Random walks on Arakelov class groups

Boer, K. de

Acknowledgments

I would like to thank my advisors Prof. dr. Léo Ducas, dr. Benjamin Wesolowski and Prof. dr. Ronald Cramer for their expert supervision.

Léo, my promotor, has shown unwavering support during my research and during the writing of this thesis as well. He always enthusiastically shared his knowledge and insights with me throughout this time. Much of the work in this dissertation is the result of our shared dedication to rigorous run-time analyses of algorithms in cryptography.

Benjamin, my co-promotor, greatly increased my interest in analytic number theory and its usage in cryptography by generously sharing his expertise. I am grateful for our cooperation, which was marked by ample room for discussing mathematical intricacies and having a good laugh as well.

Ronald, my second promotor, is gratefully acknowledged for his guidance and constructive criticism during the preparation of the final version of this thesis. I am very grateful to him for putting me on the right track scientifically and non-scientifically during the more difficult times of my PhD track.

I am also very grateful to the members of the Doctorate Committee for reading my thesis and providing useful feedback.

Additionally, I would like to thank my colleagues – from the CWI and Universiteit Leiden, but also from abroad – for providing me an inspiring and positive environment.

To my family, friends and partner I would like to say: Jullie zijn een onvervangbare en onmisbare steun geweest tijdens mijn promotietraject. Enorm bedankt voor jullie geduld, begrip en liefde — op de betere, maar ook vooral op de zwaardere momenten van deze periode.

Curriculum Vitae

Koen de Boer was born in Nijmegen, the Netherlands, on August 22, 1991. He grew up in the city Oss in Brabant, where he obtained his high school diploma from Titus Brandsma Lyceum in 2008.

After deciding to study Mathematics at the Radboud Universiteit of Nijmegen, he obtained his bachelor degree *cum laude* in 2012 and his master's degree *summa cum laude* in 2016. His master thesis, "Computing the Power Residue Symbol", was written under supervision of dr. W. Bosma and Prof. dr. H.W. Lenstra.

In 2016, Koen obtained a PhD position at the Universiteit Leiden under supervision of Prof. dr. L. Ducas, Prof. dr. R. Cramer and dr. B. Wesolowski, to do research in the Cryptology Group at Centrum Wiskunde & Informatica (CWI) in Amsterdam.

In 2022, he started to work as a post-doc at the Universiteit Leiden.

Publications

- K. de Boer and C. Pagano (2017). "Calculating the Power Residue Symbol and Ibeta: Applications of Computing the Group Structure of the Principal Units of a p-adic Number Field Completion." In: *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation (ISSAC '17).* Association for Computing Machinery, New York, NY, USA.

- K. de Boer, L. Ducas, S. Jeffery, R. de Wolf (2018). “Attacks on the AJPS Mersenne-Based Cryptosystem.” In: Post-Quantum Cryptography. PQCrypto 2018. *Lecture Notes in Computer Science*, vol 10786. Springer, Cham.
- K. de Boer, L. Ducas, S. Fehr (2020). “On the Quantum Complexity of the Continuous Hidden Subgroup Problem.” In: Advances in Cryptology – EUROCRYPT 2020. *Lecture Notes in Computer Science*, vol 12106. Springer, Cham.
- K. de Boer, L. Ducas, A. Pellet-Mary, B. Wesolowski (2020). “Random Self-reducibility of Ideal-SVP via Arakelov Random Walks.” In: Advances in Cryptology – CRYPTO 2020. *Lecture Notes in Computer Science*, vol 12171. Springer, Cham.

List of Symbols

$\lVert\cdot\rVert_{p,G}$	The Haar-measure induced p-norm on functions $G \to \mathbb{C}$, where G is a locally compact abelian group G. In this thesis, p is either $1, 2$ or ∞ in this context. The subscript G is often suppressed, as well as the subscript p in the case of $p = 2$ (page 43)
$f\rvert^{H}$	The periodization of a function $f : G \to \mathbb{C}$ with respect to a subgroup $H \subseteq G$ (page 45)
$f\big\rvert_{H}$	The restriction of a function $f : G \to \mathbb{C}$ with respect to a subgroup $H \subseteq G$ (page 45)
$\lvert\cdot\rangle, \langle\cdot\rvert, \langle\cdot\lvert\cdot\rangle$	The ket, bra and bra-ket notation, used for quantum states in a quantum Hilbert space $\mathcal{H}$ (page 41)
$\lfloor\cdot\rceil, \lfloor\cdot\rfloor, \lceil\cdot\rceil$	Respectively, rounding to the nearest integer ($x \in [-\frac{1}{2}, \frac{1}{2})$ rounds to 0), rounding down and rounding up
$\star$	The convolution operation on functions on a locally abelian group G (page 45)
$(\!\lvert\cdot\rvert\!)$	The diagonal embedding of K into the Arakelov divisor group Div_K. The notation $(\!\lvert\mathfrak{p}\rvert\!)$ and $(\!\lvert\nu\rvert\!)$ for prime ideals and places is also used for the generators in the Arakelov divisor group (page 59)
$\hat{\cdot}$	The dual group of a locally compact abelian group, e.g., $\hat{G}$ is the dual group of G (page 42)
$\tilde{\cdot}$	An approximation; for example, $\tilde{B}$ indicates an approximation of B
$\cdot^{0}$	The subgroup of elements of norm or degree one, where the norm or degree is induced by the associated number field. For example, Div_K^0, Pic_K^0 (page 60), $K_{\mathbb{R}}^0$ (page 53), $\mathcal{J}_K^0$, $\mathcal{C}_K^0$ (page 148)
$\cdot^{\mathfrak{m}}$	The ray analogue of a number field related group, involving $\mathfrak{m}$. For example, $\mathrm{Div}_{K^{\mathfrak{m}}}$, $\mathrm{Pic}_{K^{\mathfrak{m}}}$ (page 59), $\mathcal{I}_K^{\mathfrak{m}}$ (page 54), $\mathrm{Cl}_K^{\mathfrak{m}}$ (page 62)
$\ddot{\cdot}$	A discretized analogue of a continuous object. For example, $\ddot{\mathcal{D}}$ for a discretized version of a continuous distribution

$\left(\frac{\alpha}{\mathfrak{b}}\right)_{m,K}$	The m-th power residue symbol, where the top argument is an element of K and the bottom argument is an ideal of a number ring of K; if K is clear from context, this notation is dropped (page 238)
$(\alpha, \beta)_{\mathfrak{p}}$	The m-th Hilbert symbol, where both arguments α, β are elements of the $\mathfrak{p}$-adic completion $K_{\mathfrak{p}}$ of the associated number field K; the 'power' m is always clear from the context and not included in the notation (page 259)
(ϕ, M)	The signature symbol of the automorphism ϕ on a finite admissible module M (page 245)
$(x_\sigma)_\sigma, (r_\sigma)_\sigma$	Elements in $K_{\mathbb{R}}$, written as vectors indexed by the embeddings of K into $\mathbb{C}$ (page 53)
$\mathbf{1}_G$	The unit character on the locally compact abelian group G
$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$	Ideals of the ring of integers of a number field, elements of $\mathcal{I}_K$ (page 54)
$[\mathfrak{a}], [\mathfrak{b}], [\mathfrak{c}], \ldots$	Ideal classes, elements of Cl_K (page 55)
$\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots$	Arakelov divisors, elements of Div_K (page 59)
$[\mathbf{a}], [\mathbf{b}], [\mathbf{c}], \ldots$	Arakelov classes, elements of Pic_K (page 60)
$\mathbf{a}_{\mathrm{f}}, \mathbf{a}_\infty$	The finite part and respectively infinite part of an Arakelov divisor $\mathbf{a}$ (page 61)
$\mathcal{B}_r(x)$	The ball of radius r around x with respect to the 2-norm (page 77)
$\mathcal{B}_r(X)$	The union of balls $\bigcup_{x \in X} \mathcal{B}_r(x)$ over all $x \in X$ (page 91)
$r\mathcal{B}_\infty, (r_\sigma)_\sigma \mathcal{B}_\infty$	The box of radius r around 0 with respect to the ∞-norm (page 210) respectively the distorted box of component-wise radius $(r_\sigma)_\sigma$ (page 226)
C	In Chapter 3, the 'target set' of the algorithm, i.e., the set of good outcomes of a measurement (page 102)
$C(r, \mathcal{N}(\mathfrak{c}))$	The volume of the simplex with edge length $(n \log r - \log \mathcal{N}(\mathfrak{c}))$ and dimension $\mathbb{r}$, which equals $(n \log r - \log \mathcal{N}(\mathfrak{c}))^{\mathbb{r}} / \mathbb{r}!$ whenever $\mathcal{N}(\mathfrak{c}) \leq r^n$ and zero otherwise (pages 215 and 279)
$\mathcal{C}_K$	The idèle class group of a number field (page 55)
Cl_K	The class group of a number field (page 55)
$\mathrm{Cl}_K^{\mathfrak{m}}$	The ray class group of a number field (page 62)
$\mathcal{C}_M$	The hypercircle $\{(x_\sigma)_\sigma \in K_{\mathbb{R}} \mid \lvert x_\sigma \rvert = M\}$ (page 175)
$\ddot{\mathcal{C}}_M$	The discretized hypercircle (page 192)
$\mathrm{cov}_2(\Lambda), \mathrm{cov}_\infty(\Lambda)$	The covering radius of a lattice Λ with respect to the 2-norm or the ∞-norm respectively (page 72)
d	The map sending $\mathcal{I}_K$ to Div_K by using the valuations of the prime ideals as coefficients for the finite places of the Arakelov divisor (page 61)

d^0	The map sending $\mathcal{I}_K$ to Div_K^0 by using the valuations of the prime ideals as coefficients for the finite places of the Arakelov divisor, and a fraction of the negative logarithmic norm of the ideal at the infinite places (page 61)
$\mathcal{D}$	Generally, a distribution. In Chapter 6, it is a distribution over $\mathrm{Div}_{K^{\mathfrak{m}}}^0$
$[\mathcal{D}]$	The $K^{\mathfrak{m},1}$-periodization $\mathcal{D}\|^{K^{\mathfrak{m},1}}$ of a distribution $\mathcal{D}$ over $\mathrm{Div}_{K^{\mathfrak{m}}}^0$ (page 210)
$\mathcal{D}_{x\mathfrak{a}}$	The distribution representation of an ideal lattice $x\mathfrak{a}$ (page 174)
$\mathbb{D}^m$	The group $\frac{1}{q}\mathbb{Z}^m/\mathbb{Z}^m \subseteq \mathbb{T}^m$, a q-discretized version of the unit torus (page 42)
$\mathbb{D}^m_{\mathrm{rep}}$	The standard representation $\frac{1}{q}\mathbb{Z}^m \cap [-\frac{1}{2}, \frac{1}{2})^m$ of $\mathbb{D}^m$ (page 42)
$\hat{\mathbb{D}}^m$	The dual of $\mathbb{D}^m$, isomorphic to $\mathbb{Z}^m/q\mathbb{Z}^m$ (page 42)
$\hat{\mathbb{D}}^m_{\mathrm{rep}}$	The standard representation $\mathbb{Z}^m \cap [-\frac{q}{2}, \frac{q}{2})^m$ of $\hat{\mathbb{D}}^m$ (page 42)
$\deg(\cdot)$	The degree of an Arakelov divisor; a weighted sum of the coefficients associated with the places. Equivalently, the logarithm of the determinant of the ideal lattice associated with the Arakelov divisor (page 60)
$\det(\cdot)$	The determinant of a matrix, or, the determinant of a lattice Λ, which is equal to its covolume $\mathrm{Vol}(\Lambda)$ (page 72)
Div_K	The Arakelov divisor group of a number field K, consisting of formal sums of places of K (page 59)
$\mathrm{Div}_{K^{\mathfrak{m}}}$	The subgroup of the Arakelov divisor group consisting of formal sums not involving the places dividing the modulus $\mathfrak{m}$ (page 59)
$\mathrm{Exp}(\mathbf{a})$	The exponentiation map sending an Arakelov divisor $\mathbf{a} \in \mathrm{Div}_K$ to an ideal lattice in IdLat_K (page 73)
$\mathrm{Exp}(\mathbf{a})_\tau^\times$	The τ-equivalent generators of the Arakelov ray divisor $\mathbf{a}$ (page 208)
$\mathbf{f}$	In Chapter 3, the periodic function over $\mathbb{R}^m$ that 'hides' the lattice Λ (page 81)
$\mathcal{F}_G\{\cdot\}$	The Fourier transform with respect to the locally compact abelian group G (page 44)
$\mathcal{G}_{X,s}$	The (discrete) Gaussian distribution with deviation s, where the structure of the space X determines whether $\mathcal{G}$ is continuous or discrete (page 79)
$\mathbf{h}$	In Chapter 3, the 'wave packet variant' of the periodic function over $\mathbb{R}^m$ that hides the lattice Λ (page 102)
H	The hyperplane $\mathrm{Log}(K_{\mathbb{R}}^0)$ in $\mathrm{Log}(K_{\mathbb{R}})$ where the Logarithmic unit lattice $\Lambda_K = \mathrm{Log}(\mathcal{O}_K^\times)$ lives in (page 54). Occasionally, a subgroup of a locally abelian group G
$\mathcal{H}$	In Chapter 3, a finite-dimensional quantum Hilbert space (page 41). In Chapter 4, a Hecke operator (page 142).

$\mathcal{H}_{\mathcal{P}}$	The Hecke operator with respect to a finite set of prime ideals $\mathcal{P}$; this set is omitted in the notation if it is clear from context (page 142)
h_K	The class number $\lvert \mathrm{Cl}_K \rvert$ (page 53)
h_K^+	The class number of the maximal totally real subfield of K (page 55)
$\mathcal{I}_K$	The group of fractional ideals of the ring of integers of a number field K (page 54)
$\mathcal{I}_K^{\mathfrak{m}}$	The subgroup of $\mathcal{I}_K$ consisting of ideals coprime to a modulus $\mathfrak{m}$ (page 54)
$\mathcal{J}_K$	The idèle group of the number field K (page 55)
IdLat_K	The group of ideal lattices of the number field K (page 73)
K	A finite-degree number field (page 53)
$K^{\mathfrak{m},1}$	The multiplicative subgroup of K generated by the elements in $\mathcal{O}_K$ that are equivalent to 1 modulo the modulus $\mathfrak{m}$ (page 55)
$K^{\mathfrak{m}}$	The multiplicative subgroup of K generated by the elements in $\mathcal{O}_K$ that are invertible modulo the modulus $\mathfrak{m}$ (page 55)
$K_{\mathbb{R}}$	The tensor product $\mathbb{R} \otimes_{\mathbb{Z}} K$ where K is a number field; also, co-domain of the Minkowski embedding (page 53)
$K_{\mathbb{R}}^0$	The subgroup of $K_{\mathbb{R}}$ consisting of those elements whose K-induced algebraic norm equals 1 (page 54)
$K_\nu, K_{\mathfrak{p}}$	The completion of K with respect to the place ν or prime $\mathfrak{p}$ (page 55)
ℓ	Generally, a lattice point $\ell \in \Lambda$
ℓ^*	Generally, a dual lattice point $\ell^* \in \Lambda^*$
$L(\chi, s)$	The L-function associated with a Hecke character χ of a number field K(page 56)
$L_p(G)$	The metric vector space of measurable functions $f : G \to \mathbb{C}$ on a locally abelian group G for which the p-norm $\lVert f \rVert_{p,G}$ is well-defined and finite (modulo functions with norm zero) (page 43)
$\mathrm{Lip}(f)$	The Lipschitz constant of a function f between two normed spaces (page 90)
Log	The logarithmic map $K \to \mathrm{Log}(K_{\mathbb{R}})$ defined by taking the logarithm of the absolute value of each component of the Minkowski embedding (page 54)
m	In Chapter 3, the dimension of the hidden lattice; in Chapter 7 the m in the m-th power residue symbol
$\mathfrak{m}$	An ideal modulus of a number field, consisting of a formal product of finite places of that number field (page 54)
n	The degree $[K : \mathbb{Q}]$ of the number field K (page 53)
$n_{\mathbb{R}}$	The number of real embeddings $K \hookrightarrow \mathbb{R}$ (page 53)

$n_{\mathbb{C}}$	The number of conjugate pairs of complex embeddings $K \hookrightarrow \mathbb{C}$ (page 53)
$\mathcal{N}(\cdot)$	The algebraic norm of a number field element or ideal (page 55)
$o(\cdot)$	The Bachmann-Landau Small-o notation
$O(\cdot)$	The Bachmann-Landau Big-O notation
$\widetilde{O}(\cdot)$	The soft-O notation, ignoring polylogarithmic factors
$\mathcal{O}_K$	The ring of integers of the number field K (page 53)
$\mathcal{O}_K^\times$	The unit group of the number field K (page 54)
$\mathcal{O}_{K^{\mathfrak{m},1}}^\times$	The ray unit group of the number field K with respect to the modulus $\mathfrak{m}$, i.e., $\mathcal{O}_K^\times \cap K^{\mathfrak{m},1}$ (page 62)
$\mathrm{ord}_{\mathfrak{p}}$	The valuation with respect to the prime ideal $\mathfrak{p}$ (page 54)
$\mathfrak{p}$	A prime ideal of a number field (page 54)
$\mathfrak{p}_\nu$	A prime ideal of a number field uniquely associated with the finite place ν (page 53)
Princ_K	The subgroup of principal ideals in $\mathcal{I}_K$, i.e., those generated by a single element in K (page 55)
$\mathfrak{q}$	A prime ideal of a number field (page 54)
$\mathfrak{q}_\infty(\chi)$	The infinite part of the analytic conductor of a Hecke character $\chi \in \widehat{\mathrm{Pic}^0_{K^\mathfrak{m}}}$ (page 151)
q	The discretization parameter in the continuous hidden subgroup quantum algorithm (page 100)
Q	$\log(q)$, the numbers of qubits 'per dimension' in the continuous hidden subgroup quantum algorithm (page 87)
r	Generally, the radius of a ball or box in a vector space; in Chapter 3, part of the definition of a function being (r, ϵ)-separating (page 91)
$\mathbb{r}$	The rank of the unit group of a number field K, which equals $n_{\mathbb{R}} + n_{\mathbb{C}} - 1$ (page 54)
R_K	The regulator of the number field K, strongly related to the volume of T (page 53)
$\mathcal{S}$	In Chapter 3, the space of quantum states (page 90). In Chapters 6 and 7, a set of integral ideals of the ring of integers of a number field K (page 209)
$\mathcal{S}^{\mathfrak{m}}$	A set of integral ideals of the ring of integers of a number field K that are coprime with the modulus $\mathfrak{m}$ (page 209)
$\mathcal{S}_B$	The set of all B-smooth integral ideals of $\mathcal{O}_K$, i.e., all integral ideals having only prime ideal factors with norm $\leq B$ (page 205)
$\lvert\mathcal{S}(t)\rvert$	The number of ideals in $\mathcal{S}$ with norm bounded by t (page 209)
s	The deviation for the Gaussian function or the (discrete) Gaussian distribution. Occasionally, input variable of zeta functions and L-functions

$\mathrm{span}(\cdot)$	The linear subspace spanned by the vectors or the lattice within the brackets
$\mathbb{T}^m$	The unit torus $\mathbb{R}^m/\mathbb{Z}^m$ (page 42)
$\mathbb{T}^m_{\mathrm{rep}}$	The standard representation $[-\frac{1}{2},\frac{1}{2})^m$ of the unit torus $\mathbb{T}^m$ (page 42)
T	The logarithmic unit torus $H/\operatorname{Log}(\mathcal{O}_K^\times)$ (page 54)
$T^{\mathfrak{m}}$	The logarithmic ray unit torus $H/\operatorname{Log}(\mathcal{O}_{K^{\mathfrak{m}},1}^\times)$ (page 62)
$\mathcal{U}(X)$	The uniform distribution over the compact space X (page 65)
$\mathrm{Vol}(\cdot)$	Volume of the compact abelian group with respect to the fixed given Haar measure (page 42), or, the covolume of a lattice (also called the determinant of the lattice, (page 72))
$\mathcal{W}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}(B,N,s)$	The random walk distribution over the Arakelov ray class group $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ with prime ideal norm bound B, number of steps N and Gaussian deviation s (page 140)
$x\mathfrak{a}, y\mathfrak{b}$	Ideal lattices, elements of IdLat_K (page 73)
$\mathbb{Z}_H$	Orthogonal discretization of the hyperplane H where the log unit lattice $\Lambda_K = \operatorname{Log}(\mathcal{O}_K^\times)$ lives in (page 191)
$\alpha,\beta,\gamma,\ldots$	Generally, elements of a number field K (page 53)
β_z	Banaszczyk's function $z \mapsto \left(\frac{2\pi e z^2}{n}\right)^{n/2} e^{-\pi z^2}$ (page 77)
Γ_K	The maximum of the quotient between the outermost successive minima $\lambda_n(x\mathfrak{a})/\lambda_1(x\mathfrak{a})$ over all ideal lattices $x\mathfrak{a} \in \mathrm{IdLat}_K$ for a fixed number field K (page 75)
δ	In Chapter 3, the relative distance error in the dual sampling algorithm (page 93). In the rest of the thesis, generally a small distance or error
$\delta_{\mathcal{S}}[x]$	The local density of the ideal set $\mathcal{S}$ around norm x (page 209)
Δ_K	The discriminant of the number field K (page 53)
ε	A small error parameter in $[0,1]$, often indicating the failure probability of an algorithm
ϵ	A parameter in the definition of a function being (r,ϵ)-separating in Chapter 3 (page 91)
$\zeta(s)$	The Riemann zeta function
ζ_m	A primitive m-th root of unity
$\zeta_K(s)$	The Dedekind zeta function with respect to the number field K (page 56)
η	In the dual lattice sampling algorithm of Chapter 3, the failure probability of the algorithm (page 93). In the rest of the thesis, a small error or sometimes a unit $\eta \in \mathcal{O}_K^\times$
$\eta_\varepsilon(\Lambda)$	The smoothing parameter, the smallest $s > 0$ such that $\rho_{1/s}(\Lambda^*\backslash\{0\}) \le \varepsilon$ (page 77)
λ_1^*	The first successive minimum $\lambda_1(\Lambda^*)$ of the dual lattice, whenever the lattice Λ is clear from context (page 72)

$\lambda_j(\Lambda)$	The j-th successive minimum of the lattice Λ with respect to the 2-norm (page 72)
$\lambda_j^{(\infty)}(\Lambda)$	The j-th successive minimum of the lattice Λ with respect to the ∞-norm (page 72)
λ_χ	The eigenvalue of the character $\chi \in \widehat{\mathrm{Pic}^0_{K^\mathfrak{m}}}$ under the Hecke operator $\mathcal{H}$
Λ	A lattice, i.e., a discrete subgroup of a Euclidean vector space (page 72)
Λ^*	The dual of the lattice Λ (page 72)
Λ_K	The log unit lattice $\mathrm{Log}(\mathcal{O}_K^\times)$
$\Lambda_{K^\mathfrak{m}}$	The ray log unit lattice $\mathrm{Log}(\mathcal{O}^\times_{K^{\mathfrak{m},1}}) = \mathrm{Log}(\mathcal{O}_K^\times \cap K^{\mathfrak{m},1})$
μ_K	The group of roots of unity of the number field K (page 53)
ν	A formal place, associated with an absolute value $\lvert\cdot\rvert : K \to \mathbb{R}_{>0}$ on a number field K (page 53)
ν_σ	The place associated with the absolute value induced by the embedding $\sigma : K \to \mathbb{C}$ (page 53)
ρ_s	The Gaussian function $x \mapsto e^{-\pi\|x\|^2/s^2}$ (page 76)
ρ_K	The residue $\lim_{s\to 1}(1-s)\zeta_K(s)$ of the Dedekind zeta function at $s = 1$ (page 56)
σ	An embedding from a number field K into the complex numbers $\mathbb{C}$ (page 53)
ς	The deviation for the Gaussian function or the (discrete) Gaussian distribution whenever s is already used
$\phi(m)$	The Euler indicator function, $\phi(m) = \lvert(\mathbb{Z}/m)^*\rvert$ for $m \in \mathbb{N}_{>0}$
$\phi(\mathfrak{m})$	The generalized Euler indicator function for ideals $\mathfrak{m} \subseteq \mathcal{O}_K$, $\phi(\mathfrak{m}) = \lvert(\mathcal{O}_K/\mathfrak{m})^*\rvert$ (page 62)
χ	A character $\chi \in \hat{G}$ of a locally compact abelian group G, i.e., a continuous group homomorphism from G to $\mathbb{C}$ (page 42)

Index

analytic conductor, 151
    bound on the, 152
    informal description of the, 139
Arakelov ray class groups, 60
    earlier (cryptographic) work related to, 133
    informal description of, 129
    motivation for studying, 132
    example of, 66
    volume of, 64
Arakelov ray divisor, 59
    (τ-equivalent) generator of an, 208
    finite and infinite part of a, 61
Artin symbols
    algorithm to compute, 261
    Dedekind zeta function and its influence on computing, 263

Banaszczyk's bound, *see* Gaussian distribution

class group and unit group of a number field, 53
    quantumly computing the, 90
    logarithmic unit lattice, *see* logarithmic unit lattice
concentrated
    (R, q)-concentrated lattice distribution, 117
continuous hidden subgroup problem, 85
    an informal description of the, 81
    quantum algorithm solving the, 97
        correctness of the, 92
        summary of the, 87
    research directions relating to the, 88
covering radius, *see* lattice
covolume, *see* lattice
cyclotomic units, 188
    relation between the random walk theorem and the, 160

Dedekind zeta function, 55
  bound on the residue of the, 271
  influence on the computation of Artin symbols of the, *see* Artin symbols
determinant, *see* lattice
discretization
  errors in the continuous HSP quantum algorithm caused by, 100
  need for discretization in the reduction algorithm, *see* worst-case to average-case reduction on ideal lattices
distribution
  average-case distribution for ideal lattices, 180
  Gaussian, *see* Gaussian distribution
dual lattice of the hidden lattice
  recovering the full, 94, 122
dual lattice sampling problem
  an informal description of the, 87
  analysis of the quantum algorithm solving the, 107
  definition of the, 93
  quantum algorithm solving the, 101
  short analysis of the quantum algorithm solving the, 104
  theorem about the quantum algorithm solving the, 93, 115

evenly distributed
  p-evenly distributed lattice distribution, 117
exact sequences
  kernel-cokernel, 280
  the Arakelov ray class group within a diagram of, 61
extended Riemann hypothesis, 55

Fourier analysis
  on the Arakelov ray class group (informal), 131
  on the ray unit torus, 152
  on locally compact abelian groups, 43
  on the Arakelov ray class group, 65, 155

Gaussian distribution
  discrete, 296
  notation for the discrete and continuous, 79
  results on shifting a discrete, 298
  tail bounds on the discrete, 76
Gaussian quantum state
  setting up the initial, 96, 294
generator
  of an Arakelov ray divisor, *see* Arakelov ray divisor

Hecke operator, 142
    bounds on the eigenvalues of the, 143
    informal description of the, 138
hidden lattice
    recovering the basis of the, 95, 126
hidden lattice problem, *see* continuous hidden subgroup problem
Hilbert symbols, 260
    using power residue symbols to compute, 259
HSP-oracle
    (a, r, ϵ)-HSP oracle, 91

ideal density, *see* local density of an ideal set
ideal lattices, 73
    associated to a Arakelov divisor, 73
    definition of, 172
    distribution representation of, 174
        algorithm for the, 175
        definition of the, 175
        discrete algorithm for the, 194
        properties of, 176
    invariants of, 75
    isometry of, 73
    modulo isometry, *see* Arakelov ray class groups
    need for an efficient representation of, 173
    the Arakelov class group and its relation to, 74
ideals
    sampling, *see* sampling
    set of, *see* local density of an ideal set
    smooth, 228

lattice
    invariants of a, 71
Lipschitz continuity, 90
    influence on the Fourier coefficients, 79
local density of an ideal set, 210
    main theorem relating the sampling probability to the, 210
        proof of the, 216
logarithmic unit lattice, 53
    volume of the, 268

number field
    invariants of a, 53
    norm on a, 72

period finding, *see* continuous hidden subgroup problem
periodization and restriction, 45
Poisson summation formula, 46
power residue symbol
    algorithm computing the
        difference with an earlier heuristic algorithm, 237
        earlier work, 236
        efficiency of the, 259
    cyclotomic, *see* power residue symbol in cyclotomic fields
power residue symbol in cyclotomic fields
    algorithm computing the, 257
        correctness of the, 257
        informal description of the, 255
        role of the random walk in the, 256
probability-density corresponence, *see* local density of an ideal set

random walk distribution on the Arakelov ray class group, 140
    an informal description of the, 130
    intuitive argument for the uniformity of, 136
    algorithm mimicking the, 229
        correctness of the, 231
random walk theorem for the Arakelov ray class group, 141, 161
    applications of the, 162
    interpretation of the, 161
    proof overview of the, 138
reduction algorithm
    for power residue symbols, *see* power residue symbol
    on ideal lattices, *see* worst-case to average-case reduction on ideal lattices
representation
    of ideal lattices, *see* ideal lattices
Riemann hypothesis, *see* extended Riemann hypothesis
rigorously sampling elements in ideals, 204
    applications of, 206
    earlier work related to, 207
    the role of the random walk theorem in, 205

sampling
    ideal sampling algorithm, 229
        correctness of the, 228
    uniformly sampling an element in a box, 226
sampling probability of ideals, *see* local density of an ideal set
separating
    (r, ϵ)-separating function, 91

shortest vector problem
  Hermite variant of the, 72
  self-reduction of the, *see* worst-case to average-case reduction on ideal lattices
simplex
  volume of the, 267
smoothing parameter, *see* gaussian distribution
successive minimum, *see* lattice

trigonometric approximation
  usage in Fourier analysis, 51
  Yudin's result, 283

unit group, *see* class group and unit group of a number field

worst-case to average-case reduction
  informal description, 165
  other works using random walks to obtain a, 170
  on ideal lattices, *see* worst-case to average-case reduction on ideal lattices
worst-case to average-case reduction on ideal lattices
  earlier works on, 170
  informal description, 168
  relation between cryptography and the, 170
  algorithm for the, 181
    closeness of discrete and continuous, 197
    correctness of the, 183
    discrete version of the, 196
    explanation of the, 180
  discretization of, 189
    need for, 188
  main theorem, 184
    informal version, 167
    loss of shortness quality in the, 186