



Universiteit
Leiden
The Netherlands

Random walks on Arakelov class groups

Boer, K. de

Citation

Boer, K. de. (2022, September 22). *Random walks on Arakelov class groups*. Retrieved from <https://hdl.handle.net/1887/3463719>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/3463719>

Note: To cite this publication please use the final published version (if applicable).

Random Walks on Arakelov Class Groups

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof. dr. ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op donderdag 22 september 2022
klokke 11.15 uur

door

Koen de Boer

geboren te Nijmegen, Nederland,
in 1991

Promotores:

Prof. dr. L. Ducas (CWI Amsterdam & Universiteit Leiden)

Prof. dr. R. Cramer (CWI Amsterdam & Universiteit Leiden)

Co-promotor:

Dr. B. Wesolowski (Université de Bordeaux)

Promotiecommissie:

Prof. dr. F.A.J. de Haas (Universiteit Leiden)

Dr. E. Kirshanova (Technology Innovation Institute, Abu Dhabi & Immanuel Kant Baltic Federal University, Kaliningrad)

Prof. dr. R.M. van Luijk (Universiteit Leiden)

Prof. dr. R. Schoof (Università di Roma “Tor Vergata”)

Prof. dr. D. Stehlé (École Normale Supérieure de Lyon)

The research was carried out in the Cryptology Group at CWI Amsterdam. The PhD position was funded by the ERC Advanced Grant 740972 (ALGSTRONGCRYPTO) and by the European Union Horizon 2020 Research and Innovation Program Grant 780701 (PROMETHEUS).



Centrum Wiskunde & Informatica



Universiteit
Leiden

Koen de Boer

Random Walks on Arakelov Class Groups

**and Their Applications in Cryptography
and Algorithmic Number Theory**

To my family.

Contents

1. Introduction	1
1.1. Number Theory	1
1.2. Ideal Lattices	4
1.3. Arakelov Class Groups	7
1.4. Random Walks on the Arakelov Class Group	13
1.5. The Random Walk Theorem for Arakelov Class Groups . .	19
1.6. A Worst-case to Average-case Reduction	25
1.7. Ideal Sampling	30
1.8. The Continuous Hidden Subgroup Problem	34
1.9. Outline and Contributions of this Thesis	38
 2. Preliminaries	 41
2.1. General Notation	41
2.2. Fourier Theory	41
2.2.1. Groups	42
2.2.2. Norms and Fourier Transforms	43
2.2.3. The Poisson Summation Formula	45
2.2.4. The Fourier Transform of Vector-valued Functions .	48
2.2.5. Trigonometric Approximation	51
2.3. Number Theory	53
2.3.1. Algebraic Number Theory	53
2.3.2. The Extended Riemann Hypothesis	56
2.3.3. Prime Densities	57
2.4. Arakelov Theory	59
2.4.1. The Arakelov Ray Divisor Group	59
2.4.2. The Arakelov Ray Class Group	60
2.4.3. Relation with Other Number-theoretic Groups . . .	62

2.4.4.	The Volume of the Arakelov Ray Class Group	64
2.4.5.	An Example of an Arakelov Class Group	66
2.5.	Lattices	72
2.5.1.	General Lattices	72
2.5.2.	Divisors and Ideal Lattices	72
2.5.3.	The Gaussian Function and Smoothing Errors	76
2.5.4.	Gaussian Distributions	79
2.6.	The Lipschitz Condition	79
3.	The Continuous Hidden Subgroup Problem	81
3.1.	Summary	81
3.2.	Introduction	84
3.3.	Problem Statements and Results	90
3.3.1.	Notation and Set-up	90
3.3.2.	Main Theorem: Continuous Hidden Subgroup Problem	91
3.3.3.	Dual Lattice Sampling Problem	93
3.3.4.	Full Dual Lattice Recovery	94
3.3.5.	Primal Basis Reconstruction	94
3.3.6.	Gaussian State Preparation	95
3.3.7.	Proof of the Main Theorem	96
3.4.	Dual Lattice Sampling Algorithm	99
3.4.1.	The Algorithm	99
3.4.2.	The Figure of Merit	102
3.5.	Analysis	104
3.5.1.	Proof Overview	104
3.5.2.	Formal Analysis	107
3.6.	From Sampling to Full Dual Lattice Recovery	117
3.7.	Recovering a Basis of the Primal Lattice	123
3.7.1.	An Approximate Well-conditioned Basis of the Dual	124
3.7.2.	Inverting the Dual Approximate Basis	126
3.7.3.	Combining the Errors and Tuning the Parameters .	127
4.	Random Walks on Arakelov Ray Class Groups	129
4.1.	Summary	129
4.2.	Introduction	131

4.3. Random Walk Theorem for the Arakelov Ray Class Group .	138
4.3.1. Main result	140
4.3.2. Hecke Operators	142
4.3.3. Bounds on Eigenvalues of Hecke Operators	143
4.3.4. The Infinite Analytic Conductor	147
4.3.5. Fourier Analysis on the Ray Unit Torus	153
4.3.6. Splitting up the Character Decomposition	154
4.3.7. Conclusion	158
5. A Worst-case to Average-case Reduction for Ideal Lattices	165
5.1. Summary	165
5.2. Introduction	166
5.2.1. The Result	167
5.2.2. Overview	168
5.2.3. Related work	169
5.3. Representation of Ideal Lattices by Means of Distributions .	171
5.4. The Worst-case to Average-case Reduction	179
5.5. Discretizing the Reduction Algorithm	189
5.5.1. Introduction	189
5.5.2. Precise Definition of the Distributions Involved . . .	191
5.5.3. Discretized Algorithm Analogues	194
5.5.4. Closeness Proofs	198
6. Ideal sampling	203
6.1. Summary	203
6.2. Introduction	204
6.2.1. Our Technique	204
6.2.2. Applications	206
6.2.3. Related Works	207
6.3. Preliminaries	207
6.4. Probability-density Correspondence	209
6.4.1. Result	209
6.4.2. Proof Overview of Theorem 6.9	211

6.5.	Extended Proof of Theorem 6.9	216
6.5.1.	Simplify the Probability by Fixing a Single Ideal $\mathfrak{c} \in \mathcal{S}^m$ and a single Arakelov divisor $\mathbf{a} \in \text{Div}_{K^m}^0$	216
6.5.2.	Estimating the Number of Shifted Lattice Points in a Box	217
6.5.3.	Estimating the Probability of Sampling a Single Fixed Ideal for a <i>Random</i> Arakelov Divisor	220
6.5.4.	The Number $ \text{Exp}(\mathbf{a} + d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty $ Only Depends on the Arakelov Ray <i>Class</i> of $\mathbf{a} \in \text{Div}_{K^m}^0$	220
6.5.5.	Taking the Logarithmic Map into $H = \text{Log } K_{\mathbb{R}}^0$	223
6.5.6.	Applying the Abel Summation Formula	224
6.6.	Ideal Sampling	226
6.6.1.	Sampling in a Box	226
6.6.2.	The Sampling Algorithm	228
7.	The Power Residue Symbol is in ZPP	235
7.1.	Summary	235
7.2.	Introduction	236
7.3.	Preliminaries	238
7.4.	Reduction to Cyclotomic Fields	241
7.4.1.	Introduction	241
7.4.2.	Proof Strategy	242
7.4.3.	Signature Identity	244
7.4.4.	Invariant Factor Decomposition of $R/\mathfrak{b}$	248
7.4.5.	The Signature is Compatible with Short Exact Sequences	249
7.4.6.	The Determinant Formula	251
7.4.7.	Applying Induction on the Components of the Module	253
7.4.8.	Conclusion	254
7.5.	Computing the Power Residue Symbol in Cyclotomic Fields	255
7.5.1.	Main Idea	255
7.5.2.	The Full Algorithm	257

7.6. Discussion	259
7.6.1. Computing Hilbert Symbols Using Power Residue Symbols	259
7.6.2. Computing Artin Symbols in the Same Fashion . . .	261
Bibliography	265
A. Appendix	279
A.1. Number-theoretic Computations	279
A.2. Bound on the Residue of the Zeta Function for Cyclotomic Fields	283
A.2.1. Splitting $\log(\rho_K) = R_K + M_K$ into a Ramified Term and a Main Term	285
A.2.2. Estimating the Ramified Term	286
A.2.3. Splitting the Main Term in an Initial Part and a Tail Part	288
A.2.4. Estimating the Initial Part of the Main Term	289
A.2.5. Estimating the Tail Part of the Main Term	291
A.3. Exact Sequences	292
A.4. The Yudin-Jackson Theorem	294
A.5. The Gaussian State	299
A.5.1. Reducing to the One-dimensional Case	299
A.5.2. The Periodic and Non-periodic Discrete Gaussian . .	300
A.5.3. Computing the Periodic Gaussian State	301
A.5.4. Estimating the Complexity and Fidelity	303
A.5.5. Proof of Lemma A.27	306
A.6. Discrete Gaussians	308
Summary	313
Samenvatting	315
Acknowledgments	317
Curriculum Vitae	319

List of Symbols	321
------------------------	------------

Index	329
--------------	------------

List of Figures

1.1. The number ring $\mathbb{Z}[\sqrt{2}]$ visualized on the real plane	3
1.2. The Minkowski embedding of $\mathbb{Z}[\sqrt[3]{2}]$ into $\mathbb{R} \times \mathbb{C}$	4
1.3. Examples of ideal lattices and non-ideal lattices	5
1.4. Deformation of ideal lattices	6
1.5. Examples of trivial class and non-trivial class ideal lattices .	7
1.6. Ideal lattice shapes shifting seamlessly from  to 	8
1.7. Examples of ideal lattices in $\mathbb{Q}(\sqrt{3})$	9
1.8. Periodicity of the ideal lattices in $\mathbb{Q}(\sqrt{3})$	10
1.9. Circularity of the ideal lattices in $\mathbb{Q}(\sqrt{3})$	11
1.10. The Arakelov class group of a number field K consists of a union of finitely many hypertori.	12
1.11. Ideal lattices on the same torus can be transformed into each other	13
1.12. Random walk analogy with an ant	14
1.13. Gaussian distribution ‘folding around’ the torus	15
1.14. Random walks on Arakelov class groups require ‘jumps’ . .	16
1.15. Examples of prime sub ideal lattices	18
1.16. Examples of random jumps on the Arakelov class group . .	18
1.17. Infographic explaining the random walk procedure	20
1.18. An explanation of the random walk’s parameters	20
1.19. The more jumps happen in the random walk, the less crawling is needed	22
1.20. An example of the equidistribution of primes on the Arakelov class group of $\mathbb{Q}(\sqrt{3})$	24
1.21. An explanation of the Shortest Vector Problem	26

1.22. A question about the hardness of SVP being the same on all ideal lattices	27
1.23. Infographic explaining the worst-case to average-case reduction	29
1.24. Picture of all prime ideal lattices of $\mathbb{Q}(\sqrt{3})$ with norm below 25	31
1.25. Harmonics of a violin tone	35
1.26. An example of a two-dimensional periodic signal and its period lattice	35
1.27. The Fourier transform captures periodicity	36
1.28. Discretization in the Fourier transform causes intrinsic noise	37
1.29. The dependencies of the chapters in this thesis	39
2.1. Groups and their Haar measures	43
2.2. An example of restriction of a function	46
2.3. An example of periodization of a function	47
2.4. An example of $\mathbb{Z}$ -periodization of a Gaussian function . . .	48
2.5. Informal illustration of the Poisson summation formula . . .	49
2.6. The Poisson summation formula applied to a Gaussian function	50
2.7. Wide periodic Gaussians are close to uniform	51
2.8. A commutative diagram involving the Arakelov ray class group	62
2.9. A concrete picture of an Arakelov class group (parallelograms)	70
2.10. A concrete picture of an Arakelov class group (tori)	71
3.1. An example of an (r, ϵ) -separating function	91
3.2. The Lipschitz constant of a (r, ϵ) -separating function	92
3.3. Periodicity of continuous signals versus discrete signals . . .	100
3.4. A visual representation of Algorithm 2	101
3.5. A visual explanation of the target set C	103
3.6. An explanation of the indicator-like function $\iota_C(\ell^*)$	111
3.7. An example of an (R, q) -concentrated distribution	117
3.8. Examples of two distributions not being p -evenly distributed	118
3.9. A depiction of the case distinction of Lemma 3.22	120
4.1. The Arakelov class group can be thought of as $ \text{Cl}_K $ copies of the logarithmic unit torus	130

4.2. The discrete walk on the Arakelov class group	135
4.3. The continuous walk on the Arakelov class group	135
4.4. Volumetric covering argument for the Arakelov class group	136
4.5. The effect of the Hecke operator on Arakelov class group distributions	138
4.6. High and low-frequency characters on the hypertorus T^m	140
4.7. Hecke operators diminish non-unit characters	141
4.8. The effect of ‘averaging’ on complex exponential functions	143
4.9. Characters and their associated dual lattice points	154
4.10. Distributions tend to the uniform distribution under repeated action of the Hecke operator	156
4.11. The larger the Gaussian deviation s is, the less influence it has on the running time of the random walk	163
5.1. A short vector in subideals of $\mathfrak{a}$ is also a reasonably short vector in $\mathfrak{a}$ itself	169
5.2. Deformation of ideal lattices	172
5.3. The discrete hyper-circle	192
6.1. Counting lattice points in a box	219
7.1. The multiplicative action of $\langle \zeta \rangle$ on a residue field $R/\mathfrak{p}_5$	245
7.2. A depiction of the computation of the signature (ϕ, M)	246
7.3. The computation of the signature $(\phi_{1+\zeta}, R/\mathfrak{p}_5)$	248
A.1. The kernel-cokernel exact sequence	294

