2/3) \Big).$$

Variation on SampleVector

Reminder

There is an algorithm SampleVector that

- takes as input an ideal I
- computes $x \in K$ and $(n_\mathfrak{p})_\mathfrak{p} \in \mathbb{Z}^{|\mathcal{S}|}$ such that $x\mathcal{O}_K = I \cdot \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_\mathfrak{p}}$
- in time

$$\rho_K \cdot \Big(L_{\Delta_K}(1/2) + L_{n^n}(2/3) \Big).$$

From now on, we use SampleVector in a black-box way

Heuristic 2 – main idea

Algorithm `RandomVector`

sample random $\boldsymbol{v} := \big(\operatorname{Log} x, (-n_{\mathfrak{p}})\big)$ $\quad (x\mathcal{O}_K \neq \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_{\mathfrak{p}}})$
define $I := x \cdot \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{-n_{\mathfrak{p}}}$
$\boldsymbol{w} := \big(\operatorname{Log} y, (-m_{\mathfrak{p}})_{\mathfrak{p}}\big) \leftarrow$ `SampleVector(I)` $\quad (y\mathcal{O}_K = I \cdot \prod \mathfrak{p}^{m_{\mathfrak{p}}})$
return $\boldsymbol{w} - \boldsymbol{v}$

Heuristic 2 – main idea

Algorithm `RandomVector`

1: sample random $\boldsymbol{v} := \big(\mathrm{Log}\, x, (-n_{\mathfrak{p}})\big)$ $\quad (x\mathcal{O}_K \neq \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_{\mathfrak{p}}})$

2: define $I := x \cdot \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{-n_{\mathfrak{p}}}$

3: $\boldsymbol{w} := \big(\mathrm{Log}\, y, (-m_{\mathfrak{p}})_{\mathfrak{p}}\big) \leftarrow$ `SampleVector(I)` $\quad (y\mathcal{O}_K = I \cdot \prod \mathfrak{p}^{m_{\mathfrak{p}}})$

4: **return** $\boldsymbol{w} - \boldsymbol{v}$

Correctness: $yx^{-1} \cdot \mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}} - n_{\mathfrak{p}}} \quad \Rightarrow \quad \boldsymbol{w} - \boldsymbol{v} \in \Lambda_{\mathcal{S}}$

Heuristic 2 – main idea

Algorithm `RandomVector`

sample random $\boldsymbol{v} := \big(\operatorname{Log} x, (-n_{\mathfrak{p}})\big)$ $\quad (x\mathcal{O}_K \neq \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{n_{\mathfrak{p}}})$
define $I := x \cdot \prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{-n_{\mathfrak{p}}}$
$\boldsymbol{w} := \big(\operatorname{Log} y, (-m_{\mathfrak{p}})_{\mathfrak{p}}\big) \leftarrow$ `SampleVector(I)` $\quad (y\mathcal{O}_K = I \cdot \prod \mathfrak{p}^{m_{\mathfrak{p}}})$
return $\boldsymbol{w} - \boldsymbol{v}$

Correctness: $yx^{-1} \cdot \mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}} - n_{\mathfrak{p}}} \quad \Rightarrow \quad \boldsymbol{w} - \boldsymbol{v} \in \Lambda_{\mathcal{S}}$

Intuition: $\boldsymbol{w} - \boldsymbol{v}$ is random in $\Lambda_{\mathcal{S}}$ (and independent from other vectors obtained so far) because `SampleVector` cannot guess $\boldsymbol{v}$ from I.

More details

Reminder:

- $\boldsymbol{v} = \big(\operatorname{Log} x, (-n_{\mathfrak{p}})_{\mathfrak{p}}\big)$
- $I = x \cdot \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}}$
- $\boldsymbol{w} = \texttt{SampleVector(I)}$ $\quad (\Rightarrow \boldsymbol{w} - \boldsymbol{v} \in \Lambda_{\mathcal{S}})$

More details

Reminder:

- $\mathbf{v} = \left(\operatorname{Log} x, (-n_{\mathfrak{p}})_{\mathfrak{p}}\right)$
- $I = x \cdot \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}}$
- $\mathbf{w} = \texttt{SampleVector(I)}$ $\quad (\Rightarrow \mathbf{w} - \mathbf{v} \in \Lambda_S)$

Claim: $\mathbf{w}$ only depends on $\mathbf{v}$ mod Λ_S and $\mathbf{w} - \mathbf{v} \in \Lambda_S$

More details

Reminder:

- $\boldsymbol{v} = \big(\operatorname{Log} x, (-n_{\mathfrak{p}})_{\mathfrak{p}}\big)$
- $I = x \cdot \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}}$
- $\boldsymbol{w} = \texttt{SampleVector(I)}$ $\quad (\Rightarrow \boldsymbol{w} - \boldsymbol{v} \in \Lambda_{\mathcal{S}})$

Claim: $\boldsymbol{w}$ only depends on $\boldsymbol{v}$ mod Λ_S and $\boldsymbol{w} - \boldsymbol{v} \in \Lambda_S$

Proof: $x \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}} = x' \prod_{\mathfrak{p}} \mathfrak{p}^{-n'_{\mathfrak{p}}} \Leftrightarrow \boldsymbol{v} = \boldsymbol{v}'$ mod $\Lambda_{\mathcal{S}}$

More details

Reminder:

- $\boldsymbol{v} = \left(\operatorname{Log} x, (-n_{\mathfrak{p}})_{\mathfrak{p}}\right)$
- $I = x \cdot \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}}$
- $\boldsymbol{w} = \texttt{SampleVector(I)}$ $\quad (\Rightarrow \boldsymbol{w} - \boldsymbol{v} \in \Lambda_{\mathcal{S}})$

Claim: $\boldsymbol{w}$ only depends on $\boldsymbol{v}$ mod $\Lambda_{\mathcal{S}}$ and $\boldsymbol{w} - \boldsymbol{v} \in \Lambda_{\mathcal{S}}$

Proof: $x \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}} = x' \prod_{\mathfrak{p}} \mathfrak{p}^{-n'_{\mathfrak{p}}} \Leftrightarrow \boldsymbol{v} = \boldsymbol{v}'$ mod $\Lambda_{\mathcal{S}}$

$\Rightarrow I$ only depends on $\boldsymbol{v} + \Lambda_{\mathcal{S}}$

$\Rightarrow \boldsymbol{w}$ only depends on $\boldsymbol{v} + \Lambda_{\mathcal{S}}$

(provided we have a canonical representation for I)

Distribution of $\boldsymbol{v}$

$\boldsymbol{w} = f(\boldsymbol{v} + \Lambda_{\mathcal{S}})$ and $\boldsymbol{w} - \boldsymbol{v} \in \Lambda_{\mathcal{S}}$ (f might be randomized)

Distribution of $\boldsymbol{v}$

$\boldsymbol{w} = f(\boldsymbol{v} + \Lambda_{\mathcal{S}})$ and $\boldsymbol{w} - \boldsymbol{v} \in \Lambda_{\mathcal{S}}$ (f might be randomized)

Consequence: ($D_{\Lambda,\sigma}$ centered discrete gaussian distribution over Λ, deviation σ)

- $\boldsymbol{v} \leftarrow D_\sigma$
- $\boldsymbol{w} \leftarrow f(\boldsymbol{v} + \Lambda_{\mathcal{S}})$
- return $\boldsymbol{z} := \boldsymbol{v} - \boldsymbol{w}$

$\iff$ (if σ large enough)

- $\boldsymbol{v}' + \Lambda_{\mathcal{S}} \leftarrow D_\sigma \bmod \Lambda_{\mathcal{S}}$
- $\boldsymbol{w} \leftarrow f(\boldsymbol{v}' + \Lambda_{\mathcal{S}})$
- $\boldsymbol{v} \leftarrow D_{\boldsymbol{v}'+\Lambda_{\mathcal{S}},\sigma}$
- return $\boldsymbol{z} := \boldsymbol{v} - \boldsymbol{w}$

Distribution of $\boldsymbol{v}$

$$\boldsymbol{w} = f(\boldsymbol{v} + \Lambda_{\mathcal{S}}) \quad \text{and} \quad \boldsymbol{w} - \boldsymbol{v} \in \Lambda_{\mathcal{S}} \qquad (f \text{ might be randomized})$$

Consequence: ($D_{\Lambda,\sigma}$ centered discrete gaussian distribution over Λ, deviation σ)

- $\boldsymbol{v} \leftarrow D_\sigma$
- $\boldsymbol{w} \leftarrow f(\boldsymbol{v} + \Lambda_{\mathcal{S}})$
- return $\boldsymbol{z} := \boldsymbol{v} - \boldsymbol{w}$

$\Longleftrightarrow$ (if σ large enough)

- $\boldsymbol{v}' + \Lambda_{\mathcal{S}} \leftarrow D_\sigma \bmod \Lambda_{\mathcal{S}}$
- $\boldsymbol{w} \leftarrow f(\boldsymbol{v}' + \Lambda_{\mathcal{S}})$
- $\boldsymbol{v} \leftarrow D_{\boldsymbol{v}' + \Lambda_{\mathcal{S}}, \sigma}$
- return $\boldsymbol{z} := \boldsymbol{v} - \boldsymbol{w}$

$$\boldsymbol{v} - \boldsymbol{w} \sim D_{\Lambda_{\mathcal{S}}, \sigma, \boldsymbol{c}} \quad (\text{for some random center } \boldsymbol{c} = -\boldsymbol{w})$$

Distribution of $\boldsymbol{v}$

$$\boldsymbol{w} = f(\boldsymbol{v} + \Lambda_{\mathcal{S}}) \quad \text{and} \quad \boldsymbol{w} - \boldsymbol{v} \in \Lambda_{\mathcal{S}} \qquad (f \text{ might be randomized})$$

Consequence: ($D_{\Lambda,\sigma}$ centered discrete gaussian distribution over Λ, deviation σ)

- $\boldsymbol{v} \leftarrow D_\sigma$
- $\boldsymbol{w} \leftarrow f(\boldsymbol{v} + \Lambda_{\mathcal{S}})$
- return $\boldsymbol{z} := \boldsymbol{v} - \boldsymbol{w}$

$\iff$ (if σ large enough)

- $\boldsymbol{v}' + \Lambda_{\mathcal{S}} \leftarrow D_\sigma \bmod \Lambda_{\mathcal{S}}$
- $\boldsymbol{w} \leftarrow f(\boldsymbol{v}' + \Lambda_{\mathcal{S}})$
- $\boldsymbol{v} \leftarrow D_{\boldsymbol{v}'+\Lambda_{\mathcal{S}},\sigma}$
- return $\boldsymbol{z} := \boldsymbol{v} - \boldsymbol{w}$

$$\boldsymbol{v} - \boldsymbol{w} \sim D_{\Lambda_{\mathcal{S}},\sigma,\boldsymbol{c}} \quad (\text{for some random center } \boldsymbol{c} = -\boldsymbol{w})$$

Lemma: $O(B)$ samples from $D_{\Lambda_{\mathcal{S}},\sigma,\boldsymbol{c}}$ generate $\Lambda_{\mathcal{S}}$ with high probability

Heuristic 2 – summary

Algorithm `ComputeSUnits`

```
for O(B) loops do
    sample v := (Log(x), (−n_p)) ← D_σ
    w ← SampleVector(x · ∏_{p∈S} p^{−n_p})
    z_i := v − w
end for
return (z_i)_i
```

for $O(B)$ loops **do**
- sample $\boldsymbol{v} := \big(\mathrm{Log}(x), (-n_{\mathfrak{p}})\big) \leftarrow D_\sigma$
- $\boldsymbol{w} \leftarrow \mathtt{SampleVector}(x \cdot \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{-n_{\mathfrak{p}}})$
- $\boldsymbol{z}_i := \boldsymbol{v} - \boldsymbol{w}$

end for

return $(\boldsymbol{z}_i)_i$

Heuristic 2 – summary

Algorithm `ComputeSUnits`

1: **for** $O(B)$ loops **do**
2: sample $\boldsymbol{v} := \big(\mathrm{Log}(x), (-n_{\mathfrak{p}})\big) \leftarrow D_\sigma$
3: $\boldsymbol{w} \leftarrow \texttt{SampleVector}(x \cdot \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{-n_{\mathfrak{p}}})$
4: $\boldsymbol{z}_i := \boldsymbol{v} - \boldsymbol{w}$
5: **end for**
6: **return** $(\boldsymbol{z}_i)_i$

Theorem (ERH)

If `SampleVector` is correct, then `ComputeSUnits` computes a generating set of $\Lambda_{\mathcal{S}}$ with high probability in time $T(\texttt{SampleVector}) \cdot \mathrm{poly}(B)$.

Conclusion

Summary:

- remove both heuristics of Biasse-Fieker algorithm (under ERH)
- algorithm is slightly modified
- the run time is increased by a factor ρ_K

Conclusion

Summary:

- remove both heuristics of Biasse-Fieker algorithm (under ERH)
- algorithm is slightly modified
- the run time is increased by a factor ρ_K

Open question 1: is $\delta_{\mathcal{S}}[y] \approx u^{-u}$ or $\delta_{\mathcal{S}}[y] \approx \rho_K^{-1} \cdot u^{-u}$?

(**Reminder:** $\delta_{\mathcal{S}}[y] =$ density of B-smooth ideals of norm $\leq y$)

- can we improve our runtime?
- or are the runtime of the heuristic algorithms too optimistic?

Conclusion

Summary:

- remove both heuristics of Biasse-Fieker algorithm (under ERH)
- algorithm is slightly modified
- the run time is increased by a factor ρ_K

Open question 1: is $\delta_{\mathcal{S}}[y] \approx u^{-u}$ or $\delta_{\mathcal{S}}[y] \approx \rho_K^{-1} \cdot u^{-u}$?

(**Reminder:** $\delta_{\mathcal{S}}[y]$ = density of B-smooth ideals of norm $\leq y$)

- can we improve our runtime?
- or are the runtime of the heuristic algorithms too optimistic?

Open question 2: Las Vegas algorithm instead of Monte Carlo?

(check the precision needed for the linear algebra step)

Conclusion

Summary:

- remove both heuristics of Biasse-Fieker algorithm (under ERH)
- algorithm is slightly modified
- the run time is increased by a factor ρ_K

Open question 1: is $\delta_{\mathcal{S}}[y] \approx u^{-u}$ or $\delta_{\mathcal{S}}[y] \approx \rho_K^{-1} \cdot u^{-u}$?

(**Reminder:** $\delta_{\mathcal{S}}[y]$ = density of B-smooth ideals of norm $\leq y$)

- can we improve our runtime?
- or are the runtime of the heuristic algorithms too optimistic?

Open question 2: Las Vegas algorithm instead of Monte Carlo?

(check the precision needed for the linear algebra step)

Questions?